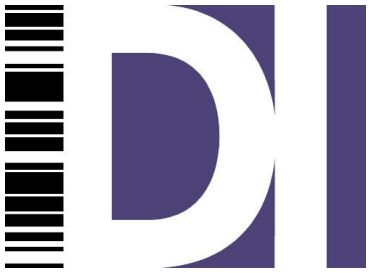
ODEX Enterprise User Guide



A Comprehensive Guide to ODEX Enterprise

Document Information

Document Date	31 January 2011
Product Version	2.5.0

Table of Contents

Product History 15
What's new in ODEX Enterprise version 2.5.0? 15
What's new in ODEX Enterprise version 2.4.0? 15
What's new in ODEX Enterprise version 2.3.0? 15
What's new in ODEX Enterprise version 2.2.0? 16
What's new in ODEX Enterprise version 2.1.0? 17
What's new in ODEX Enterprise version 2.0.0? 17
What's new in ODEX Enterprise version 1.3.0? 18
What's new in ODEX Enterprise version 1.2.1? 18
What's new in ODEX Enterprise version 1.2.0? 19
What's new in ODEX Enterprise version 1.1.0? 19

ODEX Enterprise 20
Introduction 20
Features and Functionality 20

ODEX Enterprise Overview 22
A Client/Server application 22
Running ODEX as a system service 22
Starting 22
Stopping 22
Upgrading ODEX 23

ODEX Concepts 24
OFTP (ODETTE File Transfer Protocol) 24
OFTP Commands 24
OFTP Security and Authentication (EDI Codes) 25
OFTP Session 26
Communication 27
Direct or indirect communication? 27
OFTP Revision 2 Changes 29
Security Overview 29
Secure Authentication 30
File Security 31
Signed EERP/NERP 31
Maximum File Length 31
File Compression 31
Virtual Filename Length 31
Workflows 31
Data Source 32
Message Definition Group 33
Trading Partner 33
Data Definition 33
Channels 33
Workflow 34
Error Workflow 34
Job 34
Job Definition 34
File processing in the Workflow Manager 35
Workflow Examples 36
Schedules and Event Actions 40
User Security 41
ODEX's own security 41
Windows NT security 41
Users and User Groups 42
Enforcing User Security 45
AS2 46

What is AS2? *46*
What are the advantages of AS2? *46*
What do I need in order to use AS2? *46*
Do I have to use AS2? *46*
How do I set up AS2 in ODEX? *47*
What is involved in an AS2 data transmission? *47*
What are the security features of AS2? *47*
What is XOT? 48
Overview *48*
Using XOT and X.25 in ODEX *48*
Configuring XOT in ODEX *49*
Using an XOT interface with the CISCO Router *49*
FTP (File Transfer Protocol) 52
What is FTP? *52*
What are the advantages of FTP? *52*
What are the disadvantages of FTP? *52*
What are the requirements of FTP? *52*
Advanced FTP explanation *53*
Using FTP in ODEX *53*
FTP placeholders *55*
Additional FTP acknowledgments *55*
FTP with specific trading partners *56*
FTP client folder and file naming conventions *56*
Data Security 60
Certificates 60
ODEX Certificate Store *61*
OFTP2 Certificate Exchange *62*
Trusted-service Status List *62*
Authentication and data transformations 63
Encryption *63*
Digital Signatures *63*
WebSphereMQ 63
What is WebSphereMQ? *64*
How do I use poll an MQ message queue in ODEX? *64*
How do I use write to an MQ message queue in ODEX? *64*
ENGDAT 65
What is ENGDAT? *65*
What is an ENGDAT folder? *65*
What is an ENGDAT message? *66*
What are the differences between each version of the ENGDAT message? *66*
How are folders transmitted and received? *66*
Validation Profiles *67*
Using the Gedas Com-Secure Application with ODEX *68*
EDIFACT Security 69
What is EDIFACT security? *69*
What are digital signatures? *69*
Attached and detached signatures *70*
Response messages *71*
Exchanging signed data and responses *71*
How does ODEX Enterprise support EDIFACT security? *71*
The Sign EDI workflow job *72*
The Verify Signed EDI workflow job *72*
The Process AUTACK workflow job *73*
Windows Clustering 73
What is clustering? *74*
What do I need for an ODEX cluster? *74*
Preparing ODEX for Clustering *74*
Adding ODEX as a Resource *75*
ODEX Installation 76
Introduction 76
Requirements 76

Installation and Setup 76
Configuring your ODEX Enterprise database 78
Simple configuration *78*
Advanced Configuration *79*
Database already exists *80*
Result for all configurations *80*
ODEX Directory structure 81

Getting Started 83
First steps 83
All users *83*
Using ODEX as your communications system *83*

Upgrading from a previous version 84
Initialisation Wizard 84
Upgrade *84*
Upgrade from a previous version of ODEX Enterprise *85*
Upgrade from ODEX Professional *87*
Fresh system *89*

ODEX Professional import 91
Import Wizard 91

ODEX Professional events in ODEX Enterprise 95
Introduction 95
Conversions 95
Extract Non-EDI File *96*
Extract EDI File *96*
Schedule EDI File *97*
Schedule Non-EDI File *97*
Send an E-mail *98*
Execute an Application (Event Manager) *98*
Execute an Application (Event Scheduler) *98*
Call Network *99*
File Based Report *99*
Write To Windows Application Log *99*
Other Events *99*

First time use 102
Server location 102

ODEX Server Overview 103
Introduction 103
The ODEX Server GUI 103
Product Details *103*
Registration Details *103*
Data Interchange Plc *103*
Action Buttons *104*
Stop server warning dialog *104*
Failure to connect to server warning dialog *104*
Server connection lost warning dialog *106*
Logging 107
Server log *108*
Startup log *108*
Client logs *108*
How to use the logs *108*

ODEX Applications Overview 112
Introduction 112
ODEX Administrator 112
What does the Administrator do? *112*
Finding your way around the Administrator *113*
The Navigation Panel *113*

Default pages ... *114*
How to use the Administrator ... *114*
ODEX Communications Monitor ... 117
ODEX Workstation ... 117
ODEX Batch Administrator ... 117
Common Features ... 118
Menu bar ... *118*
Status bar ... *119*
Tabs 119
Mandatory fields ... *120*
Context menus ... *120*
"Hot" keys ... *120*
Short cuts ... *120*
Tick boxes ... *121*
Radio buttons ... *121*
Filters – Changing the time period ... *121*
Editing Parameters ... *122*
Common dialogs ... *125*
System Administrator ... 139
Introduction ... 139
ODEX users, user groups and communities ... 139
ODEX System Administrator user ... 140
Users ... 140
Users – Actions page ... *141*
Adding a new user ... *142*
Importing a new user ... *149*
View user list ... *150*
User Groups ... 152
User Groups – Actions page ... *152*
Adding a new group ... *153*
Importing a new group ... *160*
View group list ... *161*
Communities ... 162
Communities – Actions page ... *163*
Adding a new community ... *164*
View Community List ... *165*
Schedules ... 166
Viewing all your schedules ... *167*
Adding/Editing Schedules ... *169*
Event Actions ... 176
Viewing all your event actions ... *176*
Adding/Editing Event Actions ... *178*
Back Office Systems ... 187
Viewing all your back office systems ... *188*
Adding/Editing SAP Back Office Systems ... *190*
Adding/Editing MQ Back Office Systems ... *194*
Certificates ... 196
Certificates ... *196*
Trusted-service Status Lists ... *203*
Global Certificate Policy ... *206*
Trusted-service List Configuration ... *208*
System Log ... 210
Monitor page ... *210*
Archive page ... *212*
System Settings ... 214
Security page ... *215*
Server page ... *218*
Logging page ... *219*
E-mail page ... *220*
Performance Page ... *222*

Counters Page *225*
Retention Periods 227
Default 227
Scheduling *229*
Advanced (workflow files) *230*
Advanced (comms files) *232*
Licence Codes 234
Components *237*
Installation Codes *239*

Comms Administrator 242
Introduction 242
User Data 242
Internal Companies 243
Viewing all your internal companies *244*
Adding/Editing Internal Companies *245*
Internal Networks 260
Viewing all your internal networks *261*
Adding/Editing an Internal OFTP Network *264*
Adding/Editing an Internal AS2 Network *274*
Adding/Editing an Internal FTP client Network *279*
Adding/Editing an Internal FTP server Network *283*
Trading Partners 287
Viewing all your trading partners *288*
Adding/Editing Trading partners *289*
Networks (Trading Partner or Clearing Centre) 303
Viewing all your networks (trading partner or clearing centre) *304*
Adding/Editing Networks *308*
Network Overviews *309*
Network – Status *320*
Network – Security *322*
Network – Inbound (OFTP) *324*
Network – Outbound (OFTP) *325*
Network – Overrides (OFTP) *326*
Network – Mailboxes *326*
OFTP Mailbox *328*
FTP client Mailbox *334*
Network – EDI Codes *338*
Network – Inbound (AS2) *343*
Network – Outbound (AS2) *344*
Network – MDN Receipts *345*
Network – Connections *347*
Adding a new Network Connection *349*
OFTP Network – Advanced *368*
AS2 Network – Advanced *370*
FTP Client Network – Advanced *372*
FTP Server Network – Advanced *374*
Network – Advanced (OFTP) *375*
Network – Advanced FTP *378*
Network – Directory Options *380*
Network – User Data *382*
ENGDAT Relationships 383
Viewing your ENGDAT relationships *384*
Adding/Editing ENGDAT Relationships *385*
ENGDAT Relationship – Overview *385*
ENGDAT Relationship – Communications *386*
ENGDAT Relationship – Contacts *389*
ENGDAT Relationship – Default Details *390*
Subsystems 392
Viewing all your subsystems *392*
Adding/Editing a CAPI2 subsystem *393*
Adding/Editing a TCP/IP subsystem *401*
Adding/Editing an HTTP subsystem *405*

Adding/Editing an XOT subsystem *409*
Adding/Editing an FTP server subsystem *412*
EDIFACT Security Settings 415
Internal EDI Code - Certificates *415*
External EDI Code – Security Options and Certificates *416*
Signing Options *417*
Verify Options *419*
Communication Settings 420
Communication Settings *420*

Workflow Manager 422
Introduction 422
How to use the Workflow Manager 422
Trading Partners 423
Data Sources 423
Viewing all your data sources *424*
Add/Edit Command data source *426*
Add/Edit Comms data source *427*
Add/Edit Directory data source *429*
Add/Edit MQ data source *430*
Data Definitions 431
Viewing all your data definitions *433*
Add/Edit Non-EDI Data Definition *434*
Add/Edit Invalid EDI Data Definition *435*
Add/Edit EDI Message *436*
Add/Edit EDI Message Group *438*
Add/Edit EDI Data Definition *440*
Workflows 448
Viewing all your workflows *449*
Workflow – Overview *451*
Workflow – Jobs *452*
Channels 462
Viewing all your Channels *463*
Channel – Overview *465*
Channel – Advanced Workflow *467*
Channel – Advanced Conditions *469*
Channel – Automated Activation *471*
Channel – Counters *474*
Channel configuration report *475*
Routing Table 476
Configuring The Routing Table *477*
Using The Routing Table *481*

Communications Monitor 483
Menu options 483
Actions – Call Selected Networks *485*
Actions – Call Network *485*
Actions – Dismiss *486*
Actions – Disconnect *486*
Communications Sessions 486
Available columns *486*
Comms Filter settings *487*
Comms configure columns *488*
Log 490
Colour coding *490*

ODEX Workstation 491
Introduction 491
Workstation Files colour coding *491*
Workflow Files *492*
Displaying Workflow File EDI Data *492*

Comms Files *492*
Workflow and comms files *493*
EDI Security Status *493*
What does the ODEX Workstation do? *493*
Workflow Files tool bar *495*
Workstation View options 496
Refresh *496*
Refresh All *496*
Search *496*
Columns *498*
Views *500*
Close Search Results *501*
Close All Search Results *501*
Workflow Files – File Details 501
File columns *502*
Interchange columns *504*
Message columns *505*
Workflow Files – Audit Log 505
Columns *505*
Workflow Files – View option 505
Filter *505*
Show Audit Trail *508*
Show All Messages *508*
Workflow Files – Actions 509
Workflow File Details *509*
Comms Details *512*
Audit Details *514*
File Analysis *515*
Archive *518*
Delete *518*
Extract *519*
Extract Pre-Job File *520*
Open With *521*
Open Pre-Job File With *521*
Submit and Resubmit Overview *522*
Export to SAP *526*
Requeue SAP status records *527*
Sign EDI *527*
Create and submit AUTACK *528*
Error Files 528
Error Files Filter *529*
Archived Files 531
Archived Files Filter *531*
Comms Files – File Details 533
Comms Files tool bar *534*
Comms Files – View option 535
Received Files Filter *535*
Scheduled Files Filter *537*
Sent Files Filter *539*
Forward Files Filter *541*
Received Files – Available columns *543*
Scheduled Files – Available columns *545*
Sent Files – Available columns *547*
Forward Files – Available Columns *548*
Comms Files – Actions 551
Comms File Details *551*
Workflow File Details *551*
Session Details *551*
File Analysis *551*
Delete *552*
Acknowledge *552*
Suspend *552*
Resume *552*

Reschedule ... *553*
Reset Attempts ... *553*
Extract *554*
Open With ... *555*
Submit *555*
Schedule File ... *556*
Call Network ... *560*

ODEX ENGDAT Workstation ... 561
Introduction ... 561
Workstation Views ... 561
Inbound folders ... *561*
Outbound folders ... *562*
Workstation Toolbar ... 563
Workstation View Options ... 563
Filter *563*
Columns ... *564*
Workstation – Common Actions ... 568
Workstation – Common Actions – Extract Folder ... *568*
Workstation – Common Actions – Extract Folder with ENGDAT Filenames ... *569*
Workstation – Common Actions – Extract and Decompress Folder ... *569*
Workstation – Common Actions – Delete Folder ... *569*
Workstation – Common Actions – Print Report ... *570*
Inbound Folders ... 571
Inbound Folders – Available Columns ... *572*
Inbound Folders – Toolbar ... *572*
Inbound Folders – Actions ... *573*
Inbound Folders – Actions – View Folder ... *573*
Outbound Folders ... 573
Outbound Folders – Available Columns ... *574*
Outbound Folders – Toolbar ... *575*
Outbound Folders – Actions ... *575*
ENGDAT Folder Editor ... 578
ENGDAT Folder Editor – Navigation Panel ... *579*
ENGDAT Folder Editor – Information Panel ... *580*
ENGDAT Folder Editor – Validation ... *582*
ENGDAT Folder Editor – Navigation ... *582*
ENGDAT Folder Editor – Folder Actions Tab ... *583*
ENGDAT Folder Editor – Folder Data Files Tab ... *585*
ENGDAT Folder Editor – ENGDAT Message Overview Tab ... *586*
ENGDAT Folder Editor – Message Exchanged Files ... *589*
ENGDAT Folder Editor – External Document Links ... *590*
ENGDAT Folder Editor – Exchanged File Overview ... *591*
ENGDAT Folder Editor – Drawing Details ... *593*
ENGDAT Folder Editor – File Details ... *594*
ENGDAT Folder Editor – Contained Files ... *594*
ENGDAT Folder Editor – File Links ... *596*

ODEX Batch Administrator ... 597
Introduction ... 597
Configuration ... 597
Connection and Logging ... *597*
Running the ODEX Batch Interface ... *598*

The ODEX Batch Language ... 600
Introduction ... 600
The Batch Interface ... 600
Commands File ... 601
Batch Invocation ... 603
Running a Batch Command File ... *603*
Batch Response File (ODEXPC.RSP) ... 605

Commands 607
ODEX batch commands and their responses 607
-CNSTRUCT – Construct an EDI File 609
-CTLUPDAT - Control File Record Update 610
-DIRADD – Add Directory Entries 614
-DIRUPDAT – Directory Update Command 619
-RCVFILE – Extract Data File 624
-RCVODETT – Extract EDI Data 628
-REPRCV – Report on Received Files 631
-REPSND – Report on Scheduled Files 635
-RUNTASK – Run a task from the Event Scheduler 639
-SNDFILE – Schedule a file to be sent 640
-SNDODETT – Schedule an EDI file to be sent 644
-STOPSERVER – Stop ODEX 648
-TRNSLATE – Translate an EDI File 649
-WRITELOG – Write a line to the ODEX log 650
-DOS – Obey a DOS command 651

Database Backup and Restore 652
Introduction 652
Perform a backup or restore 652
Using a non-default server 652
Performing the operation 653

Frequently Asked Questions 654
How do I add a new trading partner using a direct IP connection? 654
How do I add a new trading partner using a local CAPI connection? 654
How do I add a new trading partner using an HTTP connection? 655
How do I make an automatic call to a trading partner? 657
How do I test a connection to a trading partner? 657
How do I automatically pick up files from a directory and schedule them? 657
How do I automatically copy received files to a directory? 658
How do I create an error workflow? 658
How do I add a workflow to translate received files, trap translation errors and raise e-mail alerts? 659
How do I add a workflow to construct and schedule files, trap construction errors and raise e-mail alerts? 660
How do I unlock an ODEX component? 661
How can I fix connection problems? 661
How do I integrate with SAP? 661
Configure the details of your SAP system 661
Automate the import of SAP IDocs into ODEX 662
Automate the export of SAP IDocs into SAP 663
How do I use OFTP security? 664
How do I configure ODEX to send ENGDAT folders? 665
How do I configure ODEX to receive ENGDAT folders? 666

Appendices 668
Events 668
Acknowledgement Received 668
Acknowledgement Sent 668
Call Ended 668
Call Failed 668
Call Retry Limit 668
Call Started 668
Connection Failed 669
Database sweep completed 669
File Not Sent 669
File Received 669
File Retry Limit 669
File Sent 669

General System Error ... *669*
Primary Connection Failed ... *670*
SAP Export Failed ... *670*
Server Started ... *670*
Server Starting ... *670*
Server Stopped ... *670*
Workflow File Hold ... *670*
Workflow File EDI Reject ... *670*
Unexpected Receipt Received ... *671*
Unhandled Workflow Error ... *671*
Actions ... 671
Call Network ... *671*
Check Certificates ... *671*
Check EDI Acknowledgements ... *671*
Check Performance Counter ... *672*
Poll Message Queue ... *673*
Poll Monitored Directory ... *673*
Run Application ... *673*
Send E-mail ... *674*
Send SNMP Trap ... *674*
Windows Application Log ... *674*
Write File ... *675*
Write to Message Queue ... *675*
Jobs ... 675
Acknowledge ... *675*
Analyse *676*
Call Network ... *676*
Construct ... *676*
Convert File Encoding ... *677*
Copy *684*
Copy (with Xml) ... *685*
E-mail *685*
Map *686*
Print Report ... *689*
Process AUTACK ... *689*
Reformat ... *690*
Run Application ... *691*
SAP (Associate) ... *692*
SAP (Export) ... *693*
Schedule ... *693*
Schedule ENGDAT file ... *696*
Sign EDI ... *696*
Split *698*
Translate ... *698*
Update ENGDAT Folder ... *698*
Verify Signed EDI ... *700*
Wait for Acknowledgement ... *701*
Wait for Transmission ... *702*
Windows Application Log ... *702*
Write To File ... *702*
Write to MQ Message Queue ... *703*
Condition Parameters ... *703*
Placeholders ... 704
Communication File Placeholders ... *704*
Communications Details Placeholders ... *709*
Date/Time Placeholders ... *710*
Log Placeholders ... *711*
SAP System Placeholders ... *712*
User Data Placeholders ... *714*
Workflow File Placeholders ... *715*
File Analysis Placeholders ... *718*
Placeholder Processing Instructions ... *721*
OFTP Cause and Diagnostic Codes ... 722

ESID Error Codes *722*
SFNA/EFNA Error Codes *724*
ISDN Clearing Cause Codes *726*
CAPI Errors *727*
X.25 Clearing Cause Codes *731*
X.25 Diagnostic Codes *733*

Glossary 737

Product History

What's new in ODEX Enterprise version 2.5.0?

The following is a comprehensive list of the changes made in ODEX Enterprise version 2.5.0:

OFTP2 Component – OFTP protocol release 2 is now available as a licensable component which when unlocked opens up OFTP2 to be used in ODEX.

SFTP Component – SFTP protocol is now available as a licensable component which when unlocked allows connection to a FTP server using SFTP protocol.

iSeries File Deletion - FTP client Mailboxes can now be set up with the option to delete iSeries files that is meant to be used on FTP server which is running on an AS/400 machine.

Ignore Usage Restrictions - Certificates can now be edited to set the 'Ignore Usage Restrictions' option which when selected would allow certificates to be used for purposes other than those intended by the certificate issuer.

What's new in ODEX Enterprise version 2.4.0?

The following is a comprehensive list of the changes made in ODEX Enterprise version 2.4.0:

Certificate Store – ODEX now has its own internal certificate store that can be managed through global and company-specific views.

Certificate Exchange – ODEX can now exchange certificates with trading partners using Odette Certificate Exchange. Trusted-service Status Lists will be downloaded from Odette to validate these exchanged certificates.

Odette OFTP2 Interoperability – Passed Odette's latest OFTP2 Interoperability tests including certificate exchange.

SAP Transactional RFC (TRFC) support – Better SAP R/3 connections

HMRC AS2 – Validated against HMRC with COMCERT certificate

X12 Functional Acknowledgements – ODEX can now generate and process X12 functional acknowledgements

64-bit support – ODEX is now available for the x64 (AMD64) platform

Interchange and Message EDI Data – Following the analysis of an EDI file the data extracted from the interchange and message segments can be displayed in the Workstation as new columns. To show this data fully there is a new toggle 'Show All Messages' which displays each message as a single row as opposed to each file. Searching in the Workstation has been enhanced with this functionality.

What's new in ODEX Enterprise version 2.3.0?

The following is a comprehensive list of the changes made in ODEX Enterprise version 2.3.0:

ENGDAT – ODEX has been updated to include the functionality to create and process ENGDAT folders and ENGDAT messages. A new client is now included for viewing, editing and sending ENGDAT folders. A new workflow job is also now available to handle the processing of inbound ENGDAT folders.

What's new in ODEX Enterprise version 2.2.0?

The following is a comprehensive list of the changes made in ODEX Enterprise version 2.2.0:

OFTP Mailbox Settings - OFTP mailboxes now include parameters for source and target encoding. This allows files to be automatically converted to the correct encoding when they are scheduled. Additionally, the OFTP file format and record size may now be configured for individual mailboxes.

Schedule Job – The schedule job now includes parameters for sender and receiver local codes, allowing files to be scheduled based on the local codes of the sender and receiver mailboxes.

Windows Vista Compatibility – ODEX has been updated to be compatible with Windows Vista. Data files, such as workflow files and communication files as well as log files are now stored in a separate directory to the rest of the program. This directory can be changed during installation.

Microsoft SQL Server 2005 – ODEX has been updated to be able to use the latest version of Microsoft SQL Server, though ODEX is still compatible with Microsoft SQL Server 2000.

Enhanced Network Lists – The internal, trading partner and clearing centre network lists now allow all mailboxes or EDI codes associated with the networks to be displayed.

SNMP – A new event action has been added that allows ODEX to send SNMP traps in response to ODEX events. This provides a mechanism to alert System Administrators using an SNMP console of potential problems.

SSL – ODEX clients can now connect to the server using SSL connections. This feature allows for extra security particularly in environments where client and server are located on different sites and communicate over an external network connection.

Performance counters – A number of ODEX communications and workflow metrics may now be exposed as Windows performance counters and used to ensure that the expected throughput of files is maintained.

Performance counters may prove useful in Just-In-Time supply environments where the receipt of files is critical. For example, counters may be can be set up to monitor the time since a file was last received, or how many files are sent per hour. An event action can be set up to monitor counters and when they fall below a certain level perform some other action to notify the user such as send an email.

Multiple Mapping Tasks – ODEX is now able to perform Xe maps in parallel and assign a processing priority to each map. This provides a mechanism to ensure that higher priority messages are performed by a single mapping process and do not become held up by less critical maps. This can be controlled via new parameters upon the Xe job.

Xe Mapping Command – An Xe map may now pass mapped data to the workflow file and store it in the workflow files user data field. This may be viewed in ODEX from the Workstation by adding the "User Data" column to a workflow view. As the user data is accessible through placeholders this provides a mechanism to use mapped data in any other ODEX job. (See the SetWorkflowFileUserData command in the Xe user guide.)

WebSphereMQ – ODEX can integrate with IBM WebSphereMQ messaging servers and is able to both send and receive messages using either actions or jobs upon a workflow. This may be useful in environments where internal systems rely upon WebSphereMQ messaging servers, as ODEX can routinely poll a message queue using an event action. When a message is retrieved the message can be submitted to a workflow for processing.

Communities – Using the community feature, ODEX users can now be restricted to a pre-configured list of trading partners.

ODEX now allows for access to files to be restricted by trading partners and networks through association of the logged on user with a community. This facility allows different ODEX users to have different views of the system that are applicable to the users role.

What's new in ODEX Enterprise version 2.1.0?

The following is a comprehensive list of the changes made in ODEX Enterprise version 2.1.0:

File Forwarding – ODEX now allows files to be received and automatically forwarded to a trading partner.

Routing Table – Received files can be routed to trading partners based on file criteria. Files can be received and forwarded using different protocols to receive and send the files.

Placeholder Processing – It is now possible to use placeholders in parameters to the XE map job. The schedule job can now be configured to use placeholder values based on a received file. A new placeholder has been added to represent the document type of a file.

SFTP – ODEX now supports the SFTP protocol

Special Logic – ODEX now supports OFTP special logic

Client Configuration – ODEX now allows the banner colour in client applications to be changed, making each client easily identifiable on a machine running multiple client applications.

General System Error Event – The general system error event has been improved to allow errors to be caught based on the log message ID, using wildcard operators.

FTP – FTP now supports the Novell FTP server, Enterprise FTP Server, Windows FTP server in MSDOS listing mode and AS/400 using different naming formats. Additionally a "User startup commands" against an ODEX FTP client network gives the user the ability to setup specific FTP connections.

Workstation - A view is now available to manage files being forwarded to trading partners in a clearing centre environment. The existing views can now be filtered by the local codes of networks and mailboxes.

New system events – File Received, File Sent, Acknowledgement Received, Acknowledgement Sent.

What's new in ODEX Enterprise version 2.0.0?

The following is a comprehensive list of the changes made in ODEX Enterprise version 2.0.0:

- **FTP Support** – ODEX features an automated FTP client and also an FTP server for sending and receiving files

- **OFTP 2** – ODEX now offers additional OFTP security features
- **. NET 2** – ODEX now runs against version 2 of the .NET framework
- **AS2 authentication** – AS2 now allows client authentication
- **User Data Fields** – user data can now be stored against companies, networks, mailboxes and data sources and used as placeholders in various jobs and actions.

What's new in ODEX Enterprise version 1.3.0?

The following is a comprehensive list of the changes made in ODEX Enterprise Version 1.3.0:

- **New XOT subsystem** – XOT support has been added to ODEX. This includes the ability to create one or more XOT communication subsystems and link a trading partners Network connection to an XOT subsystem.

  This facility has been provided to allow ODEX to communicate using OFTP via X.25 connections as they are still used for some manufacturers.

- **Placeholder processing** – A new placeholder %OFN_E_X%, which returns the original file name extension without the dot. Substrings of placeholders may now be returned and converted to upper/lower case. For instance, if the %VFN% returns "ABCD1234" then %VFN[$.LEFT(3)]% returns "ABC" and %VFN[$.LEFT(3).LOWER()]% returns "abc". See help guide for more information.

- **Message Definitions** – Message definitions, which can be used to qualify the data files assigned to a channel, have been extended to include the 'Association Assigned code' and 'Controlling Agency' from the UNH segment.

- **Configuration Report** – A new report is available from the 'Tools' menu within the Administrator client. The report lists the workflow definitions that have been configured from the 'Workflow' tab of the Administrator. The report is a useful aid to understand the workflow configuration within ODEX Enterprise.

What's new in ODEX Enterprise version 1.2.1?

The following is a comprehensive list of the changes made in ODEX Enterprise Version 1.2.1:

- **ODEX Professional upgrade now supports Events and Actions** – most scheduled events and Event Manager events from ODEX Professional can now be upgraded into ODEX Enterprise.

- **New Job/Action to write to the Windows log** – allows ODEX to write a message to the Windows application log.

- **New Job/Action to write text to a file** – allows ODEX to use placeholders and fixed text to write text to a specified file. Equates to the “Write a file-based report” action in ODEX Professional.

- **New Job to reformat a file** – this job will enable re-formatting of workflow files using the Xlate reformat function to change to A1 format, A2 format, etc.

- **New Job to convert file encoding** – converts the encoding of a file between code pages.

- **New system events** – Call Ended, Call Started, Database Sweep Completed, Server Started, Server Starting, Server Stopped, Unexpected Receipt Received.
- **Active/inactive channels** – channels can now be triggered using schedules, system events or thresholds (number of files waiting).
- **Job conditions** – you can now specify one or more data definitions and data sources against a job, as well as against a channel.
- **E-mail attachments** – the E-mail Job and Action now support file attachments.
- **Extensions to Data Definitions** – Data Definitions can now include Application Reference and Test/Live status
- **Extra parameters for Run Application Job** – the Run Application Job now includes several extra parameters.
- **Extra placeholders added** – new placeholders and placeholder categories have been added.

What's new in ODEX Enterprise version 1.2.0?

The following is a comprehensive list of the changes made in ODEX Enterprise Version 1.2.0:

- **Addition of Batch Interface capability** – ODEX now includes a batch interface that is compatible with any previous version of ODEX you may have been running.
- **Upgrade or import from ODEX Professional** – you can now upgrade or import from ODEX Professional. Upgrade User Directory entries and Send/Receive file details immediately after installation, or import User Directory entries only.
- **Additional parameters for use in running Execute Application jobs** – additions to the Filename parameters.

What's new in ODEX Enterprise version 1.1.0?

The following is a comprehensive list of the changes made in ODEX Enterprise Version 1.1.0:

- **Addition of comms protocol AS2** – you can now send data over AS2.
- **Upgrade capability** – you can now upgrade to the latest version from a previous version of ODEX Enterprise.

ODEX Enterprise

Introduction

ODEX Enterprise is the next generation of Electronic Commerce/EDI product from Data Interchange Plc. ODEX Enterprise has been designed as a high-function Electronic Commerce gateway to cater for the needs of the most sophisticated user and demanding environment.

The features of ODEX Enterprise will cater for the most complex requirements, allowing its operation as a complete Clearing Centre, corporate Electronic Commerce gateway or high-function end user Electronic Commerce server.

The existing functionality from the Data Interchange product range has been consolidated to form the most sophisticated electronic commerce product offered so far. A key objective of the design has been to ensure that the operation of ODEX Enterprise is as simple as possible for the end user, whilst ensuring that a wealth of features are available.

The problems of managing the transmission and reception of EDI and non-EDI data are easily solved by ODEX Enterprise, which is well suited to roles as a corporate gateway or clearing centre. High level automation allows ODEX Enterprise to run unattended and its high performance, high throughput, automated front-end capabilities enable seamless integration with your production systems.

A key feature of ODEX Enterprise is its support of several communication protocols, communication sub-systems and message standards (see below) which allow the user complete flexibility when deciding which standards to adopt with different trading partners.

The design of ODEX Enterprise has allowed for additional communication sub-systems and EDI message standards to be added at a later date, without impacting the existing product structure.

ODEX Enterprise is extremely flexible, because basically it is just a file processor. It can get files from communications, monitored directories or via a GUI, and then process them differently according to where it got them from, where they are going to, and even according to the data itself. The processing might include mapping the data, recording analysis of the data, validating the data, running external applications on it and potentially outputting it, either using standard communications protocols or simply by writing it to a directory.

Features and Functionality

The following functionality and features are provided by the software, illustrating the flexibility and sophistication of this product.

Architecture

Multi-user environment based on client/server architecture

SQL Server database provides speed and flexibility

Protocols and Communication sub-systems

Supports the following protocols and communication sub-systems:

OFTP

TCP/IP

CAPI (ISDN)

AS2

FTP

SFTP

EDI functionality

Detailed EDI file analysis and interchange-level extraction

Files analysed, split, forwarded and processed according to EDI addressing and/or message type

Support of EDIFACT, UNGTDI, VDA and X12 standards.

Security

Supports a flexible user and user groups environment

Software functionality restrictions based on user privileges

Password protected access

Intelligent data processing

Just in Time functionality allows alerts to be raised if files are not transmitted or acknowledged within a configured timescale.

Automatic event scheduling available for a wide range of events

Actions triggerable by system event, scheduled event or script

Easy integration with existing in-house systems

Monitoring and auditing

Real-time system monitoring of communication sessions and statistics

Exception and full audit reporting

Audit trail and real-time session logging

Windows system logging

User-definable retention periods

Miscellaneous features

SAP R/3 support

24 hour operation and automated backup

Full on-line context Help

ODEX Enterprise Overview

A Client/Server application

ODEX Enterprise is a client/server application. This means that you can install the server on one machine and install each client on any number of other machines. The only stipulation is that the server must be installed on a machine that is accessible by each of the client machines.

The advantage of this system is that any number of people can work with the application simultaneously. Each user can access ODEX from his own machine, instead of having to walk across the office to the "ODEX" machine. Everyone has access to the same data, without having to wait for another person to finish using ODEX before they can use it.

The client/server architecture also means that you can configure ODEX to use Users and/or User Groups. This is a security feature which allows you to restrict users to certain areas of ODEX, or even to certain views within specific clients. For example, the IT Manager only needs to use the Administrator and the Communications Monitor, while most users only need to see the Workstation. Even within one client, users can be restricted to which parts of that client they can see.

When you use Users and/or User Groups, each ODEX user has to be set up in the Administrator with a user name and, optionally, a password. This also provides added security, since unauthorised users will not be able to access the system.

Running ODEX as a system service

Once you have installed ODEX, you can run it as a System Service. Running ODEX as a System Service provides a way of ensuring that ODEX runs continuously without being stopped, even when the user is logged off. This is beneficial to any user who needs to ensure that ODEX is always running, yet is not accessible to any unauthorised person.

Starting

To set ODEX running as a system service, click **Start >> Programs >> Data Interchange Plc >> Odex Enterprise 2.3.0 >> Install Server as Windows Service**. You will see a batch program start to run in a command prompt window. When the program completes, this window will disappear and ODEX will now be running as a system service. You will notice that the ODEX Server icon no longer appears in the system tray.

Stopping

If you have ODEX configured as a System Service but wish to stop it running temporarily, in order to restore the database for example, you will firstly have to open the Services applet from the Control Panel (**Start >> Settings >> Control Panel >> Administrative Tools >> Services**).

Here you must highlight ODEX Enterprise in the list of services, then click the '**Stop**' button. After a few moments the status of ODEX will change from 'Started' to blank. You can restart ODEX by repeating these steps but this time clicking the '**Start**' button.

To stop ODEX permanently from running as a system service, you should run the batch program UNISVR.bat, which is found in the installation directory.

Upgrading ODEX

When you upgrade to a new version of ODEX, you will need to stop the old system service, as described above, and set it not to start automatically when Windows starts.

To do this, right-click on ODEX Enterprise in the list of services and select Properties from the dropdown menu. On the dialog that appears, select Disabled as the Startup type and then click **OK**.

Then set the new server to run as a system service, as described above.

ODEX Concepts

OFTP (ODETTE File Transfer Protocol)

As the name suggests, this protocol was developed by the ODETTE organisation, and consequently it is used by most major European motor manufacturers and their suppliers. It is also used by the chemical industry and white goods manufacturers, and is currently being adopted by other business sectors such as banking and transportation.

An OFTP session does not require any interaction from the user. The two machines involved control the session, taking turns to send data until the session is closed by mutual agreement.

OFTP Commands

The following is a list of all possible OFTP commands. You may see these commands in the ODEX log when OFTP tracing has been set on. The two commands highlighted in red (SFNA and EFNA) indicate problems in the exchange of data.

SSRM	Start Session Ready Message	The first command to be sent after a session has been physically made. It indicates to the person that initiated the session that he is communicating with another OFTP capable machine.
SSID	Start Session IDentification	Contains User ID/Password information to identify the session partner together with indication of session capabilities. These capabilities are in the form of session negotiation information that allows the partners to request / accept /deny the use of special logic, compression and restart.
SFID	Start File IDentification	A request to send a file. It contains such information as the destination code for the file, the file name and file size.
SFPA	Start File Positive Acknowledge	This command is returned in response to an SFID and it gives the confirmation that the file may be sent.
SFNA	Start File Negative Acknowledge	This command is returned in response to an SFID and it refuses permission to send a file. The SFNA command should indicate whether origin or destination of the file is unrecognised.
DATA	The actual file data.	
CDT	CreDiT	Sent in response to a number of data blocks. This depends on the OFTP window size which defaults of 7. This means that 7 data blocks are sent before a CDT is sent in response. If the window size is too low, the machine sending data has to wait excessively for CDTs. Too high and there will be problems.
EFID	End of File IDentification	This command is sent after file data transfer has completed for an individual file to indicate the End of File condition. It also contains control totals to ensure the integrity of the sent file.

EFPA	End of File Positive Acknowledge	Sent in response to an EFID to indicate successful receipt of a file.
EFNA	End of File Negative Acknowledge	Sent in response to an EFID to indicate unsuccessful receipt of a file. Corrective actions will be taken. This usually occurs when the two systems cannot agree on the status of the file (usually after restarting).
EERP	End to End ResPonse	An EERP command is sent when a file reaches its ultimate destination, this is sent to the originator of the file to tell them that the file has been received.
RTR	Ready To Receive	This command is sent in response to an EERP. It just passes control of the session back to the sender of the EERP (in case they have anything else to send).
CD	Change Direction	Sent when no more files or EERP's are available to be sent to the trading partner. It assigns control of the session to the trading partner who may then send files or EERP's etc. If the recipient of the CD also has nothing to send, then they will issue an ESID.
ESID	End of Session IDentification	Requests that the session be terminated and disconnected. An error code is also generate, 00 indicates that the session ended successfully, anything else may indicate the both systems did not send all of their files.

OFTP Security and Authentication (EDI Codes)

The term “EDI code” should be used carefully as it could cover one (or more) of the 3 codes used in OFTP to identify a given party.

SSID Code/Network Node

The SSID code is sent to your trading partner at the start of an OFTP communication session. It informs them who you are as a company. The SSID command includes the SSID code and also an OFTP password. They then send back their SSID code and OFTP password in another SSID command. Either party can terminate the session if they do not like the contents of an SSID command.

SFID Code/File Node

Once the session is established, an SFID command is sent. This is a request to send a file. It includes the SFID code of the origin and the destination. In the most simple case the SFID code will be the same as the SSID code, but if you are exchanging files with multiple entities within a company, they may have a different SFID for each entity within the company.

The recipient of the SFID can then either accept (send back an SFPA command) the file, or reject it (send back an SFNA command) if they do not recognise the origin or destination.

Message Level EDI Code/Message Node

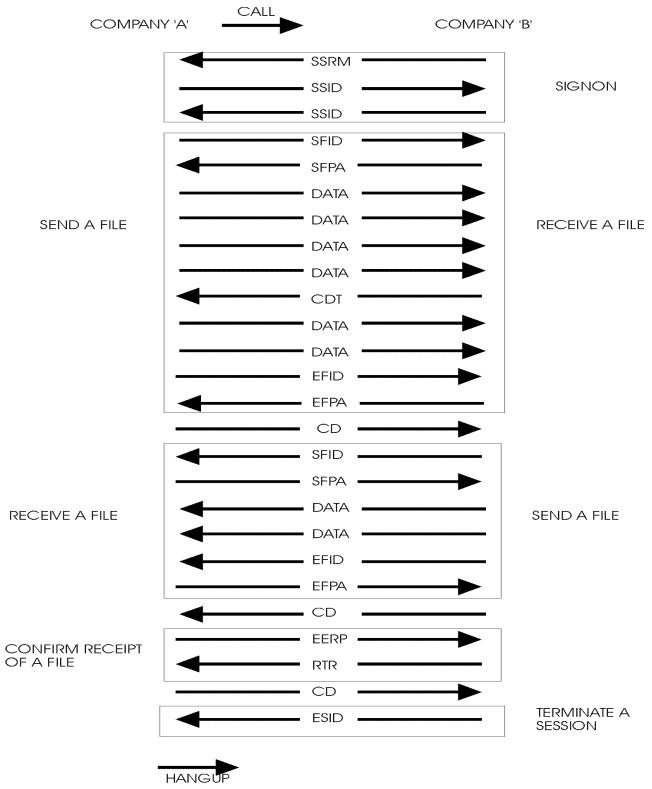
Inside each EDI message is yet another EDI Code. The first record in each EDI message contains the origin and destination. Depending on the format of the

file this could be referred to as something else, such as ANA number for ANSI X.12, or UNB code for EDIFACT/ODETTE.

Again this often refers to an entity within an organisation, although it could be the same as the SFID code, if a company has a different SFID code for each entity.

OFTP Session

The following example demonstrates a very simple OFTP session, using arrows to indicate the direction of the command flow.



Company A makes a call out to Company B.

Company B responds with an SSRM stating that they are ready to start using the OFTP protocol.

The companies then swap SSID commands. (This is the equivalent of telling each other their identity).

Company A then sends an SFID stating that they have a file to send.

Company B responds with an SFPA stating that they are willing to accept that file.

Company A proceeds to send the data.

After 4 data blocks, Company B sends back a CDT. (This is the equivalent of making a small response to indicate you are still on the line).

At the end of the file, Company A sends an EFID to state that this is the end of the file.

Company B then sends back an EFPA stating that the file was successfully received.

Company A has no more files to send, so now gives Company B the opportunity to send their files, by sending a CD (Change Direction command).

The process then starts again (there is no need to sign on again with the SSRM and SSIDs), and Company A receives a file from Company B.

At the end of the file, they change direction again with a CD command.

Company A acknowledges the file by sending an EERP.

Company B acknowledges the receipt of the EERP by sending the RTR.

Company A has nothing more to say so passes control to Company B.

Company B also has nothing to say and so sends an ESID, on receipt of which Company A hangs up the line.

Communication

When the OFTP protocol was created there were few methods of obtaining a secure connection between two companies (machines were not quick enough to encrypt data as it was sent). The X.25 protocol was therefore chosen as the recommended connection method for OFTP. This could be used either in "native" form, in which a dedicated X.25 line is purchased from a local telecom provider, or used on top of an ISDN connection (layers 1-2 are ISDN, layers 3-4 are X.25).

Note that the connection method needs to be the same at both ends.

TCP/IP was later added to the recommended protocols for OFTP. Since TCP/IP occurs at layers 3-4 this means that any layer 1-2 protocols can be used (providing they are the same at both ends). This could include a connection over the Internet, an existing network/WAN connection, or a dial-up connection using a standard Modem or ISDN. The protocol uses a single port (3305).

The deciding factor in choosing a connection method is usually the trading partner. If they already have connections to other companies and do not want to change, e.g. large manufacturers, then you do not have much choice, unless they allow connections via a VAN (see below).

On the whole, X.25 is very secure, but is slow and very expensive. TCP/IP is cheap and fast but can lack security (unless a secure point-to-point dial-up connection is made or an encrypted VPN tunnel is used).

X.25 over ISDN falls in the middle, as it is secure and reasonably cheap.

There are other methods of using X.25, whereby a standard modem connection is made to a local X.25 provider which then makes an X.25 connection on the sender's behalf. This is called X.28 or, where the modem connection is encrypted, X.32.

Connections can also be made to the X.25 network for free using the D channel of an ISDN line (the D channel usually just controls the two B channels which are used for data). This method, X.31, is currently not available in the UK, but is available in several European countries.

Direct or indirect communication?

There is another option, rather than connecting to a trading partner directly, which is to connect via a VAN (Value Added Network), also known as a Clearing Centre. This is analogous to a postal service. It would be rather time consuming to hand deliver all mail, so you simply write the address on the mail and delivery it all to a third party.

With a VAN you make a single connection (exchanging SSID commands with the VAN rather than each trading partner), and then send/receive all of your data in one go. Depending on the way the VAN in question operates, you will

either send to different SFID destinations, or to different Message Level EDI code destinations.

The main advantage of using a VAN is that you require only one communications link in order to communicate with all your trading partners. This means that you may only need to make one call per day to send and receive your EDI documents to and from all your trading partners.

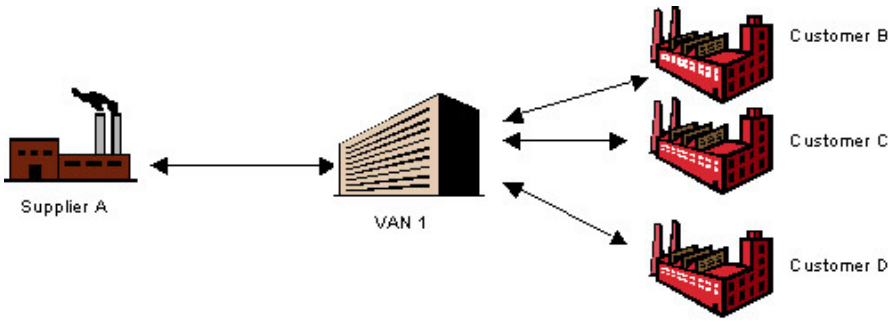
A VAN can either make calls proactively to send data on receipt, or wait for the recipient to collect it. The person sending the data will know when it has been received by the final recipient, as they will only receive the EERP once the final recipient has sent an EERP command to the VAN.

You can also connect to a VAN using a different protocol to your Trading partner. For example, if they only accept X.25, you could save around £5000 in line rental alone by sending your data to a VAN using ISDN. The VAN then sends it to your trading partner using X.25.

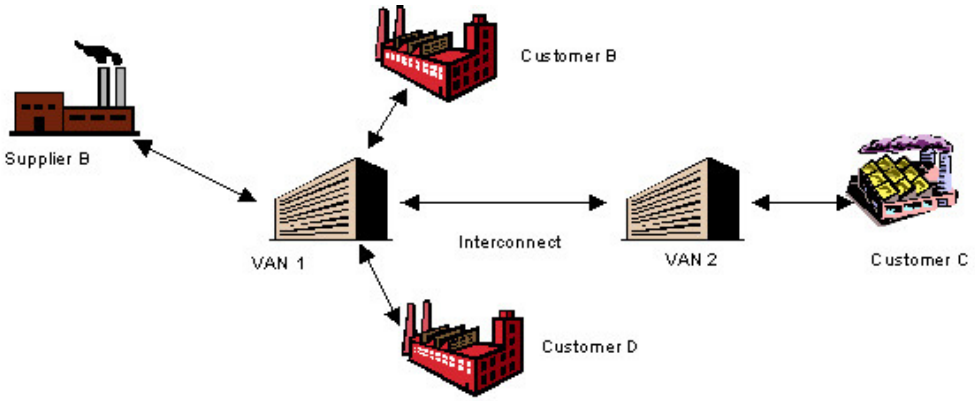
The only scenario in which you would not want to use a VAN, would be if you were sending excessively large amounts of data to a single trading partner (for example CAD/CAM data which can be 100Mb in size or more). Since VANs usually charge for the amount of data sent, it may be more cost effective to pay the line rental yourself.

Even if your trading partner prefers to use a different VAN from the one you have chosen, an interconnect can be set up between the two VANs to enable you to communicate.

The illustrations below show how different companies might communicate with each other.



The illustration above shows that Supplier A communicates with all his customers via VAN 1.



The more complex situation above can be described as follows:

Supplier B uses VAN1 to connect to all his customers (B, C and D).

Customer B and Customer D also use VAN1 to connect to their trading partners.

Customer C uses VAN2 to connect to his trading partners.

Supplier B connects to Customer C via an interconnect between VAN1 and VAN2. Once the interconnect has been set up, connections between Supplier B and Customer C appear no different from those between Supplier B and Customer B.

Supplier C connects to Customer C directly. If Supplier C increases the number of customers he supplies to, he will probably find it easier to use a VAN to communicate with them.

OFTP Revision 2 Changes

Revision 2 of the OFTP sought to ensure that it remained the mainstay protocol of choice for business-to-business communications. To that end the following changes/additions were made -

- Session level encryption (using SSL/TLS)
- Secure authentication
- File level encryption
- File compression using the DEFLATE algorithm
- Signed EERP/NERP
- Maximum permitted file size increased to 9PB (petabytes)
- Virtual filename length increased to 255 characters

Security services have been added to allow OFTP to be secure over the Internet and over X.25 networks and features like an enhanced compression routine have been added in response to the user community's wishes.

The security features in the OFTP are centred on the use of X.509 certificates (see the section entitled "Encryption and signatures"). All algorithms and enveloping technologies are standards that have been widely implemented on the major platforms. The use of self-signed certificates is allowed.

OFTP 2 has been designed so that a secure session can be established with only one of the trading partners requiring a certificate, this being the party that is the recipient of a connection attempt. This means that session security between an OEM and its trading partners can be achieved without requiring all the trading partners to obtain a certificate, assuming that trading partners connect to the OEM.

Backward compatibility is important and OFTP 2 has been designed so that the new and changed commands can still be understood by applications supporting older versions of OFTP (1.4 and below). OFTP 2 capable applications, like ODEX, can negotiate the protocol level down to the highest level supported by both applications.

Security Overview

OFTP 2 provides three security services:

- Session level encryption (TLS / SSL)
- File level encryption
- OFTP Authentication

These security services are entirely optional and can be combined together in any combination. Session level encryption encrypts all of the OFTP session data between two trading partners so that an external party cannot see the data going between them. In order to achieve session level security trading partners may agree to utilise SSL/TLS. This negotiation occurs outside of the OFTP session and so is transparent to the OFTP.

In addition, a file can be encrypted and sent via OFTP using file level encryption. File encryption essentially offers the same level of security as session level, so two trading partners may choose to use one or the other. File encryption does not encrypt the OFTP session, and so it may be possible to uncover useful information e.g. if you use the VFN: TOPSECRETNEWFORD then a third party could potentially get hold of this information. There is no such danger when using the session level encryption.

It may well be that two companies wish to prevent external third parties from looking at the data being sent between them, and this is accomplished using session level security, but with additional file level security that is required so that only specific departments or individuals are able to read the file when it arrives at the recipient company.

OFTP Authentication ensures that both parties are who they say they are, and based on this knowledge a company can allow (or disallow) a party to send them files. No company wants just anybody to send them files (such as viruses). OFTP Authentication increases the confidence that can be placed in the OFTP EDI codes and passwords that are exchanged in SSIDs.

Secure Authentication

The SSID command now contains a 'Secure Authentication' indicator that may request that new OFTP commands be exchanged to confirm the true identities of the trading partners in session.

The new commands are AUCH (authentication challenge), AURP (authentication response) and SECD (security change direction). They flow after SSID exchange as follows -

```
Initiator <-------------SSRM --        Responder
          -- SSID ------------>        Identification
          <------------ SSID --        Identification
          -- SECD ------------>        Security Change Direction
          <------------ AUCH --        Challenge (the Initiator)
          -- AURP ------------>        Response
          <------------ SECD --        Change Direction
          -- AUCH ------------>        Challenge (the Responder)
          <------------ AURP --        Response
```

Both the initiator and the responder exchange SSIDs as normal so that the protocol options, including whether authentication is required, can be negotiated.

The Secure Authentication phase authenticates the initiator first and then the responder. The Secure Authentication phase changes direction first using the Security Change Direction to allow the responder to send out a plain text

challenge to the initiator. The initiator sends back a response, which is the signature of the challenge. Assuming the certificate is valid for the signature and the responder trusts the issuing authority, then the initiator has verified him. A Security Change Direction is then sent to allow the responder to authenticate himself to the initiator.

File Security

The content of a file is kept from third parties by encryption. Signing ensures that it has not been corrupted (accidentally or maliciously) and that it was sent by the originator claimed.

New SFID fields indicate if a file has been signed, compressed and/or encrypted. Any or all of the processes are optional but they are always preformed in this sequence -

1. Sign the original data
2. Compress the signed data
3. Encrypt the compressed/signed data

Signed EERP/NERP

Another new indicator in the SFID may optionally request that any EERP (or NERP) returned for the file must be signed. An EERP is an acknowledgment that a file has been delivered to its final destination. By checking a digital signature, the originator of a file knows that the EERP was sent by the claimed trading partner and is a true acknowledgment of receipt.

Maximum File Length

The SFID has been changed to allow for a maximum file length of 9.3PB (petabytes), which is well beyond what is currently considered a realistic file size.

File Compression

Improved compression is provided in OFTP 2 by the Deflate algorithm. This compresses a whole file before transmission unlike the old compression method inside OFTP, which compressed buffers as they were transmitted.

Virtual Filename Length

The length of the virtual filename in the SFID has been extended from 26 to 255 characters to reflect the wide variety of file name lengths on different platforms.

Workflows

ODEX Enterprise offers you a new way to control and process your files automatically. Along with this new control system comes a set of terms and concepts that you will not have met before. This section aims to define and explain what each of these terms and concepts are, and how they can be used to unleash the power of ODEX.

The new system requires some preliminary analysis on your part:

- What differentiates the files that will be arriving in the system?
- What similarities do the files have?
- What do you want ODEX to do with each file that arrives in the system, according to their differences and similarities?

Having analysed your requirements, you can then configure the Workflow Manager section of the Administrator to get ODEX to do exactly what you want with each file.

However, there are several concepts that you need to understand before you start to configure the Workflow Manager.

Data Source

ODEX Enterprise has various ways of receiving files into the system. Each "gateway" into the system is deemed to be a data source i.e. somewhere that ODEX gets data from.

Data sources fall into three different categories:

- Communications
- Directory
- Commands

Communications

A communications data source is a definition of the networks and/or mailboxes that are being used for communications. A communications data source is made up of:

- Originator Network
- Originator Mailbox (depending on comms protocol)
- Destination Network
- Destination Mailbox (depending on comms protocol)
- A filename mask (optional)

You could also define a data source that represents files received via <Any> network and <Any> mailbox.

Directory

A directory data source is simply one or more directories that ODEX is monitoring or a directory that ODEX is told to look in (either by an event or by a user).

A directory data source is made up of:

- The directory path
- A file mask

Commands

The final type of data source exists to allow users to use commands (maybe from a batch file, or via a GUI of some sort) to tell ODEX to import a file or files.

When using this mechanism, the command used (e.g. "Schedule EDI File") will be part of the definition of the data source, as will the directory and filename.

A command data source is made up of:

- The command name
- The directory path

- A file mask

Message Definition Group

A message definition group is a logical grouping of message definitions, where a message definition is a definition of an EDI message, such as EDIFACT DELFOR D96A or VDA 4905.

A message definition group can have more than one message definition in it. For example, you might define a message definition group to represent all the invoices in the system, called “invoices”. It would contain a message definition for each type of invoice you expected to encounter – EDIFACT INVOIC, ODETTE INVOIC, VDA 4908, UNGTDI INVHDR, etc…

Trading Partner

A trading partner is a set of logically related interchange level routing addresses (i.e. EDI codes). For example, you might define a ”Peugeot” trading partner containing all Peugeot’s EDI codes.

Data Definition

ODEX Enterprise can process various types of files, but it is particularly adept at processing EDI files. A data definition describes a logical grouping of data (e.g. all the invoices, or all the ASCII files). The data definition can also contain information about message level routing.

A data definition has the following properties:

- Format (EDI, XML, Non-EDI…)
- Encoding (ASCII, EBCDIC…)
- Message Definition Group (a collection of message definitions)
- One or more Trading Partners

It should be noted that not all the properties have to be present. You could for instance define a data definition that represents all EDI files (regardless of encoding, message and trading partner).

Channels

A channel is a flow of a particular type of data. A channel might represent all the invoices in the system, or it might represent all the data going to a particular trading partner. In short, a channel is used for processing a logical grouping of data.

ODEX Enterprise uses the concept of channels to allow conditional processing of data through the system.

Whenever a file is entered into the system (by whatever route), ODEX will associate the file with a channel and base all processing of the file and its data on the configuration set up for that channel.

A channel contains definitions of the data that should be processed by that channel. It uses Data Definitions and Data Sources to do this. A channel consists of:

- Zero or more Data Sources
- Zero or more Data Definitions

As there may be more than one channel in the system, and as a given file could be valid for more than one channel, the channels are ordered. When a file is

received, if it fits the first channel in the list, it will be processed according to the instructions against that channel. If it does not fit the first channel, it will be compared to the second channel, and so on… You must determine the order of the channels when you create them.

Once a file is matched with a particular channel, the file is processed according to the Workflow associated with that channel.

Workflow

A workflow is a list of jobs to be done on a file. Each job is carried out in order. When a job has finished, the next one is performed. If a job produces one or more output files, each output file is then submitted to the rest of the workflow.

> *N.B. The original file remains unchanged and is not itself moved through the workflow. Likewise, each output file that is created during workflow processing remains in its original form. Only copies of the files are actually processed. In this way, traceability can be maintained.*

As well as having a list of jobs to be performed, a workflow can reference other workflows:

- Next workflow – triggered when a file reaches the end of the workflow
- On error workflow – triggered when a file is being processed by a workflow but an error occurs

Error Workflow

An error workflow is a special workflow that can be triggered when an error occurs while a file is being processed.

Job

A job is one step of a workflow. It indicates a single job to be done on a file and the parameters for doing that job. A job is:

- Job definition – defines the job to be done
- Job parameters – defines the parameters to use to do the job
- On error workflow – overrides the workflow's “on error workflow” for this particular job

Job Definition

A job definition simply indicates the job that needs to be performed. ODEX Enterprise will be able to perform a multitude of jobs on a file, and the list of jobs is extendable. The following list gives some examples of the jobs that can be carried out:

- Translate from EDI into in-house format
- Construct into EDI from in-house format
- Record EDI Analysis
- Analyse EDI (syntax, interchange control reference, digital signatures)
- Copy to a directory
- Schedule to a network/mailbox
- Notifications (e-mail)
- Run an external application

- Process a received ENGDAT file

File processing in the Workflow Manager

This section is designed to explain the way the Workflow Manager works, thus giving you an understanding that will enable you to configure your Channels, Workflows and Jobs appropriately.

The Workflow Manager processes files using workflows to determine jobs to do on a file. A workflow is just another name for a series of jobs to perform on a file. Each job has a name (e.g. Translate) and a set of parameters to dictate how the job will be carried out.

The Workflow Manager uses Channels to determine which workflow(s) to use to process a given file. A channel links particular types of files, from particular data sources, to a configuration (which is made up of one or more workflows) of how a file should be processed. A channel contains the following information:

- Zero or more data sources
- Zero or more data definitions
- One or more workflows (with an execution order)
- A flag to indicate if an audit log should be recorded for files in this channel
- A flag to indicate if the file should be split into interchanges
- A flag to indicate if interchange information should be saved after the file is processed
- A flag to indicate if the original file should be deleted
- A workflow to be used if an error occurs

To determine if a file "fits" a channel, the file must be from a Data Source that is against the channel and match one of the Data Definitions against the channel. As it is possible that a particular file could satisfy more than one channel, the channels in the system have an order that determines which order they will be checked in. When the Workflow Manager gets a new file, it starts to compare the file to each of the channels in turn.

Every file that enters the system will have data source information associated with it. A file will have the following information associated with it:

- For files received via communications:
  - Protocol (OFTP or AS2)
  - Connection (TCP/IP, CAPI, etc…)
  - Network
  - Mailbox
  - VFN
- For files picked up from monitored directories:
  - Directory
  - Filename
- For files received using commands (e.g. Schedule File command):
  - Command name

- Directory
- Filename

As the Workflow Manager works its way through the list of channels, it compares the file and its associated information to each channel.

In any data source definition, some or all of the fields can contain a wildcard ("*") to indicate that any values are a match for that field.

A data definition contains the following information:

- Format (EDI, non-EDI, XML, etc…)
- Encoding (ASCII, EBCDIC, etc…)
- One or more messages (in the form of a message category), where a message consists of:
  - Syntax
  - Version
  - Release
  - Message Type
- One or more trading partners (in the form of a trading partner group), where a trading partner is essentially a message node, which is:
  - EDI code
  - EDI code qualifier
  - Reverse routing address
  - Test/Live
  - Application Reference
  - Syntax Identifier
  - Syntax Version

In any data definition, some or all of the fields can contain a wildcard ("*") to indicate that any values are a match for that field.

The channels in the system should be sequenced in the order that they should be checked. This is necessary because, by using wildcards (for the source or message type for example), some files will fit into more than one channel, but should only be processed by one of the channels. More general cases (such as any "all OFTP files") should be towards the bottom of the list, allowing more specific cases (such as "invoices received via OFTP") to be caught first.

As the Workflow Manager searches through the list of channels in the specified order, it tries to match the file to each channel. The file matches if all the data specified in the channel (anything that is not a wildcard) matches the data against the file.

Workflow Examples

The descriptions above provide all the factual information about the new ODEX concepts, but what you really need to know is how to use them in a real situation. Therefore we have described below two ways in which you might want to use ODEX – in a simple scenario and in a more complex scenario.

Simple scenario

A simple scenario is one in which your company might have only one trading partner, from whom you receive one or more EDI message types e.g. DELFOR and INVOIC. You want to automate ODEX so that incoming messages are recognised by their type, and then translated into a specified in-house format according to that type. You want each translated file to be placed in a holding directory according to its content (i.e. order or invoice), from where it can be picked up by another application and imported into your back office system.

Complex scenario

A complex scenario is one in which your company will have more than one trading partner, from whom you will receive a variety of files, both EDI and non-EDI. The EDI messages may conform to different standards (e.g. EDIFACT and VDA) but contain similar information (e.g. orders and invoices).

You want ODEX to recognise which trading partner has sent a file before processing it according to its type. You may want to take a copy of the file prior to its translation into a specified in-house format and then run an in-house application on the translated file before it is placed in a holding directory, from where it can be picked up by another application and imported into your back office system.

The ODEX solution

In both the scenarios described above, you need to be able to automate the system so that ODEX deals with your incoming files according to who they have come from and what their content is. Not only that – you probably also want ODEX to process the files in a variety of ways before the data gets to its final destination in your in-house systems.

The system allows you to define:

- a set of criteria which ODEX will use to compare with incoming files.
- Different processing jobs that ODEX will perform depending on where a file is from or what it contains or what type of file it is, or a combination of any of these criteria

When a match is found, ODEX will then process the file in the way you have pre-determined for a file of that type or from that trading partner.

As a first step, then, you need to decide exactly what you want ODEX to do with each file when it arrives in the system. If you want ODEX to handle files differently depending on their type or their origin, you need to understand the first two concepts we are going to discuss: Data Sources and Data Definitions.

Data Sources

There are three different ways in which files can get into the ODEX system:

- Comms – they can arrive via the communications system, in which case they will be placed initially in the ODEX Comms_In directory.
- Directory – they can be placed in a directory to be monitored by ODEX, in which case they will be taken from the monitored directory and placed initially in the ODEX Current directory
- Command – they can be imported "manually" via a command.

These three ways are called data sources. You can use any or all of these methods to get files into ODEX – it all depends on your own system restrictions and requirements.

Data Definitions

EDI files can be defined very precisely, by means of their message type, their senders and their encoding. These three elements make up the data definitions part of ODEX.

Data definitions allow you to specify criteria relating to EDI messages, file encoding and trading partners, which will be used by ODEX to determine what to do with specific file types in a particular encoding from specific trading partners.

ODEX will also handle non-EDI files, but these cannot be identified as being from a specific partner, unless they arrive via comms, nor can their content be determined.

To take an EDI example, you might receive the following types of file from these trading partners:

Ford – VDA orders encoded in EBCDIC

GM – EDIFACT D97A orders encoded in ASCII

Peugeot – EDIFACT D96A orders encoded in ASCII

If you want to ensure that files from each trading partner are processed differently e.g.

- Ford files are to be translated into ASCII before processing;
- a copy of each file is to be taken and stored in a directory specific to its sender;
- each GM and Peugeot file is to be translated into an in-house format;

then you should set up as many data definitions as required in order to distinguish all your files from each other.

Workflows

Once you have set up your data definitions and specified what data source(s) you will be using, you need to specify to ODEX how your files are to be processed. This is the purpose of the workflows.

A workflow, as its name suggests, tells ODEX exactly what tasks it is to perform, and in what order, on each file that arrives in the ODEX system.

You can create any number of different workflows, containing any number of different tasks. How many you create depends on how you want your system to work.

You can even process a single file using more than one workflow. This is achieved by using return codes, where applicable, to determine the course of action. One return code may result in the file continuing down the same workflow, while another return code may switch the file to be processed by a different workflow.

Besides the normal workflow tasks that you want to perform on a file, you will probably want to define a special error workflow whose task(s) will be performed if a file results in an error condition during normal processing. Error workflows can be created in the same way as a normal workflow, but should

only contain tasks that will not themselves result in an error condition. By checking return codes, where applicable, you can switch a file from a normal workflow to an error workflow.

Channels

Once you have set up your workflows, you need to allocate them to "channels". When a file arrives in ODEX, from one of the three data sources, ODEX has to work out what to do with it. It does this by checking the file against each of the channels you have defined, in turn, until it finds a channel whose criteria match that of the file.

To take our earlier example of the files from Ford, GM and Peugeot, you would probably want to have a channel set up for each of these trading partners.

To extend the example, if you were receiving two types of file from GM – DELFOR and DELJIT, say – you might want to set up two GM channels, one for each message type.

The main thing to remember is that, as soon as ODEX finds a channel which matches the file it has received, it will do no further matching and will use that channel to process the file.

If you have set everything up correctly, you will find that each file that arrives in the ODEX system, from whatever data source, will be matched with a specific channel. This channel will determine what tasks are to be performed on the file, and in what order they will be performed.

Summary

To summarise, you need to do the following:

Consider how many trading partners you have, and all the different file types that they send to you.

Decide how you want their files to be processed. These are just some of the questions to be considered:

- Can files of the same type from different trading partners be processed in the same way?
- Can files of different types from the same trading partner be processed in the same way?
- Do you need to translate incoming EDI files into an in-house format?
- Do you need to process any files using an in-house application?
- Do you want to take a copy of any files?

Define the data source(s) to be used.

Define the data definitions you will need to cover all your incoming files.

Set up one or more workflows that show, in the correct order, all the tasks you want to be performed on a particular type of file or on files from a particular trading partner.

Add one or more workflows to one or more channels. Your aim should be to have as many channels as necessary to ensure that every file arriving in your system will match one of the channels.

Schedules and Event Actions

ODEX allows you to automate any processing you want to carry out on your files.

One way to achieve this is to set up Channels so that ODEX will process the files as you have specified, as they arrive in the ODEX system.

Another way is to set up Schedules and Event Actions so that ODEX will take specific actions at specific times or when specific system events occur.

These two ways can be used in conjunction with each other or exclusively. It all depends on what you want your system to do.

Schedules are a way of setting up timings. For example, you can create a schedule that will trigger an event every day at 9.00 a.m.

Some schedules have already been set up for you.

- Daily (8am) – a schedule that occurs daily at 8am
- Daily (midday) – a schedule that occurs daily at midday
- Daily (midnight) – a schedule that occurs daily at midnight
- Hourly – a schedule that occurs every hour, on the hour
- Weekly – a schedule that occurs at midnight on Sunday morning every week

Event Actions are actions that can be triggered in one of two ways:

- When a schedule is met (i.e. when the time of a schedule occurs)
- When a system event occurs

System events are things that might happen during everyday use of ODEX. Currently the following system events are available to trigger event actions.

- Acknowledgement Received
- Acknowledgement Sent
- Call Ended
- Call Failed
- Call Retry Limit
- Call Started
- Connection Failed
- Database Sweep Completed
- File NAK received
- File Not Sent
- File Retry Limit
- General System Error
- Primary Connection Failed
- SAP Export Failed
- Server Started
- Server Starting

- Server Stopped
- Workflow File Hold
- Unexpected Receipt Received
- Unhandled Workflow Error

Whereas channel processing occurs when a file enters the ODEX system, event actions occur when triggered by a specific schedule or system event.

Schedules alone do nothing. They are only triggers for actions that you have set up. These actions will only occur if they are associated with a schedule or with a system event.

User Security

User security is a feature of ODEX which, if used as intended, guarantees the security of the system within your company. Although you do not have to enforce any security measures, it is advisable, at the very least, to prevent unauthorised users from gaining access to any part of ODEX.

User security serves two purposes:

- To stop unauthorised users from accessing the system
- To restrict authorised users' permissions within the system

User security is turned on or off at a global level (i.e. it affects all the applications). When turned on, it can be set to one of two modes:

- Use ODEX's own security
- Use Windows NT security

ODEX's own security

ODEX security is built into the system, but has to be selected explicitly if you want to use it.

For full security to be maintained, someone at your company must be designated to manage the security settings from within the ODEX Administrator. For this purpose, we have pre-configured a System Administrator for you. This user has been set up with full edit permission for the ODEX Administrator. You can view the System Administrator details in the same way as for any other user you set up yourself, but you cannot edit his settings, except to choose whether to use passwords for him.

Using ODEX security, when an application connects to the server the user will be asked for a username and password (though passwords may be blank if the Use passwords option has not been selected). The username and password are then validated to see if the user is authorised to log on.

Windows NT security

ODEX can also make use of Windows NT security instead of using its own internal security. This is particularly useful for people who are already running a Windows network and do not want to have to re-profile all users in another system.

Using Windows NT security, ODEX can import users and groups from the Windows Active Directory. Users will have to be logged on to Windows with a valid account in order to access any features of ODEX. Imported users can be

used in all the same ways as ODEX users to access other user-based functionality.

Even when using Windows NT security, a designated System Administrator must still be present in the ODEX security configuration. He will be able to log on to the ODEX Administrator and set user permissions for each Windows user group. He will also have full access to all the ODEX clients.

When somebody logs onto the server using a Windows NT account, ODEX checks the active directory to make sure that the user is a member of one of the groups that allows access to ODEX.

Users and User Groups

We have already briefly mentioned users and their permissions. In this section we will explain why it may be useful to allocate users to user groups and how their access to ODEX can be controlled.

ODEX is a multi-user application that enables various people within a company to handle various aspects of file processing within that company.

However, not everybody will want to see the same data. For example, the IT Manager, who needs to administer the ODEX system, will only need to see the Administrator application, whereas those people concerned with the actual sending and receipt of files will only be interested in the Workstation application.

ODEX already aims to satisfy this requirement using multiple user interfaces (the application programs). It may also be desirable, however, to restrict users in what they can and cannot modify or view. Or, to take it a step further, it could be necessary to completely prevent certain people from ever entering the system.

To achieve these restrictions, ODEX needs to force users to use usernames to gain access to the system. Once they have logged on, ODEX will know exactly who they are and will be able to restrict their permissions accordingly.

Many actions in ODEX only need to be performed by certain users. For example, only the System Administrator needs to be able to enter licence codes, view the log and change system settings.

This brings us to the concept of users and user groups. A user is a single person, and associated with that person will be a set of access rights that allows him to perform a certain set of actions and to view a certain set of ODEX screens.

At the simplest level this may just restrict particular users to logging onto particular applications. But at a more complicated level, it will be possible to restrict an individual's use of a particular application.

There are various categories of user who will want to interact with specific sections of the process and perform specific actions. There are many different people in an organisation, each with their own specific requirements of ODEX.

In a situation where many people will be using ODEX, it would be unrealistic to expect an administrator to set up exact permissions for each and every user of the system by setting permissions on an individual basis. Instead it is easier and friendlier to allow the administrator to assign users to one or more user groups and then override any specific permissions as necessary.

A user group is a set of permissions that can be assigned as a group to any number of users.

Users

Defining users in the system allows each person who uses ODEX to be identified. Anyone not recognised by ODEX security is denied access to the system.

In order to use ODEX User Security, at least one user must be profiled in the system. Each user has a unique username and, optionally, a password, which can be used to gain access to the system.

If Windows NT security is being used, then the user must be defined on the Windows Network.

We have defined two types of user:

- the basic user, who begins with no permissions at all and is granted a minimum of permissions
- the power user, who begins with no restrictions at all and may have some of his permissions removed

User Permissions

User permissions can be used for two purposes:

- for security, to restrict users to specific areas
- for simplicity, to show users only what they need to see

User permissions define the areas of ODEX to which the user may have access, and the functions that he can carry out within those areas. A user can be given one or more user permissions. A user permission might be, for example, being able to use the ODEX Administrator.

> *Please note that user permissions do not specifically state the functions that can be performed, but are a result of the access level that the user has been given. For example, if a user has been given View access to a specific view (page) of an application, he will be able to read the data, but will not be able to edit it.*

Every user can have their own set of permissions that dictate what they can or cannot do within the system. If the user attempts to do something that their permissions will not allow, a message box will appear on the screen to tell them that they have tried to perform an unauthorised operation and that they should contact their system administrator to extend their permissions.

There are basically two levels of user permissions – granting access to one or more specific applications, and granting access to specific areas within those applications.

User Groups

A user group is a convenient way to allow a number of users to share the same permissions. A user group has a set of permissions associated with it. Any users who are assigned to that group are automatically given those permissions.

You can define users without assigning them to a group. Then you would assign individual permissions to them.

Users can be assigned to any number of groups, and are automatically given the permissions from all the groups they have been assigned to.

Once a user is assigned to a group, he enjoys all that group's privileges. You cannot override his privileges by removing from him some of the permissions of that group. If you want him to have fewer permissions, he should be removed from that group and added to a different group.

If Windows NT Security is being used, then the user groups defined in Windows NT will be used. ODEX allows users to assign a set of ODEX permissions to a Windows NT user group. In this scenario, the relationship between users and user groups has to be managed from within the Windows environment, not from within ODEX.

We have defined two types of user group:

- the basic user group, which begins with no permissions at all and is granted a minimum of permissions
- the power user group, which begins with full permissions and may have some of its permissions removed

Communities

A community is a way to restrict the data that users and groups can view in the ODEX applications. A user or group can be a member of one or more communities.

In the administrator client, when a user logs on who is a member of one or more communities, that user can then only view networks and trading partners that are associated with the communities that they are members of.

In the workstation client, when a user logs on who is a member of one or more communities, they will only see files that are associated with networks that they have permission to view.

In the communications monitor client, only sessions between networks that the user has permission to view are visible in the session list.

The Role of the System Administrator

As already mentioned, for full security to be maintained, at least one authorised user (the System Administrator) must be designated to manage ODEX's security settings from within the ODEX Administrator. It is a good idea to designate more than one person to do this job, as you do not want to be in a position where the only person who can control security is on holiday or has forgotten the System Administrator password!.

ODEX comes already set up with one administrator user. His username is “Admin” and his password, to begin with, is blank. (Of course, if you do not want to use ODEX security, the group and user will not be activated). The administrator user has full access to all views in the ODEX Administrator and his level of permission cannot be changed. You may only change his password. If you do try to change the System Administrator's settings, you will see a message box telling you that this is a system user and cannot be changed.

The role of the System Administrator is to ensure that security is maintained in the ODEX system. He must decide, at the very least, which people are to be allowed access to ODEX. He can also decide whether to restrict these individuals' access to certain parts of ODEX.

Having designated people as users and, optionally, allocated them to user groups with specific permissions, the System Administrator must inform each

user of their username and, optionally, password, so that they can access the system.

Another important aspect of the System Administrator is that he can reset passwords.

Passwords

Although you may allocate a password to each user, it is quite acceptable to forego the use of passwords. This means that users can take advantage of the restricted views enforced by users and user groups, without enforcing strict security.

Users can change their own passwords from any client machine to which they have access. A System Administrator can change any user's password at any time (useful if a user has forgotten their password). However, a System Administrator cannot view other people's passwords – he simply resets them to a fixed value, such as "password", which the user should then change after logging back onto ODEX.

> ***Important**: If the System Administrator forgets the administrator password he could potentially be locked out of the system completely. If this happens, users should contact the Data Interchange Plc Support department which has an application that can reset the administrator password in the database. However, checks will first be made to ensure that an attempt is not being made to breach security. One more reason to designate more than one System Administrator!*

Shared Machines and User Settings

There is one area in which User Security can easily be compromised, and that is when people share computers. Of course, if the people sharing the computer are all ODEX users and members of the same user group with the same permissions, there is no problem – they can all use the same machine without any breach of security.

However, if the machine is shared with people who have different permissions or who are not even ODEX users, then it is of paramount importance that each ODEX user logs off or closes each client application after he has finished using it, to prevent unauthorised access.

When the machine is shared by other ODEX users, inconvenience is kept to a minimum because ODEX makes sure that each user is presented with his own personalised GUI. Client applications store local settings (such as column widths, filters and default views) on a per-user basis so that, if more than one user is using the same application on the same machine, they can each tailor the ODEX environment to suit their particular needs.

Enforcing User Security

To turn on user security, first select the System page tab of the ODEX Administrator. Then highlight the System Settings node within the tree view of the Navigation panel and select the Security page. For full details of how to set up the different types of user security, please refer to the Help section entitled "Security page".

For details of how to set up and edit users and user groups within ODEX, please refer to the sections entitled "Users" and "User Groups".

AS2

This section is an introduction to AS2. It aims to answer your questions about AS2 and its use within ODEX.

What is AS2?

AS2 is a draft specification developed by the Internet Engineering Task Force (IETF) for the secure exchange of business documents and business-to-business (B2B) transactions over the Internet.

AS2 uses HTTP (hypertext transmission protocol) as its transport protocol. AS2 utilises HTTP and MIME (Multipurpose Internet Mail Extensions) to provide a secure solution for the exchange of data over the Internet.

AS2 can be used to exchange almost any type of data, not just EDI.

AS2 in effect provides an envelope for your data, allowing transactions to be sent and received securely and directly over the Internet instead of via the more traditional VAN.

AS2 is not concerned with the content of the data you send. It is concerned only with the means to connect, deliver, validate and return receipts for the data securely and reliably.

AS2 is now widely used in the retail industry.

What are the advantages of AS2?

AS2 provides the means to transfer data directly to your network in a way that is fast, practically instantaneous and always available.

Using AS2 can save money in network costs (no VAN fees or long-distance dial-up costs to pay) and increased flexibility and control over the data.

Advantages of using AS2 include:

- 24 x 7 availability
- fast and reliable connectivity
- security features
- faster turnaround time for business processes, giving improved supply-chain efficiency
- non-repudiation of receipt. This means that the intended receiver is proved to have received the data.

What do I need in order to use AS2?

There is only one requirement for exchanging data using AS2:

- A dedicated Internet connection with 24 x 7 availability.

You would normally also need a web server, but using ODEX as your AS2 software means that you do not need a separate web server, since ODEX performs all the functionality of a web server that is required by AS2.

Do I have to use AS2?

You only have to use AS2 with those of your trading partners who require you to use it.

How do I set up AS2 in ODEX?

To use AS2 with your trading partners you need to set up an Internal AS2 Network, an HTTP Subsystem and an External AS2 Network for each of your AS2 trading partners and clearing centres. For details of how to do this, please refer to the following sections:

Adding/Editing an Internal AS2 Network

Adding/Editing an HTTP subsystem

Adding/Editing Networks

What is involved in an AS2 data transmission?

The following steps are usually involved in AS2 transmissions, whether they are sent by you to your trading partners or by your trading partners to you.

- Data repository – data to be sent is placed somewhere ready to be picked up
- Encryption – the data is picked up and encrypted
- Signing – after encryption, a digital signature is generated and attached to the transmission
- Transmission – the data is transmitted from one trading partner to another using HTTP or HTTPS
- Signature Verification – on receipt, the signature attached to the transmission is verified to ensure it was sent from an accepted sender and the integrity of the data is checked to ensure there have been no alterations since it left the sender
- Decryption – the data is decrypted by the recipient
- File storage – the decrypted file is delivered to the recipient's system for processing
- Return of MDN – a Message Disposition Notification (MDN) is generated and returned to the sender to acknowledge successful receipt of the data by the receiver (if the MDN is signed, this provides non-repudiation of receipt)
- Verification of MDN signature – the data sender verifies the MDN signature to ensure that the data was received by the expected recipient

What are the security features of AS2?

AS2 makes use of several optional security features

- Data Encryption
- Digital signatures
- Transmission encryption (HTTPS)

Data encryption and signatures ensure that:

- Only the intended receiver can view the data
- The document is authenticated with digital signatures
- The document has not been altered during transmission

You can send encrypted data via HTTP and be confident that it will arrive at its intended destination without being intercepted or altered. However, for added security you can use HTTPS, which simply provides an extra level of security for the means of communication.

What is XOT?

Overview

XOT is an abbreviation for X.25 Over TCP. This allows X.25 packets to be sent over a Transmission Control Protocol/Internet Protocol (TCP/IP) network instead of an X.25 network.

In essence, XOT tunnels X.25 traffic through an IP “cloud”. This allows ODEX to make a native X.25 call to a remote trading partner, without the need for X.25 hardware within the PC. Instead, ODEX communicates with an XOT-capable router using XOT over a TCP/IP network, and the router then makes the actual X.25 connection.

This ability to utilise an IP connection to an XOT router provides a cost reduction and also allows for the possibility of using an existing IP network to access an XOT router located at a remote site.

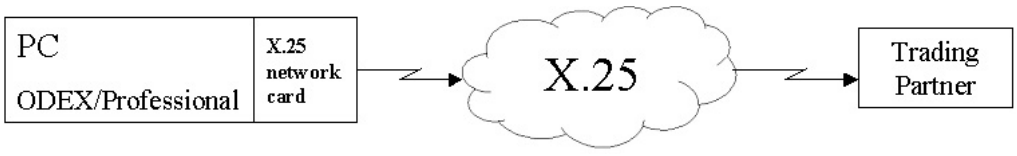
X.25 is based on packet-switching technologies. Packet-switching technologies are protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message.

X.25 defines layers 1, 2, and 3 in the OSI Reference Model. OSI is an ISO standard for worldwide communications that defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

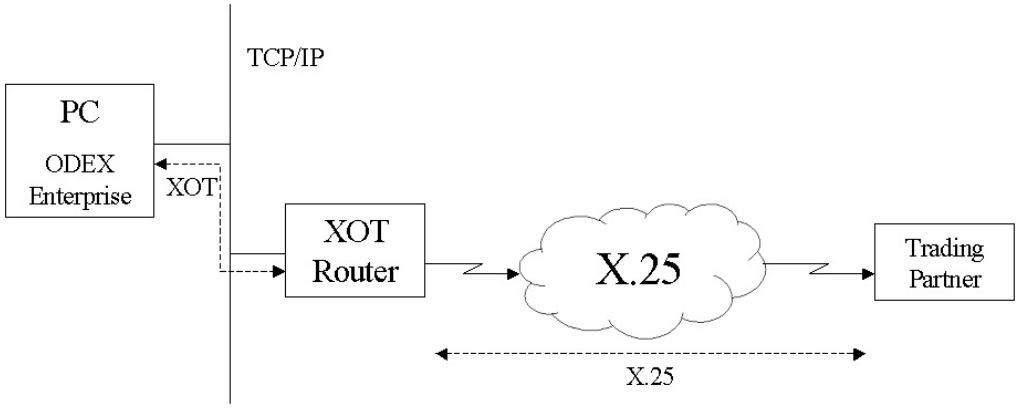
In the Connections section of the external Networks area of the ODEX Administrator, you will see references to Window size and Packet size, which are handled by Level 3 (the X.25 layer) of the OSI 7-layer model.

Using XOT and X.25 in ODEX

ODEX/Professional (the forerunner of ODEX Enterprise) allowed you to communicate with your trading partners using X.25. If you are currently using ODEX/Professional or another product to communicate with your trading partners using X.25, this diagram shows the way your system is probably configured.



In ODEX Enterprise, you can still communicate with your X.25 connected trading partners by using an external XOT router such as a CISCO, but now the system setup will look more like this.



Configuring XOT in ODEX

To use XOT with your trading partners you need to set up an XOT Subsystem and an External Network utilising an XOT connection for each of your trading partners and clearing centres.

In the Subsystem configuration you will provide:

- the TCP/IP address of the router that will be used to make the X.25 call
- the local IP address of the PC on which ODEX is running and which is configured in the router for X.25 calls that should be passed to ODEX

In the External XOT Network configuration for each trading partner using X.25, you must select the XOT subsystem and provide the X.25 Network User Address (NUA) of your trading partner.

XOT Logging

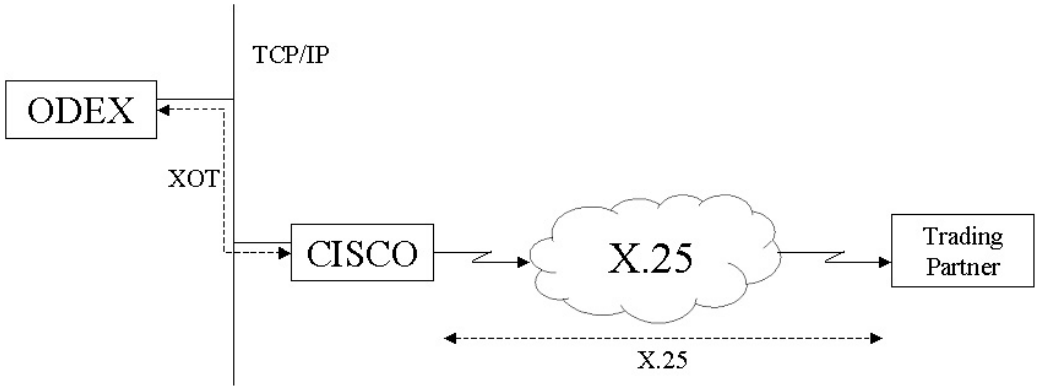
In order to view all of the X.25 packets that are being transmitted and received by ODEX, you should select the 'Buffer' option against the XOT protocol on the Communications Settings node (accessed from the Comms tab in the Administrator). To view the actual hex contents of the XOT buffers, select 'Buffer' against the TCP protocol there too.

Using an XOT interface with the CISCO Router

These sample configurations assume that the Cisco router is configured correctly for TCP/IP and is part of the same network as the ODEX machine. Further details of each command and sample configurations can be found on the Cisco Web site (www.cisco.com).

To perform any routing of X.25 calls, the following command must be entered in the Cisco configuration: **x25 routing**

To Access an X.25 network using XOT



The Cisco interface which is connected to the X.25 network needs to be configured with the correct number of Virtual Circuits (which will be dependent upon your X.25 line)

```
interface Serial1/0
 description Link to X.25 PSS
 no ip address
 encapsulation x25
 x25 ltc 1024
 x25 htc 1063
```

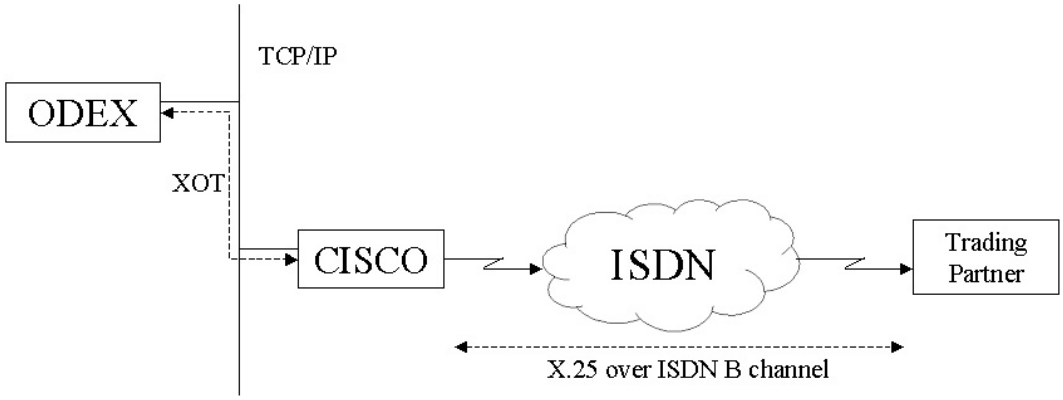
An X25 route then needs to be added to ensure that calls to the trading partner's NUA are routed to the external X.25 network. This allows different trading partners to be accessed via different external interfaces. Additional entries can be added routing different NUAs to the same interface.

```
x25 route 1234 interface Serial1/0
```

Incoming calls then need to be routed to an ODEX machine via TCP/IP

```
x25 route 4321 xot 62.189.141.75
```

To Access an ISDN trading partner using XOT



The Cisco interface which is connected an ISDN line needs to be configured with a reference to a dialer pool

```
interface BRI0/0
 description ISDN Interface
 dialer pool-member 1
 isdn switch-type basic-net3
```

A dialer Interface needs to be configured which then gives the Cisco an ISDN number to dial when calls are routed via ISDN

```
interface Dialer0
 no ip address
 encapsulation x25
 dialer pool 1          (must match the entry configured against the ISDN interface)
 dialer remote-name dinet
 dialer string 01733390025    (the ISDN number to be dialled)
 dialer max-call 1
 dialer-group 1
 x25 address 1234
 x25 htc 1
```

```
x25 win 7
x25 wout 7
x25 facility windowsize 7 7
x25 facility packetsize 128 128
```

A route can then be added to map an X.25 NUA to the dialler interface

```
x25 route 1234 interface Dialer0
```

FTP (File Transfer Protocol)

This section aims to introduce FTP and then explain how it is implemented into ODEX and how it can be setup.

What is FTP?

A program like Windows Explorer allows you to copy files between folders on your computer but not between you and your trading partners computers. TCP/IP over the Internet or an intranet allows you to connect your computer with your trading partners computers. File Transfer Protocol (FTP) uses TCP/IP to provide a means for you to copy files between folders on your own computer or on your trading partner's computers.

FTP is a protocol that involves two systems, one that requests a file transfer (the *client*) and one that approves the request and does the sending or receiving (the *server*). An FTP server runs continuously in the background and waits for a connection request from an FTP client. When an FTP client requests a connection, the FTP server verifies the logon user ID and password and, if valid, waits for the next request. After a user has logged on, his access to the FTP host's file system is determined by permissions assigned to files and folders. The user sends commands to the server to cause the exchange of files and finally logs off.

What are the advantages of FTP?

These are just some of the advantages of using FTP.

- FTP is a very common protocol that is used over many platforms.
- FTP has been around for a long time.
- It is a relatively simple protocol that is easy to use (It is supported by clients through most web browsers, explorer in Windows and through the 'ftp' command in most Linux, Unix and MSDOS distributions).
- A directory structure can be represented, allowing the organisation of files.
- Security is implemented through username and passwords.
- The client can choose which files they wish to download.

What are the disadvantages of FTP?

There are a few disadvantages, some of which are detailed below.

- Standard FTP is not encrypted or highly secure.
- Since clients choose which files they take, a server cannot ensure the other party takes all the files.
- It can be difficult to detect and ensure that files have been received correctly. However some safeguards have been built into the ODEX implementation to minimise this disadvantage.

What are the requirements of FTP?

The client requires only a connection to the FTP server machine, so if the server is on a LAN, the client must be able to establish a connection to that computer on the LAN and if the server is on the Internet then the client must be connected when the client tries to make an outgoing call.

The server cannot make outgoing calls, so it must be switched on and connected to a network at the time when a client wishes to connect. This could involve having the server and server machine switched on and connected 24/7, depending on arrangements with the trading partner using an FTP client.

In addition the server requires an open port, usually 21 and if passive mode (see the Advanced FTP section) is enabled then an additional range of ports must be open for the data connection.

Advanced FTP explanation

This section explains some more of the workings of FTP needed to use the advanced settings for FTP in ODEX.

When an FTP connection is established, it does so on the control connection. The client can then send commands over this control connection, the first of which has to be a username command, followed by a password command. This logs the client in and allows the client to send more advanced commands that get directory listings, send files and receive files. To get directory listings and transfer files, an additional connection is needed, known as the data connection. There are two ways in which this data connection can be established, first the client can send a 'PORT' command which instructs the server to connect at a specified IP address and port on the client machine. This mode requires the client to have ports on their computer open to the network.

Instead of this, the client can opt for Passive mode, where the server gives the client an IP address and port and then the client must establish the connection with an open port on the server. Passive mode is common as it leaves the client closed with no need to have any ports open for incoming connections.

There are three modes of file transfer, stream, block and compressed although it is quite common to only support stream transfer. This is when the data connection is closed to indicate the end of file. Since this can be unreliable, ODEX has implemented some methods to acknowledge a file as successfully sent or received and these will be explained in the following sections.

Using FTP in ODEX

ODEX can function as both a client and a server. With each trading partner, you configure whether ODEX will be a client, a server or both. If you wish to call out to a trading partner, you configure ODEX as a client. If your trading partner calls in to you, configure ODEX as a server. Configure ODEX as a client and a server if calls are to be made both ways. In both situations files can be exchanged both ways.

At the heart of FTP are the commands "retrieve" and "store" (commonly worded as "get and "put" in command line ftp clients). A client issues "retrieve" to request files from the FTP server to which the connection is made and download them to a folder on the local machine. "Store" sends files from a local folder and writes them in to a specified folder on the FTP server. The ODEX implementation of FTP isolates you from the need to issue these commands; instead you specify a mask of files to get/put and the directories that these files are in.

Unlike OFTP where a single trading partner network is created that allows incoming or outgoing calls, FTP in ODEX has been divided up into two distinct areas, an automated FTP client and an FTP server. Each will now be looked at separately.

FTP client

In ODEX, a user must create an FTP client trading partner network to define an FTP server that exists externally, perhaps on a trading partners network or an internal LAN. So an FTP client trading partner network has the IP Address, port to connect to, username and password required to log in. Mailboxes for this network then define directories from which files are to be retrieved and directories in which to put files.

Typically a file mask is given so that ODEX will retrieve all files with a similar name. ODEX places the files it gets in your inbox, from where they can be processed by a workflow. By default “get” copies, not moves files from the server, meaning files could remain on the server if you don’t ask ODEX to delete them. Most conventional FTP servers, which mirror part of a file system, will not remove files that have been retrieved, however some servers (such as ODEX) can be configured to delete files once they have been successfully transferred. If they are not removed, you will retrieve the same files every time the client connects to the server.

To put files onto an FTP server, you must tell ODEX the folder on your trading partner’s computer that the files are to be placed in and the filename the client is to give it. When you schedule a file to be sent, ODEX takes a copy of your data and queues it to your trading partner. When a communications call is established, the file is sent and FTP writes it on to your trading partner’s disk in the folder you specified and with the name you specified. Typically a mask is given for file names so that unique names are used for each file written and they don’t destroy the contents of previously sent files (putting “file” on to a standard FTP server and then putting “file” again will most likely overwrite the original).

FTP server

An FTP server has to be listening at any time for a connection from a client. This part of the FTP server is defined by an FTP server subsystem. When you create this subsystem you can specify the port and the local IP address you will listen on. Additionally you specify options not relevant on a user-by-user basis such as an initial welcome message (for instance to tell people to use the username and password given to them by email or otherwise), whether passive mode is supported and the port range that is open.

Additionally a trading partner network defines a user that can log on to the FTP server. This user can be sent files and give files to ODEX. It is a trading partner network because it defines a single connection to another party that can be used for receiving and sending files. Each FTP server network has a single hidden mailbox in order that it can integrate with ODEX and have a node to send files to, however additional mailboxes cannot be created, as they would serve no purpose.

The ODEX FTP server does not reflect any directories or files that are present on your hard-drive. Instead it creates a virtual directory tree presented to FTP clients that has clearly named folders, each with a specific use and purpose. When an FTP client logs in, they are initially at the root level in the virtual file system (“\”). From here there are potentially five folders.

- ‘Confirmed’ – When the mode of working is set to rename, the client must rename a file to this directory to acknowledge it as correctly stored on the server.

- ‘In’ – This is the normal incoming directory for the server. Files to be given to the FTP server from the client are stored into this directory initially. If the mode is rename then they may later be moved to the Confirmed directory.
- ‘InArchive’ – This is an archive of all files which have been received from previous sessions with an FTP client using the same network configuration (e.g. having the same username and password).
- ‘Out’ – All files that have been sent to the external network with the username and password the FTP client logged in as will appear in this directory.
- ‘OutArchive’ – This is an archive of all files that have been sent to the external network for which the FTP client is logged in to.

When a file is given to the server by uploading to the correct directory, that file will be given to the workflow manager and handled by ODEX. When a file is scheduled to a particular trading partner network, it appears in their ‘Out’ directory until they have retrieved (and possibly deleted) it.

FTP placeholders

A new placeholder created for files coming from an FTP source is the remote filename. This is the name of the file as it is on a server and retrieved by the ODEX FTP client or the name of the file that a client put on to the ODEX FTP server. This placeholder can be used throughout ODEX in the same way as other placeholders for all files coming from an ODEX FTP source.

The filename of a file scheduled to FTP is defined in the network for a server and in the mailbox for a client. Under the client, we have Filename under put options and the server has Filename shown under directory options. The two predefined placeholders for a Filename are original filename with extension (“%OFN_W_E%”) and system filename with extension (“%C_SFN_W_E%”).

The original filename will be the name of the file if it came from a directory source, the VFN (Virtual File Name) if it came from OFTP and the RFN (Remote file name) if it came from FTP. Files from a different source, such as AS2 will replace this placeholder with nothing, so some thought must be put into the source of files before the filename is decided.

The system filename is the ODEX generated name of its file on disk and will be unique for every file. Please note the additional C_ on the system filename is to denote that it is the Comms file system filename, which could differ from the normal system filename that comes from a workflow. Only Comms file placeholders may be used to define a filename. More information on placeholders can be found in the placeholder’s section of this manual.

Additional FTP acknowledgments

Both the FTP server and client support options to let the client acknowledge and confirm a successful get or put of a file. When the client is retrieving files, it can be set up to delete a file from the server once it has been successfully copied to the client’s machine. For the ODEX FTP client this is supported through a check box defining whether the user wishes retrieved files to be deleted.

The server supports this acknowledgment through its “Client File Transfer Options”. For files sent, they can be “deleted by client” or they can be “deleted by ODEX”. When deleted by the client, the client must delete the file before ODEX marks that file as sent by the server. When deleted by ODEX, when the

file has been sent once, the file is automatically deleted and only obtainable again by using the “OutArchive” directory.

Consider the case where your trading partner is monitoring a folder for the arrival of new files and you start to send a large file to him that takes a long time to transmit. He sees the file start to come over but cannot be sure when it is complete. If FTP renames it when it is complete, he knows that he need only look for files with the ‘renamed’ name and that any that are found have completed transmission.

So for files the client is storing on the server, the client can rename the file to signal that the file has been successfully uploaded to the FTP server. For the ODEX FTP client this is achieved through a rename mask to allow uploaded files to be renamed after uploading.

The ODEX FTP server also supports renaming to confirm files, however it insists that a file is renamed in to the Confirmed directory. A rename command in FTP can be used move a file from one folder to another. In this mode of working, known as “uploaded to In directory and moved to Confirmed”, ODEX does not mark a file as received until it has been moved in to the “Confirmed” directory.

For example to setup the system for an ODEX FTP client to connect to the ODEX FTP server, a user would take the following steps:

- Set the server mode of working to “uploaded to In directory and moved to Confirmed”.
- Set the client remote path to “\In”.
- Set the rename mask to “\Confirmed\%OFN_W_E%” (although any place holders could be used).

FTP with specific trading partners

Honda

Honda do not allow the deletion of files from their FTP server, so ODEX now has a “get new files only” which looks at the date/time of files and decides whether it is a new file, or whether it is older than the last file downloaded. This option should be enabled.

GXS & CAT

These trading partners use the Enterprise FTP server. This server does not go against a file system but works by interpreting FTP as an interface to an EDI mailbox system. Information on naming conventions is given below.

The mailbox directory listing showing files to be picked up has a status flag indicating whether a file has been extracted or not. This flag is used if the get new files only option is selected. Otherwise you can delete the files after retrieving them in the same way as a standard FTP server.

FTP client folder and file naming conventions

Folder and file naming conventions differ between operating systems and hardware platforms. You may need to be aware of these differences to be able to tell ODEX about your trading partner when you use the Administrator to configure them.

Windows platforms

Under Windows a typical file name might be for example "C:\DIP\Xlate200\Delins2.edf". Here "Delins2.edf" is the file name, the rest is the file path. In "Delins2.edf", "edf" is called the file extension and typically describes the contents of the file.

To get this file from a Windows machine you would specify the following in the Administrator –

Files : Use custom mask

Custom mask : Delins2.edf

Remote path : \DIP\Xlate200\

To get all files with extension "edf", specify –

Files : Use custom mask

Custom mask : *.edf

Remote path : \DIP\Xlate200\

To put a file and have it keep its original file name, specify –

File name : Original filename

Remote path : \DIP\Xlate200\

So if the Workstation were used to Schedule a file named "C:\MyFolder\MyFile.ext" it would be written at your trading partner as "\DIP\Xlate200\MyFile.ext".

To send a file and ensure it is written with a unique name, specify –

File name : System filename

Remote path : \DIP\Xlate200\

"C:\MyFolder\MyFile.ext" would be written at your trading partner as "\DIP\Xlate200\nnnnnnnn.CMS" where "nnnnnnnn" is an eight digit number incremented for each file written.

To use the "rename" feature to indicate that a file has been transmitted completely and is eligible for processing, specify –

File name : System filename

Remote path : \DIP\Xlate200\

Advanced put options – Custom mask : NEWNAME%C_SFN_W_E%

"C:\MyFolder\MyFile.ext" would initially be written at your trading partner as "\DIP\Xlate200\nnnnnnnn.CMS" and when transmission was complete would be renamed as "\DIP\Xlate200\NEWNAMEnnnnnnnn.CMS"

UNIX Platforms

On a UNIX platform the example file might be called "/usr/DIP/Xlate200/Delins2.edf" which, apart from the name delimiters, is a very similar format to Windows. UNIX platforms are configured like Windows above.

AS/400

On an AS/400 the example file might be called "XLATE200/TABLES(DELINS2E)". Here "XLATE200" is the name of a library, "TABLES" the name of a file and "DELINS2E a member name.

To get this file from an AS/400 you would specify the following in the Administrator –

Files : Use custom mask

Custom mask : TABLES.DELINS2E

Remote path : XLATE200

To get all the "DELINS" members of the file "TABLES", specify –

Files : Use custom mask

Custom mask : TABLES.DELINS*

Remote path : XLATE200

To send a file and have it keep its original file name, specify –

File name : Original filename

Remote path : XLATE200

So if the Workstation were used to Schedule a file named "C:\MyFolder\MyFile.ext" it would be written at your trading partner as "XLATE200/MyFile(ext)".

To use the "rename" feature to indicate that a file has been transmitted completely and is eligible for processing, specify –

File name : Original filename

Remote path : XLATE200

Advanced put options – Custom mask : NEW%OFN_W_E%

"C:\MyFolder\MyFile.ext" would initially be written at your trading partner as "XLATE200/MyFile(ext)" and when transmission was complete would be renamed as "XLATE200/NEWMyFile(ext)"

To send a file and ensure it is written with a unique name, specify –

File name : System filename

Remote path : XLATE200

"C:\MyFolder\MyFile.ext" would be written at your trading partner as "XLATE200/#nnnnnnn(CMS)" where "nnnnnnn" is a seven digit number incremented for each file written.

AS/400 Naming Format

Additionally, it is possible to access files on the AS400 which have a different naming structure. To do this, insert the name format command into the user startup commands section against the ftp client external network on the advanced tab. Typically this command may be "site namefmt 1".

After this is put in, non-library files may be accessed and paths such as "/home" may be accessed. This can be configured in the same way as a UNIX server.

Enterprise FTP Server

Enterprise is an ftp server used by some companies that does not have a typical directory structure and instead uses the FTP commands to get information about an EDI mailbox.

The paths should be left blank or specify a trading partner relationship as specified by your trading partner. If you are using EDI files then the filename does not matter. If you are using non-edi files then either the filename should be formatted as instructed by your trading partner or an EDI line should be inserted at the beginning of the file.

IBM Mainframe

On an IBM mainframe the example file might be called "DIP.XLATE200.TABLES(DELINS2)". Here "DIP.XLATE200.TABLES" is the name of a partitioned dataset and "DELINS2" the name of a member.

To get this file from a mainframe you would specify the following in the Administrator –

Files : Use custom mask

Custom mask : DELINS2

Remote path : DIP.XLATE200.TABLES

To get all the "DELINS" members of the PDS "TABLES", specify –

Files : Use custom mask

Custom mask : DELINS*

Remote path : DIP.XLATE200.TABLES

To send a file and have it keep its original file name, specify –

File name : Original filename

Remote path : DIP.XLATE200.TABLES

So if the Workstation were used to Schedule a file named "C:\MyFolder\MyFile" it would be written at your trading partner as "DIP.XLATE200.TABLES (MyFile)".

To use the “rename” feature to indicate that a file has been transmitted completely and is eligible for processing, specify –

File name : Original filename

Remote path : DIP.XLATE200.TABLES

Advanced put options – Custom mask : N%OFN_W_E%

“C:\MyFolder\MyFile” would initially be written at your trading partner as “DIP.XLATE200.TABLES (MyFile)” and when transmission was complete would be renamed as “DIP.XLATE200.TABLES (NMyFile)”

Data Security

ODEX is designed to keep your data safe and trusted when communicating with trading partners by utilising multiple layers of data security. This is achieved through methods of authentication and data transformations based upon the principle of asymmetric keys.

The principle of asymmetric keys follows that there are unique key pairs containing two related keys, public and private, which are coupled in such a way that a transformation performed with one key can only be reversed by using the related key. Which key is used for each direction depends upon the transformation involved, following the rule that the private key is used for the direction that is considered private to your organisation whilst the public key is used for the direction that is considered public and open to all.

As an example, consider a simple encryption scenario. You do not mind who encrypts your data but you really would rather it be only yourself who can decrypt it. This way, anybody can encrypt data into a scrambled form and send it across a public domain with the guarantee that only you can transform that data back into its usable form. The public key is used in the public domain to encrypt the data whilst the private key is used in your internal domain to decrypt the data.

Asymmetric key pairs are associated with a special entity called a certificate. These certificates contain the public key and associate it with additional data that describe the owner of the key and guidelines to its use. This association can be used to guarantee the logical identity of the holder of the asymmetric key pair and is thoroughly exploited in ODEX to ensure the security of your data.

Certificates

To exploit the possibilities of asymmetric key pairs you need to be dealing in the exchange and management of certificates. If you are utilising secure communications in ODEX, which are based upon the principle of asymmetric keys, then you will need some familiarity with certificates.

Your own certificate contains your public key, which you distribute into the public domain, and an attached private key, which must only be used internally for private data transformations and authentication. You also need access to your trading partners’ public key certificates.

In most cases, you will have to obtain your own certificate from a Trusted Certification Authority.

In simplified terms, the system works like this. The Certification Authority issues you with a certificate that encapsulates your public key, your private key, and some extra information, such as the name of the issuing authority and the

certificate's date of expiry. The certificate issuer signs your certificate, using their private key. This means that when you use your private key to sign data, the certificate you use is traceable, if necessary, back to the issuer. This allows your trading partners to decide whether the certificate you are using is trusted.

When you receive your private certificate from the Certificate Authority and public certificates from your trading partners, you should import them into a secure local certificate store.

ODEX offers you a further possibility for obtaining your own private certificate: creating it locally and signing it using your private key. Such certificates are called self-signed certificates and their use should be discouraged due to no automatic guarantee of their identity.

ODEX Certificate Store

ODEX has its own local certificate store that operates in co-operation with the Windows certificate stores.

You can view the ODEX certificate store from two angles: a global view of all certificates ('Certificates' node in the 'System' administrator) and a view of the certificates associated with individual internal companies or trading partners ('Certificates' tab against a company). Both views are functionally identical.

There are four ways to add certificates into the ODEX store:

- Import from a file containing the certificate data
- Import from a certificate that is already in the Windows certificate stores
- Create a self-signed certificate directly in ODEX
- Register the identification data of a certificate you expect to receive from a trading partner through certificate exchange

If you choose to 'Edit' an existing certificate, you are presented with a dialog to view the details of the certificate and manage its considered state. It is important to understand a few principles regarding certificates in the ODEX store for successful management.

The status of a certificate is determined by the triplet:

- Life state – Is the certificate currently live? I.e. can be used for security purposes; is it new and therefore not yet entered its living period? Has it now expired from its living period? Or is the certificate expected to be received through certificate exchange? It is important to realise that only one certificate in a chain of renewals can ever be live at one point, and ODEX will strive to uphold this rule.
- Validity state – Is the certificate regarded as valid? If it is invalid, this may be acceptable if the certificate has expired, otherwise you would expect to find a warning indicating the reason why the certificate is invalid. We also check whether the issuer of the certificate is trusted by Odette.
- Accepted state – Have you accepted this certificate into the ODEX store? If the certificate is not accepted, it exists in the store but is not usable.

Whenever there is a problem with a certificate, you will find a warning has been issued and a system event has been thrown.

Certificate Policy

ODEX automatically manages the certificates contained within its certificate store. All of this automatic management can be controlled by setting certificate policy.

- Certificate Validation – use to control when ODEX will perform validation of the certificates in the store
- Certificate Acceptance – use to control how ODEX will automatically accept certificates that have been received from trading partners through certificate exchange
- Certificate Exchange – use to control whether ODEX will use certificate exchange to update trading partners' certificates and distribute your certificates to trading partners
- Automatic Management – use to control whether ODEX will automatically determine which certificate in a renewal chain should be currently marked as live.

Certificate policy can be managed at a global level and overridden against internal companies and trading partners.

OFTP2 Certificate Exchange

OFTP2 provides the capability to exchange certificates between trading partners using special files. This procedure is called Certificate Exchange.

You begin this procedure by importing your own private certificates in the usual way into the ODEX certificate store. Set the certificate against the appropriate network or mailbox for signing and/or decryption. Normally you would set it as the signing certificate for your internal network, and then its use as a decryption certificate is implied.

You need to exchange identification information about the certificate to your trading partner using manual methods such as a telephone call or email. It is up to you to ensure that this exchange of information is secure. You can view all the information you need by opening the 'Manage Certificate' dialog for your certificate from one of the certificate views. Normally, you should exchange the following information:

- Serial number OR Subject and Issuer OR Domain name OR IP Address
- Key usage
- What the trading partner should use your certificate for

If the certificate you are exchanging is self-signed, you will also need to exchange the MD5 sum.

Trusted-service Status List

As an additional security check of CA-signed certificates, Odette make available Trusted-service Status Lists that list those CAs that are deemed trusted for issuing certificates.

If configured to do so, ODEX will automatically download TSL files from Odette into ODEX. A TSL is validated before being imported, at which point it is loaded into memory for use in CA validation. The TSL contains the certificates of all the authorities it lists along with the trusted state of those certificates. If configured

to do so, ODEX will import all the CA certificates into its store and set their state according to the TSL.

All certificates in the ODEX store are validated against the latest TSL to determine their valid state. If they are CA-signed, and that CA is trusted in the TSL, then the certificate will be marked as fully valid. You can also enforce that certificates you receive through certificate exchange have been issued by a trusted CA in order to qualify for automatic acceptance.

From the 'OFTP2 Certificates' node in the Administrator, you can view the content of all the downloaded TSLs.

Authentication and data transformations

Ultimately, you use certificates and the keys they contain to authorise yourself to trading partners and transform the data you exchange. There are many instances of such scenarios in ODEX to ensure secure communications:

- OFTP2 file encryption
- OFTP2 file signing
- OFTP2 acknowledgement signing
- OFTP2 session authentication
- OFTP2 over SSL
- AS2 encryption
- AS2 signing
- AS2 MDN signing
- AS2 over SSL
- EDIFACT signing and verification

Encryption

Encryption is the process whereby data is made unusable to all except someone who possesses the appropriate key to decipher it.

Decryption is the process of deciphering encrypted data.

The public key of a trading partner is used encrypt data that is being sent to them, who decrypt the data using their private key.

Digital Signatures

Digital signatures are used to add a further level of security. Signatures provide proof that received data has genuinely come from an accepted sender. They also provide proof that the data has not been modified (maliciously or otherwise) during the transfer.

Your private key is used to sign data that is being sent to any trading partner, who use your public key to verify the signature, and thus confirm that data originated from your systems.

WebSphereMQ

This section introduces WebSphereMQ, it aims to answer any questions about WebSphereMQ and how WebSphereMQ can be used within ODEX.

What is WebSphereMQ?

Odex can integrate with MQ messaging servers and is able to both send and receive messages using either actions or jobs upon a workflow.

WebSphereMQ (formerly MQ series) is a consistent mechanism to allow for the exchange of messages between applications running upon differing platforms.

WebSphereMQ is based on the idea of a queue system. A queue is a named destination and a data structure used to store messages. These messages are read by a receiving application. Queues use a store and forward mechanism, this means the receiving application need not be running at all times. When the receiving application is running it must poll the queue to receive messages. Messages can be placed onto the queue by the holder of the queue, other machines on the network, and the receiving applications.

For example, an MQ server running upon an IBM mainframe could be used to coordinate message that are exchanged between Windows and Unix based applications using the MQ clients applicable to those operating systems.

How do I use poll an MQ message queue in ODEX?

The first step in using WebSphereMQ is to set up an MQ back office system, this can be done from the System tab in the administrator. This is where the settings of the queue you are going to poll. If you do not know these settings you will need to contact your System Administrator.

The second step is to set up an MQ data source, this can be done from the Workflow tab in the administrator. When creating the data source in the queue drop down box please select the name of the MQ back office system you wish to use.

The third step is to set up a new event action, this can be done in the System tab of the administrator. Under single action select “Poll Message Queue”. In the following parameter box select the MQ data source you wish to use under the “MQ Data Source” parameter.

Finally configure a workflow to use the MQ data source you have defined.

How do I use write to an MQ message queue in ODEX?

There are two ways to write to write to an MQ message queue, through an event action or through a workflow job.

Event Action

The first step in using WebSphereMQ is to set up an MQ back office system, this can be done from the System tab in the administrator. This is where the settings of the queue you are going write messages to. If you do not know these settings you will need to contact your System Administrator.

The third step is to set up a new event action, this can be done in the System tab of the administrator. Under single action select “Write to Message Queue”. In the following parameter box select the MQ queue you wish to use under the “MQ System” parameter. Under the “Message” parameter type the message you wish to place using any of the placeholders if you wish.

Workflow Job

The first step in using WebSphereMQ is to set up an MQ back office system, this can be done from the System tab in the administrator. This is where the

settings of the queue you are going write messages to. If you do not know these settings you will need to contact your System Administrator.

The second step is to set up a data source for the workflow as desired such as a monitor directory data source. Thus when a file is submitted to the directory it can be written to the message queue.

The third step is to set up the workflow itself. Add a new workflow and then select the jobs tab. Add a new job with the name “Write to MQ Message Queue”.

The fourth step is to select the queue you wish to use under the “MQSystem” parameter.

The fifth step is to create a message under the “Message” parameter.

The sixth step is to set the “Received” parameter, this allows you to specify if you wish to use inbound file placeholders in your message.

The seventh step is to set the “Include File” parameter, this allows you to include the workflow file as part of the message you write to the queue.

Please note that if you include the file in the message using the “Include File” parameter the file will be appended to the end of the message written to the queue. You do not need to define a message to be written to the queue, you can just write a file.

ENGDAT

This section introduces ENGDAT in ODEX. It aims to answer any questions about ENGDAT and how ENGDAT can be used within ODEX.

What is ENGDAT?

ENGDAT is a specification produced by ODETTE describing how CAD and CAM files can be transferred between two parties. Each ENGDAT transmission or exchange typically consists of one or more CAD/CAM files and optionally an ENGDAT message, packaged in an ENGDAT ‘folder’.

What is an ENGDAT folder?

A folder is a group of files which may be in any format, such as engineering documents, CAD/CAM drawings, files created by a word processor application or any other computer-generated file. There are no restrictions on the file types that may be included in a folder.

An ENGDAT folder may also contain an ENGDAT message describing the contents of the folder, though this is not compulsory. The ENGDAT message can be an EDI or XML message, depending on which ENGDAT version is in use.

A folder has an origin (the company which creates the folder), a destination (the recipient of the folder), an 'exchange reference number', as well as a creation date and time.

An example ENGDAT folder is described below:

File 1 - ENGDAT EDI File - Header

File 2 - CAD File, containing a drawing of part number 23560.

File 3 - Formatted text file generated by a word processor, describing changes to part number 23560.

File 4 - CAD File, containing 3 drawings of a proposed new part.

Files 2, 3 and 4 were generated by various applications such as CAD / drawing applications and word processors. File 1 is the ENGDAT EDI file itself - this contains detailed information regarding the other three files, so they may be interpreted by the recipient of the folder.

What is an ENGDAT message?

The ENGDAT message itself is a 'header' – it describes the contents of an ENGDAT folder in detail. This allows the files in the folder to be processed and interpreted. There are 3 different versions of the ENGDAT message.

The ENGDAT message may contain the following:

- Origin and destination company and contact details
- File characteristics of each exchanged file, such as the file name, format of the file and the generating system that was used to create the file.
- Details of the drawings contained in a file (ENGDAT versions 1 and 2 only). This includes a drawing reference number and name, description, engineering change numbers, etc.
- Details of a part described by a file (ENGDAT version 3 only). This includes the part number, description, engineering change numbers etc.
- Links between files in the folder. This allows the relationships between files to be described by the message.
- References to documents that are not included in the ENGDAT folder. For each document, a document name, number, date and time are stored. A folder can have many related documents.
- Details of files contained within other files (ENGDAT version 3 only). This mechanism may be used to describe ‘archive’ files containing other files.

The message details can be viewed and modified in the ENGDAT workstation’s folder editor.

What are the differences between each version of the ENGDAT message?

ENGDAT message versions 1 and 2 are both ODETTE EDI messages, with a very similar structure. They contain the same fields, though version 2 of the message includes support for contact routing addresses.

ENGDAT version 3 is a new XML message format. It contains some of the fields used in versions 1 and 2, but many additional fields have been added, removed and changed.

How are folders transmitted and received?

Files are transmitted and received using the ODETTE file transfer protocol (OFTP). When ENGDAT files are being transmitted, the files are all treated as individual files – OFTP has no concept of a folder.

When sending files using OFTP, a unique name is given to each file. This 'Virtual Filename' (VFN) is used by the receiving party to interpret and process the file. For example, a VFN may simply be the same as the filename of the file, e.g. 'CHANGES.DOC', or a short description such as 'CHANGES DESCRIPTION'.

The specification of the OFTP states that a VFN may contain up to 26 characters.

When transmitting an ENGDAT folder, there will be several files which are all related. Because the files are completely separate, but need to be 'linked' to form a folder, the VFN is used to link common files. The format of the VFN is shown below:

Characters 1 – 3	The text 'ENG', to identify this file as a member of an ENGDAT folder.
Characters 4 - 20	Exchange reference number of the folder
Characters 21 – 23	Total number of files within the folder (including the ENGDAT header).
Characters 24 – 26	Sequence number of this file within the folder (the ENGDAT header is always sequence number 1).

It is therefore possible to determine from the VFN that a file belongs to an ENGDAT folder, the number of files in the ENGDAT folder and the position of the current file within that folder.

Validation Profiles

Validation profiles are used to store the requirements of companies that use ENGDAT messages. Generic validation profiles are also included with ODEX. Each validation profile contains the following settings:

- ENGDAT message version
- Fields that are mandatory in the ENGDAT message
- Fields that are not used in the ENGDAT message
- Exchange reference pattern
- Maximum field lengths and field formats

When you create an ENGDAT relationship between your company and one of your trading partners, you choose a validation profile from which the above settings will be used.

When you create a new ENGDAT folder, ODEX checks the settings in the validation profile. ODEX will then only display fields in the ENGDAT folder editor that are appropriate to the ENGDAT message version and for company validation profiles, the requirements of the trading partner company.

The validation profile settings also serve the following purposes:

- Prevents data being entered in the wrong format for the ENGDAT message (e.g. alphabetic characters in a numeric field).
- Prevents data being entered that breaches the maximum length defined in the ENGDAT message specification.
- Provides warnings when mandatory field values are omitted from the ENGDAT message.

ODEX is currently distributed with 3 generic validation profiles. A validation profile is provided for each ENGDAT message version. When you use these validation profiles, all of the fields applicable to the particular ENGDAT message version will be available. Fields marked as mandatory in the ODETTE ENGDAT specification will be marked as mandatory in the ENGDAT folder editor.

Three company-specific validation profiles are provided; BMW, Swedish OEMs and John Deere. The following sections describe the differences between the validation profiles in more detail.

The BMW validation profile is based on BMW's ENGDAT message specification and is almost identical to the standard ENGDAT version 1 standard. The exchange reference required by BMW is the current date and time followed by the "address code" of the recipient. The address code may be specified in the Routing Code field of the destination engineering contact.

The Swedish OEM validation profile is based on a specification for ENGDAT as used by Volvo, Scania and Saab. The Swedish OEM validation profile uses ENGDAT version 2.

The John Deere validation profile uses version 1 of the ENGDAT standard. The exchange reference contains the date, recipient routing code and a single character for the file format.

When you create an ENGDAT folder, you may add an ENGDAT message and add exchanged file details to the message, including the file format. If you work in this way with the John Deere validation profile, ODEX can automatically create the correct exchange reference for the folder, based on the selected file format of the first file in the folder.

Using the Gedas Com-Secure Application with ODEX

Often before sending an ENGDAT folder to a trading partner, additional processing is required for each file in the folder. An ENGDAT relationship can be configured so that the 'Schedule Action' of the ODEX ENGDAT Workstation can submit the folder to a workflow. This workflow can perform any additional actions before the folder is sent with the 'Schedule ENGDAT file' job. An example of how to configure the Gedas Com-Secure application to encrypt files will illustrate this. The steps assume that Com-Secure is already installed and configured on the machine.

First the workflow must be created. The example workflow will be created with two jobs, but any of the jobs can be included in the workflow. In order to invoke Com-Secure, the 'Run Application' job should be added. The recommended parameters are as follows:

Parameter	Value
Application	gdcomsec.exe
Arguments	-g –c RSB "%SFP_F%" "C:\test\%FID%.out"
Wait for exit	**True**
Timeout	-1
Delay	0
Synchronized	**True**
Output Filename	"C:\test\%FID%.out"
Working Directory	C:\Program Files\gedas\Com-Secure\
New Window	**False**
Window Style	**Hidden**
Received	**False**

In ‘Arguments’ a public key of ‘RSB’ is specified, this should be changed to match the registered ID of the certificate you are using within Com-Secure. The forth argument is a placeholder for the full system file path of the file to be encrypted. The final argument is a file location for Com-Secure to write the completed file too. This matches the file location specified in the ‘Output Filename’. It is important these are the same so that ODEX can use the encrypted file in the next job. For the filename we have used the parameter ‘Workflow file ID’ which ensures the created file is unique.

Several fields are highlighted in bold; it is highly recommended that these values are not changed.

The other job required by the workflow is the ‘Schedule ENGDAT file’ job. This requires no parameters as it takes all the schedule information from the ENGDAT relationship. If the ENGDAT folder’s files reach this job in the incorrect order, the job will error with the return code ‘PREVIOUS FILE UNSCHEDULED’. It is recommended that this is handled accordingly.

Once the workflow has been saved, a Channel must be set up that links to it. Ensure that unwanted files are not processed by this channel by placing it at the bottom of the Channel list or adding a dummy definition that will not match any files. Any definition set here will not be checked when the ENGDAT folder is submitted.

Finally, select or create the ENGDAT relationship you wish to use the Com-Secure application. On the ‘ENGDAT Relationship – Communications’ tab, ‘Schedule Action’ section, select the ‘Submit the ENGDAT folder to Channel’ option and choose the Channel you created. Once saved, whenever the file is scheduled from the ENGDAT workstation, the folder will be placed on the workflow and each file will be encrypted with the Com-Secure application before being sent.

EDIFACT Security

This section contains an introduction to EDIFACT security and a brief explanation of the support provided in ODEX enterprise for creating and validating secured EDI messages.

What is EDIFACT security?

EDIFACT security was introduced in version 4 of the EDIFACT syntax specification. It comprises several mechanisms for applying security services to EDIFACT messages and interchanges, including encryption, digital signing and secure acknowledgements. The following discussion is limited to the creation and validation of digital signatures and acknowledgments, for which support is now available in ODEX Enterprise.

What are digital signatures?

Digital signatures provide a mechanism for trading partners to meet the following security requirements:

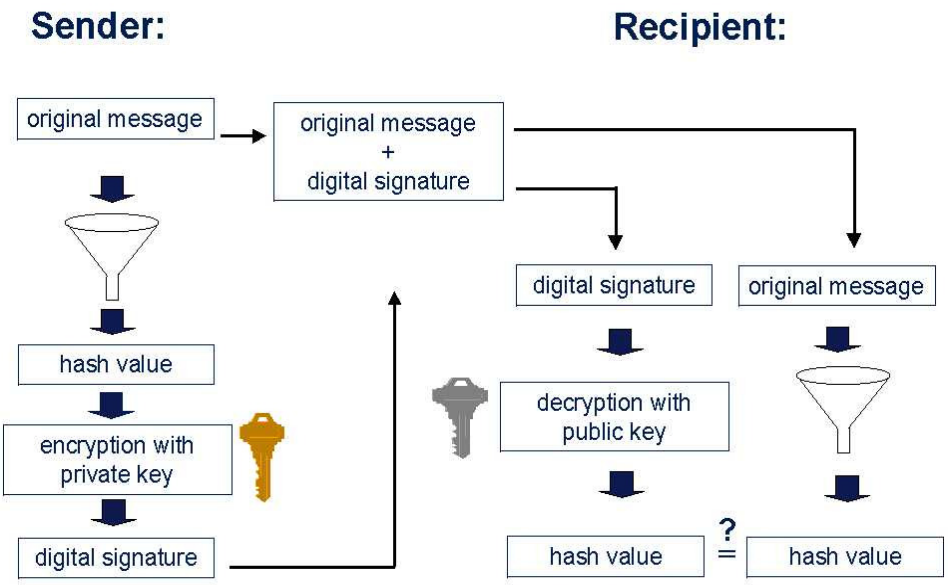
- Integrity – guaranteeing that EDI data was not altered during transmission.
- Authenticity - verifying the identities of the parties involved in an electronic transmission.
- Non-repudiation of origin - ensuring that no party involved in an electronic transaction can deny their involvement in the transaction.

A digital signature consists of a small, structured package of data created by applying a security algorithm to a unique representation (the ‘hash’ value) of the

message or interchange to be signed. The sender of data creates the signature and transmits it to the recipient of the EDI data. The recipient is then able to match the data to the signature and verify that the signature is valid.

The process used to create the signature from the data, and the associated process used to verify the signature against the data, are complementary, but not the same process in reverse. Consequently, they are referred to as 'asymmetric'. While anyone may verify the validity of the signature, only the sender may create it.

The asymmetric nature of the process is achieved using cryptographic keys that have two parts: a public key that may safely be made available to anyone, and a related private key that is used only by the sender. The private key is used to create the signature and the public key to verify it. The keys used by ODEX Enterprise for EDIFACT security processing are stored in a standard format known as a digital certificate, or X.509 certificate. These may be provided by a third party Certification Authority or by your trading partner, or you may create them yourself. The steps in the signing and verification processes are illustrated below:



- The sender uses a hash function to create a has value representing the original message, then uses the private key to encrypt the hash value and build a digital signature.
- The original message and the digital signature are sent to the recipient (not necessarily in the same transmission). The public key that relates to the private key used for signing may be sent also.
- The recipient applies the same hash function as the sender to the original message and uses the senders public key to decrypt the digital signature.
- If the values generated by the recipient from the signature, and the signature sent by the sender are identical (and the certificate itself is valid) then the signature is valid and the security requirements are fulfilled.

Attached and detached signatures

The EDIFACT specification allows for digital signatures to be:

- **Attached** – where the signature and associated information is included with the EDI data to be secured. Attached signing is achieved using security-specific service segments that were introduced in EDIFACT version 4. These segments are written into the message or interchange to be signed and therefore always transmitted along with the secured data.
- **Detached** – where the signature is separate from the EDI data to be secured. Detached signing is achieved by placing the signature in a separate message of type AUTACK, which references the interchange or message to be signed. The AUTACK may be sent in the same file as the secured EDI data, but it doesn't have to be.

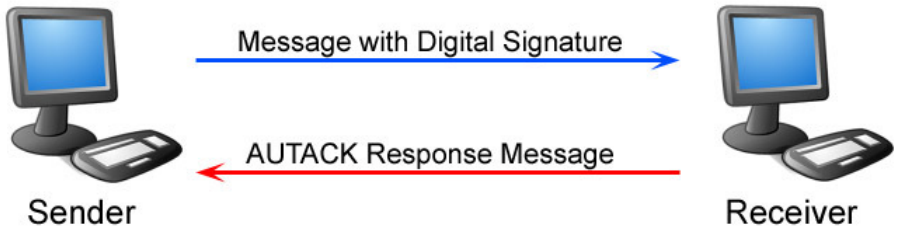
Response messages

The EDIFACT specification also allows for the transmission of AUTACK messages as responses to acknowledge the receipt and verification of signed data. The AUTACK can be used in response mode to return a positive or negative acknowledgement of signed data. The response AUTACK may itself be signed, to allow the security services (integrity, authenticity and non-repudiation) to be applied to the acknowledgment.

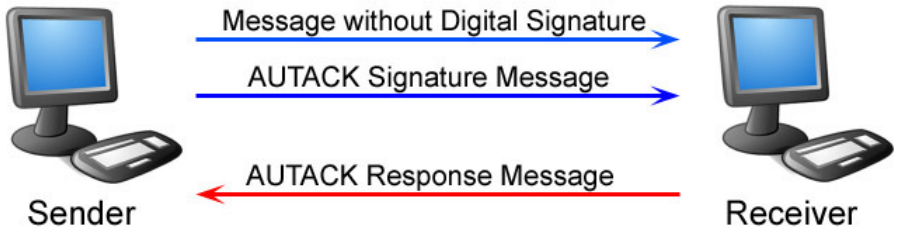
Exchanging signed data and responses

The exchange of a signed EDI message between two parties will vary depending on the signing method being used. This is illustrated in the following diagrams.

Using the **Attached** Digital Signature method, (1 message to send)



Using the **Detached** Digital Signature method, (2 messages to send)



The overall principals for both the Attached and Detached signing methods are the same. The sender creates an EDI message, that message is then signed and transmitted to the receiving party, they validate the signed file and generate an AUTACK response message which is sent back to the original sender to indicate the success of their validation of the signed file.

How does ODEX Enterprise support EDIFACT security?

Support for EDIFACT security is provided through three workflow jobs:

- The **Sign EDI** job is used to create digital signatures in respect of EDI data.
- The **Verify Signed EDI** job is used to process signed EDI data.

- The **Process AUTACK** job is used to process received AUTACKs representing both detached signatures and responses.

These jobs are described more fully in the following sections.

The Sign EDI workflow job

When a workflow file is processed by the Sign EDI job the data is signed according to the options selected for the job, overridden (if required) by values specified against the sender and/or receiver EDI code. The main options are as follows:

- Signing certificate – select a default signing certificate for which you have a private key
- Sign on client – a flag which specifies whether the data should be signed immediately on the server or held on the workflow to be signed manually on the client (ODEX Workstation). Signing on the client allows you to use a digital certificate that requires a password, including a certificate on a smartcard. When signing on the client the 'sequence on release' flag can be used to specify that workflow files held for signing should be released in the sequence that they were first submitted to the workflow manager.
- Signing method – select attached or detached signatures. If detached signing is selected, the 'detached file' flag can be used to specify whether the detached signature AUTACK message should be sent in a separate file. If this flag is set to true then the job will create a child workflow file in respect of the detached signature. To ensure that the detached signature is transmitted, you will need to specify a child file return code action to move the child file to a channel that includes a suitable schedule job.
- Signing level – specifies whether to sign at the level of the message or the interchange.
- Signature options – including the hash algorithm, padding mechanism and filter function that affect the way in which the signature is created and rendered to the message.

The other options are listed in the section defining the job.

The Verify Signed EDI workflow job

When a workflow file is processed by the Verify Signed EDI job the data is verified according to the options selected for the job, overridden (if required) by values specified against the sender and/or receiver EDI code. The main options are as follows:

- Verification certificate – specifies a default certificate to use for verification. If a certificate is not specified then ODEX attempts to determine from the EDI message which certificate to use.
- Signing method – select attached or detached signatures. If attached signing is selected then the job will attempt to verify signatures straight away. If the detached method is specified and there are signature AUTACKs in the same file then the job will also attempt verification immediately. If ODEX detected that an AUTACK has already been received containing a detached signature for the received data then the AUTACK will be retrieved and the signature verified. Finally, if the detached signature file does not yet appear to have been received, the file will be marked to indicate a signature is expected and saved until the relevant AUTACK arrives.

- Remove security – flag indicating whether security segments should be stripped from a message or interchange with an attached signature.
- Create response – indicates whether to create an AUTACK response message when a signature is verified. If this flag is set then ODEX will create a child workflow file containing the response AUTACK. To ensure that the response is transmitted, you will need to specify a child file return code action to move the child file to a channel that includes a suitable schedule job.
- Signing certificate to use for the response AUTACK – required when the verify job is to produce an AUTACK response.
- Signature options for the response AUTACK – including the hash algorithm, padding mechanism and filter function that affect the way in which the signature is created and rendered to the message.

The other options are listed in the section defining the job.

The Process AUTACK workflow job

When a workflow file is processed by the Process AUTACK job the action taken by ODEX depends on whether the AUTACK is a response (acknowledgement) or a detached signature.

In the case of a response, ODEX tries to locate the outbound file to which the response refers. If the original file is found then its security status is updated to reflect the response received.

Where a detached signature is received the signature is verified according to the options selected for the job, overridden (if required) by values specified against the sender and/or receiver EDI code. The main options are as follows:

- Verification certificate – specifies a default certificate to use for verification. If a certificate is not specified then ODEX attempts to determine from the EDI message which certificate to use.
- Create response – indicates whether to create an AUTACK response message when a signature is verified. If this flag is set then ODEX will create a child workflow file containing the response AUTACK. To ensure that the response is transmitted, you will need to specify a child file return code action to move the child file to a channel that includes a suitable schedule job.
- Signing certificate to use for the response AUTACK – required when the job is to produce an AUTACK response.
- Signature options for the response AUTACK – including the hash algorithm, padding mechanism and filter function that affect the way in which the signature is created and rendered to the message.

The other options are listed in the section defining the job.

Windows Clustering

This section contains an introduction to clustering before explaining the steps needed to set up ODEX within an existing cluster.

What is clustering?

Windows Clustering allows multiple computers sharing a common storage area or quorum to provide services with increased availability. ODEX Enterprise supports Windows Clustering in order to provide increased resilience with failover support and to minimise downtime. If you are considering implementing a cluster system it is worth noting that these require additional server-grade hardware and software as well as SAN or Fibre Channel Disk Array storage, for most ODEX Enterprise installations it is often sufficient to have an off-site back up with which to provide a failover option.

This guide will assume you have experience in Windows clustering and already have a cluster established with a clustered SQL server running as a resource.

What do I need for an ODEX cluster?

- A Windows cluster running on at least two nodes running the IP address and Network Name resources.
- A form of high-availability storage (SAN, FCDA) running with the cluster
- A Clustered SQL Server running on the cluster. This type of server is not included with ODEX. Data Interchange recommends using Microsoft SQL Server 2005 Enterprise Edition.
- An ODEX licence for each node that ODEX is to be deployed on.

Preparing ODEX for Clustering

To begin clustering you must install ODEX on each node. Each installation should use a common Data directory on the clustered Physical Disk. This is set before installation when prompted.

After installation has taken place there will be a prompt for SQL server selection. Configure this to connect to the clustered SQL server. During the installation of the first node, the database will be created on this SQL Server. For more information see Advanced Configuration

In order for clustering to be supported, ODEX must be running as a system service on the node. To do this selected the start menu option “Install Odex as a system service” underneath the Data Interchange Plc folder or run the program “InstallService.exe” which is situated in the ODEX installation directory. This will set up ODEX as a system service, for more information on this see Running ODEX as a system service. It is important to stop this service when ODEX has been set-up

Once ODEX has been installed and configured on all nodes, ensure none of the services are started and proceed to the next section.

Adding ODEX as a Resource

Cluster support with in ODEX is offered through a custom resource type. In order to add this resource type to your cluster you must run the application "ResType" from one of your nodes. First ensure that the node with ODEX installed is active and you are connected to the cluster. Using command prompt, navigate to the ODEX installation folder (defaults to \Program Files\DIP\Odex Enterprise\Version Number\) and use this command to create the resource type:

C:\ODEX….install dir> restype create

This will create the resource type "Monitor of ODEX (version)" on the cluster. To delete the resource type when removing ODEX cluster support use the command *'restype delete'*.

The resource is then added by selecting 'Add a new resource' from the Windows Cluster administrator and selecting the newly added resource type. In order to run in a Cluster group ODEX requires the prerequisite resources of 'IP Address', 'Network Name' and one of the storage resource types.

Once these have steps are performed you are ready to start ODEX within your cluster. Bring the resource online and this should start the ODEX service on the currently active node. It is a good idea to test ODEX failing by stopping the service and ensuring the cluster responds in the correct way.

ODEX Installation

Introduction

First of all, please read the License Agreement included in the package containing the distribution media. It is very important that you understand and agree to the terms and conditions relating to the software before opening the CD and installing it.

Requirements

To install and run ODEX, you will require Windows 2000, Windows XP, Windows 2003 Server or Windows Vista, with Internet Explorer 6 or above already installed.

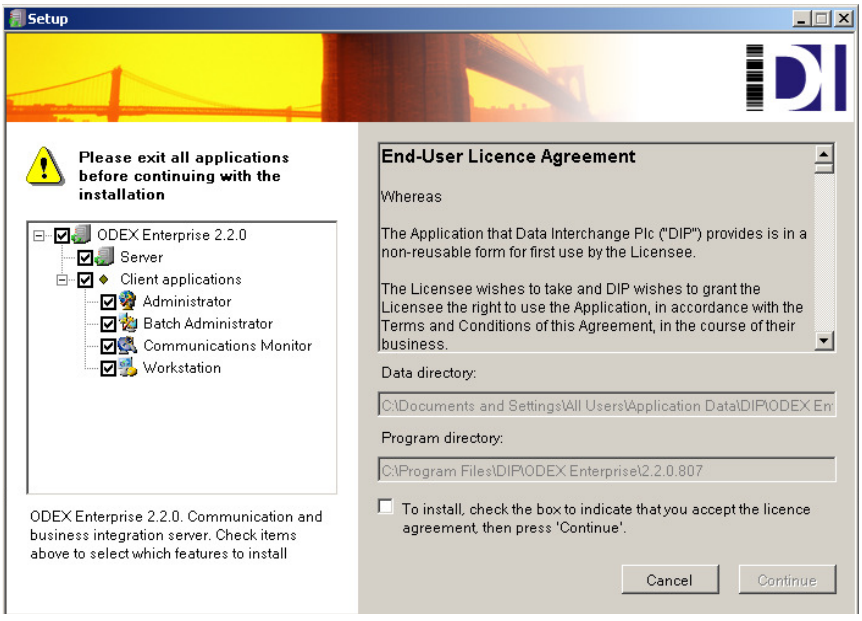
If you are going to use ODEX for communications, you will need a means of electronic communication with the outside world. Whichever communications protocol you use, you will require a telephone line and modem that can be used by the computer that has been designated to perform your EDI communications.

Installation and Setup

Before installing the ODEX software, please ensure that you close all other applications.

Now insert the ODEX CD into the CD-ROM drive of your computer. The installation program should begin automatically after a few moments but, if it does not, select **Start >> Run** from your Windows toolbar, and type in D:\setup.exe (where D is your CD-ROM drive) then click the **OK** button. This will begin the installation process.

The first thing you will see is the following dialog, which contains the License Agreement. This is an exact copy of the License Agreement contained in the distribution media package. You should already have read this carefully to ensure that you understand and accept the terms and conditions of the software.



This dialog allows you to choose the directories in which ODEX is to be installed. The program files will be installed in the program directory. Any files

that the application creates or modifies, such as workflow files, communication files and log files will be installed in the data directory.

This dialog allows you to choose whether or not to install the ODEX server, Microsoft SQL server 2005 and the client applications on this machine. The option to install Microsoft SQL Server 2005 is only given if the machine does not already have Microsoft SQL Server 2005 installed on it.

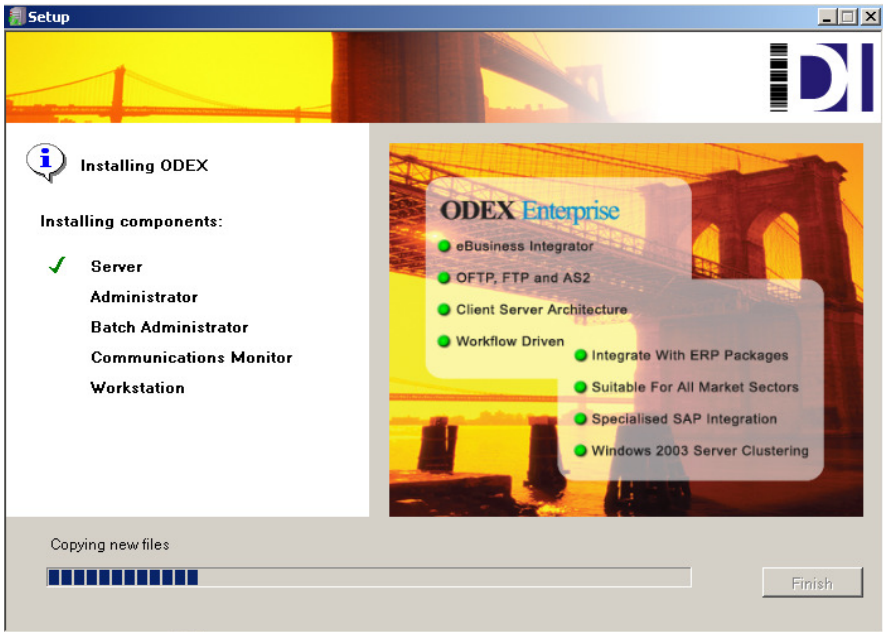
The client/server architecture means that you can install the four client applications on as many different computers as required. If you do not install the server on this machine, you must install it on a machine that will be accessible to all the clients on your local area network.

Installing Microsoft SQL Server 2005 is optional. By default, ODEX will be installed with Microsoft SQL Server 2005, though ODEX can use an existing SQL server to host its database. The server can be an instance of Microsoft SQL Server 2000 or Microsoft SQL Server 2005. If you plan to use an existing SQL server to host the ODEX database, you do not need to install Microsoft SQL Server 2005.

Please consider carefully which application(s) to install, as you will only be able to undo your choice by cancelling the installation after this point.

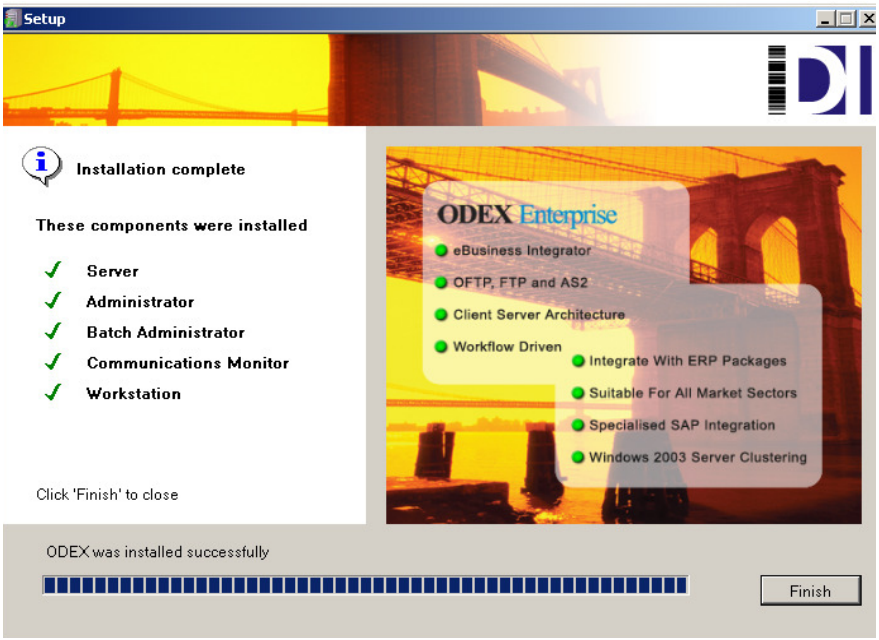
When you have decided which application(s) to install on this machine and you have read and agree to the terms and conditions, select the check box to indicate your agreement to the terms and conditions. This will enable the **Continue** button. Click **Continue** to continue with the installation. If you click **Cancel**, the installation will close.

After clicking **Continue**, you will see the following dialog while the installation proceeds.



This shows you how the copying of files is progressing.

When the installation is complete, you will see the dialog below:



Click the **Finish** button to close the installation program.

You will find that new shortcut icons have appeared on your desktop – one for each of the components you have installed on this computer.

Configuring your ODEX Enterprise database

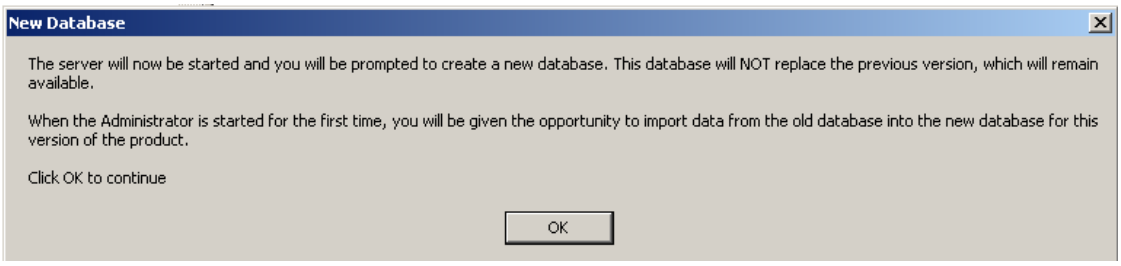
Once installation is complete, depending on the version of Windows you are working with, you will see one of two message boxes.

- **Setup succeeded**. Just click **OK** to continue. You must now configure the ODEX Enterprise database server. Select Start >> Programs >> Data Interchange Plc >> ODEX Enterprise >> ODEX Enterprise Server, or use the ODEX Enterprise Server shortcut icon on the desktop.
- **Restart computer**. This informs you that the computer must be restarted for the changes to take effect. Click **Yes** when asked if you wish to restart the computer now. This will restart your computer and automatically start the ODEX Enterprise Server.

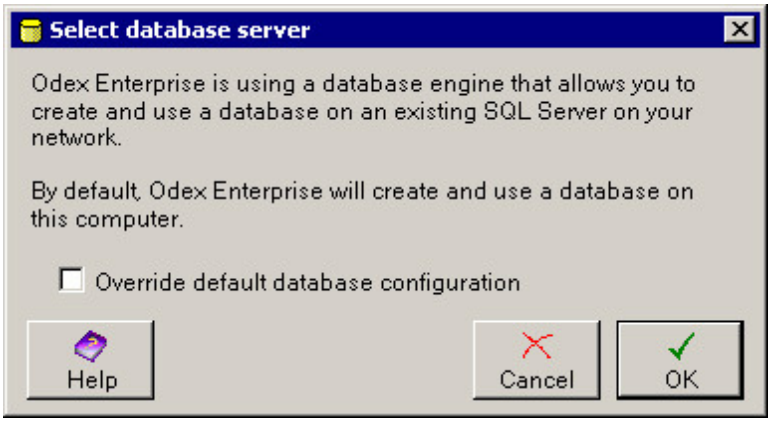
The database configuration dialog will now appear. Please read the section entitled "Simple configuration".

Simple configuration

On starting the ODEX Enterprise Server, you will see the following dialog:



Click OK to continue setting up the ODEX database.



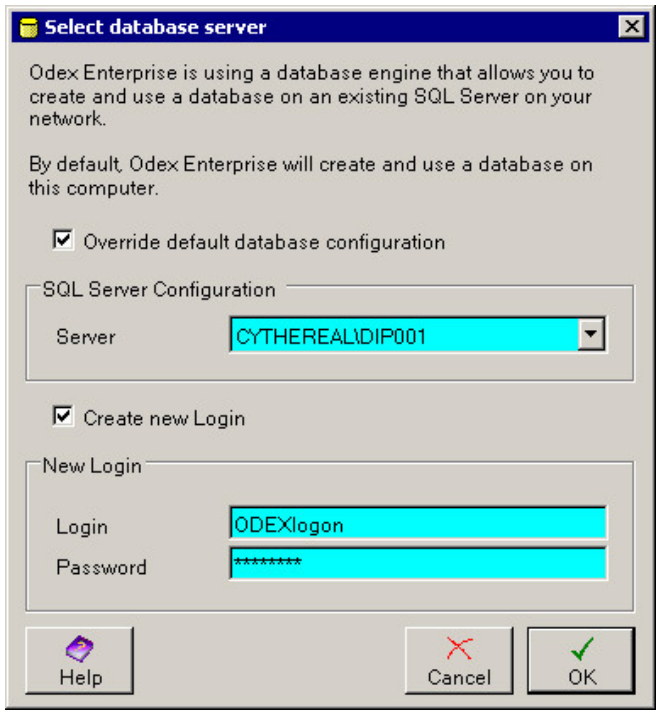
This explains that ODEX Enterprise uses a database engine that allows you the choice of creating and using a database on this computer, or creating and using a database on an existing SQL Server on your network.

If you want to create and use a database on this computer, just click the **OK** button.

If, instead, you want to use an existing SQL Server on your network, select the Override default database configuration tick box. This will expand the dialog to allow you to change the settings. For details of how to change the settings, please refer to the section entitled "Advanced Configuration".

Advanced Configuration

This option is for users who want to create a database on an existing SQL Server.



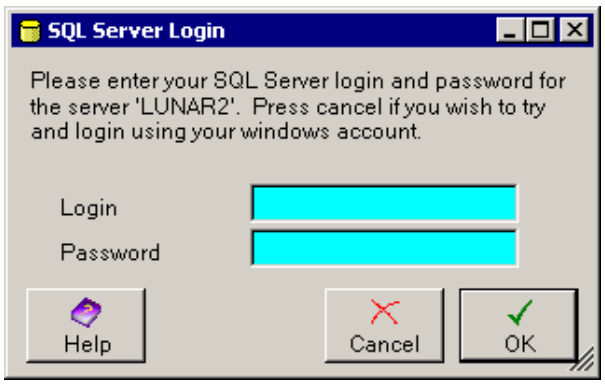
Server – This is the name of the SQL Server on which the ODEX Enterprise database will be created. In the Server field, use the dropdown arrow to select the existing SQL Server where you want to install the ODEX Enterprise database.

New Login – This is the Login and Password that will be created to enable the software to access the ODEX Enterprise database. Deselect the "Create new Login" tick box if you want to force ODEX Enterprise to login to the selected SQL server using the Windows account under which it is being run. You will

need to do this if the selected SQL server does not support 'Mixed Mode Authentication'. Note that any Windows users that may run the ODEX Enterprise software will need to be explicitly enabled against the selected SQL Server using your SQL Server client tools.

SQL Server Login details

If you select a different Server location (i.e. not the local machine), you may see a dialog similar to the one shown below:

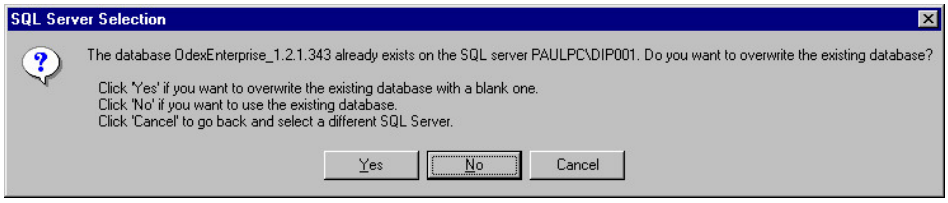


Type in the Login and Password to be used to access the SQL Server and click **OK**.

Alternatively, if you wish to try and login using your Windows account, click the **Cancel** button.

Database already exists

If the database already exists on the selected machine, you will see the following message.



You have 3 options:

Click **Yes** if you want to overwrite the existing database with a blank one, losing any data you previously had

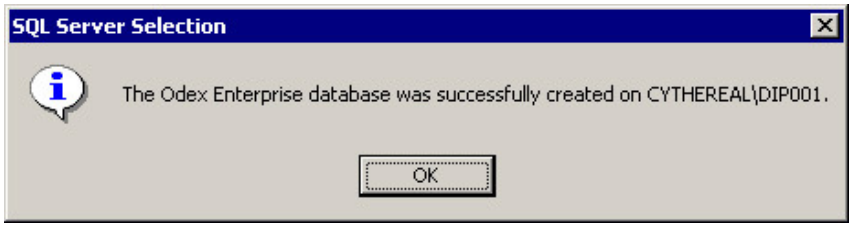
Click **No** if you want to use the existing database and keep all existing data.

Click **Cancel** to return to the previous screen and select a different SQL server.

The default option is to use the existing database and keep all existing data.

Result for all configurations

If the selected Server, Login and Password are all compatible, or if you chose the simple configuration option, you will see the message box below. The new database has been created on the selected SQL Server and will now be ready for use.



The ODEX Enterprise Server icon will appear in your system tray.

ODEX Directory structure

Once you have installed the ODEX Server, you will be able to view the ODEX directory structure. In most cases, you will have installed the ODEX program files in the default program directory and data directory. The default program directory is C:\Program Files\DIP\ODEX Enterprise. The default data directory is dependent on the operating system on which ODEX was installed. For Windows 2000 and Windows XP, this is C:\Documents and Settings\All Users\Application Data\DIP\ODEX Enterprise. On the Windows Vista operating system, this is C:\ProgramData\DIP\ODEX Enterprise.

Below the ODEX Enterprise program and data directories you will see one or more directories which are named after the Build number of ODEX e.g. 1.0.0.043. The first three numbers (here 1.0.0) indicate the version of ODEX, while the last number (here 043) indicates the Build within that version. Each time you upgrade your ODEX system a new one of these sub-directories will be created. For simplicity, we will refer to the sub-directory in the program directory as the installation directory and the sub-directory in the application data directory as the data directory.

Below the installation directory and data directory you will see that a set of sub-directories has been created. Most of these sub-directories are not for general use and are not to be accessed manually by any users.

Let's go through each of these sub-directories and find out what they are used for. The following directories are sub-directories of the data directory:

Data

This directory has a number of sub-directories that are used to store the different types of data file. These sub-directories have self-explanatory names:

Archived – files that have been archived

Comms_In – files that have arrived via a communications session

Comms_Out – files that are waiting to be sent via a communications session

Current – files that are being processed by the workflow manager

JobLogs – files containing log details of the workflow processing

Temp – a temporary storage area

Log

This directory is used to store a log file for each session you are logged on to the ODEX Server.

Monitor

This is the default directory that will be monitored by ODEX for new files that have not arrived via a communications session.

Xe

This directory is the default location of the Xe index file "xeindex.xml". It is also the default location for the definition files which Xe will use.

Xlate

This directory is the default location of the Xlate index file "xlatepc.idx". It is also the default location for the control blocks and tables which Xlate will use.

The following directories are sub-directories of the installation directory:

Utils

This directory contains a number of utilities and files that can be used by the Run Application event action or the Run Application workflow job. They have been included in ODEX Enterprise to maintain consistency with ODEX Professional.

Convert.exe and Ebcdic.tbl can be used for conversion between ASCII and EBCDIC encoding.

MapA2E.txt and MapE2A.txt are provided as examples of customised mapping files which could be used by the Convert File Encoding workflow job.

Delim.exe can be used to add CR/LF delimiters to EDI files, so that each EDI segment begins on a new line.

FileSplitter.exe and FileSplitter.cfg can be used to split files, based either on the UNB or the tax reference (GFF files). They are mainly used for splitting payroll data for Inland Revenue installations, where payrolls need to be in different directories or to have different filenames.

Sleep.exe is useful for batch file processing, to pause execution of one program while another program is completed.

Getting Started

First steps

This chapter is designed to help you set up the ODEX system now that you have installed it.

If you are using ODEX as your communications system, there are several areas that must be configured before you can use the product to communicate with your trading partners. Please refer to the section entitled "Using ODEX as your communications system".

If you are simply using ODEX as a file processing system, please refer to the section entitled "All users"

We recommend that you test the system prior to using it, to ensure that you have everything set up correctly.

All users

If you want to automate ODEX or use ODEX security, you may configure the following areas:

- System settings, users and user groups (ODEX security) – System section
- Trading partners, data sources, data definitions, workflow and channel details (automation) – Workflow section
- Schedules and Event Actions (automation) – System section

Using ODEX as your communications system

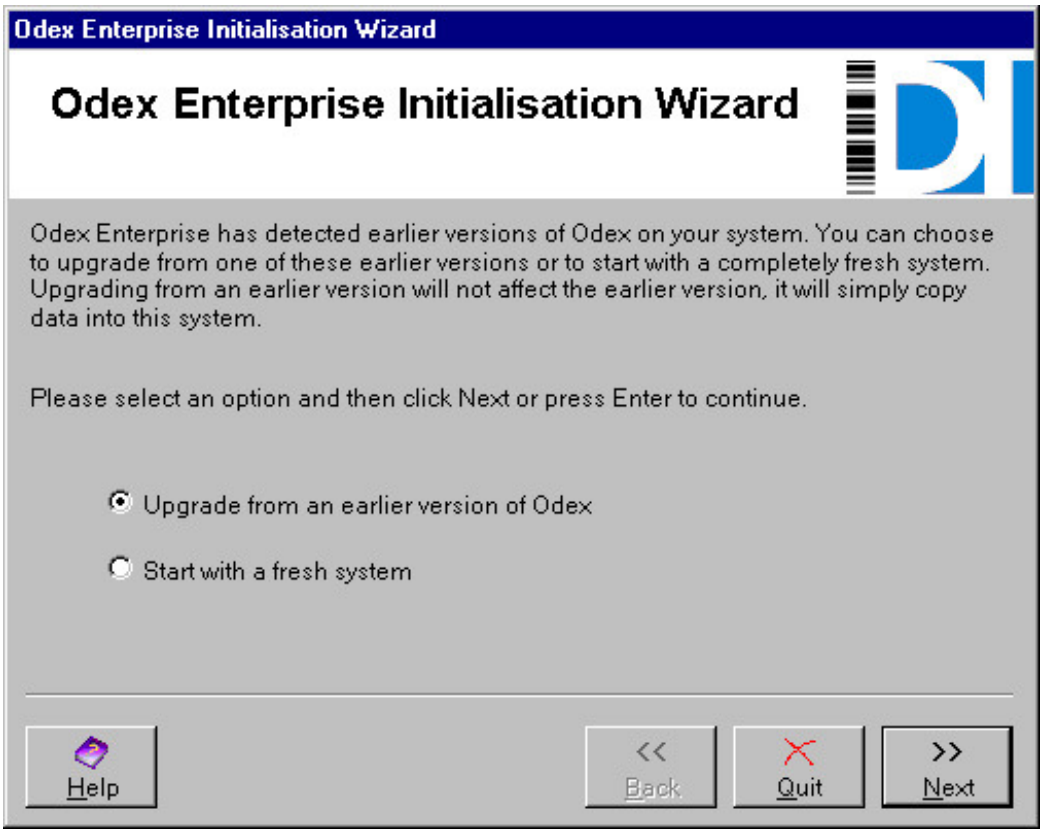
As a minimum, you need to set up your trading partners and communication details in the Comms section of the Administrator, in the following order.

- Internal companies
- Internal networks
- Trading partners
- Subsystems
- Trading partner networks and/or clearing centre networks

Upgrading from a previous version

Initialisation Wizard

If you have a previous version of ODEX (Enterprise or Professional) on your machine, this will be detected the first time you try to start the ODEX Administrator in your new version of ODEX Enterprise. The following dialog will be displayed.



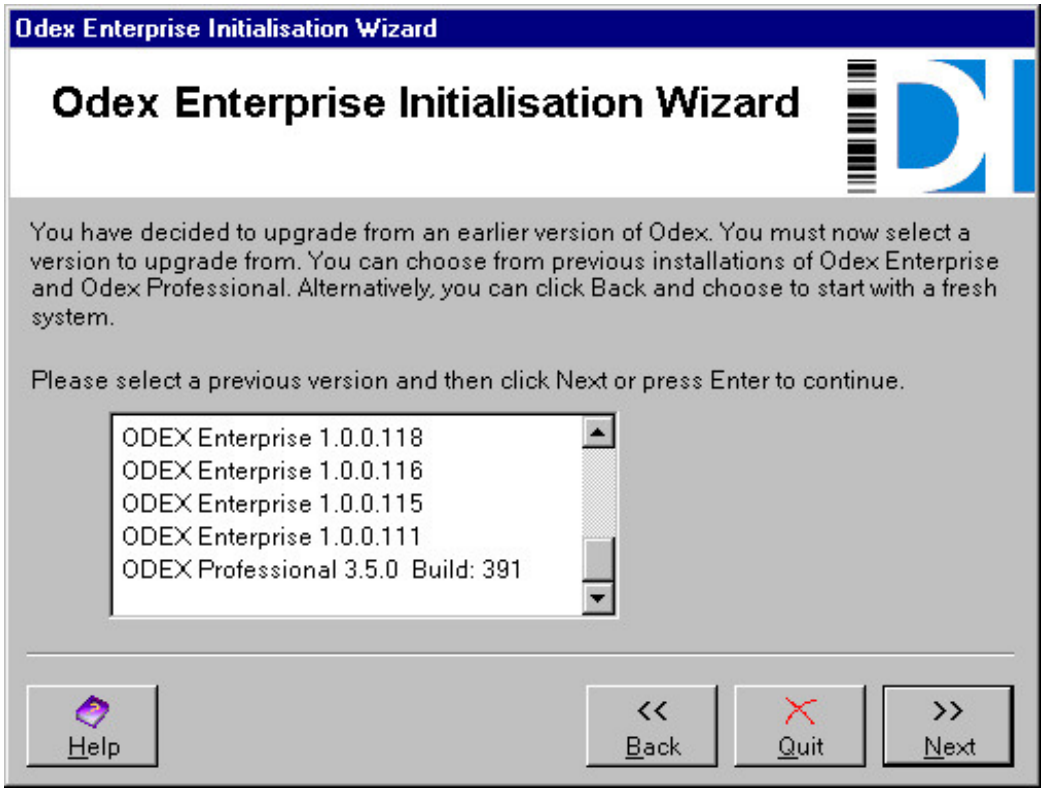
This gives you the choice of whether to upgrade from an earlier version of ODEX, or to start again with a fresh system.

Select one of the options and click the **Next** button or press **Enter**.

Please note that, at any time during the upgrade procedure, you may click the **Quit** button which will close the application. If you quit during the upgrade process (i.e. while files are being copied), any changes that have been made will be undone and the database will be “rolled back” to how it was before the upgrade began.

Upgrade

If you select the upgrade option, this will bring up the next dialog, shown below.



This dialog displays a list of all the existing versions of ODEX (Enterprise and Professional) on your machine.

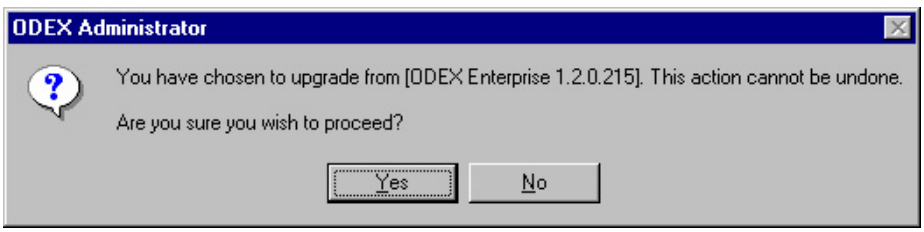
If you choose to upgrade from an earlier version of ODEX Enterprise, all your existing workflows, events, files and trading partners will be copied to the new version. This will not affect the old version, which will remain in place and fully usable.

If you choose to upgrade from an earlier version of ODEX Professional, all your User Directory entries, your Received, Scheduled and Sent File details, and most of your scheduled events, time profiles and event manager events (if selected on the next dialog) will be copied to the new version. This will not affect your existing version of ODEX Professional, which will remain in place and fully usable.

At this point, you still have the chance to click the **Back** button in order to return to the first page and choose to start with a fresh system. Or you can select one of the displayed versions and continue to upgrade from a previous version by clicking the **Next** button.

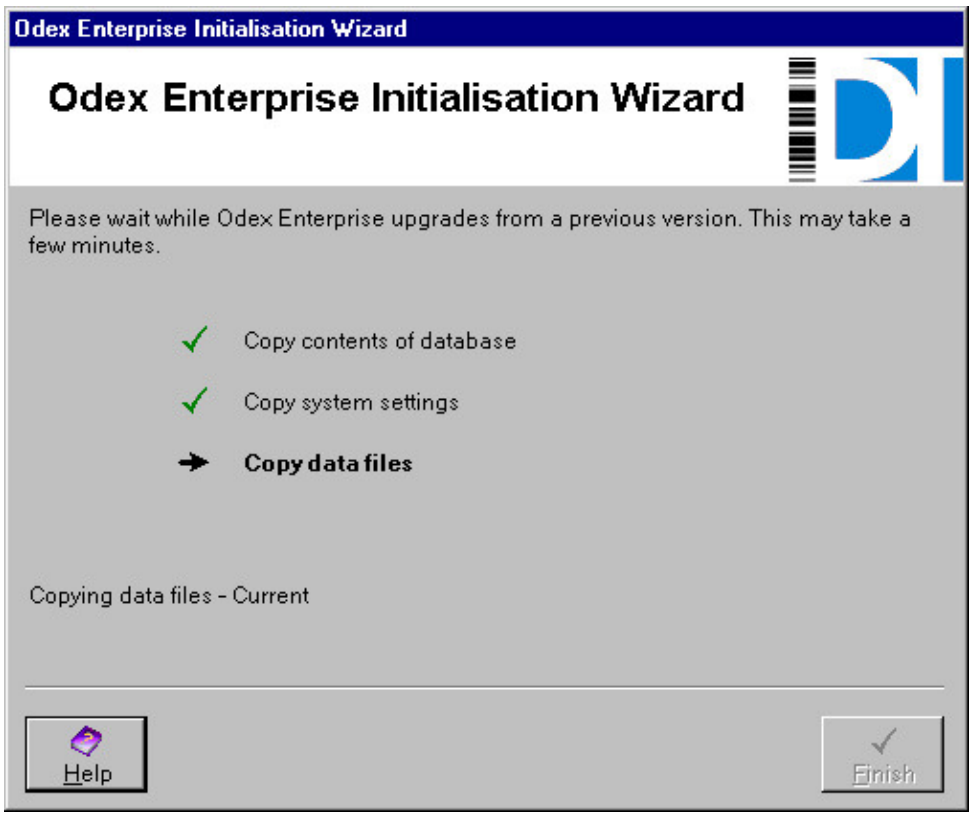
Upgrade from a previous version of ODEX Enterprise

If you chose to upgrade from a previous version of ODEX Enterprise, you will see a confirmation message, confirming the version you have chosen and asking if you still want to go ahead with the upgrade process, as this action cannot be undone.



Click **Yes** to proceed or **No** to return to the Wizard.

If you click **Yes**, you will see the following dialog.



This dialog will show you how the upgrade process is progressing. When everything has been copied, the message at the bottom will change to say "Upgrade complete" and the **Finish** button will become enabled.

Restart Server

You will see a note at the bottom of the dialog, stating that the server must be restarted before some upgraded settings will take effect. These settings concern the Server Port and User Security. If you had made changes to the Server Port or User Security in the previous version, you will need to restart the server in

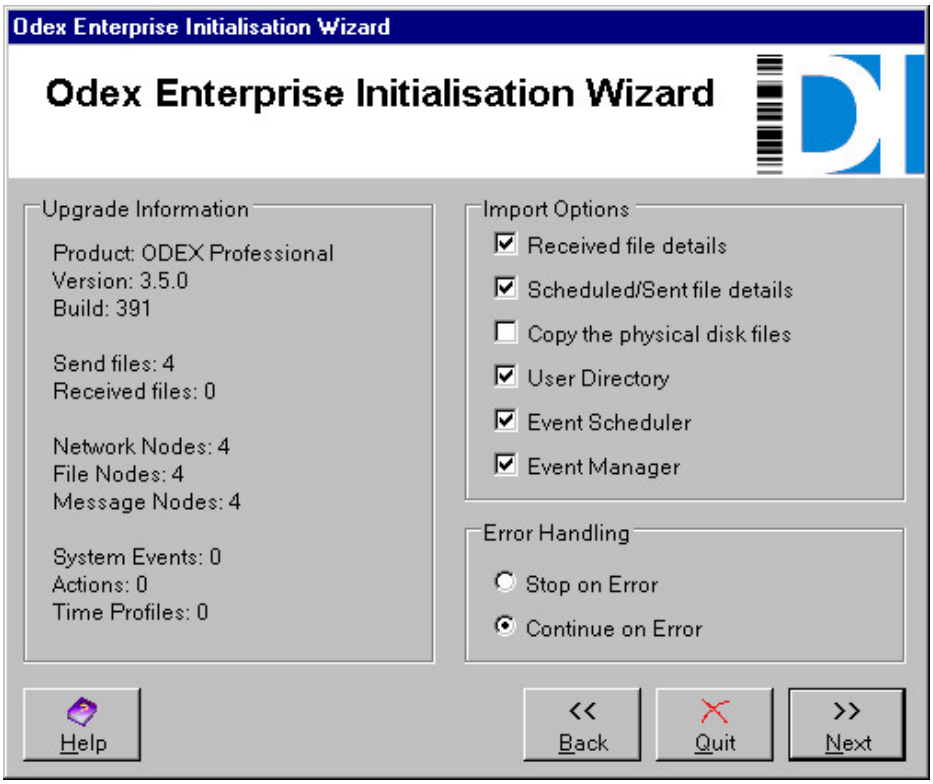
order for these changes to take effect in the new version. If you are not sure, it will do no harm to restart your server anyway.

First click the **Finish** button in order to complete the upgrade process. The Administrator will then start up.

You should now restart your ODEX Server in order for the upgraded settings to take effect. To do this, right-click on the ODEX Enterprise Server icon in the System tray and select the **Restart** option. This will momentarily stop the Server and restart it automatically. You will then see the Connection Lost dialog, indicating that the Administrator has lost its connection to the Server. Simply click the **Connect** button to reconnect it.

Upgrade from ODEX Professional

If you chose to upgrade from a previous version of ODEX Professional, you will see the following dialog.



Please note that upgrading from ODEX Professional to ODEX Enterprise will copy your User Directory details, your Received, Scheduled and Sent file details, and most of your scheduled events, time profiles and event manager events (if you select these options). The upgrade will NOT copy any VFN overrides, ENGDAT details etc.

For a description of how the scheduled events, time profiles and event manager events from ODEX Professional will be handled by ODEX Enterprise, please refer to the section entitled “ODEX Professional events in ODEX Enterprise”. That section also lists those events and actions from ODEX Professional which will not be upgraded.

At this point you can still change your mind. Clicking the **Back** button will take you back to the previous dialog, where you can choose to upgrade from a different version of ODEX. Clicking the **Quit** button will stop the upgrade and close the application.

This dialog is divided into three sections:

Upgrade Information

The Upgrade Information section confirms which version of ODEX Professional you have chosen to upgrade from. It also shows you the number of Send files, Received files, Network Nodes, File Nodes, Message Nodes, System Events, Actions and Time Profiles that are currently in your system.

The upgrade will attempt to import all these entities (if you select them on the next dialog) to ODEX Enterprise. Any failures, for whatever reason, will be listed at the end of the upgrade process.

Import Options

This section allows you to choose whether to import the details of your Received, Scheduled and Sent files into ODEX Enterprise, and whether to copy the physical disk file for each file you import.

If you do not copy the physical disk files into ODEX Enterprise, you will only have the details of each file but not the file itself.

If you deselect one or both of the File imports (Received and Scheduled/Sent), the physical files for the deselected files will not be copied. If you deselect both, you will not be able to select the Physical files option as it will be disabled.

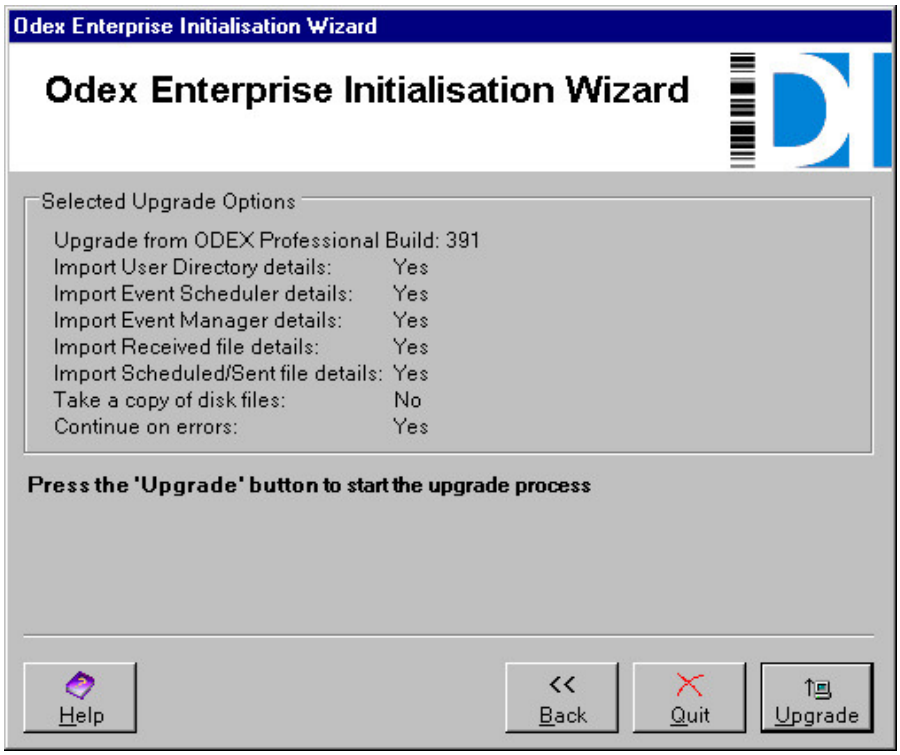
You may also choose to import all entries from your existing User Directory, Event Scheduler and Event Manager.

Error Handling

This section allows you to choose whether to halt the progress of the upgrade if an error is encountered, or whether ODEX should continue with the upgrade and try to handle any errors. Errors will be displayed in the status area on the final page of the upgrade procedure, once the upgrade is complete.

Once you have selected your preferred options, press the **Next** button to bring up the next dialog.

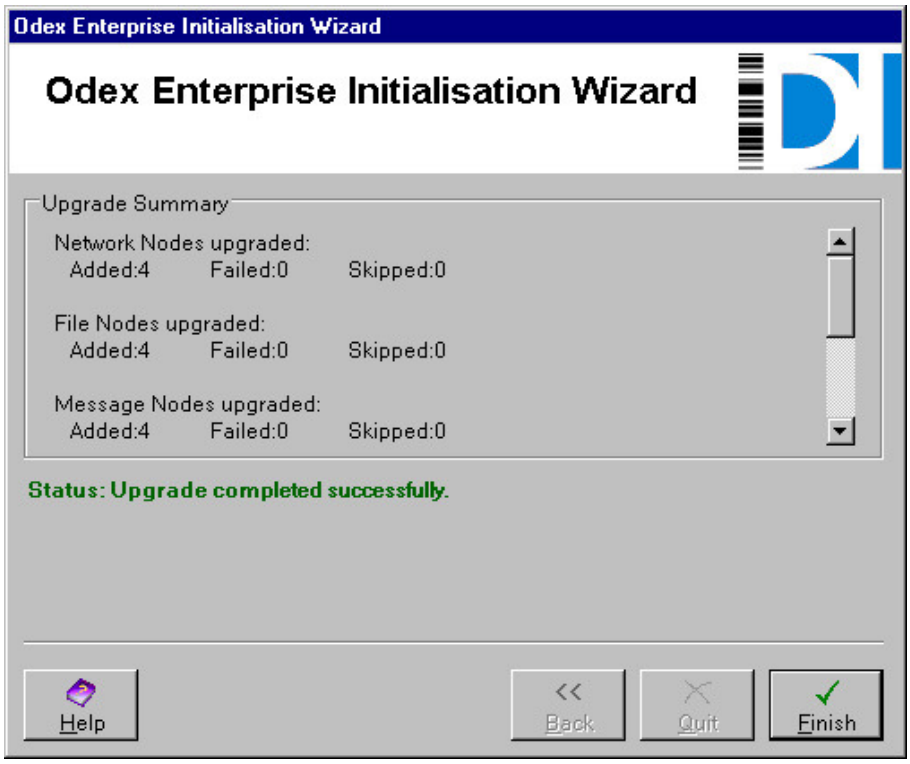
Check upgrade options



Take a moment to check the upgrade options you have selected.

At this point you can still change your mind. Clicking the **Back** button will take you back to the previous dialog, where you can choose different settings if you wish.

Once you are satisfied, click the **Upgrade** button to begin the upgrade process. The next dialog will show you how the upgrade is progressing, both with a status bar and a summary of upgrade steps that have been performed so far.



If you selected “Stop on Error” in the Error Handling section, the first error encountered will stop the upgrade process. If possible you should correct the reason for the error in ODEX Professional so that you can repeat the upgrade process. Alternatively you could select the “Continue on Error” option in order to upgrade as many entities as possible.

If you selected “Continue on Error” in the Error Handling section, once the upgrade has completed the dialog will show the “Status: Upgrade completed successfully” or “Status: Upgrade completed with errors” message, together with a tally of all the entities that have been upgraded. The **Back** and **Quit** buttons will have become disabled and the **Finish** button is enabled.

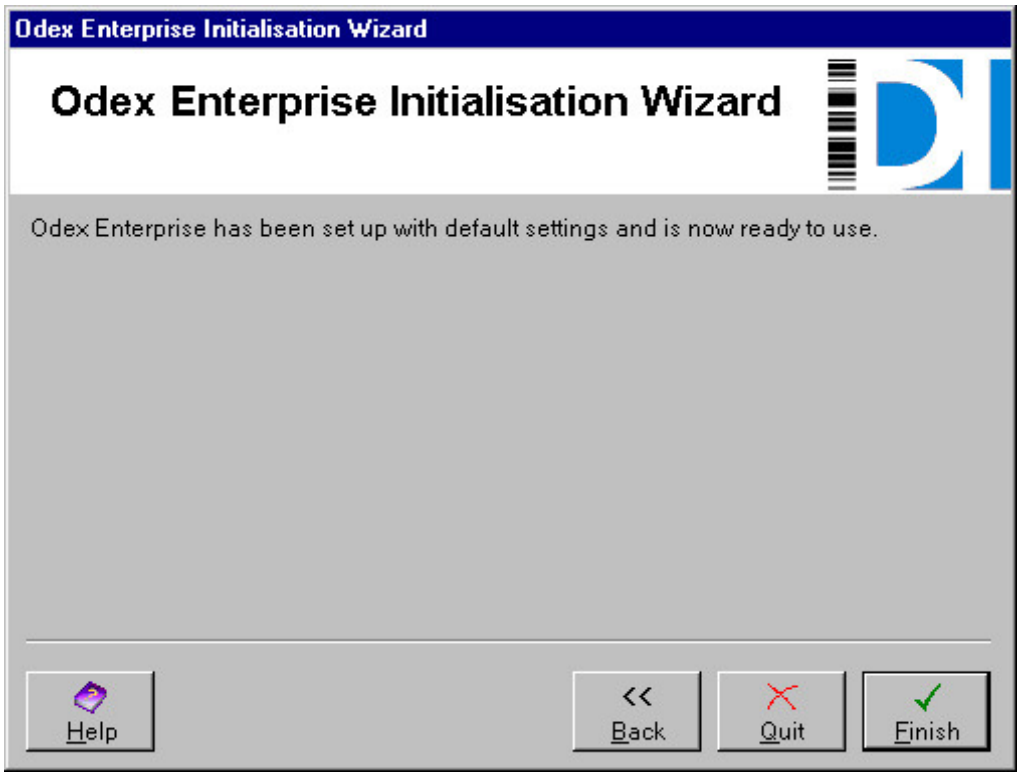
If the value of any Failed or Skipped tally is greater than zero, a reason for the failure or skipping will be shown in the Status section of the dialog. Failures will generally indicate an error which prevented the upgrade, while skipped entities generally indicate a duplicate in the system or, in the case of events and actions, an event or action that ODEX Enterprise does not support.

Use the scroll bar on the right to view all the upgrade details. At the end you may see a heading entitled “Unsupported Events and Actions”. This will list the events and actions (if applicable) that could not be imported from ODEX Professional because they are not supported by ODEX Enterprise.

Click the **Finish** button to complete the upgrade process. The ODEX Administrator will now start up.

Fresh system

If you select the fresh system option, this will bring up the next dialog, shown below.



This dialog tells you that ODEX has been set up with default settings and is now ready to use.

At this point you can still change your mind. Clicking the **Back** button will take you back to the previous dialog, where you can choose to upgrade from a previous version instead.

If you still want to set ODEX up with a fresh system, click the **Finish** button and the Administrator will start up.

ODEX Professional import

Import Wizard

If you did not upgrade from an existing version of ODEX Professional when you installed ODEX Enterprise, you can still choose to import details from your old system.

The ODEX Professional import facility is available from the Tools option of the ODEX Administrator. Select **Tools >> ODEX Professional Import** to see the following dialog.

Please note that importing from ODEX Professional to ODEX Enterprise will copy your User Directory details, your Received, Scheduled and Sent file details, and most of your scheduled events, time profiles and event manager events (if you select these options). The import will NOT copy any VFN overrides, ENGDAT details etc.

For a description of how the scheduled events, time profiles and event manager events from ODEX Professional will be handled by ODEX Enterprise, please refer to the section entitled “ODEX Professional events in ODEX Enterprise”. That section also lists those events and actions from ODEX Professional which will not be imported.

The dialog has three sections – Data source, Import options and Error handling.

Data source

You can either import from a version of ODEX Professional that has been detected on the ODEX Enterprise server machine, or browse for an ODEX Professional database on the local machine (i.e. where the Administrator application is installed).

If no previous version of ODEX Professional was detected on the ODEX Enterprise server machine, the first option will not be enabled.

To select a location on the local machine, use the **Browse** button, which will become enabled when you select the Browse option.

Import options

This section allows you to import all entries from your User Directory, Event Scheduler and Event Manager. They are all selected by default, so simply uncheck the tickboxes of any option you do not wish to import.

This section also allows you to import the details of your Received, Scheduled and Sent files into ODEX Enterprise, and to copy the physical disk file for each file you import.

If you do not copy the physical disk files into ODEX Enterprise, you will only have the details of each file but not the file itself.

If you deselect one or both of the File imports (Received and Scheduled/Sent), the physical files for the deselected files will not be copied. If you deselect both, you will not be able to select the Physical files option as it will be disabled.

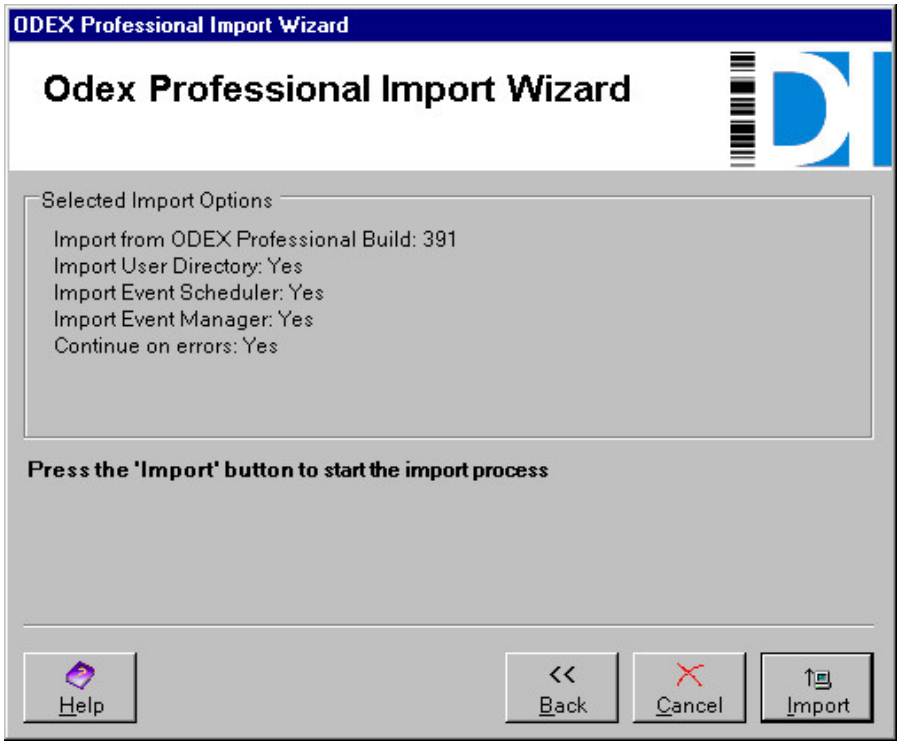
Error handling

This section allows you to choose whether to halt the progress of the import if an error is encountered, or whether ODEX should continue with the import and try to handle any errors.

Errors will be displayed in the status area on the final page of the import procedure, once the import is complete.

Once you have selected your preferred options, press the **Next** button to bring up the next dialog.

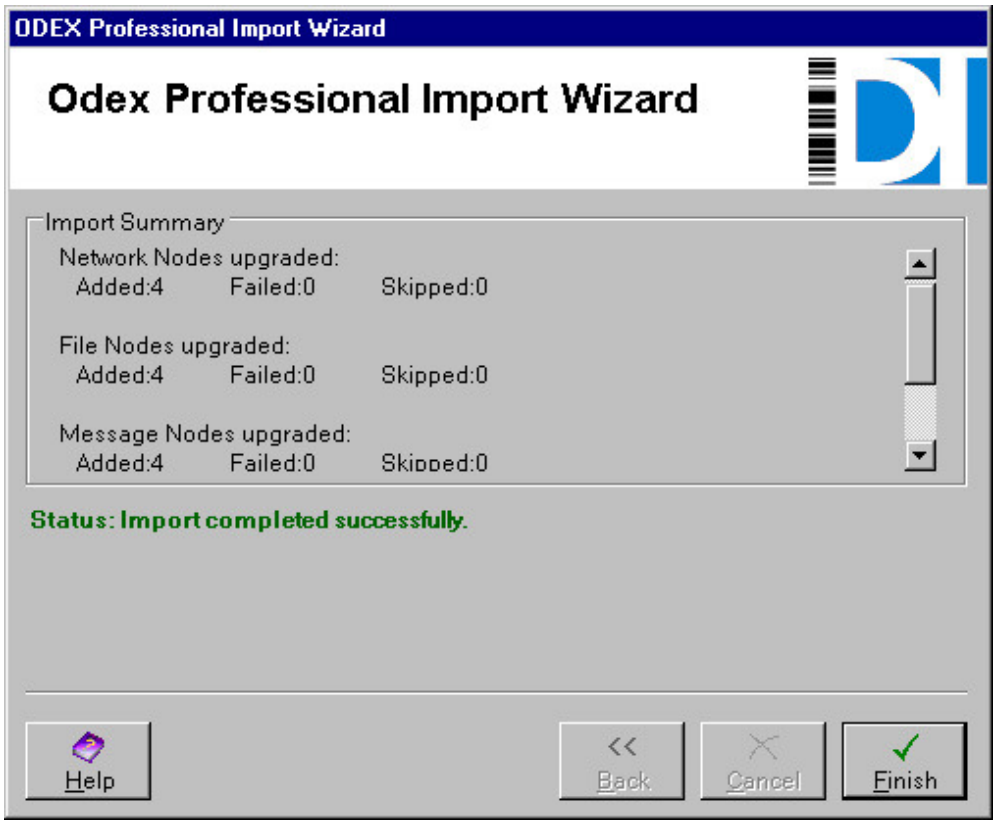
If you click **Next** you will see the following dialog.



Take a moment to check the import options you have selected.

At this point you can still change your mind. Clicking the **Back** button will take you back to the previous dialog, where you can choose different settings if you wish. Or you can click the **Cancel** button if you want to quit the import process.

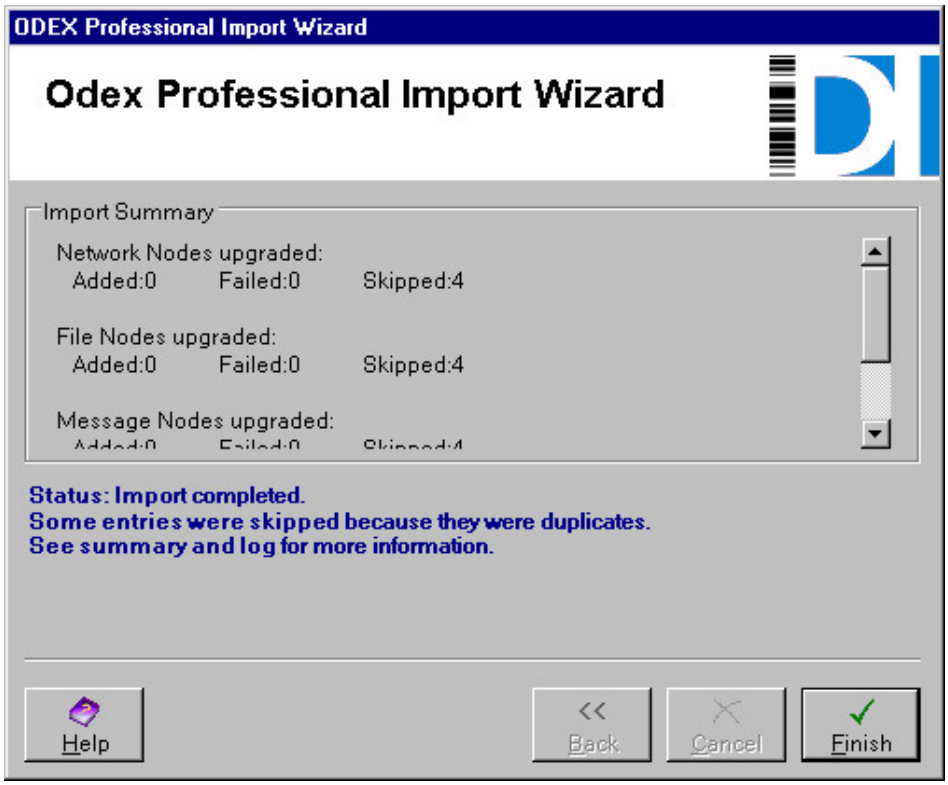
If you have no changes to make and want to continue with the import, click the **Import** button. The next dialog will show you how the import is progressing, both with a status bar and a list of import steps that have been performed so far.



If you selected “Stop on Error” in the Error handling section, the first error encountered will stop the import process. If possible you should correct the reason for the error in ODEX Professional so that you can repeat the import process. Alternatively you could select the “Continue on Error” option in order to import as many entities as possible.

If you selected “Continue on Error” in the Error handling section, once the import has completed the dialog will show the “Status: Import completed successfully” or “Status: Import completed” message, together with a tally of all the entities that have been imported, skipped and failed. The **Back** and **Cancel** buttons will have become disabled and the **Finish** button is enabled.

If the value of any Failed or Skipped tally is greater than zero, a reason for the failure or skipping will be shown in the Status section of the dialog. Failures will generally indicate an error which prevented the import, while skipped entities generally indicate a duplicate in the system or, in the case of events and actions, an event or action that ODEX Enterprise does not support. An example showing skipped entities is shown below.



Use the scroll bar on the right to view all the import details in the Summary section. At the end you may see a heading entitled “Unsupported Events and Actions”. This will list the events and actions (if applicable) that could not be imported from ODEX Professional because they are not supported by ODEX Enterprise.

Click the **Finish** button to close the dialog.

ODEX Professional events in ODEX Enterprise

Introduction

Most scheduled events and Event Manager events and actions can now be upgraded from ODEX Professional to ODEX Enterprise. However, the list below shows those events and actions which are **not** handled by ODEX Enterprise.

Events:

- Encryption key file received
- Failed to analyse encrypted file
- File Decryption failed
- File Encryption failed
- Received File deleted
- Send File deleted
- Automated user event executed
- Receipt transmitted
- File Extracted (for manual file extraction only)

Actions:

- Generate an SNMP trap
- Play a sound
- Speak
- Run a DLL library function

Conversions

ODEX Enterprise has taken a completely different approach to automation compared to the one you are familiar with in ODEX Professional. Previously, ODEX Professional offered an Event Manager and an Event Scheduler to enable you to automate the triggering of events.

The Event Manager offered a selection of actions that could be performed when specific events occurred within the ODEX system. For example, you could set up the Event Manager to execute an external application when the event 'Automated EDI Extract Completed' occurred.

The Event Scheduler offered a different set of actions that could be performed either at specific times of day (using the Time Profiles facility) or, in conjunction with the Event Manager, when specific ODEX events occurred. For example, you could set up an event in the Event Scheduler to extract an EDI file and, using the 'Run a User Scheduled Event' action in the Event Manager, you could trigger it to occur when the 'File Received and Analysed' event occurred.

As this shows, the Event Manager and the Event Scheduler are closely interlinked with each other. In ODEX Enterprise, the actions that can be performed are available in two distinct and discrete areas. The Workflow Manager is responsible for all actions which involve file processing, while the Event Actions area of the System Administrator is responsible for all scheduled events and all actions that do not involve file processing.

When you upgrade from ODEX Professional to ODEX Enterprise, most of your existing system events and all of your existing scheduled events will be converted seamlessly into the ODEX Enterprise system. However, they will not all be upgraded directly to events and actions; instead, those events and actions which act against files will be converted into workflows. For an explanation of workflows, please refer to the section entitled “ODEX Concepts”.

The following sections describe briefly how ODEX Professional events are converted into ODEX Enterprise. Each sub-section describes an event or action from ODEX Professional and explains how it will be handled by ODEX Enterprise.

Extract Non-EDI File

In ODEX Professional

Extract Non-EDI File takes a file, specified by VFN, destination etc. and copies it to a specified directory with a given filename.

There are options for specifying to extract only from/to specified Trading Partners and with the specified VFN. The extraction folder and filename can be specified, including using placeholders. Also the extracted file can be specified whether to overwrite or append to an existing file.

After the extraction is complete an application can be fired off.

ODEX Enterprise solution

In ODEX Enterprise, a workflow will be created that contains the Copy job and, if an application is to be run, the Run Application job as well.

The Copy job will specify the Output filename, whether to append or overwrite and any placeholders (e.g. counter in the filename).

The Run Application job will specify the application to run.

A channel will be created, which uses the comms data source and executes the workflow described above.

Extract EDI File

In ODEX Professional

Extract EDI File may be quite complicated, using any of the following options:

(1) File received (event File Received and Analysed and/or Incoming/Outgoing Session End)

(2) Event Manager initiates one or more file extraction(s) –

by EDI message type, version and release

by test or live status

by application reference

by SFID from, to and VFN

into a named directory with a file name determined by a mask.

(3) The EDI data may be translated, in-house data being written to the named directory.

(4) If translated, the original EDI data may be archived.

(5) A user application may be run against the extracted file (EDI or, after translation, in-house).

ODEX Enterprise solution

In ODEX Enterprise, a channel will be created using the following Data Source Message Definition and Workflow Jobs (some of which are optional, depending on what was set up in ODEX Professional):

(1) Comms Data Source identifying the SFID From, SFID To and VFN

(2) EDI Data Definition Message Definition identifying the EDI message type, version, release, test/live status and application reference

(3) Workflow Jobs –

(3.1) Copy identifies any EDI file archive directory and file name

(3.2) Translate identifies any translation profile (In-House definition) to use

(3.3) Copy identifies any output In-House file directory and file name

(3.4) Run Application identifies any user application to be run

Schedule EDI File

In ODEX Professional

Schedule EDI File will (optionally) construct an EDI file from an in-house file, schedule the file, then either copy or delete it.

The file is taken from a specified directory and optional filemask. The file is then constructed using the specified in-house definition. The EDI file can then be archived if necessary.

After construction the file is scheduled to the trading partner specified in the file. It is scheduled with the VFN, priority, format and record size specified.

After scheduling, the file is either deleted or moved to a specified archive directory.

A call is then made to send the scheduled file.

ODEX Enterprise solution

In ODEX Enterprise, a Monitored Directory Data Source will be created to specify the directory (and optionally the file mask) to get the file from.

A workflow will be created that contains, at most, the following jobs –

- Construct – only required if EDI construction is required.
- Copy – only required if the EDI file created from the Construct is to be archived.
- Schedule – this schedules the file to the trading partner specified in the file.
- Copy – only required if the scheduled file is to be copied.
- Call Network – calls the network to send the scheduled file.

A channel will be created, which uses the Monitored Directory data source and executes the workflow described above.

Schedule Non-EDI File

In ODEX Professional

Schedule Non-EDI File schedules the file to the specified trading partner, then either copies or deletes it.

The file is taken from a specified directory and optional filemask. The file is then scheduled to the trading partner specified. It is scheduled with the VFN, priority, format and record size specified.

After scheduling, the file is either deleted or moved to a specified archive directory.

A call is then made to send the scheduled file.

ODEX Enterprise solution

In ODEX Enterprise, a Monitored Directory Data Source will be created to specify the directory (and optionally the file mask) to get the file from.

A workflow will be created that contains, at most, the following jobs –

- Schedule – this schedules the file to the trading partner specified.
- Copy – only required if the scheduled file is to be copied.
- Call Network – calls the network to send the scheduled file.

A channel will be created, which uses the Monitored Directory data source and executes the workflow described above.

Send an E-mail

In ODEX Professional

This action sends an e-mail to/from the addresses specified. The e-mail can contain a subject, body and attachment. In addition, a MAPI logon password can be specified if required.

ODEX Enterprise solution

In ODEX Enterprise, there is a Send Email action and a Send E-mail job that map directly to the Send E-mail action in Odex Professional.

Both have to/from addresses, a subject and a body and can handle attachments.

NOTE: There is no password functionality.

Execute an Application (Event Manager)

In ODEX Professional

Execute an Application allows the user to specify an application, arguments for the application and various other details to run the application. The action runs the application as specified by the user.

ODEX Enterprise solution

In ODEX Enterprise, the Run Application action and Run Application job map directly to the Odex Professional Execute an Application action.

Execute an Application (Event Scheduler)

In ODEX Professional

Execute an Application allows the user to specify an application and working directory to run the application. The action runs the application as specified by the user.

ODEX Enterprise solution

In ODEX Enterprise, the Run Application action and Run Application job map directly to the Odex Professional Execute an Application action.

Call Network

In ODEX Professional

Odex Professional makes a call to the specified network.

ODEX Enterprise solution

In ODEX Enterprise, the Call Network action and Call Network job map directly to the Call Network action in Odex Professional.

File Based Report

In ODEX Professional

Writes a set of text and placeholders to a specified file. Can append or create new file.

ODEX Enterprise solution

In ODEX Enterprise, the Write File action and the Write To File job map directly to the Create a File Based Report action in Odex Professional.

Write To Windows Application Log

In ODEX Professional

This allows the user to specify the details of a log message to write to the Windows Application log. It is written with the specified type, ID and message. If specified it can be written to a different machine.

ODEX Enterprise solution

The ODEX Enterprise Write to Windows Application Log action and Write to Windows Application Log job map directly to the ODEX Professional Write to Windows Application Log action.

Other Events

The following events in ODEX Professional map directly to events in ODEX Enterprise:

- ODEX Error maps to General System Error
- System Error maps to General System Error
- Local Call Failure maps to Call Failed (Direction = Outgoing)
- Node Retry Limit Reached maps to Call Retry Limit
- Outgoing Call Failed maps to Call Failed (Direction = Outgoing)
- ODEX End maps to Server Stopped
- ODEX Started maps to Server Started
- ODEX Starting maps to Server Starting
- Database Sweep Complete maps to Database Sweep Completed
- Incoming Session End maps to Call Ended (Direction = Incoming)
- Incoming Session Start maps to Call Started (Direction = Incoming)
- Outgoing Session End maps to Call Ended (Direction = Outgoing)
- Outgoing Session Start maps to Call Started (Direction = Outgoing)
- Invalid Receipt Received maps to Unexpected Receipt Received
- Remote Call Failure maps to Call Failed (Direction = Incoming)

- Remote File Rejection maps to File Not Sent

Files Received

These events map to the point in ODEX Enterprise when a file is received and submitted to the workflow manager. Any actions associated with these events can be performed in a workflow that is executed on the received file.

- File Received
- File Received and Analysed

Automation complete/failed

The following events can be fired in ODEX Professional when another event action has completed (when a User Schedule – time based or otherwise) has run successfully or has failed.

- Automated EDI extract complete
- Automated EDI extract failed
- Automated EDI Schedule Completed
- Automated EDI Schedule failed
- Automated non-EDI extract complete
- Automated non-EDI extract failed
- Automated non-EDI Schedule Completed
- Automated non-EDI Schedule failed
- Merge EDI Failed (happens when a translation fails during automated extraction)

The actions for the “completed” events are added to ODEX Enterprise as workflows, and the workflows added to the end of channels created for the Extract and Schedule events. They are effectively extensions of the workflows for Extract EDI, etc…

The actions for the “failed” events are added to ODEX Enterprise as error workflows for the workflows created for the Extract and Schedule events. They are effectively error handlers of the workflows for Extract EDI, etc…

Comms triggers

The following events are all triggered by events in comms. In ODEX Enterprise these are worked into the workflows required for sending and dealing with received files. For example, waiting for an EERP to be received (using the Wait For Acknowledgement job) before doing the actions associated with the event.

The note alongside each event indicates how and where it is added to ODEX Enterprise during an upgrade.

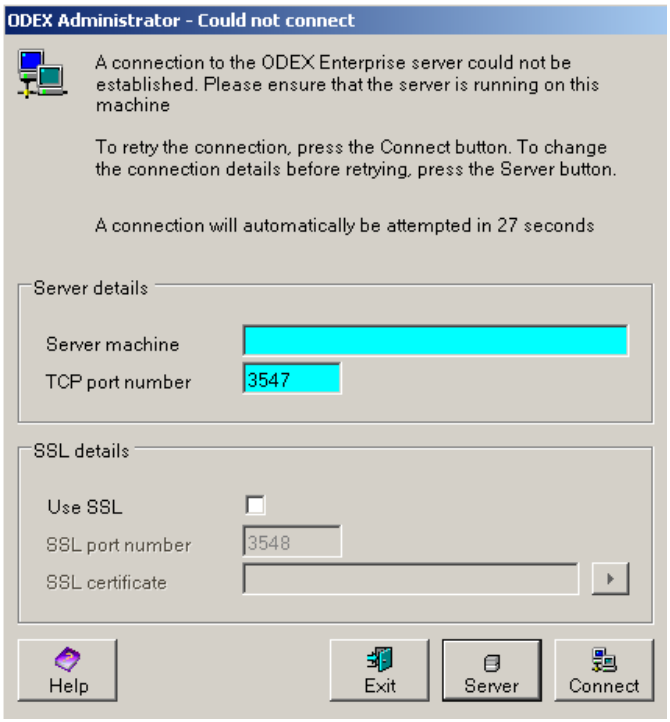
- **Receipt received** – insert Wait For Acknowledgement job and then associated actions after any Schedule job added as part of the upgrade
- **File Acknowledgement Timeout** – insert Wait For Acknowledgement job and then associated actions as error handlers after any Schedule job added as part of the upgrade

- **File Transmission Timeout** – insert Wait For Transmission job and then associated actions as error handlers after any Schedule job added as part of the upgrade
- **File Transmitted** – insert Wait For Transmission job and then associated actions after any Schedule job added as part of the upgrade
- **File Extracted (for automated file extraction)** – insert associated actions after any Copy job added as part of the upgrade

First time use

Server location

If you did not install the server on your local machine (i.e. the one you are currently using), then the first time you try to start an ODEX application after installation or after upgrade, you will see a dialog box telling you that the client cannot currently connect to the server. You must click the 'server' button to specify the name or IP address of the machine the server is running on.



Type the server name or its IP address in the Server name field.

The Port number will only need to be changed if it is being used by other software on that machine.

If your server is configured to accept SSL connections, select the 'Use SSL' checkbox. You must then specify the certificate to be used for authentication by clicking the button next to the SSL certificate field.

Click **OK** to continue starting the ODEX application.

ODEX Server Overview

Introduction

In this section we will show you what the ODEX Server GUI looks like and how to use it. Please remember that the ODEX Server is the control centre of ODEX and as such should not be made accessible to unauthorised personnel.

The ODEX Server GUI

When the ODEX Server is up and running, you will see the Server icon in the system tray (this is usually at the right hand side of the task bar, which in turn is usually at the bottom of your screen). It looks like this: 

To show the ODEX Server GUI, click on the Server icon with your right-hand mouse button. This will bring up a popup menu with the options: **Stop**, **Restart**, **Control panel**, **System log** and **Shut Down**. Choose the **Control panel** option to see the GUI, as shown below.

The GUI is split into three sections: Product Details, Registration Details and Data Interchange Plc. Below these are the options available to you in the form of buttons. At the very bottom is the status bar, which shows the current status of the ODEX Server. In the example above, the status of the server is "Running".

Product Details

This section tells you the Server Name and the Product Version. These details are important and should be quoted if you ever need to contact Data Interchange Plc for support purposes.

Registration Details

This section shows the registered User Name, your Company name and the product Serial Number. These details should also be quoted if you ever need to contact Data Interchange Plc for support purposes.

Data Interchange Plc

This section gives the contact details for Data Interchange Plc. You will need these if you ever have to contact Data Interchange Plc for support purposes.

Action Buttons

These buttons cover all the actions you can perform on the ODEX Server GUI.

Start – On the example above, this button is disabled because ODEX is already started.

Stop – This button stops the ODEX Server. This means that the Server stops working until the **Restart** button is used. If the ODEX Server is stopped, none of the client applications can continue working. Any users logged on will be disconnected.

Restart – This button can be used to stop and restart the ODEX Server. Any users logged on will be disconnected.

Hide – This button minimises the ODEX Server GUI, so that it can only be seen as an icon in the system tray.

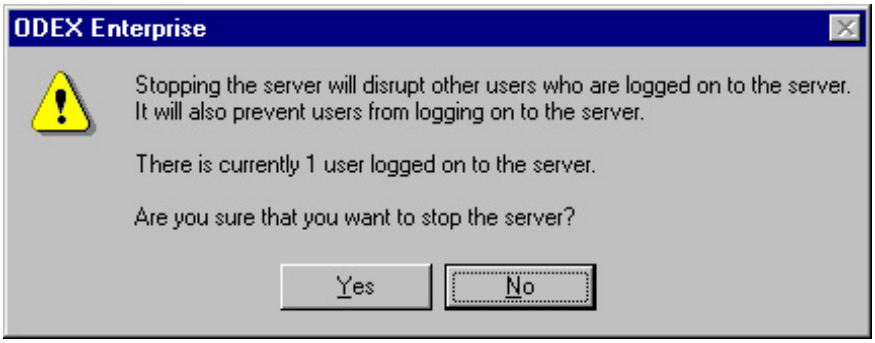
Shut Down – This button stops the ODEX Server and closes the application down. Any users logged on will be disconnected.

Obviously, the **Stop, Restart** and **Exit** buttons should only be used by authorised personnel and only with good reason.

Stop server warning dialog

If you try to stop, restart or shut down the server, you will see a message box warning you that this action will disrupt other users who are currently logged on to the server. The message tells you how many users are currently logged on.

If you are still sure that you want to stop, restart or shut down the server, you should click **Yes**. If you want to wait until there are no users logged on to the server, you should click **No**.



Failure to connect to server warning dialog

If you try to start an application when the server is not running, you will see a message box telling you that the application has failed to connect to the server.

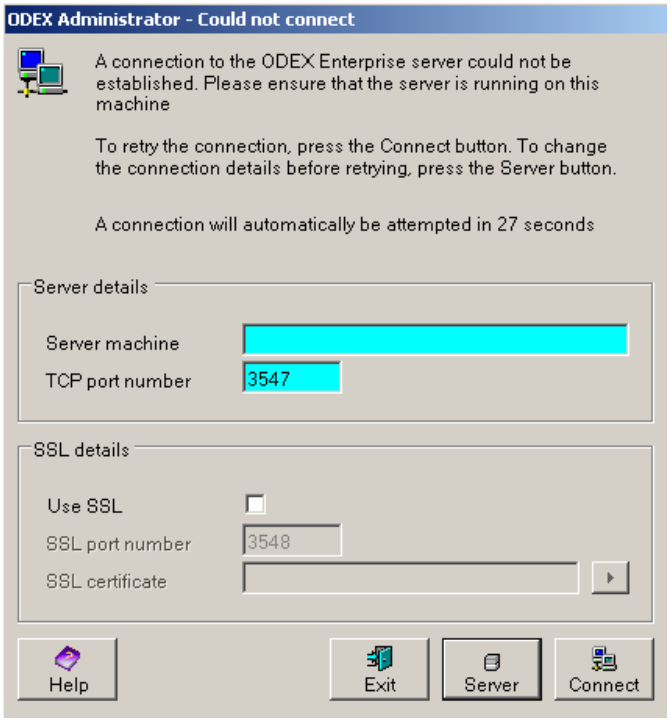
The message box will show a countdown from 30 seconds, at which point the application will attempt to connect to the server again. If you want to try and connect to the server before the countdown ends, press the **Connect** button. If the connection still cannot be made, the message box will appear again.

If you do not press the **Connect** button, the application will try to connect to the server every 30 seconds until it is successful.

There are several possible reasons why you might be unable to connect to the server, such as:

- the server has been shut down
- the server's cable has become unplugged
- the server machine reference was mistyped when installing the application
- the server has been renamed
- the server has been moved from one machine to another
- the client failed to authenticate with the server

If you have reason to believe that the server has been renamed, or that the location of the server has changed, press the **Server** button. This will expand the dialog to show you the current information about the name and location of the server.



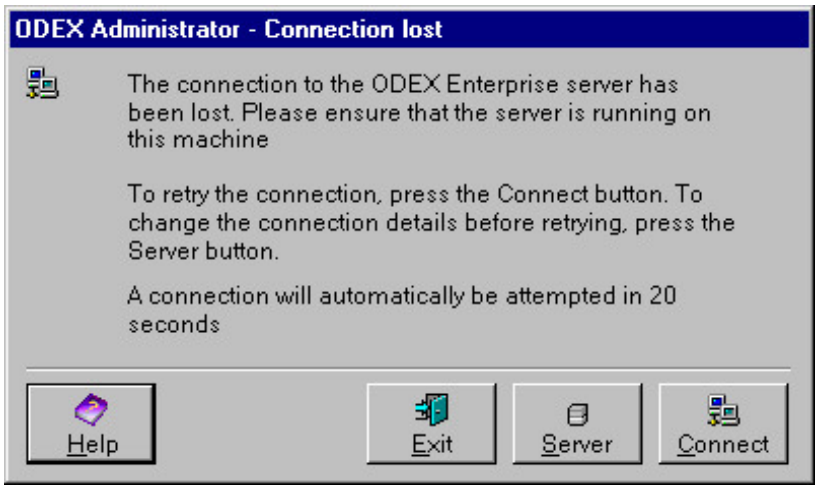
If you know the new location or new server name, type it into the Server machine field. If necessary, type the new port number into the Port field too. If the server is configured such that you are required to use SSL to connect, select the check box. If necessary, enter the port number and click the button to the right of the field to select an SSL certificate. For more information on selecting a certificate, see the section entitled 'Select certificate dialog'.

Now click the **Connect** button again. If you are still unable to gain a connection to the server after this, please refer to your IT Manager.

If you want to stop trying to connect, press the **Exit** button.

Server connection lost warning dialog

If, for whatever reason, your connection to the server is lost while you are using an application, you will see a message box telling you that the connection to the server has been lost.



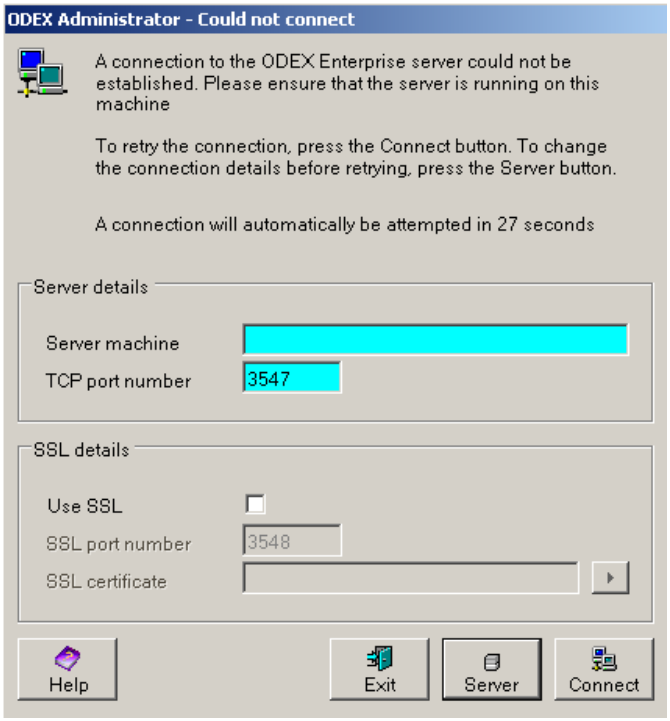
The message box will show a countdown from 30 seconds, at which point the application will attempt to connect to the server again. If you want to try and connect to the server before the countdown ends, press the **Connect** button. If the connection still cannot be made, the message box will appear again.

If you do not press the **Connect** button, the application will try to connect to the server every 30 seconds until it is successful.

There are several possible reasons why you might be unable to connect to the server, such as:

- the server has been shut down
- the server's cable has become unplugged
- the server has been renamed
- the server has been moved from one machine to another

If you have reason to believe that the server has been renamed, or that the location of the server has changed, press the **Server** button. This will expand the dialog to show you the current information about the name and location of the server.



If you know the new location or new server name, type it into the Server machine field. If necessary, type the new port number into the Port field too. If the server is configured such that you are required to use SSL to connect, select the check box. If necessary, enter the port number and click the button to the right of the field to select an SSL certificate. For more information on selecting a certificate, see the section entitled 'Select certificate dialog'.

Now click the **Connect** button again. If you are still unable to gain a connection to the server after this, please refer to your IT Manager.

If you want to stop trying to connect, press the **Exit** button.

Logging

Logging is a very useful feature of the ODEX software. Most of the time you will probably not come into contact with it, but it can be used to help you sort out any problems, in conjunction with our Support department.

There are various types of log within ODEX: the Server log, the Startup log and the client logs. The Server log and the Startup log are always used, but the client logs are an optional feature. Let's have a look at where you can find each log and what purpose each serves.

Server log

The Server log can be viewed from the System Log section of the ODEX Administrator. It shows in "real time" what the Server is currently doing i.e. the log is updated on your screen as events occur.

Previous Server logs can be viewed by using the **Load** button on the Archive page tab of the System Log section.

You can choose to include different types of log messages in the log, by selecting them from the **Log Type** button.

You can also choose how much information you want to see for each log message, by selecting column headings from the **View** button.

Startup log

The Startup log, as its name suggests, is created each time you start up the ODEX Enterprise Server. It contains information specific to what occurs when the Server is started, such as the initialisation of various Server components and various other tasks.

You can view the Startup log by selecting the "Single startup log file" option on the Load dialog. (The Load dialog is accessed using the **Load** button on the Archive page tab of the System Log section of the ODEX Administrator).

Once this option has been selected, you can choose a startup log to view by using the dropdown arrow alongside the Filename field.

You will normally see that there are several Startup logs in this directory – one for each time the Server has been started. The naming convention for the Startup log makes it easy to find the correct one if you want to view the contents for a particular startup. The naming convention is as follows:

The first 7 characters will always be STARTUP

The next 8 digits will be the date of the log in DDMMYYYY format (in the example below, the date is 06102003 i.e. October 6th 2003)

The next 6 digits will be the time of the log in HHMMSS format (in the example below, the time is 101741 i.e. 10:17a.m. and 41 seconds.

Each file ends with .log

Example – STARTUP06102003101741.log

Client logs

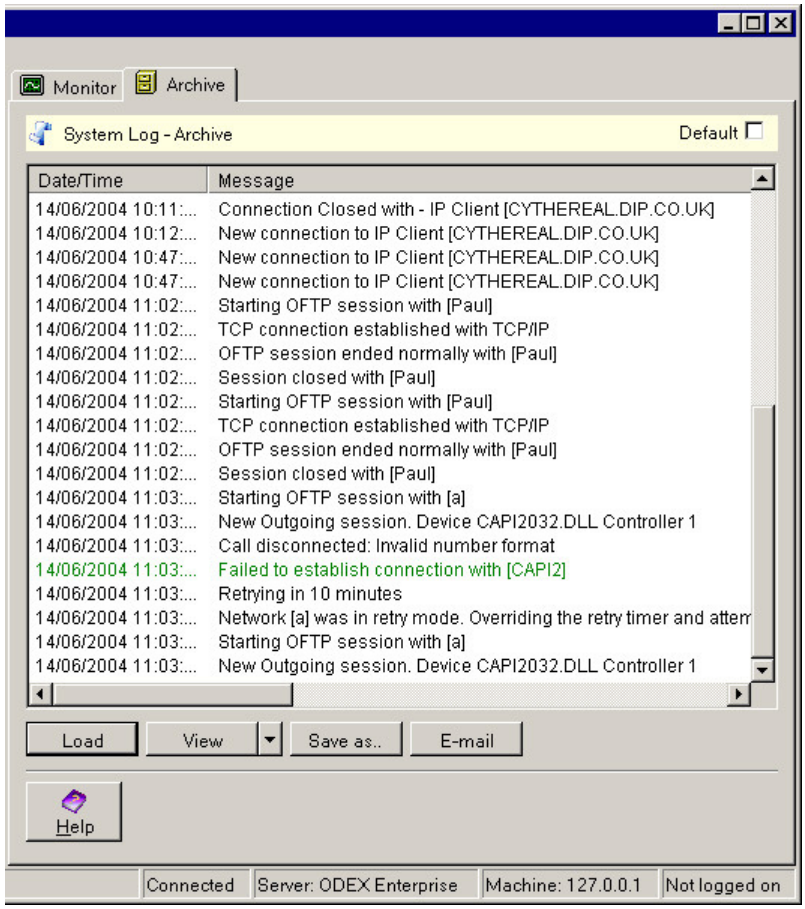
The Client logs are only useful for support purposes and we do not expect you to have much need for them. The Client logs are not available until you have specifically requested them using the Options dialog in each of the applications. For details of how to do this, please refer to the description of the Logging page in the section entitled "Options dialog".

How to use the logs

Why might you want to view the log files, and how do you know what to look for? First of all, it is important to stress that you may never have to use the logs at all. ODEX has been created to be as failsafe as possible, but there are still

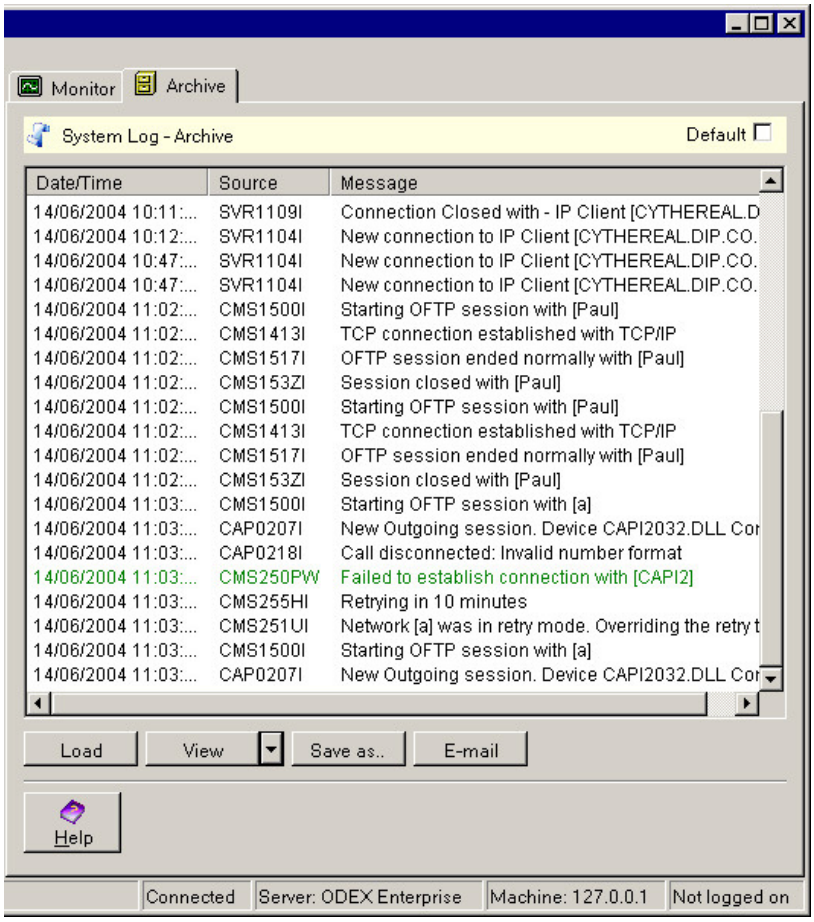
times when something may cause an error and you will need to find out what went wrong. Usually ODEX will spot an error condition and inform you, with a message box, of the action you need to take to rectify it. Occasionally an error will be such that you cannot correct it by immediate action, and this is when an error message will be generated in one of the log files.

Now let's have a look at the contents of a log file, so you can understand what you are looking at. The default settings for all the logs is to show just the Date/Time and Message columns. These two columns are shown in the example below.



Use the **View** button to select the Source column as well. You can select other column headings to be included, but the Source column contains the information you need to look for.

Below is the same log file, now showing the Source column too.



The log gives you a chronological picture of what has been happening in ODEX.

The Date/Time column pinpoints the exact date and time at which an event occurred.

The Active Session ID and Unique Session ID (if you choose to show them) show an ID related to a communications session. These columns are only relevant if you are having problems with the communications side of ODEX.

The Type column (if you choose to show it) indicates what type of log message this is (SQL refers to the query language used to obtain information from the ODEX database, while Xn refers to a message relating to a transaction within ODEX).

The Source column shows a unique message identification code which indicates exactly which part of the ODEX software has generated the message. The last letter of the message identification code indicates the severity of the message: "I" means Information, "T" means Trace, "W" means Warning, and "E" means Error.

The Message column shows you the actual message that has been logged.

When you are checking the log for error messages, you should be looking for message identification codes ending with the letter "E".

You should then e-mail our Support department, sending them the following information:

The log in which the error code has been generated, preferably highlighting the line(s) relating to the error, or giving the exact date and time of the error as shown in the log.

Information about the type of log i.e. Server log, Startup log or specific client log.

A description of the error i.e. what caused you to realise there had been an error.

Our Support department will then be able to tell you how to resolve the error.

ODEX Applications Overview

Introduction

In this section we will show you what the ODEX applications look like, what their function is and, in general terms, how to use them. For full details of how to use each application please refer to the appropriate chapters later in the guide.

The ODEX applications, listed below with their shortcut icons, are:

- ODEX Administrator 
- Communications Monitor 
- ODEX Workstation 
- ODEX Batch Administrator 

You can start each of the applications from their short cut on your desktop, or from the Start menu, using **Start >> Programs >> Data Interchange Plc >> ODEX Enterprise**

ODEX Administrator

The ODEX Administrator is the administrative control centre of ODEX. Before you can begin to use ODEX to process your files, you must use the ODEX Administrator to set up all your details, including information about your company, your trading partners, and your communication details. The ODEX Administrator is also used to set up the ODEX application to suit your system requirements.

What does the Administrator do?

The ODEX Administrator consists of three configuration and management areas – the System Administrator, the Comms Administrator and the Workflow Administrator.

System Administrator

The System Administrator is responsible for the administrative aspects of the ODEX system. It covers such areas as Licence Codes, the System Log, System Settings, Retention Periods, Schedules, Event Actions, Users and User Groups. All these things are explained in full detail in the section entitled "System Administrator".

Comms Administrator

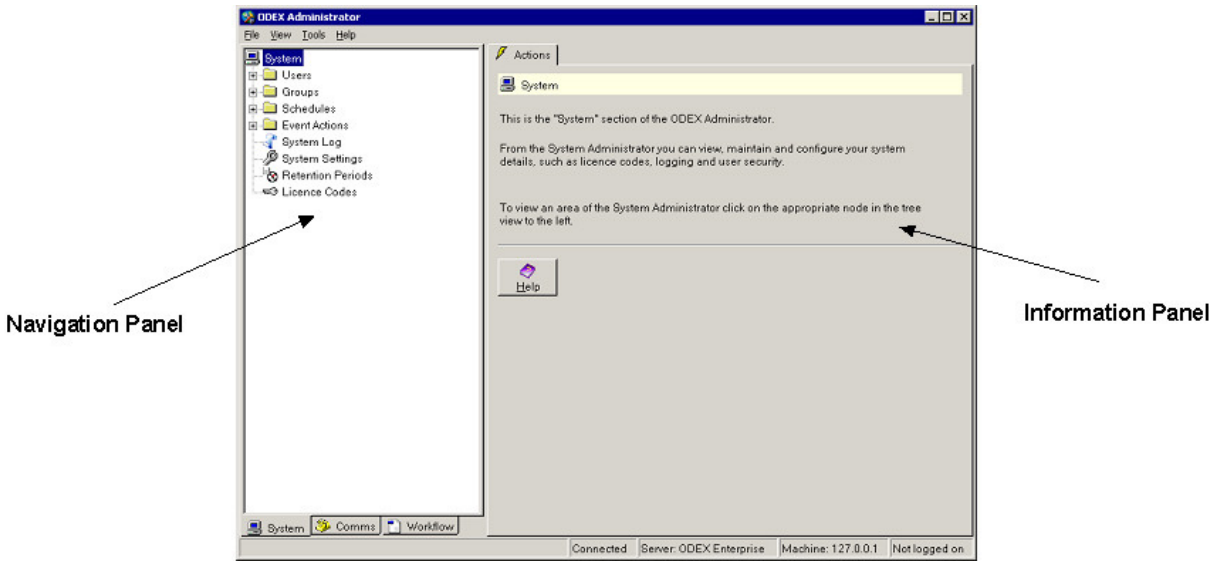
The Comms Administrator is responsible for all matters relating to the ODEX communication system. It covers such areas as your own company's internal networks, your trading partners and their communication details, the communication details of the clearing centres you have accounts with, and sub-systems. All these things are explained in full detail in the section entitled "Comms Administrator".

Workflow Administrator

The Workflow Administrator allows you to configure how you want ODEX to process the files in your system. Its flexibility means that you can process any file from any trading partner in exactly the way you require. Processing 'channels' can be defined according to trading partner, data source and data type. Everything you need to know about how to configure these details is explained in full detail in the section entitled "Workflow Manager".

Finding your way around the Administrator

The diagram below shows the Actions page of the System Administrator. As you can see, the screen is divided into two main sections. On the left is the Navigation Panel, and on the right is the Information Panel. This division of the screen is found throughout the ODEX Administrator.



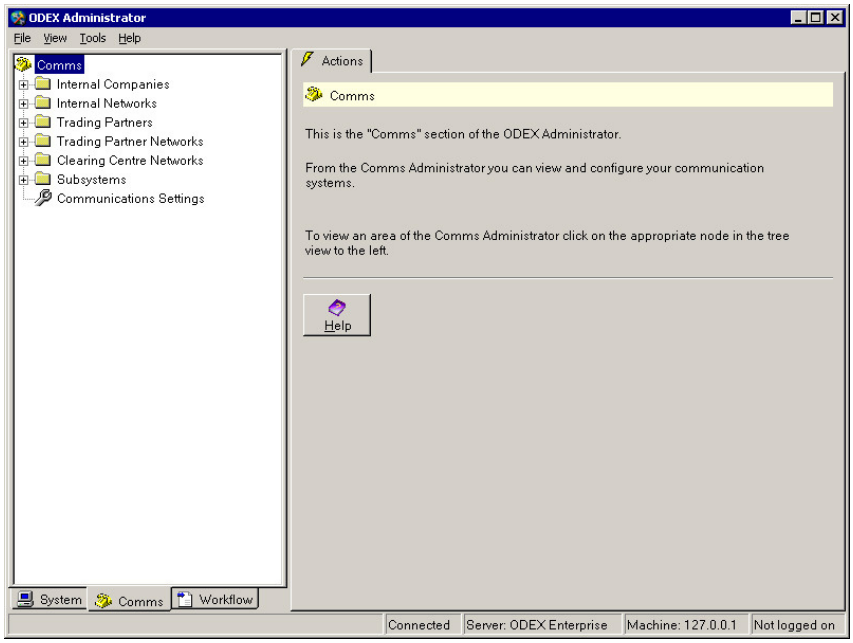
The System Administrator, the Comms Administrator and the Workflow Administrator are accessible via page tabs at the bottom of the Navigation Panel. Simply click on the appropriate page tab to see the list of items within each. You can then use the tree view in the Navigation Panel to find your way around.

The Navigation Panel

The Navigation Panel provides you with a simple way of making your way round (i.e. navigating) the ODEX Administrator.

System, Comms and Workflow Administrators

In each of the Administrator areas, the Navigation Panel shows a vertical list of items within the ODEX Administrator, in the form of a tree view.



This is a convention you will be familiar with if you have ever used the Microsoft Windows Explorer. A tree view shows a vertical list of items. As shown in the example above, the items in the Comms Administrator are Internal Companies, Internal Networks, Trading Partners, Trading Partner Networks, Clearing Centre Networks, Subsystems and Communication Settings.

Any items with a plus sign on their left contain entries which can be seen if you click on the plus sign with your mouse (or use the arrow keys on your keyboard to highlight the item, then the right-arrow to see the entries). The plus sign then becomes a minus sign, which, if you click on it (or use the left-arrow on the keyboard), will hide all the contents again. Some entries may even have their own sub-entries, which can be viewed in the same way. Entries or sub-entries without a plus or minus sign contain no further sub-entries.

Clicking on one of the items in the Navigation Panel will display the default page for the selected item, from where you can edit its details.

Default pages

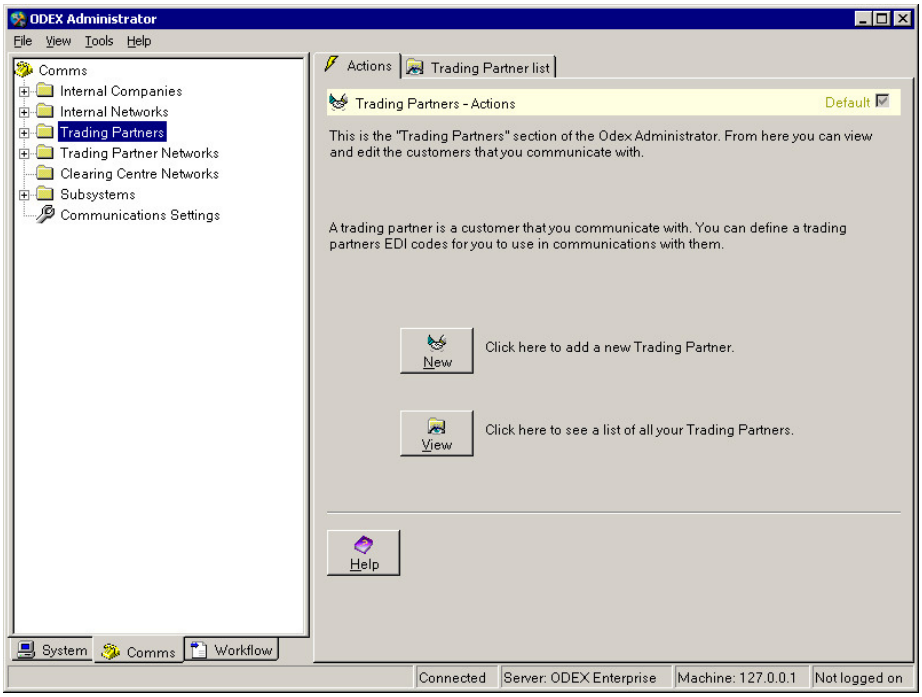
The concept of default pages is used throughout the ODEX Administrator. Each section of the ODEX Administrator consists of one or more pages, accessible via page tabs at the top of the page. The default page is the page that is shown to you when you open up a new item. For most items, the default page will initially be the Actions page, which describes what you can do with the entries in the selected section.

If you want to change the default page setting for any section, this is how they work. At the top of every tab page is a title banner, at the right-hand side of which is the default page tickbox. If the box is ticked, it indicates that this is the default page for this section. When you first use ODEX, the default page is always the leftmost tab of a section. If you prefer a different page to be the default, simply select the tickbox from one of the other pages. Next time you open up this section, the default page will be the one you have chosen.

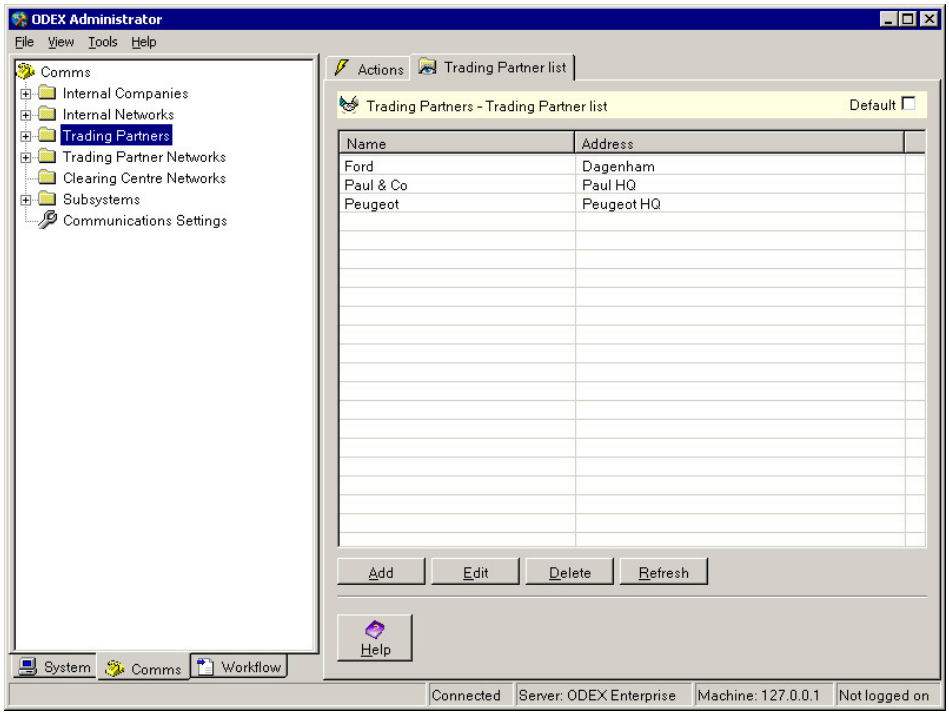
How to use the Administrator

There are two ways to navigate the Administrator, either via the Navigation Panel or via the Information Panel.

Let's take one of the items in the Navigation Panel and explain the differences. The example below shows that the Trading Partners item has been selected from the Navigation Panel, showing you the default page in the Information Panel.

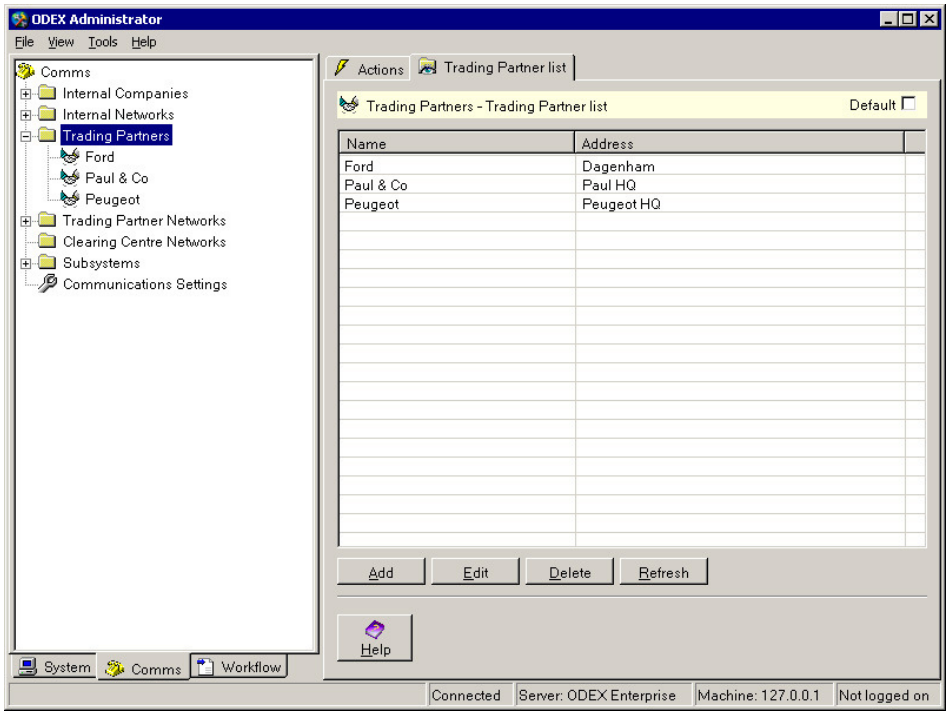


If you then click on the list page tab (the Trading Partner list tab in our example), or click the **View** button, you will see a list of all entries in this section in the Information Panel. This is illustrated below, where the list of all Trading Partners is shown.

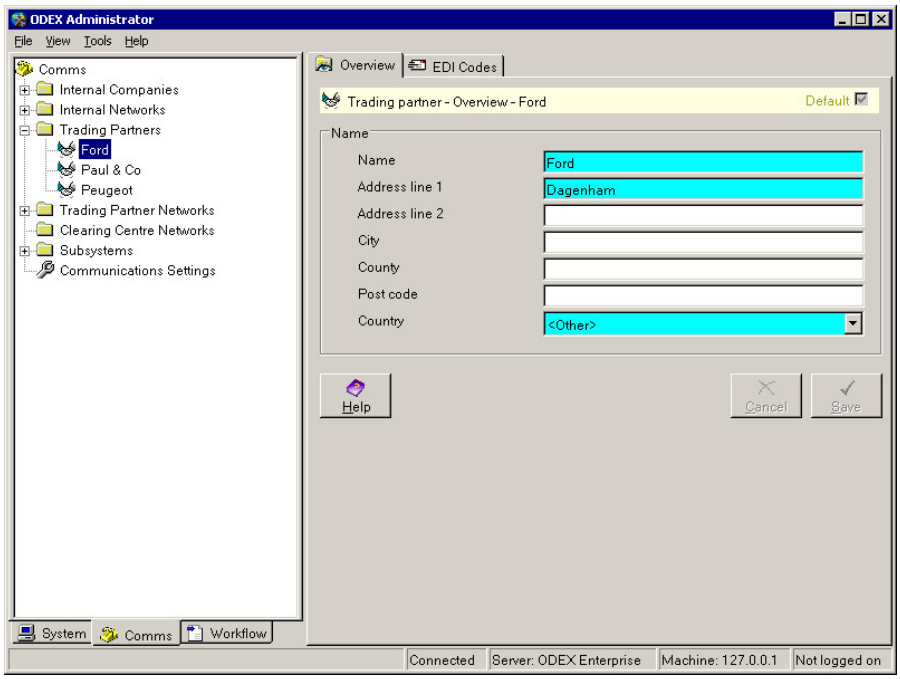


You can then select a trading partner from the list on the right (the Information Panel) to edit or delete, using the buttons at the bottom of the Information Panel.

You can also see the same list in the Navigation Panel, by clicking on the plus sign to expand the selected item, as shown in the illustration below.



Clicking on an entry in the expanded tree view, or double-clicking on an entry in the Information Panel, will bring up the details of the selected entry in the Information Panel on the right, as shown below.



In the above example, a trading partner in the tree view has been selected and its details are shown in the Information Panel on the right. These details can then be edited. Note that the details are held on one or more pages (in this example the pages are Overview and EDI Codes) that can be opened using the page tabs at the top of the screen.

Context menus

You can also use context menus, available by right-clicking on a folder in the tree view, to expand or collapse a tree node or to add a new object to that folder.

Summary

- To **view** all entries for an item, use one of these methods:
  - In the Navigation Panel, expand the item by clicking on the plus sign on its left.
  - In the Navigation Panel, expand the item by right-clicking on the appropriate folder and selecting Expand from the context menu.
  - In the Navigation Panel, click on the item's name to see the default page in the Information Panel, then select the list page tab or the **View** button.
- To **add** a new entry to a list, use one of these methods:
  - In the Navigation Panel, click on the item's name, then select the Actions page in the Information Panel and click the **New** button.
  - In the Navigation Panel, right-click on the appropriate folder and select New Object (e.g. New Trading Partner)
  - Use the third View method above to see all entries for an item, then click the **Add** button.
- To **edit** an entry in a list, use either of these methods:
  - In the Navigation Panel, expand the item by clicking on the plus sign on its left. Find the entry you want to edit in the expanded list and double-click on it with your mouse. This will bring up its details in the Information Panel.
  - Use the third View method above to see all entries for an item, select the entry you want to edit from the list, then click on the **Edit** button.
- To **delete** an entry from a list, use this method:
  - Use the third View method above to see all entries for an item, select the entry you want to delete from the list, then click on the **Delete** button.

ODEX Communications Monitor

The communications monitor allows users to view statistics and live information about communications sessions in ODEX Enterprise. This client application is purely a monitor and therefore has very little functionality. Other clients are available for the functional aspects of ODEX Enterprise.

ODEX Workstation

The workstation application is the main day-to-day usage application of ODEX Enterprise.

Initially, unless restrictions have been made under ODEX security, you can see a list of inbound and outbound workflow files, files that have been received, sent or scheduled via ODEX comms, as well as error files and archived files. You can also manually schedule files and extract files from the system.

Advanced users can add and remove views, and create named, customised views of the system, which they will be able to filter.

You can also make calls and view the communications log while a call is being made.

ODEX Batch Administrator

The ODEX Batch Interface allows you to automate tasks such as setting up new Comms entries, scheduling files for immediate sending and many other tasks.

If you have a sequence of operations to be performed regularly or if you want ODEX to be run by non-computer personnel, you may automate it by setting it to run in batch mode.

The Batch Administrator allows you to configure the settings for running ODEX in batch mode.

Common Features

Now let's have a look at the features of ODEX that are used throughout the system.

Menu bar

Each application has a menu bar at the top showing several menu options. The options common to each application are:

- File
- View
- Tools
- Help

Selecting any of these options will present you with further options.

File option

The File option allows you to do the following:

- Log off from the ODEX application (only applicable if User Security is enforced)
- Disconnect the application from the ODEX server (reconnect using the **Connect** button on the "Lost connection" dialog that appears)
- Exit from the ODEX application

The Log Off option allows you to change the user of the application without closing the application down. For full details of this option, please refer to the section entitled "Logon dialog".

View option

The View option contains a variety of sub-options which differ according to which application you are looking at. Each option is described in the relevant section.

Tools option

The Tools option contains the following sub-options:

- Options
- Upgrade Settings
- Change Password (only applicable if User Security is enforced)
- ODEX Professional Import (only applicable to the Administrator application)
- Print Odex configuration report (only applicable to the Administrator application)

The Options dialog allows you to configure certain information within the ODEX application. It also allows you to select the language in which you want to run

the ODEX application. For full details of this dialog, please refer to the section entitled "Options dialog".

The Upgrade settings option will only be available if you have any previous versions of ODEX Enterprise installed on your computer. This option allows you to copy settings, such as those from filters and display styles, from a previous version to the current version. For full details of this option, please refer to the section entitled "Upgrade settings dialog".

The Change Password option allows you to change your password at any time while using an application. For full details of this option, please refer to the section entitled "Change password dialog".

The ODEX Professional Import option allows you to import your User Directory details, your Received, Scheduled and Sent file details, and most of your scheduled events, time profiles and event manager events from ODEX Professional to ODEX Enterprise. For full details of this option, please refer to the section entitled “Import Wizard”.

The Print Odex configuration report option allows you to print or view a report that shows your current Channel configuration details. For full details of this option, please refer to the section entitled “Channel configuration report”.

Help option

The Help option gives you access to the following:

- The page(s) of the ODEX on-line Help manual that describe and explain the application
- A dialog giving technical details about the application

Status bar

The status bar tells you about the current status of the application. There should be 5 different status boxes. If there are fewer, it means the application is not connected to the server. You must be connected to the server in order to use the application.

- Box 1 - tells you the status of the application e.g. Ready. It will also inform you if the displayed data is out of date – just click the Refresh icon to update it.
- Box 2 – tells you if the application is connected to or disconnected from the server
- Server – tells you the name of the application running on the server to which the application is connected (in this case, ODEX Enterprise)
- Machine – tells you the name of the machine (computer) on which the server is installed
- Username – tells you the logon name of the user who is currently using the application

Tabs

Tabs allow you to see different pages of the screen you are looking at. They are usually found at the top of the information on the screen, and look like the page markers of a binder. Each tab displays an icon and a caption, to indicate the contents of the page it is marking. Simply click on the tab with your mouse to open that page.

The only exception to their positioning is in the ODEX Enterprise Administrator, where the tabs are found at the bottom of the Navigation Panel.

Mandatory fields

Within most of the ODEX Enterprise applications, there are dialogs which require you to provide information. Some of this information is optional i.e. you may provide it if you wish or omit it if you prefer. Other information is mandatory i.e. you must provide it before ODEX will allow you to close that dialog. All mandatory fields have been given a bright blue background.

Context menus

Context menus are only available in ODEX Workstation. A context menu is a shortcut to the options contained in the main menu Actions option. A context menu is not visible until you hold your mouse over the data area of a page and click the right mouse button. A menu will then appear, from which you can select an option by pointing your cursor at it to highlight the option, then pressing the left mouse button. As the name suggests, the options contained in a context menu are dependent on the page you are currently looking at.

"Hot" keys

For people who prefer to use the keyboard rather than the mouse, a hot key can be used as a quick way to get at menu options from the menu bar.

To use the menu bar with the keyboard, press the **Alt** key to make the "hot keys" visible on the menu bar. Each option on the menu bar will now have a letter underlined to indicate the hot key. Having pressed the **Alt** key, press the letter indicated by the hot key of the option you want e.g. **Alt+F** for the File options. This will show you a dropdown menu which you can then navigate in two ways.

One way is by using the up and down arrow keys on your keyboard. When the option you want is highlighted, hit the **Enter** key to select it.

The other way is by using the hot key of the dropdown menu item you want. The hot key may be indicated by being underlined, otherwise it will be the first letter by default. To use the appropriate hot key, just press the matching letter on the keyboard. This method is indicated in the user guide by the convention **Alt+F+P** for example.

Hot keys are also used on dialog buttons in exactly the same way.

Short cuts

Short cuts are something you will become familiar with as you use ODEX. They allow you to get to menu options directly instead of making your way via dropdown menus etc. When you begin, if you are using the menu bar options, you will see that alongside some of the dropdown options is a reference to one or more keyboard keys. For example, if you select the View menu option, the resulting dropdown menu shows Filter…. **Ctrl+F** and Refresh **F5**. These are the short cuts for these particular options. Once you have remembered the short cut keys, you can use the short cut from the main view to go straight to the option. For example, pressing **Ctrl+F** from the Confirmed Orders view will take you straight to the Confirmed Orders filter dialog.

Tick boxes

The data area of each view contains data lines appropriate to the particular view. For example, the Orders view data area contains order lines, while the Despatches view data area contains despatch lines.

To select one or more specific lines, place the tip of your cursor (which is in the form of an arrowhead) in the tickbox to the left of the required line and click the left mouse button. This will make a tick appear in the tickbox. Do the same for any other lines you wish to select.

Alternatively, using the keyboard, use the tab key and arrow keys to highlight a line, then press the space bar to make a tick appear in the tickbox.

If you want to select all the lines in the data area (including any lines you cannot see because there are too many to show at one time), either click the **Select All** button on the context tool bar or click the rightmost option on the menu bar and choose the **Select All** option from the resulting dropdown menu. Alternatively, use the appropriate hot keys as described above.

Tickboxes are also a feature of some of the ODEX filters, described in the following section.

Radio buttons

These are a feature of some dialogs, such as filter dialogs. Radio buttons allow you to choose between two or more mutually exclusive options. Their appearance is of a small white circle alongside a description of each option. The currently chosen option is indicated by a black spot in the radio button.

Filters – Changing the time period

If you want to change the default time period of a filter, you need to select a different option in the Import Date section.

Your five choices are as follows:

- See files for all dates
- See only today's files
- Select a particular number of days (up to and including today) for which you want to see files
- Select a particular number of months (up to and including this month) for which you want to see files
- Select a time period for which you want to see files, using the From and To fields (this is the Custom option)

Last 7 days / Last 6 months

If you select the **Last 7 days** or **Last 6 months** option, you will be able to change the number of days/months in the box, either by clicking on the up and down arrows alongside the number with your left mouse button (up arrow to increase the number of days, down arrow to reduce the number of days), or by using the up and down arrows on your keyboard (after using the **Tab** key to place the focus in the number of days/months box). The number displayed will be the number of days/months (up to and including today/this month) for which you want to see files.

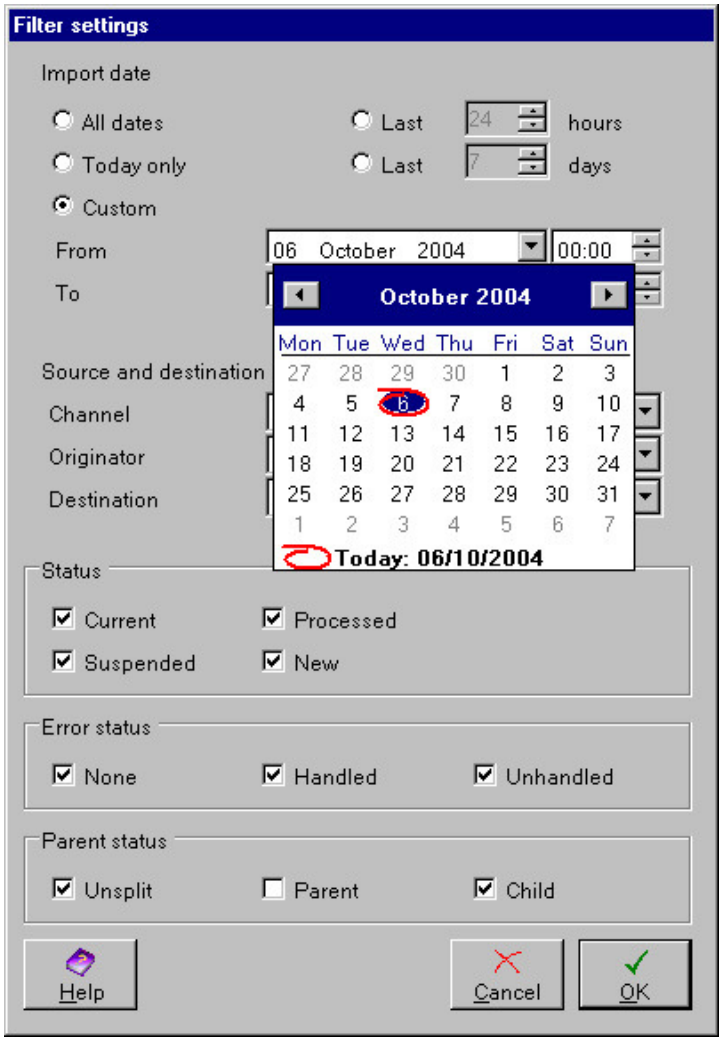
Please bear in mind that, if there are no files for that time period, nothing can be displayed in the data area of the selected view.

Custom

If you select the **Custom** option, you will see that the Start Date and End Date data boxes become available to you (i.e. they are no longer greyed out). To change the dates shown, you have two options:

Highlight the part of the date you want to change, either using your mouse or by using the left and right arrows on your keyboard. Then change that part of the date by using the up and down arrow keys on your keyboard.

Alternatively, with the mouse use the dropdown arrow to the right of the date you want to change. This will bring up a calendar dialog like the one shown below:



The red ring indicates today's date, and the blue mark indicates the date currently shown on the filter dialog. Use your mouse, or your keyboard up and down arrows, to select the date you want. The left and right arrows at the top of the calendar dialog enable you to change the month (left goes back in time, right goes forward in time).

Clicking a date with the left mouse button will return you to the filter dialog with the new date. If you are using the keyboard, press the **Enter** or **Return** button on your keyboard to return to the filter dialog with the new date.

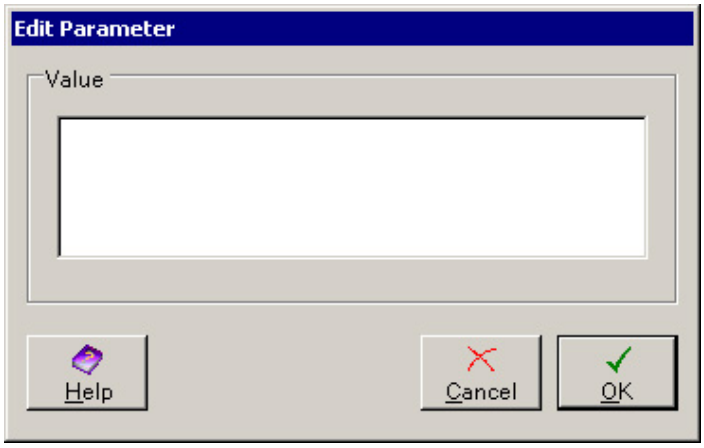
Editing Parameters

Edit Parameter dialogs can be found in the Event Actions section and in the Workflow (Jobs) section. Although some of the dialogs described here are only

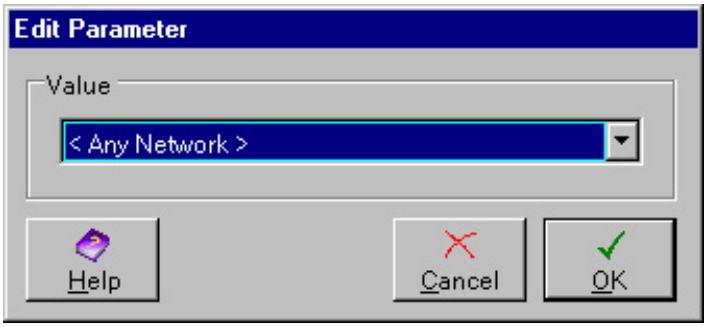
applicable to one of these areas, they will give you a good idea of how to use the Edit Parameter dialogs.

To edit a parameter, simply double-click on the entry in the Parameters list. This will bring up one of several editing dialogs, depending on the parameter you have selected. If the main window of the dialog is coloured blue, this indicates that a value must be provided. White indicates that the parameter is optional (in some cases ODEX provides its own default value that is not displayed, such as the XLATEPC.IDX file for XLATE translation and construction jobs, which is located in the ODEX Enterprise root directory).

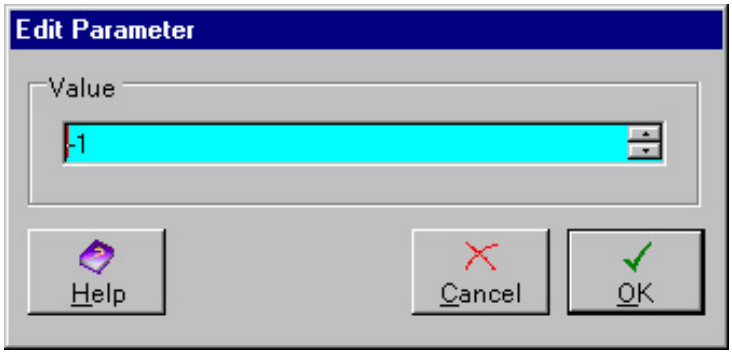
The Edit Parameter dialog shown below is the simplest editing dialog. It allows you to type in the value of the parameter you require. No options are given because this type of parameter is specific to your system.



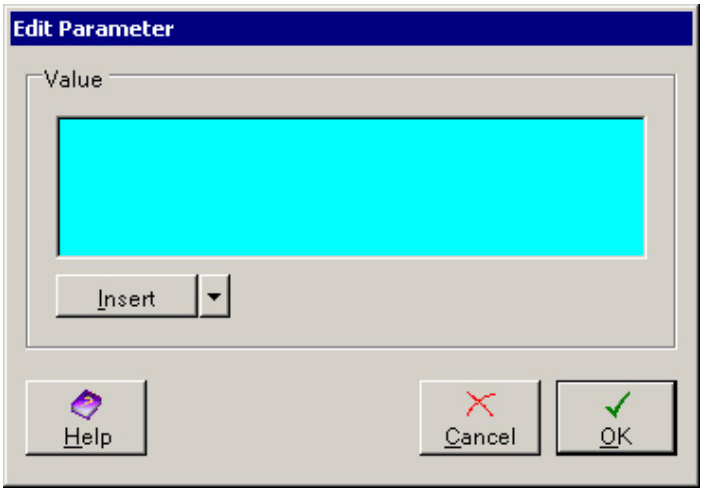
The Edit Parameter dialog shown below is what you will see if the possible values for the parameter are limited to a list of things that have been defined within ODEX, such as networks, as shown in the example. Use the dropdown arrow to see the full list and select the appropriate value.



For any parameter for which a numeric value is required, you will see the Edit Parameter dialog shown below. Use the up and down arrows to the right of the Value field to select the appropriate value.

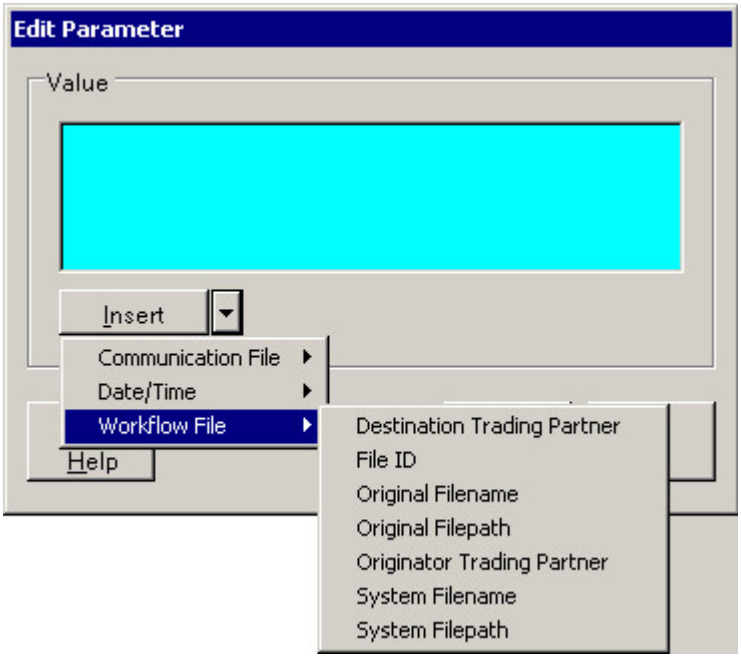


For any parameter for which placeholders can be used, you will see the Edit Parameter dialog shown below (the background may be blue or white).



Here you may type in the appropriate value for the parameter, but you can also include placeholders that are accessible from the **Insert** button. An example of this is shown below, where the list of Workflow File placeholders is displayed.

Placeholders can be used in many of the Edit Parameter dialogs. For example, they can be used to create unique filenames, to route files into directories named after a trading partner, or to provide information in an e-mail. These are just three possibilities, but there are many more. For a full list of available placeholders, please see the section entitled “Placeholders”.



If you select a placeholder from any of the **Insert** button sub-options, the selected placeholder will be inserted at the cursor position.

Placeholders are available for the following Jobs and their parameters:

- Copy – Output Filename, Condition
- Copy (with Xml) – Output Filename, Xml Output Filename
- E-mail – Subject, Body
- Run Application – Application, Arguments, Output Filename, Output Filemask

- Schedule – VFN
- Windows Application Log – Message Text
- Write to File – Filename, Text

Placeholders are available for the following Event Actions and their parameters:

- Run Application – Application, Arguments
- Send E-mail – Subject, Body
- Windows Application Log – Message Text
- Write file – Filename, Text

Common dialogs

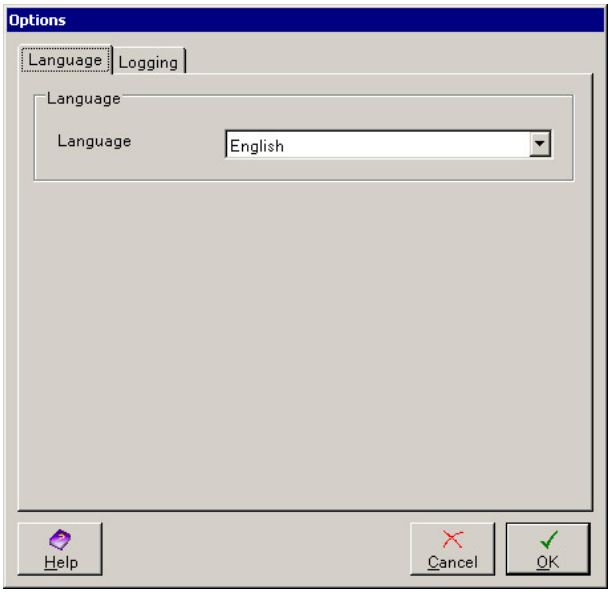
There are several dialogs that you may come across in any of the ODEX applications. These are described below.

Options dialog

An Options dialog is accessible from each of the ODEX applications. The settings shown in the Options dialog are only applicable to the application in which you are viewing them. Likewise, any changes you make will only affect the particular application in which you make those changes.

The Options dialog in the Communications Monitor has an extra page that is described in the "Comms Monitor Options dialog" section below.

When you click on the **Tools >> Options** menu item, you will see the following dialog.



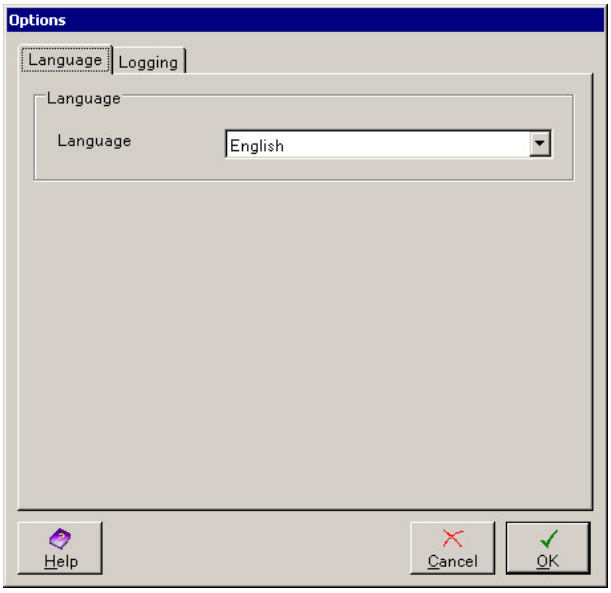
All the Options dialogs share three page tabs:

The **Language page** allows you to select the language in which you want to run the application.

The **Logging page** allows you to turn on client-side logging. This will only be necessary if you are having problems and our Support department has asked you to send them some specific log information.

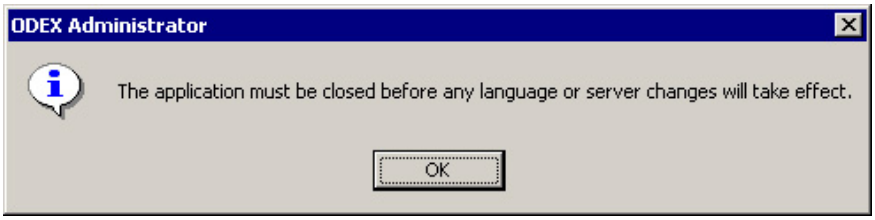
Language page

The Language page dialog is shown below.



This page allows you to change the language in which the application is displayed. Changes made here affect most of the text displayed in the application, including text on buttons, page tabs, field captions and most reports. It does not change the language of the Help files.

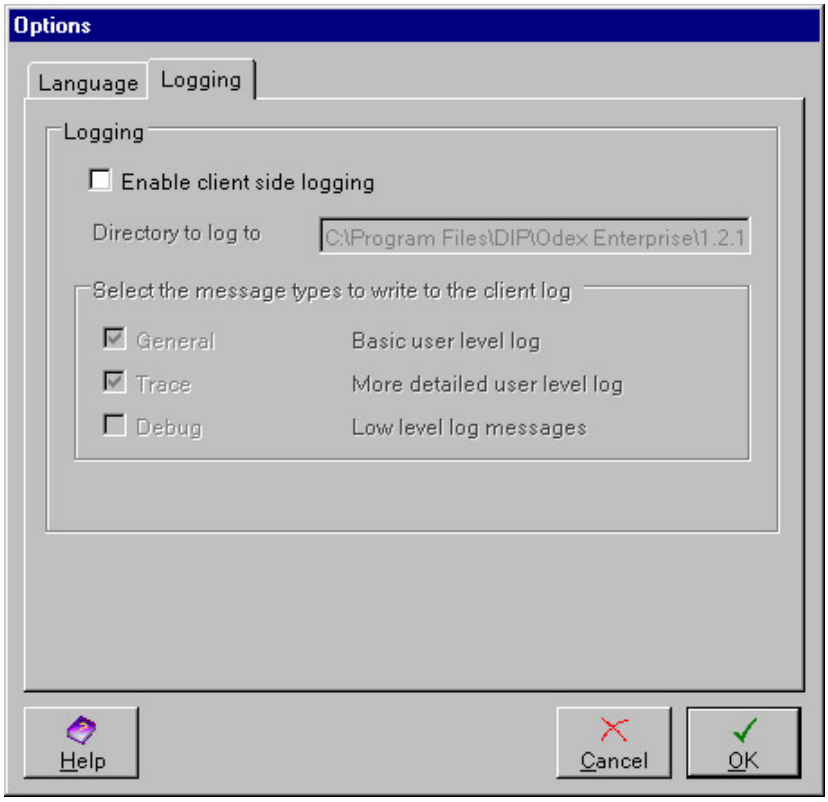
Use the dropdown arrow to view the available languages – currently these are English, German (Deutsch), Spanish (Español), French (Français) and Chinese (simplified). If you select a different language you will see a message warning that you will have to close the application before the change can take effect, as shown below.



Click the **OK** button to return to the Options dialog. You may continue to use ODEX until it is convenient for you to close it down. Then next time you open that application, the language change will take effect.

Logging page

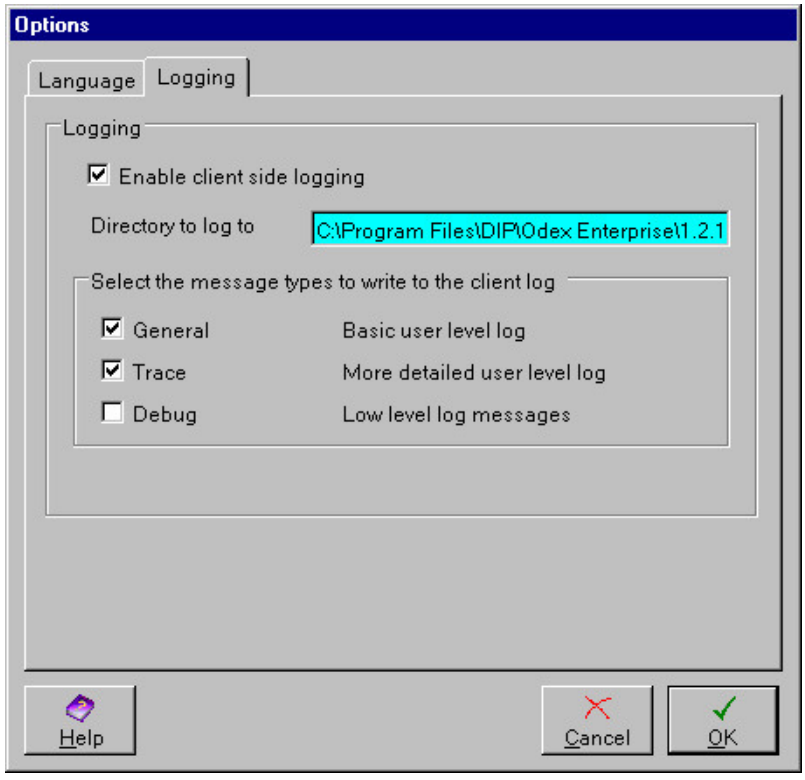
The Logging page dialog is shown below.



When you first open the Logging page, none of the fields are enabled i.e. you cannot edit them. This is because, most of the time, you will never need to use client-side logging.

By default, no log messages are generated by the applications – all log messages in the System Log refer only to activity on the ODEX Server. Server log messages can be viewed using the System Log section of the ODEX System Administrator.

If you want to change these settings, so that logging will also be done for the ODEX client application, place a tick in the "Enable client side logging" tickbox. This will enable all the fields, as shown in the dialog below.



You can now choose a directory to which the log messages for this application will be written. You may type in a directory of your choice, but the default directory for each application is as follows:

- ODEX Administrator – C:\Program Files\DIP\Odex Enterprise\Installation Directory\AdministratorLog
- Communications Monitor – C:\Program Files\DIP\Odex Enterprise\Installation Directory\Comms Monitor Log\
- Workstation – C:\Program Files\DIP\Odex Enterprise\Installation Directory\Workstation Log\

Where Installation Directory indicates the current build you have installed e.g. 1.0.0.051

The files in each of these log directories will be named according to the following naming convention:

The first 3 characters will always be LOG

The next 8 digits will be the date of the log in DDMMYYYY format (in the example below, the date is 06102003 i.e. October 6th 2003)

The next 6 digits will be the time of the log in HHMMSS format (in the example below, the time is 101741 i.e. 10:17a.m. and 41 seconds.

Each file ends with .log

Example – LOG06102003101741.log

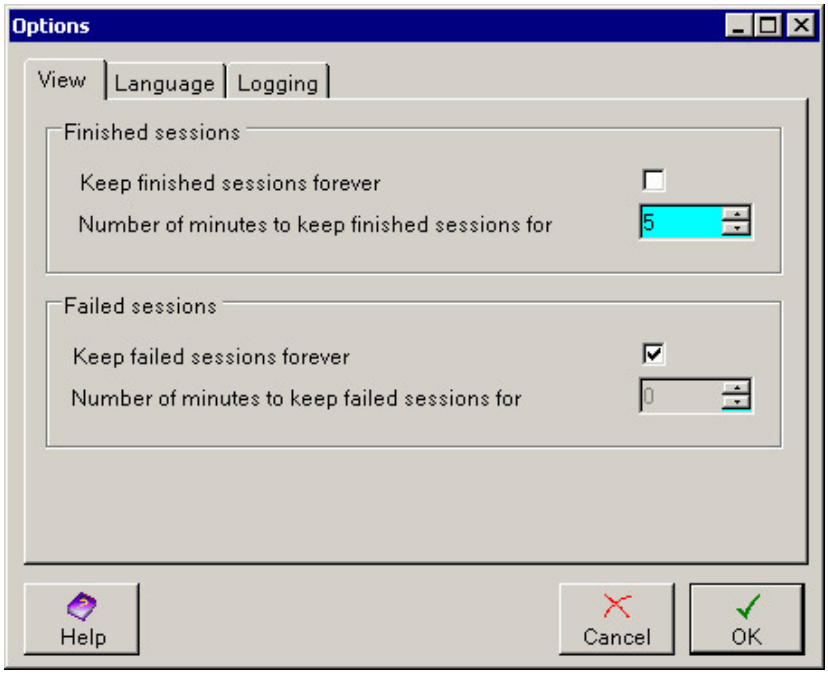
Using the Logging page you can also choose how much information, and of what kind, is written to the client log. This is done in the section headed "Select the message types to write to the client log". The settings shown above are the default settings for logging within the application.

There are three message types to choose from. By default, only General messages are selected, as these are probably the most useful for general purposes. If more detailed information is required by our Support department, they may suggest that you select one or more of the remaining message types too.

For more information about logging in ODEX, please refer to the section entitled "Logging".

Comms Monitor Options dialog

The Comms Monitor options dialog has an extra page, described below. For details of the other two pages, please refer to the section entitled "Options dialog".



This dialog is divided into two sections: Finished sessions and Failed sessions.

Finished sessions

The default setting for finished sessions is to remove them from the Comms Monitor view after 5 minutes. You can change the number of minutes to suit your system.

If required, you can temporarily select the "Keep finished sessions forever" option. Once you have deselected it again, the normal operation will commence once more.

Failed sessions

The default setting for failed sessions is to keep them in the Comms Monitor view forever. This enables you to see how many failed sessions have occurred and to investigate the reason why.

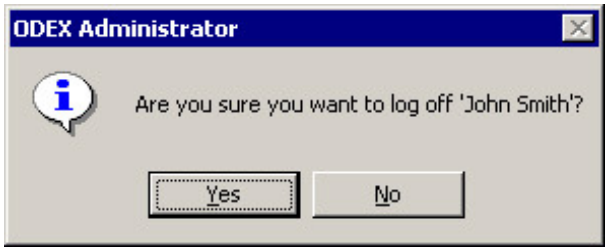
Any failed sessions that you are no longer interested in can be removed from the Comms Monitor view using the Dismiss option from the main menu.

Logon dialog

The Logon dialog will only be a feature of ODEX if User Security is being enforced.

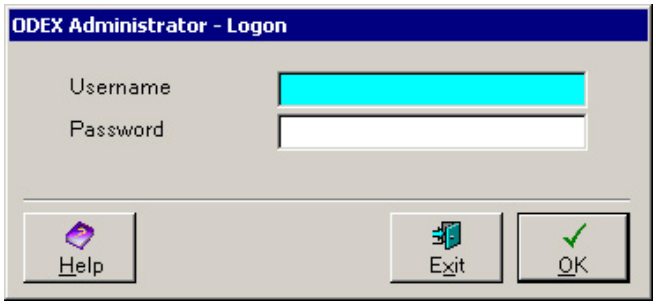
If you are using User Security, the Logon dialog will appear whenever you try to start an ODEX application or whenever you select the **File >> Log Off** option from any of the ODEX applications. Logging off enables another user to log on without having to close the application first.

If logging off, you will first be asked if you are sure you want to log off the current user, with the message box below (the banner content will depend on which application you are currently logged on to).



Click **Yes** to proceed with the logoff, or **No** to remain logged on.

If you click **Yes**, or if you are starting an application, you will then see the following dialog:



If logging off, you can now leave the computer, ready for the next user to come along.

The next user types his username in the Username field, and, if he has been set up to use passwords, his password in the Password field.

There are a few rules about the characters that may be used in the password:

The password must contain at least 5 characters, up to a maximum of 12 characters

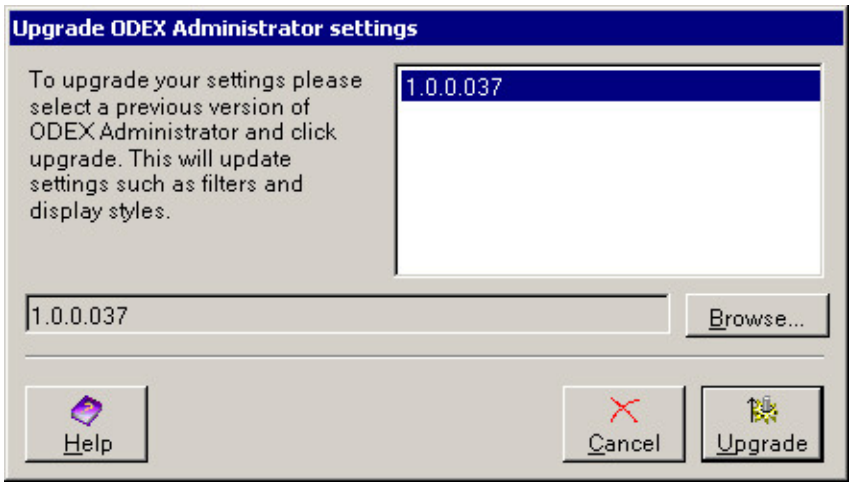
The password must be alphanumeric i.e. it may only include numbers and letters and the underscore character (no punctuation and no spaces are permitted)

The password is case sensitive.

Click **OK** to proceed with the logging on of the new user, or **Exit** if you have decided instead to close the application.

Upgrade settings dialog

The Upgrade ODEX settings dialog is the same for all applications, though each will refer to the application you are currently using.

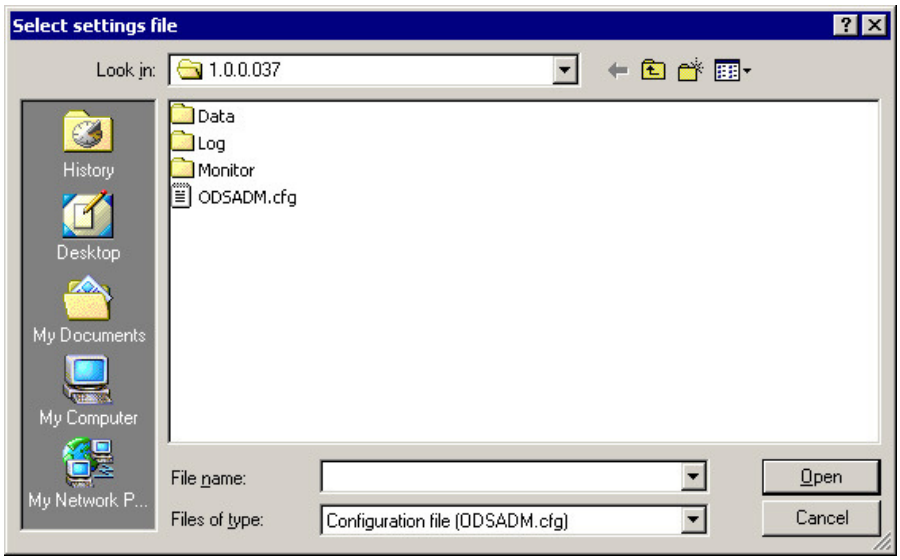


To upgrade your settings, you need to select a previous version of ODEX to upgrade from.

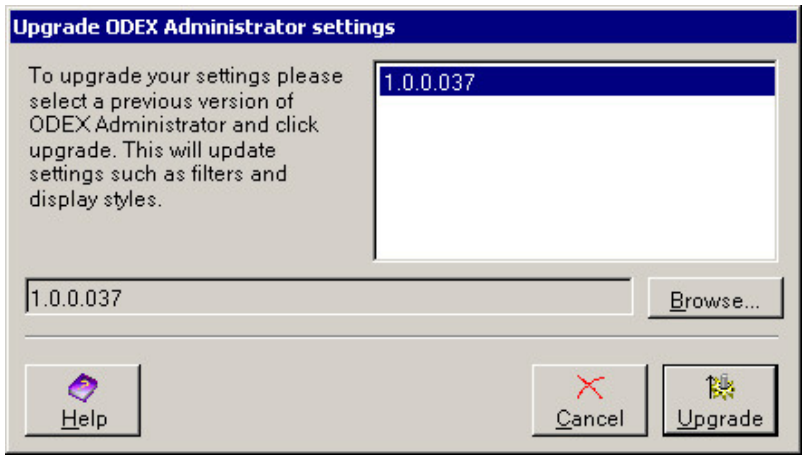
Previous versions that have been installed in the default ODEX installation directory will be listed in the main window of this dialog, so you will normally just select one of them to upgrade from, by highlighting it.

If you have installed a previous version of ODEX somewhere other than in the default directory, you can use the **Browse** button to find it.

If you use the **Browse** button, you will see the Select settings file dialog, as shown below.



The file type you have to use (i.e. the appropriate configuration file) will be provided for you in the 'Files of type' field. You need to search for a file with that name in the directory where you have installed a previous version of ODEX. When you have found it, double-click on it to return to the Upgrade ODEX settings dialog, where the directory name will now be displayed in the field alongside the **Browse** button, as shown below.



Having selected the previous version to upgrade from, click the **Upgrade** button to proceed with the upgrade. Or click the **Cancel** button to abandon the upgrade procedure.

If you proceed with the upgrade, you will then see the following message box, informing you that the upgrade was successful.

Click **OK** to return to the application you are using.

Change password dialog

The Change password dialog will only be a feature of ODEX if User Security is being enforced.

The Change password dialog, shown below, will appear if you select the **Tools >> Change password** option from any of the ODEX applications.

This dialog allows you to change the password of the user who is currently logged on to the application from which you have opened the dialog.

> *The password of someone who is not logged on can only be changed from the Users section of the ODEX Administrator.*

Type in the current password of the user in the Old password field.

Type in the new password in the New password field.

Type the same new password in the Confirm password field.

There are a few rules about the characters that may be used in the password:

The password must contain at least 5 characters, up to a maximum of 12 characters

The password must be alphanumeric i.e. it may only include numbers and letters and the underscore character (no punctuation and no spaces are permitted)

The password is case sensitive.

Click **OK** to keep the new password, or **Cancel** to keep the current password.

Timeout dialog

The Timeout dialog may appear when you have requested ODEX to do something that may take a few minutes to complete. It gives you the option to cancel the request if you wish.

If you want to cancel the request, click the **Cancel** button. You will be returned to the previous screen.

If you prefer to wait until the action has been completed, you need take no action.

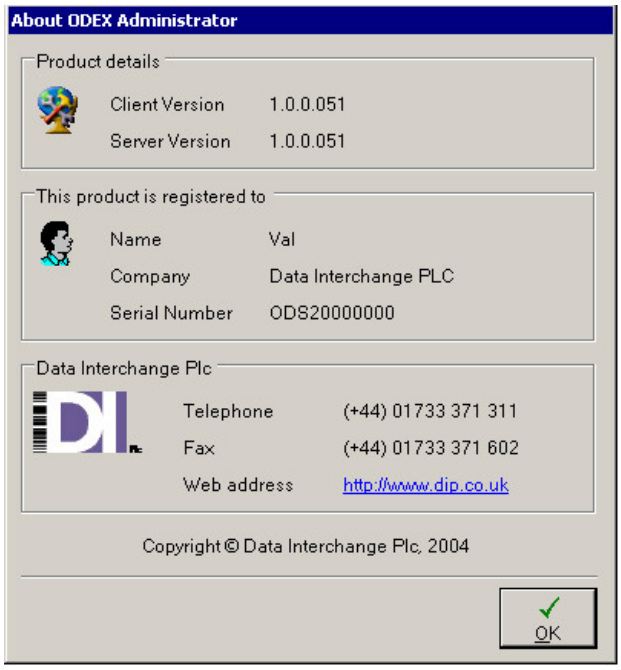
Waiting for Response dialog

The Waiting for Response dialog may appear when you have requested ODEX to do something that may take a few minutes to complete.

This dialog does not give you the option to cancel your request. The type of action you have requested is one that must be completed before control is returned to you.

Help About …. dialog

The Help About dialog is accessible from the menu bar of any of the ODEX applications. Click **Help >> About *Application***, where *Application* is the name of the application you are currently looking at. The example below shows the Help About dialog from the Administrator application.



This dialog is divided into three sections: Product details, Registration details and Data Interchange Plc.

Product details

This section shows the version of the Client (i.e. application) and the ODEX Server. These details are important and should be quoted if you ever need to contact Data Interchange Plc for support purposes.

Registration Details

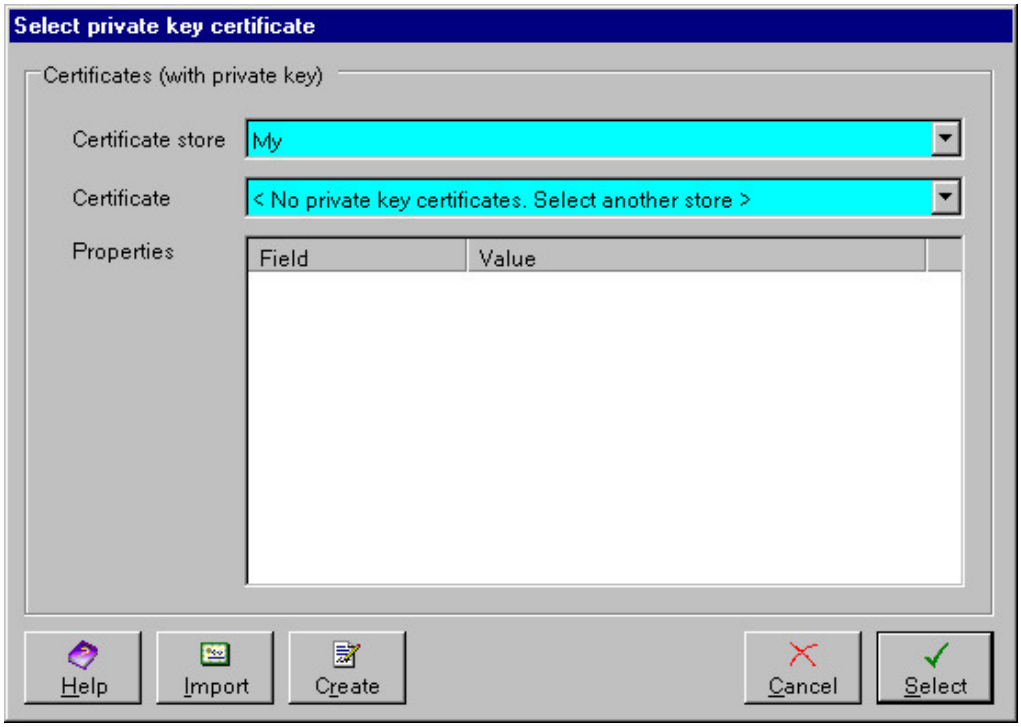
This section shows the registered User Name, your Company name and the product Serial Number. These details should also be quoted if you ever need to contact Data Interchange Plc for support purposes.

Data Interchange Plc

This section gives the contact details for Data Interchange Plc. You will need these if you ever have to contact Data Interchange Plc for support purposes.

Select Certificate dialog

The Select Certificate dialog allows you to choose the certificate to encrypt and or sign data.



Certificate store

Use the dropdown arrow alongside this field to select the appropriate certificate store i.e. the store where the certificate you want to use is kept.

Certificate

If the certificate store you have selected contains no key certificates of the type you require (i.e. private or public, depending on the function for which you are selecting the certificate), the Certificate field will display a message to that effect, telling you to select another store.

Once you have selected a certificate store containing certificates of the type you require, use the dropdown arrow to select the certificate you want from that store. Any properties of that certificate will be displayed in the Properties section.

Properties include:

- Whether or not the certificate encapsulates a private key
- The signature algorithm
- Issuer details
- Validity dates

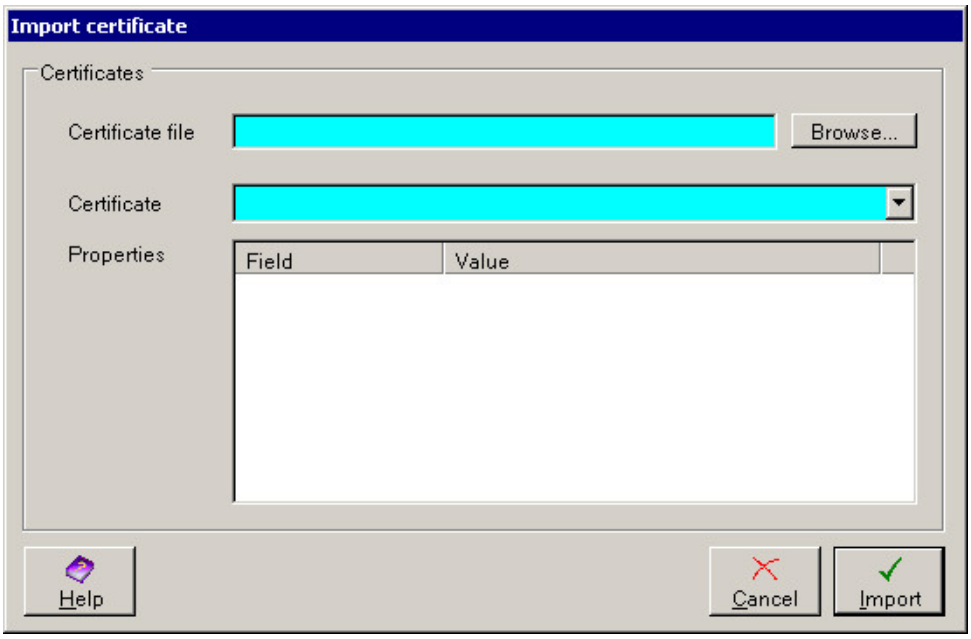
Import button

If the certificate you want is not held in any of the certificate stores in the dropdown list, you can import another certificate by clicking on the **Import** button. This will bring up the “Import certificate” dialog.

Create button

If you are unable to select or import a certificate, you can create your own certificate by clicking on the **Create** button. This will bring up the “Create certificate” dialog.

Import certificate



Certificate file

Find the certificate file you want by using the **Browse** button.

Certificate

Once you have selected a certificate file, the certificate dropdown list will be populated with a list of certificates that the file contains (in most cases a certificate file contains a single certificate, but sometimes it contains more). Use the dropdown arrow to select the certificate you want from that file. Any properties of that certificate will be displayed in the Properties section.

Click the **Import** button to complete the import process and return to the Select Certificate dialog.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

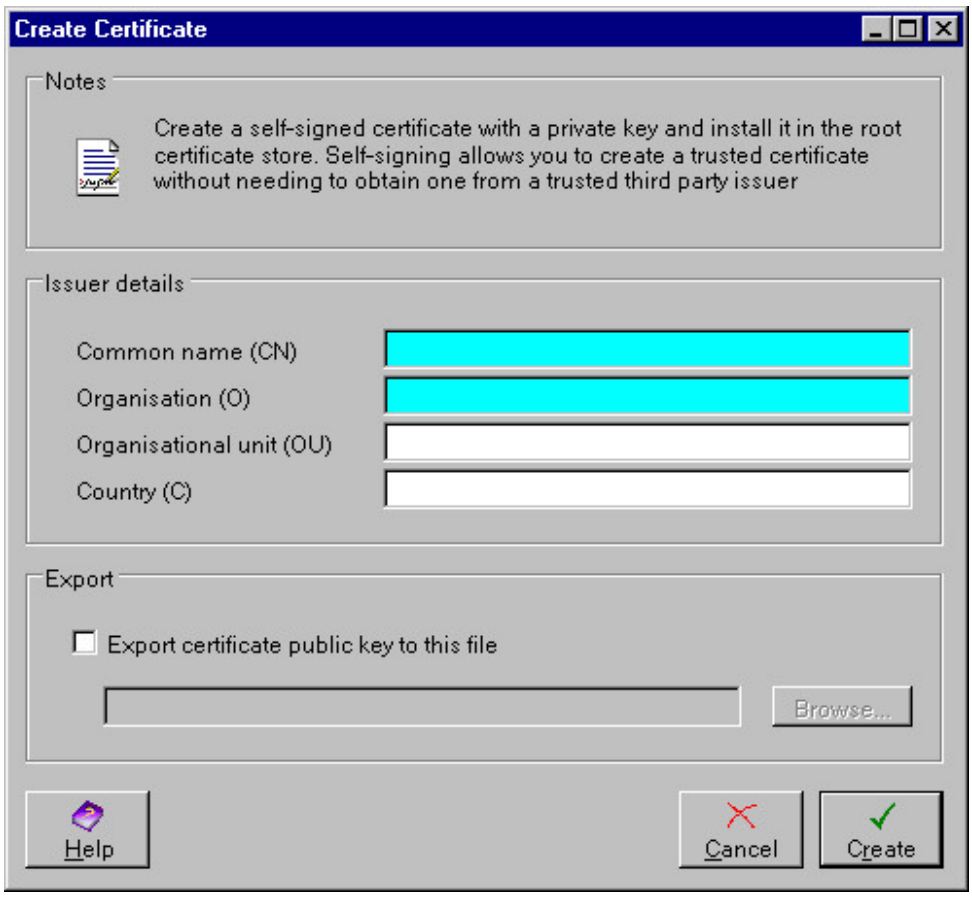
If you want to discard all the changes you have made, click the **Cancel** button.

Import

To import the certificate you have selected, click the **Import** button.

Create certificate

This dialog allows you to create a self-signed certificate with a private key and install it in the root certificate store. Self-signing allows you to create a trusted certificate without needing to obtain one from a third-party issuer.



The issuer details allow you to provide information that can be viewed in the Properties section when choosing a certificate.

Issuer details – Common name

Type in the common name that you wish to give to this certificate.

Issuer details – Organisation

Type in the name of the organisation with which this certificate is associated

Issuer details – Organisational unit

Type in the name of the organisational unit with which this certificate is associated

Issuer details – Country

Type in the name of the country in which this certificate was issued.

Export – tickbox

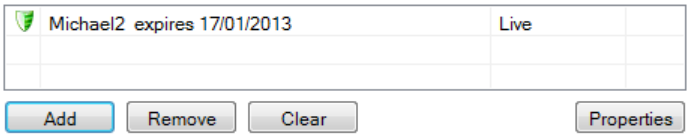
If you wish to export the public key for this certificate to another file, select the tickbox and use the **Browse** button to choose the name and location of the file to which you want to export it.

Once you have provided the required details, click the **Create** button to create the certificate. You will be returned to the Select certificate dialog, where you will now see that your self-signed certificate has been added to the root certificate store and can be selected. The Issuer details you provided on the Create certificate dialog can be viewed in the Properties section against the 'Issuer' caption.

Dynamic Certificate Selection

In many places in the ODEX Administrator, one or more certificates can be selected for use in a particular function, e.g. signing, encryption, verification.

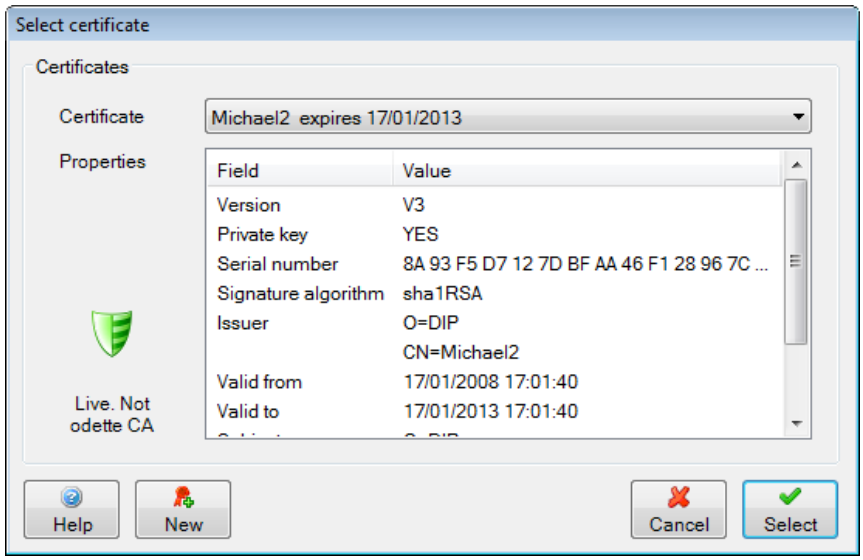
The interface is common for all.



This type of interface allows you to select a chain of related certificates to use for the function, but only one of these certificates will be used in practice. The reason for this is not to allow for a choice, but rather to allow for slick transitioning between certificate renewals.

You will generally find that you can only add one certificate for a single function using this interface. But as soon as you get a renewal for that certificate, now you can also add that certificate alongside the existing certificate. As soon as the new certificate becomes live, it will immediately get used for the function.

Click the **Add** button to add a new certificate to the function. You will see the following dialog.



Use the **Certificate** dropdown to select an existing certificate from the ODEX store to use for the function.

If the ODEX store does not contain any appropriate certificates, the Certificate field will display a message to that effect.

The **Properties** section shows the details relating to the selected certificate. Properties include:

- Whether or not the certificate encapsulates a private key
- The signature algorithm
- Issuer details
- Validity dates

The current status of the certificate in the ODEX store will be displayed to the left-hand-side of the Properties section.

If you have not yet imported a suitable certificate into the ODEX store for the required function, you may do so here by clicking the **New** button. You will be presented with the following sub-options:

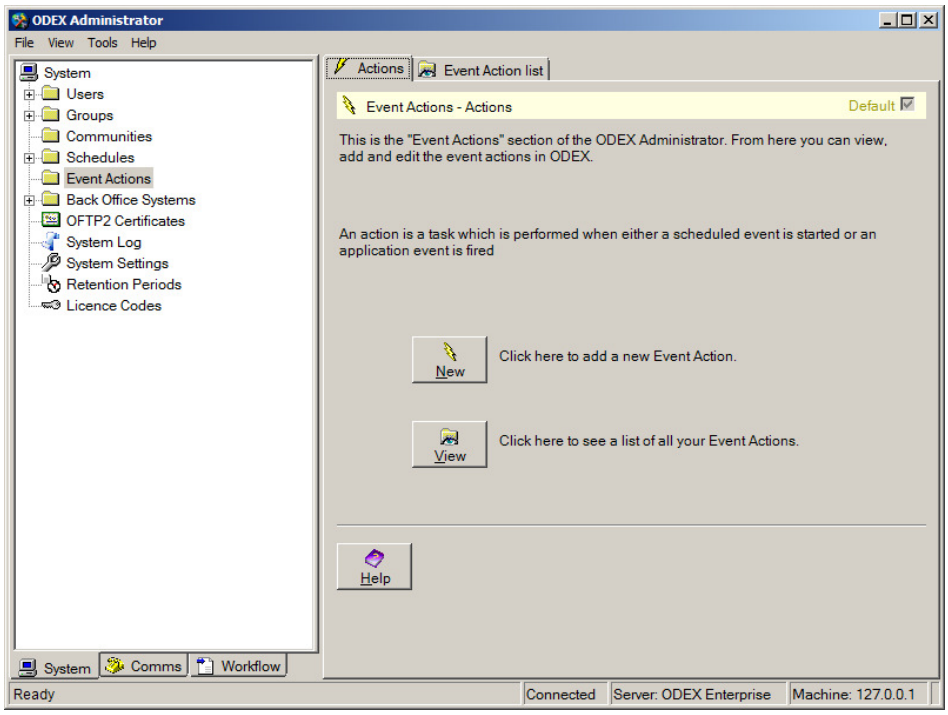
- Import certificates from a file on disk – see ‘Import certificate from file’
- Import certificates from the windows certificate store – see ‘Import certificate from windows’
- Create a new self-signed certificate in the ODEX store – see ‘Create Certificate Dialog’
- Register identification data for a certificate you are expecting to receive through certificate exchange – see ‘Register Identification Data’

System Administrator

Introduction

The ODEX Administrator is where everything internal to the ODEX Enterprise program is maintained.

When you first open the ODEX Administrator, you will see the following screen. The Navigation Panel, on the left, comprises three page tabs: System, Comms and Workflow. Each page tab displays a tree list, showing the areas included in that section. For example, the System section contains tree nodes for Users, Groups, Communities, Schedules, Event Actions, Back Office System, System Log, System Settings, Retention Periods and Licence Codes. In the Information Panel, on the right, you will see a description of the selected page tab and how to use it.



Let's go through each of the sections one by one.

ODEX users, user groups and communities

Before reading this section, please refer to the section entitled "User Security", in order to understand what users, user groups and communities are all about.

When using ODEX's own security, it doesn't matter whether you add the users, user groups or communities first. However, you may create users without necessarily creating any user groups or communities. If you do create user groups or communities, they are ineffective until you have created one or more users and allocated them to the user groups or communities.

When using Windows security, it doesn't matter whether you add the users or the user groups first. Unlike ODEX's own security, you can import user groups without importing any users. They will be effective because Windows user groups already have users belonging to them.

Both users and user groups allow you to specify permissions i.e. you can specify which areas of the software the user or user group has access to and what actions they can perform within those areas.

Communities allow you to restrict the access of users and user groups to individual companies, networks and any associated files.

A user who is a member of one or more user groups is subject to all the privileges and restrictions allocated to those user groups. He can also be given more privileges and fewer restrictions by setting his own user permissions higher and his restrictions looser than those of the group(s) he belongs to.

However, this does not work in the opposite way – a user cannot have his privileges reduced or his restrictions tightened by setting his own user permissions lower and restrictions tighter than those of the group(s) he belongs to. If you want to restrict a user's privileges you should re-allocate him to a different group.

Stated simply, if the permissions of a user do not match those of the group he belongs to, the higher permission level will always be used.

A user that is not a member of any communities can view all companies, networks and files in the system. When a user is a member of one or more communities, that user only has access to companies, networks and associated files that belong to that community. If a user is a member of a group that is a member of one or more communities, that user has access to networks, companies and associated data that belong to any communities that the user is a member of and any communities that the user group is a member of.

Again, this does not work in the opposite way. The user's permissions to view networks, trading partners and associated files cannot be reduced by setting the user's permissions lower than those of the group(s) he belongs to.

ODEX System Administrator user

This section of the System Administrator allows you to add new users, and view and edit the users you have profiled in ODEX. However, you will not be able to access this part of the System Administrator unless you have been given the required permission.

For this purpose, we have pre-configured a System Administrator for you. This user has been set up with full edit permission for the ODEX Administrator application. The administrator user is not a member of any communities so can always view all data in the system. You can view the System Administrator details in the same way as for any other user you set up yourself, but you cannot edit his settings, except to choose whether to use passwords for him.

Users

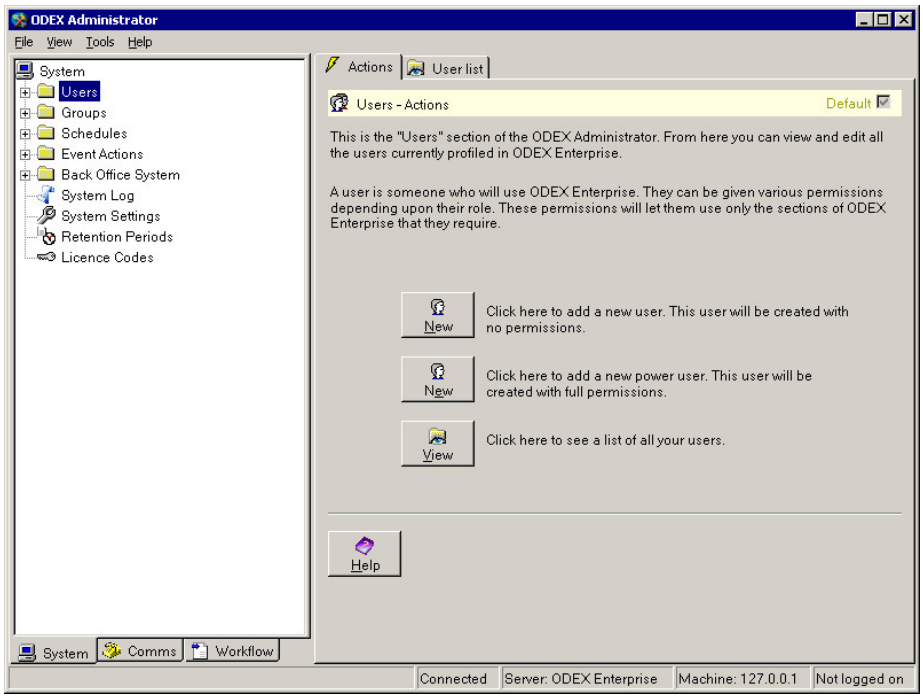
This section of the System Administrator allows you to add new users, and view, edit and delete the users you have profiled in ODEX. However, you will not be able to access this part of the System Administrator unless you have been given the required permission.

For this purpose, we have pre-configured a System Administrator for you. This user has been set up with full edit permission for the ODEX Administrator application. You can view the System Administrator details in the same way as for any other user you set up yourself, but you cannot edit his settings, except to choose whether to use passwords for him.

You can access the Users section either via the Navigation Panel tree view or via the Information Panel on the right.

To see the Users section, click on the Users name in the Navigation Panel of the System Administrator. This will bring up the default page of the Users section in the Information Panel on the right, as shown below.

Please note that the wording alongside the **New** buttons will be slightly different if you are using Windows security.



There are two pages in the Users section, called Actions and User List.

Let's have a look at these two pages and see how to use them.

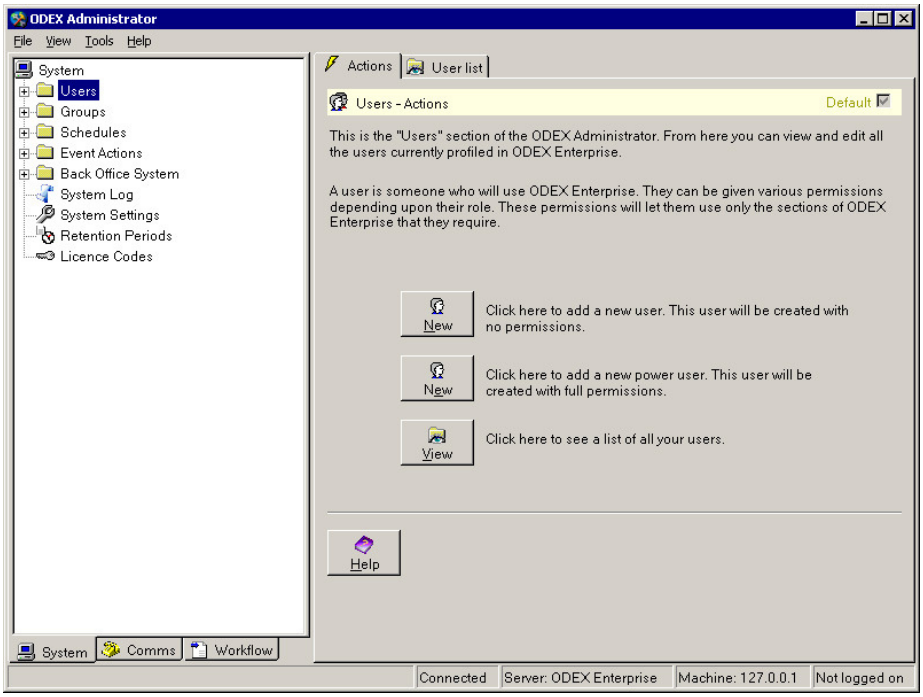
Users – Actions page

Before editing the Users section, please refer to the section entitled "User Security", in order to understand what users and user groups are all about.

You need to edit the System Settings section before editing this section, in order to choose what type of user security you want to use.

To add a new user or view a list of all users, click once on the Users node in the tree view. This will bring up the Users – Actions page.

There are three buttons on this page – **New**, **New** and **View**.



There are two approaches to adding a new user. One is to add a user with no permissions and grant him a few privileges. The other is to add a user with full permissions and, optionally, remove a few privileges from him.

Whichever approach you take, for your chosen method of security, the set of pages you will be presented with will be exactly the same. The only difference will be in the initial level of permission that is set for each view of each application. For a user with no permissions, the permission level will be set to None. For a user with full permissions, the permission level will be set to Edit.

Since the pages and their fields are identical, we only need to describe them once.

If you want to add a new user with no permissions, click on the top **New** button and refer to the section entitled "Adding a new user".

If you want to import a new Windows NT user with no permissions, click on the top **New** button and refer to the section entitled "Importing a new user".

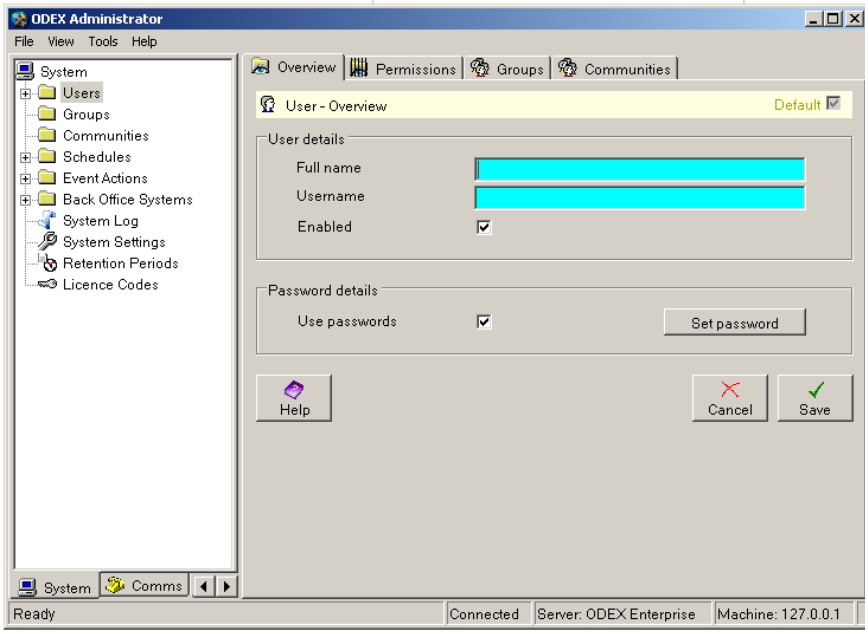
If you want to add a new user with full permissions, click on the second **New** button and refer to the section entitled "Adding a new user".

If you want to import a new Windows NT user with full permissions, click on the second **New** button and refer to the section entitled "Importing a new user".

If you want to view a list of all users, click on the **View** button and refer to the section entitled "View user list". This option also allows you to edit existing users.

Adding a new user

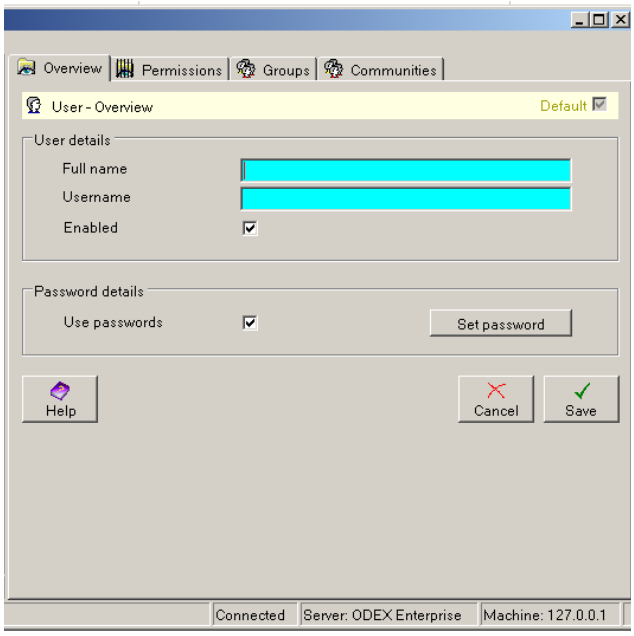
When you click a **New** button from the Users – Actions page, you will see the User – Overview page, as shown below.



As you can see, it has four page tabs: Overview, Permissions, Groups and Communities. Let's have a look at each one in turn and find out how to use them.

Overview

This page allows you to add the details of the person who is to be a new user of ODEX.



The fields and buttons on this page are as follows:

User details – Full name

Type in this field the full name of the person who is to be a new user of ODEX. For example, type in John Smith, not simply John.

User details – Username

Type in this field the name you want to give to this person as a user. This name must be no more than twelve characters long and must be unique and preferably easy to distinguish. We suggest you use the first name of the user, with one or more initials if it is necessary to distinguish them.

For example, if you have two John Smiths you could give one the username of JohnRS and the other JohnGS (using their middle initial to distinguish them). This would be preferable to John1 and John2, as somewhere down the line you may forget which is which.

User details – Enabled

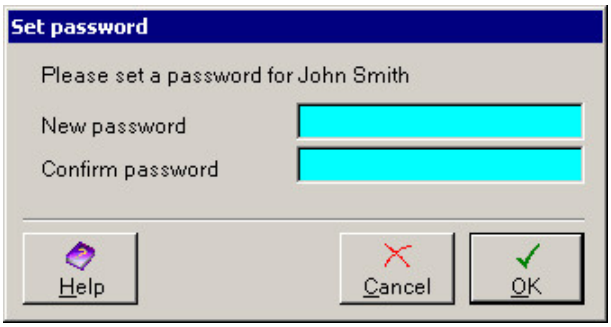
This tickbox allows you to enable or disable this user as a user of ODEX. Most of the time you will select the tickbox in order to enable the user, thus allowing him access to ODEX. If a user were to be absent from work for a length of time, through illness for example, for greater security you could disable him as a user until his return to work. This would prevent anybody taking advantage of his absence to "borrow" his identity.

Password details – Use passwords

When you add a new user, the **Use passwords** checkbox will initially be enabled and checked. If you keep this setting, you will not be able to save the details for this new user until you provide a password for him. However, if you do not want to use passwords for this user, uncheck the checkbox. The **Set password** button will then become disabled.

Password details – Set password / Reset password

The **Set password** button is used to set the initial password of the new user. Once the password has been set and saved, the button will be renamed as **Reset password**. This can then be used for anyone who has forgotten their password, or anyone whose password has been compromised. Pressing this button will bring up the following dialog:



You need to type the new password into both fields. This helps to prevent a mistyped password being saved.

There are a few rules about the characters that may be used in the password:

The password must contain at least 5 characters, up to a maximum of 12 characters

The password must be alphanumeric i.e. it may only include numbers and letters and the underscore character (no punctuation and no spaces are permitted)

The password is case sensitive.

Click **OK** to save the new password and return to the User – Overview page.

Help

If you need more information about the fields on the Overview page and how to fill them in, click on the **Help** button.

Cancel

If you do not want to save changes you have made, click the **Cancel** button to discard your changes.

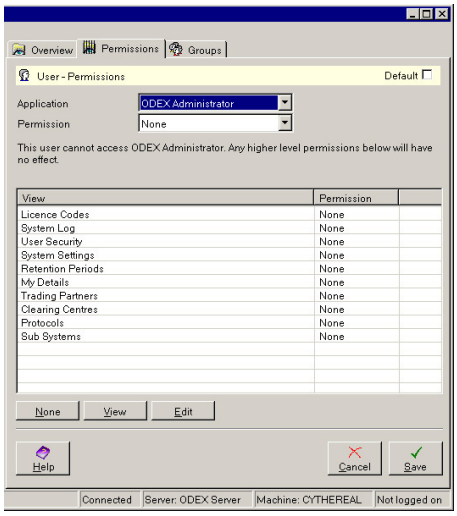
Save

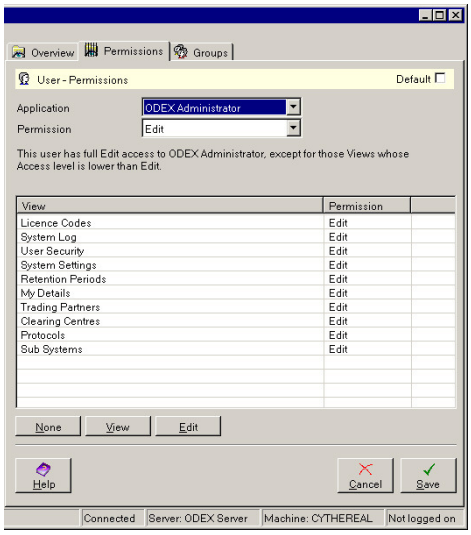
To save all the changes you have made on the Overview page, click the **Save** button.

User Permissions

This page allows you to grant or restrict access to applications, and to views within those applications, for this user.

The values in the Permissions column will initially be None or Edit, depending on whether you are adding a user with no permissions or a user with full permissions. This is illustrated in the two dialogs shown below.





The fields and buttons on this page are as follows:

Application

The Application field contains a list of all the applications within the ODEX software. Use the dropdown arrow at the right-hand side of the field to select the application you want to view or edit the restrictions for, as applicable to this user.

Permission

The Permission field contains a list of different types of permission that may be granted to this user for the selected application. Use the dropdown arrow at the right-hand side of the field to select the highest level of permission you wish to grant to this user for the selected application.

For a user with no permissions, the default settings allow no access to any view within any application.

For a user with full permissions, the default settings allow full Edit access to each view within each application.

You will see, as you choose different permissions, that the description below the Permission field changes to describe the effect your choice will have.

To set the same permission for every view of an application, use the Permission field. This value overrides any higher level value selected in the View/Access list. Edit is the highest level, followed by View, followed by None at the lowest level.

- None – the user will not even be able to see the view
- View – the user will be able to see the view and look at the information in it, but they will not be able to edit the information in any way
- Edit – the user has full access to look at and to modify the information

To set different permissions for different views, set the Permission field to the highest level you want to set, then, in the View/Access list below, select the required lower level access for each view that does not share the higher level access.

For example, in the case of the ODEX Administrator application, if you want a user to have Edit access to the Retention Periods view and View access to all other views, you would do the following:

- select ODEX Administrator in the Application field
- select Edit in the Permission field
- highlight each entry in turn in the View/Access list, with the exception of the Retention Periods entry, and click the **View** button. The View value in the View/Access list will take precedence over the Edit value in the Permission field.
- leave the Retention Periods entry as Edit.

View/Permission list

The View/Permission list on this dialog shows a list of all the views belonging to the selected application, and the type of permission this user has to each of those views. To begin with, all views will show a permission type which matches that in the Permission field above.

None, **View**, **Edit**

These buttons should only be used if you want to set different access permissions for different views of the application. If you want to set the same permission for every view of an application, just use the Permission field above.

Use these buttons to apply a lower level of access than that selected in the Permissions field, to some of the views for this user. Highlight each affected view in the list and press the appropriate button at the bottom.

For example, in the case of the ODEX Administrator application, if you want a user to have no access to the Licence Codes view and View access to all other views, you would do the following:

- select ODEX Administrator in the Application field
- select View in the Permission field
- highlight the Licence Codes entry in the View/Access list and click the **None** button, to set the Licence Codes Access to None
- leave all the other views' access as Edit – the View value in the Permission field will take precedence over the Edit value in the View/Access list.

Help

If you need more information about the fields on the Permissions page and how to fill them in, click on the **Help** button.

Cancel

If you do not want to save changes you have made, click the **Cancel** button to discard your changes.

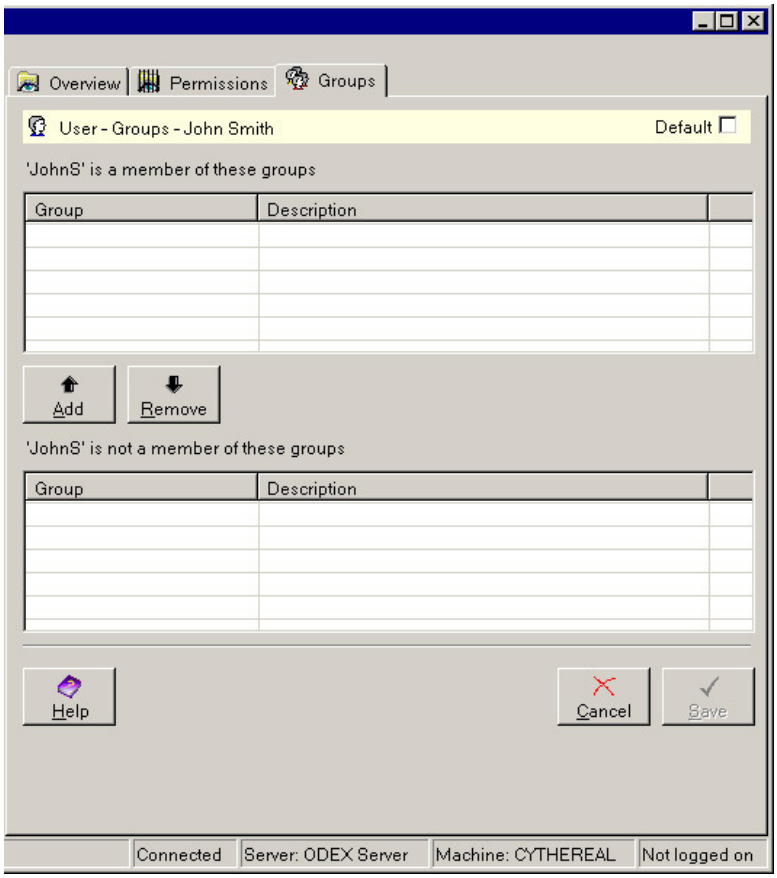
Save

To save all the changes you have made on the Permissions page, click the **Save** button.

Groups

This page will not be present if you are using Windows NT security.

This page allows you to add this user to a user group or remove him from a user group.



The fields and buttons on this page are as follows:

Members list

The members window shows a list of all the user groups to which this user belongs.

Add, Remove

You may add groups from the non-members list to the members list by pressing the **Add** button, and remove groups from this list by pressing the **Remove** button. Using the **Add** button removes a group from the lower list and adds it to the upper list. Using the **Remove** button removes a group from the upper list and adds it to the lower list.

Non-members list

The non-members list shows a list of all the user groups to which this user does not belong.

Help

If you need more information about the fields on the Groups page and how to fill them in, click on the **Help** button.

Cancel

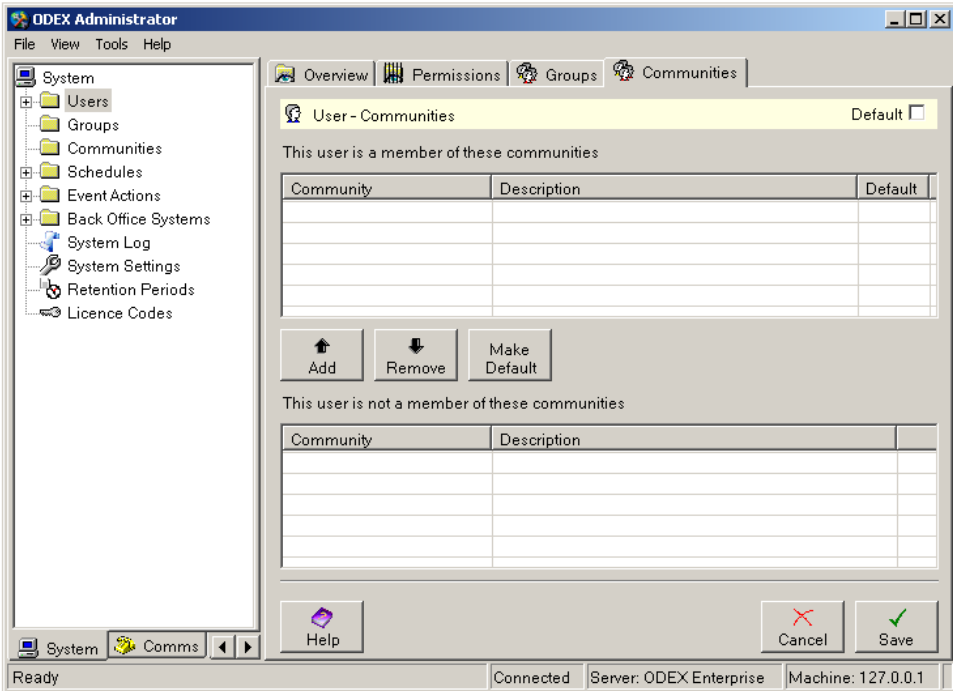
If you do not want to save changes you have made, click the **Cancel** button to discard your changes.

Save

To save all the changes you have made on the Groups page, click the **Save** button.

Communities

This page allows you to add this user to a community or remove him from community.



The fields and buttons on this page are as follows:

Members list

The members window shows a list of all the communities of which this user is a member.

Add, Remove

You may add communities from the non-members list to the members list by pressing the **Add** button, and remove communities from this list by pressing the **Remove** button. Using the **Add** button removes a community from the lower list and adds it to the upper list. Using the **Remove** button removes a community from the upper list and adds it to the lower list.

Make Default

When a user is a member of multiple communities, this allows you to set the default community. When a user that is a member of one community creates a company or network, the company or network will be associated with that user's community and will only be visible to members of that community.

When a user is a member of multiple communities, any companies or networks that they create will be associated with the default community, unless the user selects a different community when they create the company or network.

Non-members list

The non-members list shows a list of all the communities to which this user does not belong.

Help

If you need more information about the fields on the Groups page and how to fill them in, click on the **Help** button.

Cancel

If you do not want to save changes you have made, click the **Cancel** button to discard your changes.

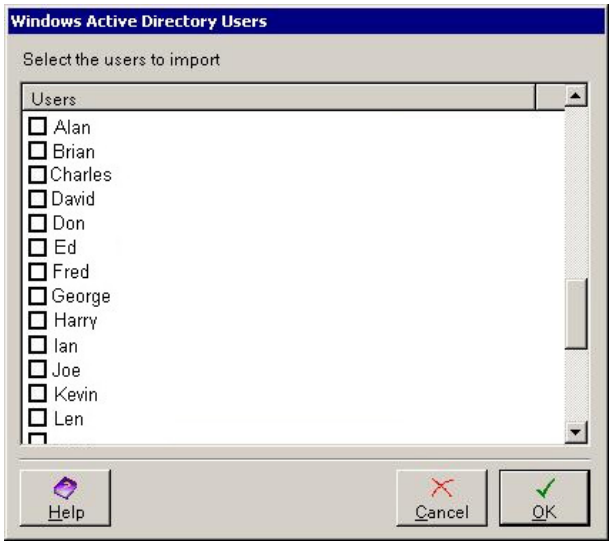
Save

To save all the changes you have made on the Groups page, click the **Save** button.

Importing a new user

This section is only relevant if you are using Windows NT security.

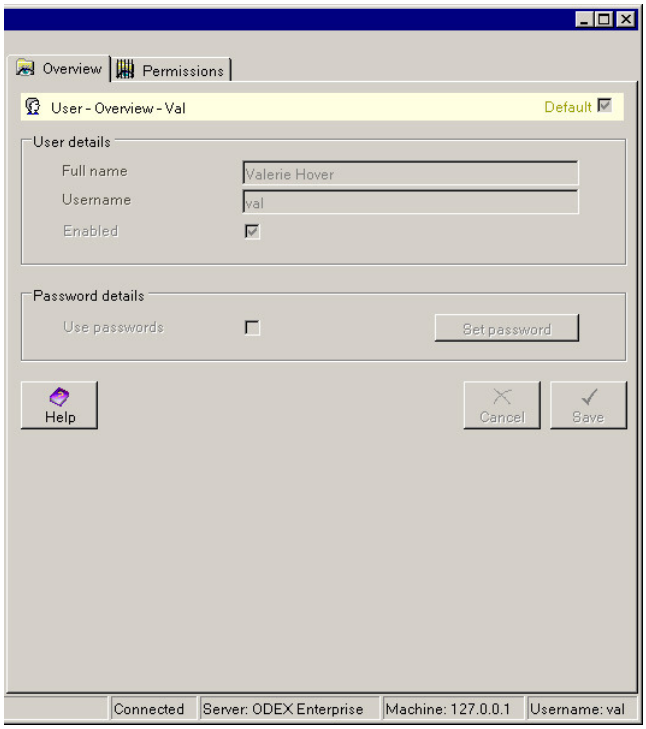
When you click a **New** button from the Users – Actions page, you will see the Windows Active Directory users dialog, as shown below.



This dialog does not show users that have already been imported into Odex.

Using the checkboxes, select the users you want to import as ODEX users, then click **OK**. This will return you to the Users – Actions page where, if you expand the Users tree node, you will be able to see the imported users in the list.

Select one of the imported users in order to see the User – Overview page, as shown below.



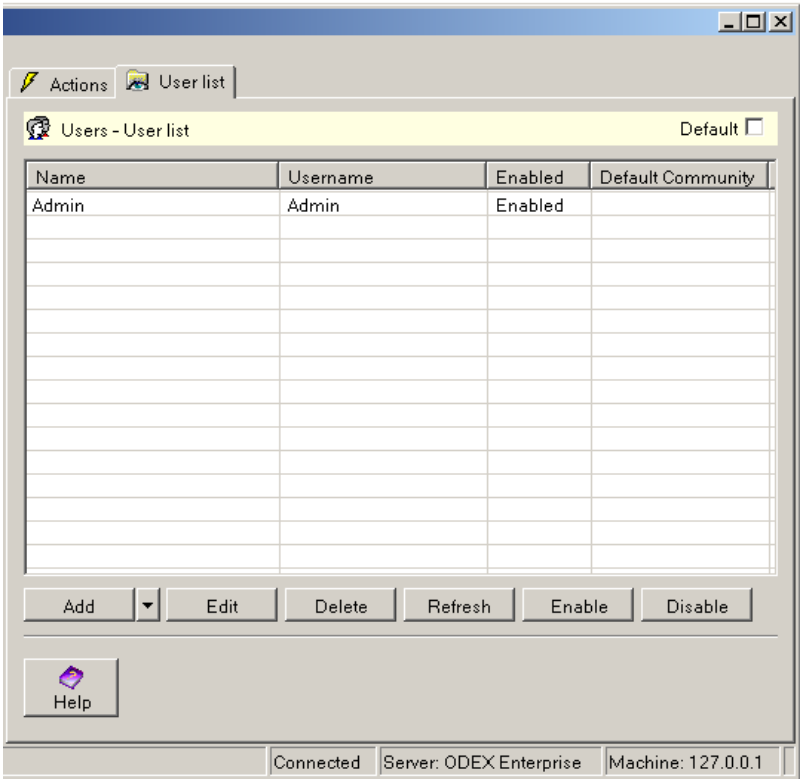
For the user designated as the ODEX Administrator, all fields and checkboxes on this page are disabled. This is because none of these fields may be changed for the Administrator.

For all other users, all fields on this page are disabled, with the exception of the Enabled checkbox, since you cannot change anything to do with Windows user accounts from within ODEX. You can use the Enabled checkbox to enable or disable the user. A user who is disabled cannot log on to any of the ODEX applications.

The remaining pages for importing a user are the same as those for adding a new user, except that there is no Groups page. Again, this is because you cannot change anything to do with Windows user accounts from within ODEX. For details of these remaining pages, please continue reading from the section entitled "User Permissions".

View user list

When you click the **View** button to see a list of all ODEX users, you will then see a page which looks like the one shown below.



The main part of this page consists of a window with four columns: Name, Username, Enabled and Default Community. This window lists all the ODEX users that are currently profiled, showing their name, their username, whether they are enabled and the name of their default community, if they have one.

This page also has seven buttons: **Add**, **Edit**, **Delete**, **Refresh**, **Enable**, **Disable** and **Help**. Let's have a look at each one in turn and find out what they do.

Add

Click on the **Add** button if you want to add a new user to the user list. You will be able to choose between adding a user with no permissions or a power user. This will bring up the set of pages described in the section entitled "Adding a new user".

Edit

Highlight a user in the list and click on the **Edit** button if you want to amend the details for the selected user. This will bring up the set of pages described in the section entitled "Adding a new user".

Delete

Highlight a user in the list and click on the **Delete** button if you want to delete the selected user from the list.

Refresh

Click on the **Refresh** button to refresh the details on this page e.g. if a change you have just made is not reflected in the details you can see.

Enable

Highlight a user in the list and click on the **Enable** button to enable a user who is currently disabled.

Disable

Highlight a user in the list and click on the **Disable** button to disable a user who is currently enabled. A user who is disabled cannot log on to any of the ODEX applications.

Help

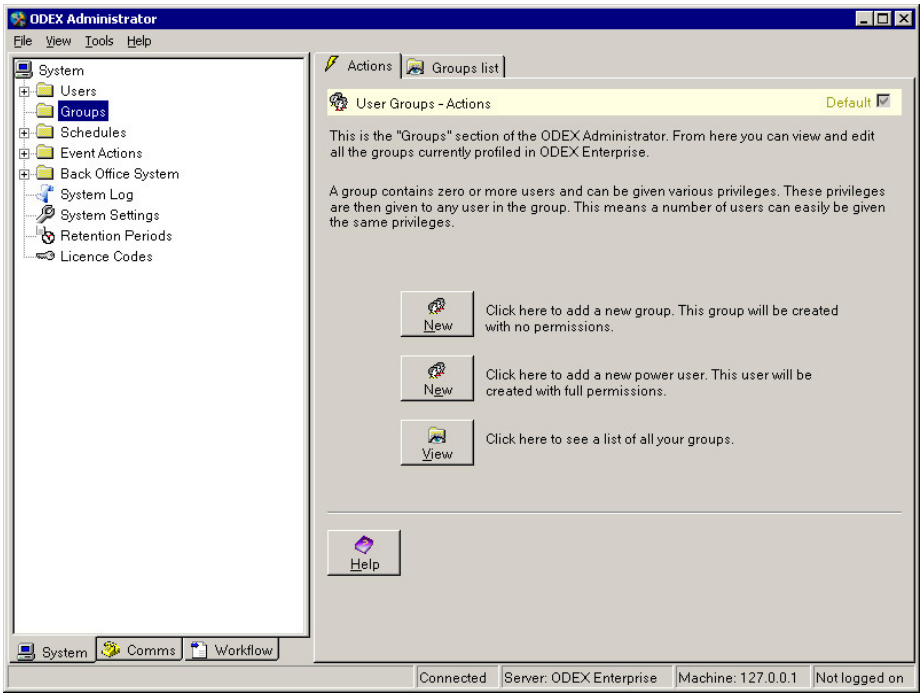
If you need more information about the User list page and how to use it, click on the **Help** button.

User Groups

This section of the System Administrator allows you to add new user groups, and view and edit the user groups you have profiled in ODEX. However, you will not be able to access this part of the System Administrator unless you have been given the required permission.

You can access the User Groups section, as any other section of the System Administrator, either via the Navigation Panel tree view or via the Information Panel on the right.

To see the User Groups section, click on the Groups name in the Navigation Panel of the System Administrator. This will bring up the default page of the User Groups section in the Information Panel on the right, as shown below.



There are two pages in the User Groups section, called Actions and Groups list.

Let's have a look at these two pages and see how to use them.

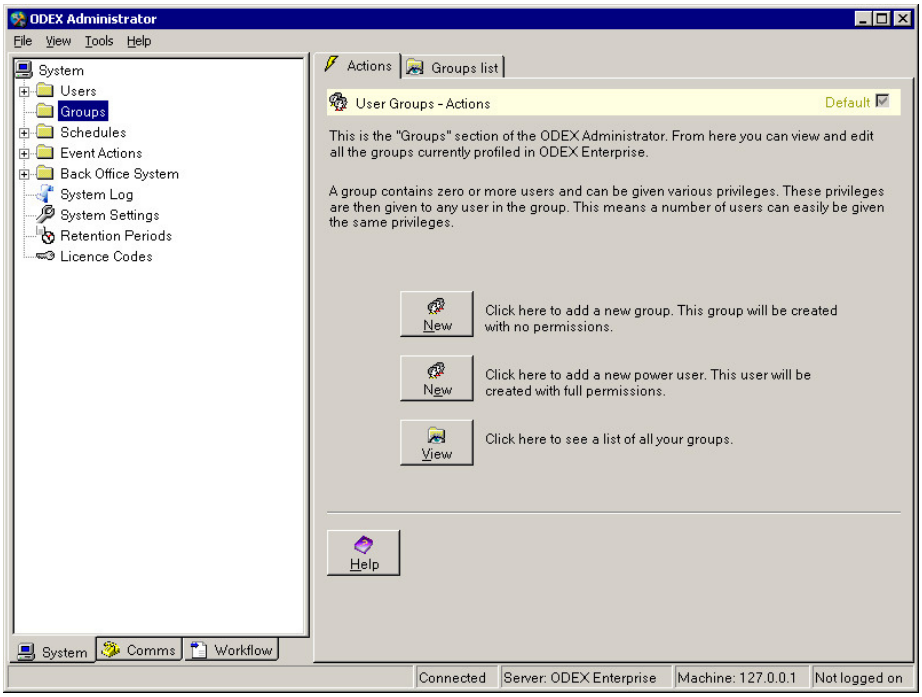
User Groups – Actions page

Before editing the User Groups section, please refer to the section entitled "User Security", in order to understand what users and user groups are all about.

You need to edit the System Settings section before editing this section, in order to choose what type of user security you want to use.

To add a new user group or view a list of all user groups, click on the Groups node. This will bring up the User Groups – Actions page.

This page has three buttons – **New**, **New** and **View**.



There are two approaches to adding a new user group. One is to add a user group with no permissions and assign a few privileges to it. The other is to add a user group with full permissions and, optionally, remove a few privileges from it.

Whichever approach you take, for your chosen method of security, the set of pages you will be presented with will be exactly the same. The only difference will be in the initial level of permission that is set for each view of each application. For a user group with no permissions, the permission level will be set to None. For a user group with full permissions, the permission level will be set to Edit.

Since the pages and their fields are identical, we only need to describe them once.

If you want to add a new user group with no permissions, click on the top **New** button and refer to the section entitled "Adding a new group".

If you want to import a new Windows NT user group with no permissions, click on the top **New** button and refer to the section entitled "Importing a new group".

If you want to add a new user group with full permissions, click on the second **New** button and refer to the section entitled "Adding a new group".

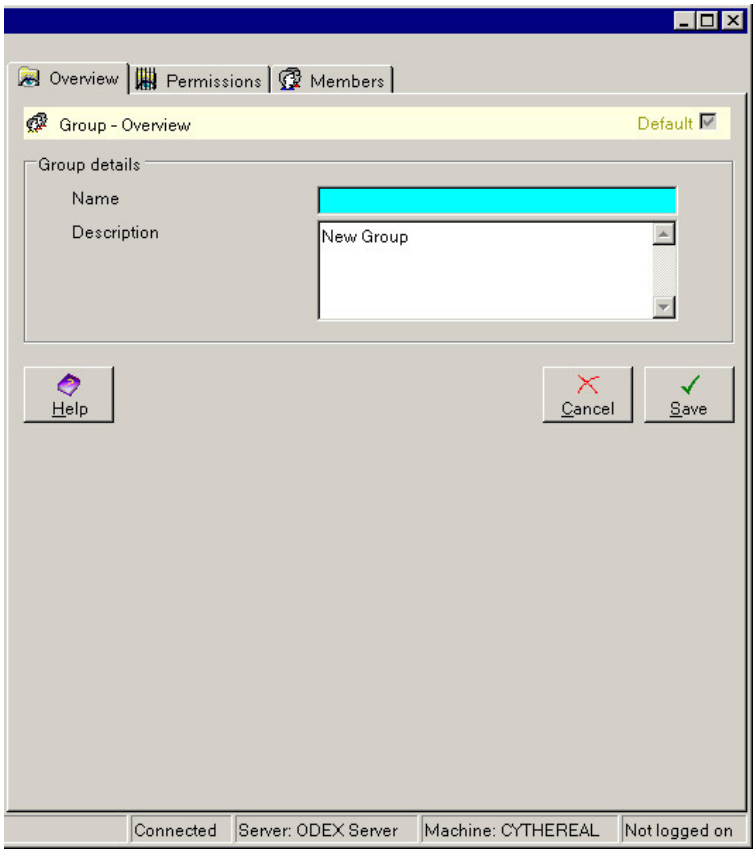
If you want to import a new Windows NT user group with full permissions, click on the second **New** button and refer to the section entitled "Importing a new group".

If you want to view a list of all user groups, click on the **View** button and refer to the section entitled "View group list". This option also allows you to edit existing user groups.

Let's take a look at each of these areas and find out how to use them.

Adding a new group

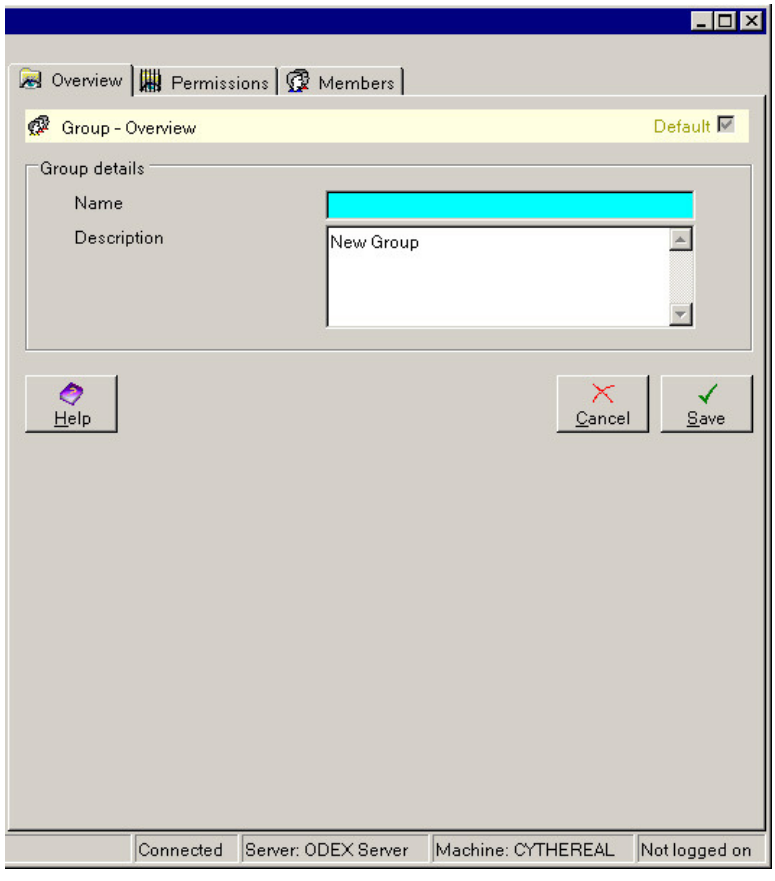
When you click a **New** button from the User Groups – Actions page, you will see the Group – Overview page, as shown below.



As you can see, it has three page tabs: Overview, Permissions and Members. Let's have a look at each one in turn and find out how to use them.

Overview

This page allows you to add a new user group to ODEX.



The fields and buttons on this page are as follows:

Group details – Name

Type in here the name of the new user group. Try to choose a meaningful name which reflects accurately what the group will be allowed to do within ODEX. For example, a group that is only allowed access to the ODEX Administrator could be called ODEX Administration.

Group details – Description

You may type in this field a description of the user group. This will be for the assistance of anyone who has to administer user groups in the future, as it allows you to give some background information about the group. For example, to describe a group called ODEX Administration which is to have full editing permissions, the description could be "This group can perform any function in the ODEX Administrator application, but in no other applications".

Help

If you need more information about the fields on the Overview page and how to fill them in, click on the **Help** button.

Cancel

If you do not want to save changes you have made, click the **Cancel** button to discard your changes.

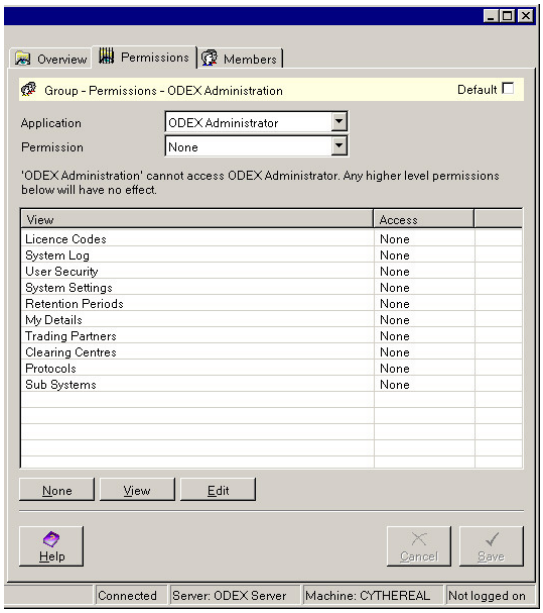
Save

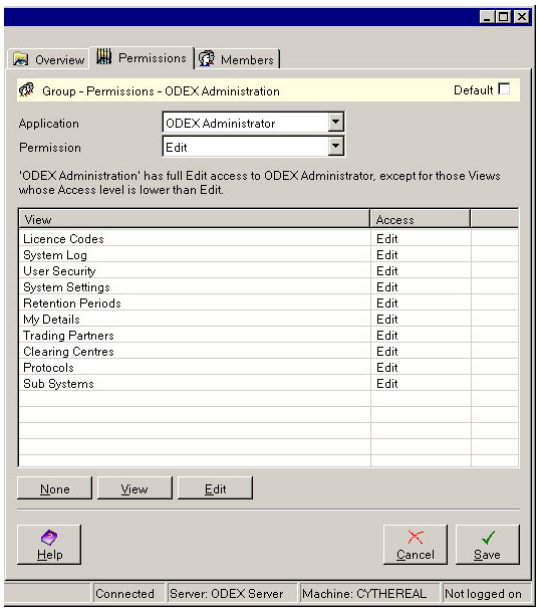
To save all the changes you have made on the Overview page, click the **Save** button.

User Group Permissions

This page allows you to set access restrictions for this user group. You can either set a global permission for an application, using the Permission field, or set permissions on a view by view basis.

The values in the Permissions column will initially be None or Edit, depending on whether you are adding a user with no permissions or a user with full permissions. This is illustrated in the two dialogs shown below.





The fields and buttons on this page are as follows:

Application

The Application field contains a list of all the applications within the ODEX software. Use the dropdown arrow at the right-hand side of the field to select the application you want to view or edit the restrictions for, as applicable to this user group.

Permission

The Permission field contains a list of different types of permission that may be granted to this user group for the selected application. Use the dropdown arrow at the right-hand side of the field to select the highest level of permission you wish to grant to this user group for the selected application.

For a user group with no permissions, the default settings allow no access to any view within any application.

For a user group with full permissions, the default settings allow full Edit access to each view within each application.

You will see, as you choose different permissions, that the description below the Permission field changes to describe the effect your choice will have.

To set the same permission for every view of an application, use the Permission field. This value overrides any higher level value selected in the View/Access list. Edit is the highest level, followed by View, followed by None at the lowest level.

- None – the user will not even be able to see the view
- View – the user will be able to see the view and look at the information in it, but they will not be able to edit the information in any way
- Edit – the user has full access to look at and to modify the information

To set different permissions for different views, set the Permission field to the highest level you want to set, then, in the View/Access list below, select the required lower level access for each view that does not share the higher level access.

For example, in the case of the ODEX Administrator application, if you want a user group to have Edit access to the Trading Partners view and View access to all other views, you would do the following:

- select ODEX Administrator in the Application field
- select Edit in the Permission field
- highlight each entry in turn in the View/Access list, with the exception of the Trading Partners entry, and click the **View** button. The View value in the View/Access list will take precedence over the Edit value in the Permission field.
- leave the Trading Partners entry as Edit.

View/Access list

The View/Access list on this dialog shows a list of all the views belonging to the selected application, and the type of permission this user group has to each of those views. To begin with, all views will show a permission type which matches that shown in the Permissions field above.

None, **View**, **Edit**

These buttons should only be used if you want to set different access permissions for different views of the application. If you want to set the same permission for every view of an application, just use the Permission field above.

Use these buttons to apply a lower level of access than that selected in the Permissions field, to some of the views for this user group. Highlight each affected view in the list and press the appropriate button at the bottom.

For example, in the case of the ODEX Administrator application, if you want a user group to have no access to the System Settings view and View access to all other views, you would do the following:

- select ODEX Administrator in the Application field
- select View in the Permission field
- highlight the System Settings entry in the View/Access list and click the **None** button, to set the System Settings Access to None
- leave all the other views' access as Edit – the View value in the Permission field will take precedence over the Edit value in the View/Access list.

Help

If you need more information about the fields on the Permissions page and how to fill them in, click on the **Help** button.

Cancel

If you do not want to save changes you have made, click the **Cancel** button to discard your changes.

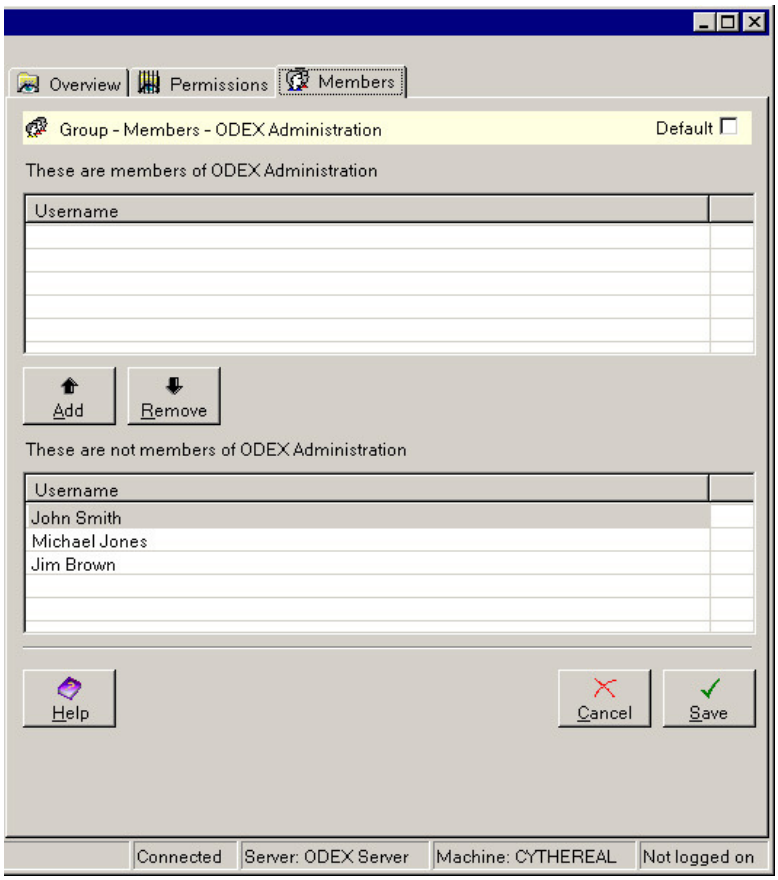
Save

To save all the changes you have made on the Permissions page, click the **Save** button.

Members

This page will not be present if you are using Windows NT security.

This page allows you to add members (users) to or remove members from this user group.



The fields and buttons on this page are as follows:

Members list

The members list displays all the users belonging to this user group.

Add, Remove

You may add users from the non-members list to the members list by pressing the **Add** button, and remove users from the members list by pressing the **Remove** button. Using the **Add** button removes a member from the lower list and adds it to the upper list. Using the **Remove** button removes a member from the upper list and adds it to the lower list.

Non-members list

The non-members list displays all the users that do not belong to this user group.

Help

If you need more information about the fields on the Members page and how to fill them in, click on the **Help** button.

Cancel

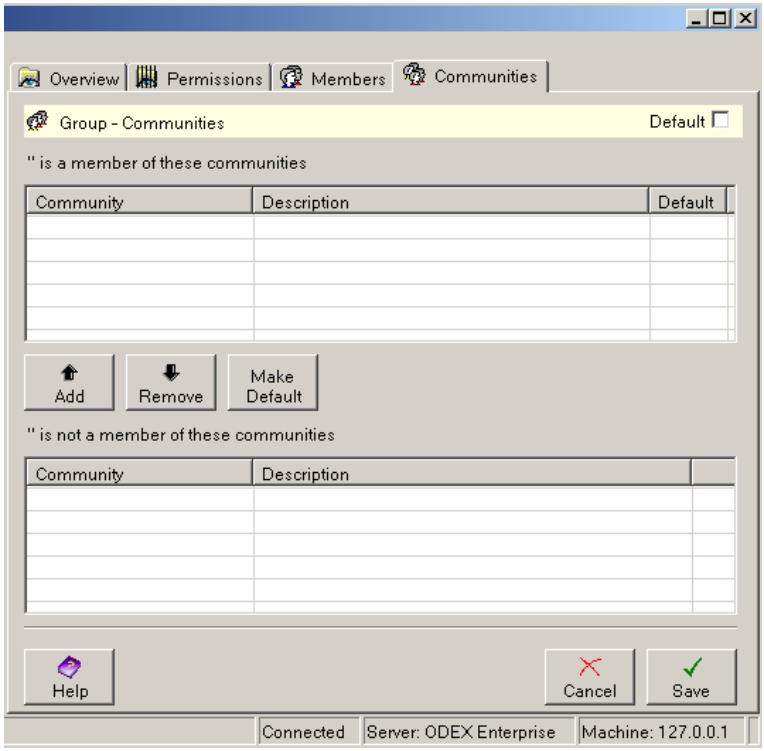
If you do not want to save changes you have made, click the **Cancel** button to discard your changes.

Save

To save all the changes you have made on the Members page, click the **Save** button.

Communities

This page allows you to add the group to or remove the group from a community.



The fields and buttons on this page are as follows:

Members list

The members window shows a list of all the communities of which this group is a member.

Add, Remove

You may add communities from the non-members list to the members list by pressing the **Add** button, and remove communities from this list by pressing the **Remove** button. Using the **Add** button removes a community from the lower list and adds it to the upper list. Using the **Remove** button removes a community from the upper list and adds it to the lower list.

Make Default

When a group is a member of multiple communities, this allows you to set the default community for the group. When a user that is a member of a group that is a member of one community creates a company or network, the company or network will be associated with that group's community and will only be visible to members of that community.

When a group is a member of multiple communities, any companies or networks created by members of that group will be associated with the default community, unless the user selects a different community when they create the company or network.

If a user has a default community and that user is a member of a group that has a different default community, the user's default community will be used as the default.

Non-members list

The non-members list shows a list of all the communities to which users that are a member of this group do not have access.

Help

If you need more information about the fields on the Groups page and how to fill them in, click on the **Help** button.

Cancel

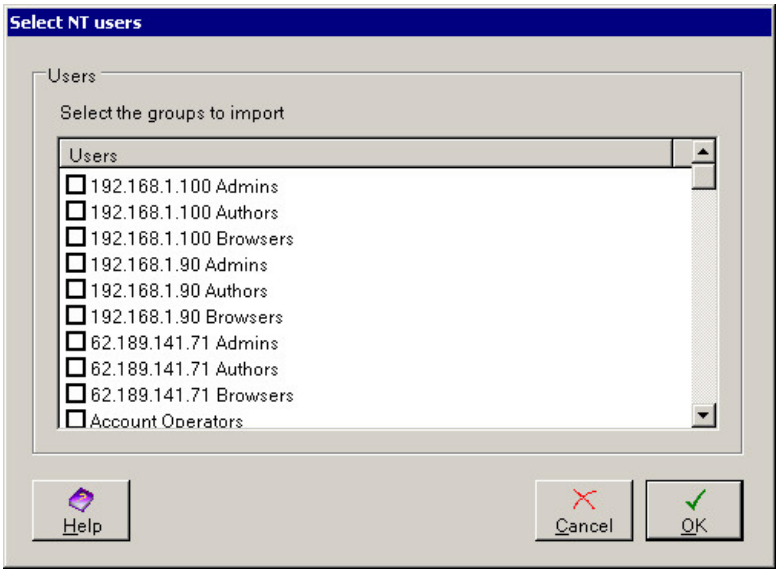
If you do not want to save changes you have made, click the **Cancel** button to discard your changes.

Save

To save all the changes you have made on the Groups page, click the **Save** button.

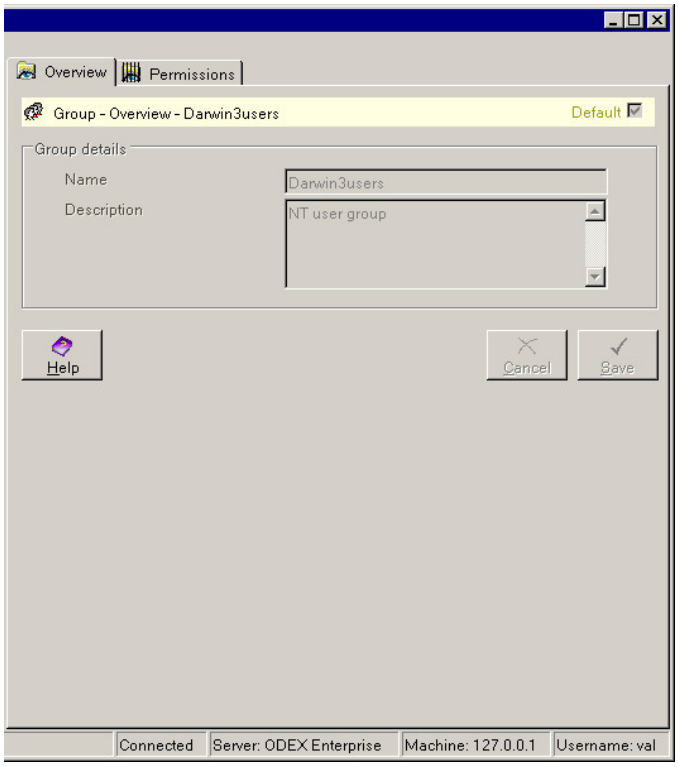
Importing a new group

When you click the **New** button from the User Groups – Actions page, you will see the "Select the groups to import dialog", as shown below.



Using the checkboxes, select the user groups you want to import as ODEX user groups, then click **OK**. This will return you to the User Groups – Actions page where, if you expand the User Groups tree node, you will be able to see the imported user groups in the list.

Select one of the imported user groups to see the Group – Overview page, as shown below.

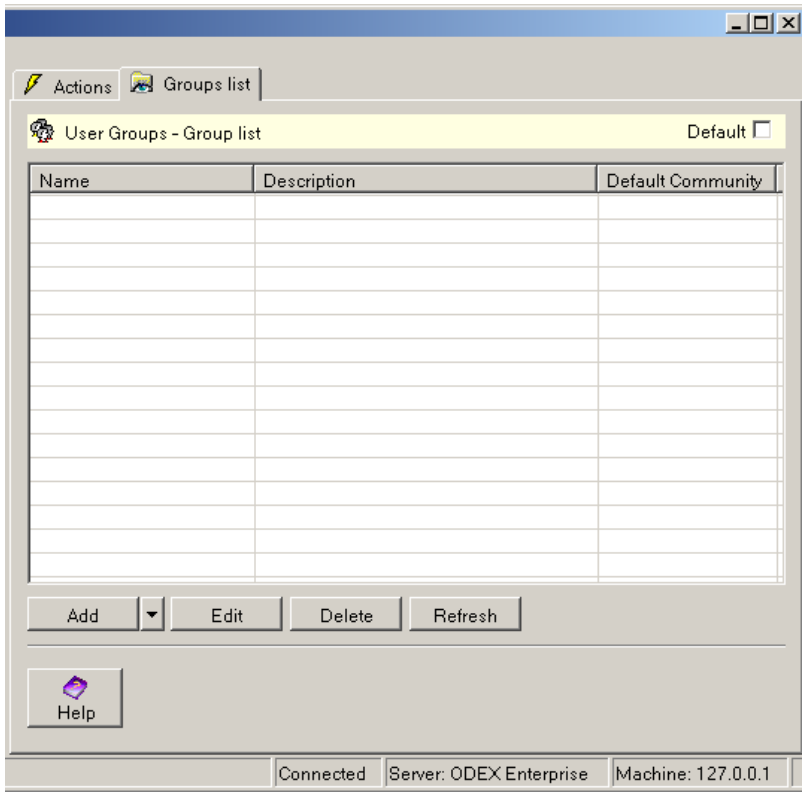


All fields on this page are disabled, since you cannot change anything to do with Windows user accounts from within ODEX.

The remaining pages for importing a user group are the same as those for adding a new user group, except that there is no Members page. Again, this is because you cannot change anything to do with Windows user accounts from within ODEX. For details of these remaining pages, please continue reading from the section entitled "User Group Permissions".

View group list

When you click the **View** button from the Groups – Actions page, you will then see the User Groups – Group list page, as shown below.



The main part of this page consists of a window with three columns: Name, Description and Default Community. This window lists all the ODEX user groups that are currently profiled, showing their name, a description (if you have provided one) and the name of the group's default community, if they are a member of any communities..

This page also has five buttons: **Add**, **Edit**, **Delete**, **Refresh** and **Help**. Let's have a look at each one in turn and find out what they do.

Add

Click on the **Add** button if you want to add a new group to the group list. You will be able to choose between adding a group with no permissions and a power group. This will bring up the set of pages described in the section entitled "Adding a new group".

Edit

Highlight a group in the list and click on the **Edit** button if you want to amend the details for the selected group. This will bring up the same set of pages described in the section entitled "Adding a new group".

Delete

Highlight a group in the list and click on the **Delete** button if you want to delete the selected group from the list.

Refresh

Click on the **Refresh** button to refresh the details on this page e.g. if a change you have just made is not reflected in the details you can see.

Help

If you need more information about the Group list page and how to use it, click on the **Help** button.

Communities

A community is a way to restrict the data that users and groups can view in the ODEX applications. A user or group can be a member of one or more communities.

In the administrator client, when a user logs on who is a member of one or more communities, that user can then only view networks and trading partners that are associated with the communities that they are members of.

In the workstation client, when a user logs on who is a member of one or more communities, they will only see files that are associated with networks that they have permission to view.

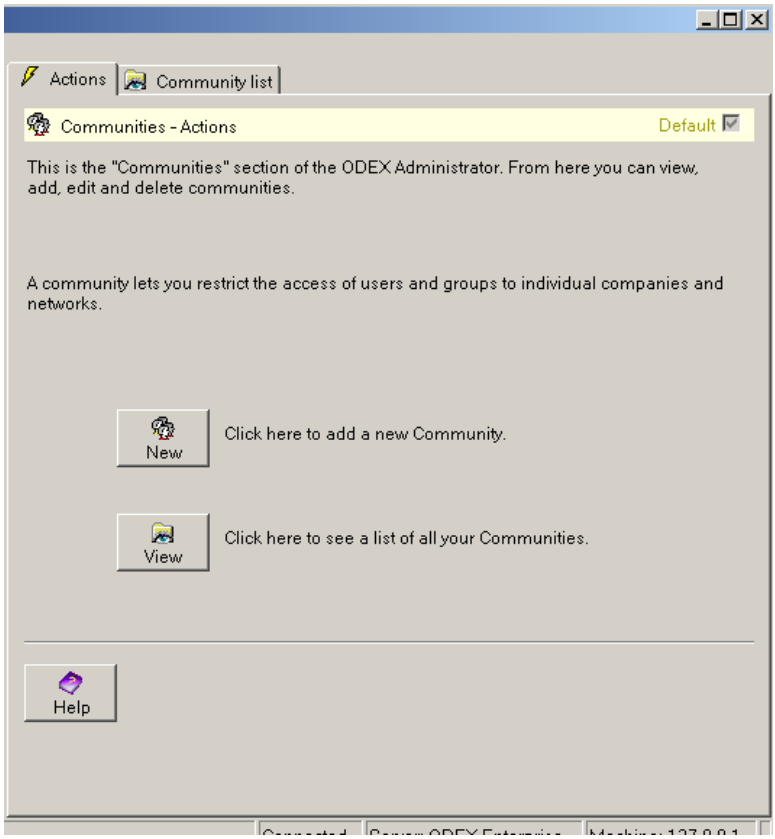
In the communications monitor client, only sessions between networks that the user has permission to view are visible in the session list.

This section of the System Administrator allows you to add new communities and view, edit and delete the communities that you have profiled in ODEX. However, you will not be able to access this part of the System Administrator unless you have been given the required permission.

You can access the Communities section either via the Navigation Panel tree view or via the Information Panel on the right.

To see the Community's section, click on the Community's name in the Navigation Panel of the System Administrator. This will bring up the default

page of the Community's section in the Information Panel on the right, as shown below.



There are two pages in the Communities section, called Actions and Community List.

Let's have a look at these two pages and see how to use them.

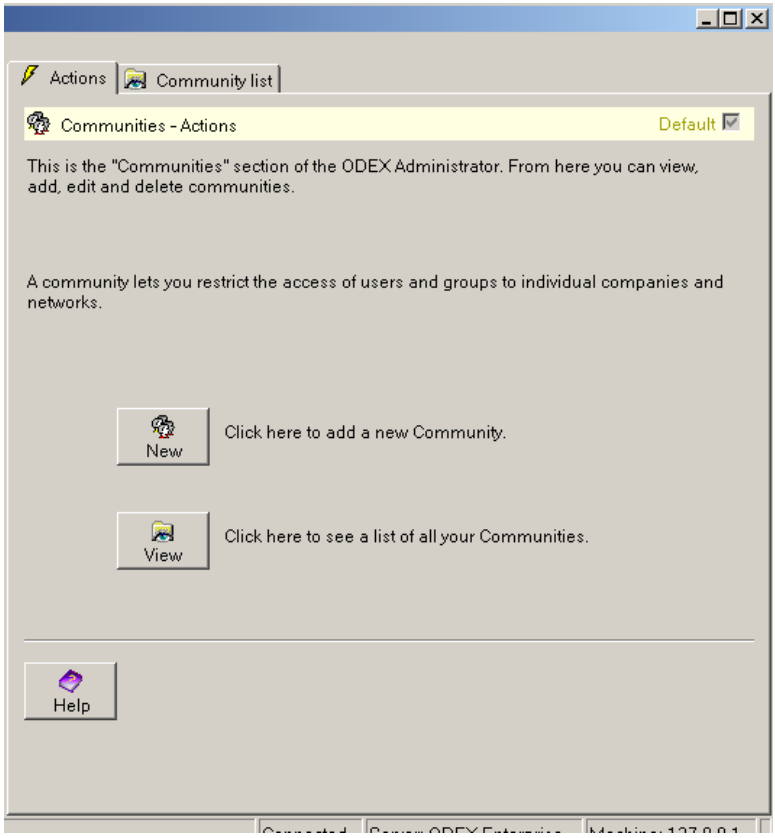
Communities – Actions page

Before editing the Communities section, please refer to the section entitled "User Security", in order to understand what users, user groups and communities are all about.

You need to edit the System Settings section before editing this section, in order to choose what type of user security you want to use.

To add a new community or view a list of all communities, click once on the Communities node in the tree view. This will bring up the Communities – Actions page.

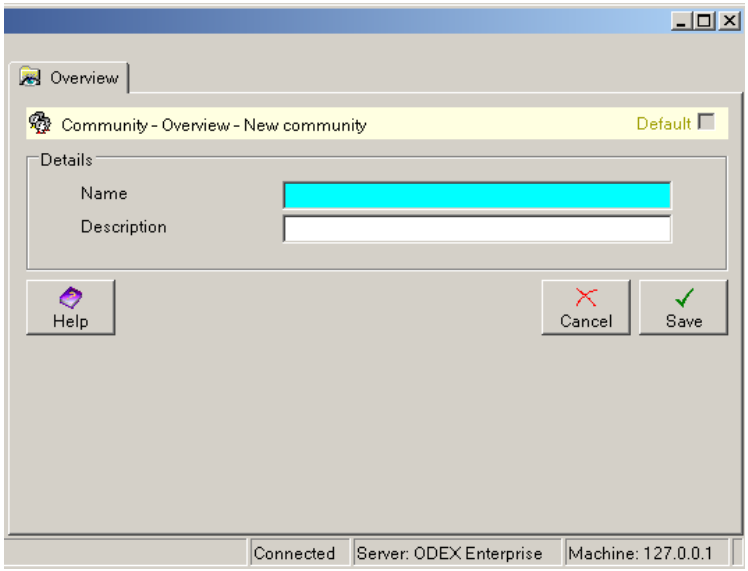
There are two buttons on this page – **New**, and **View**.



Adding a new community

Before editing the Communities section, please refer to the section entitled "User Security", in order to understand what users, user groups and communities are all about.

When you click the **New** button from the Communities – Actions page, you will see the Community – Overview page, as shown below.

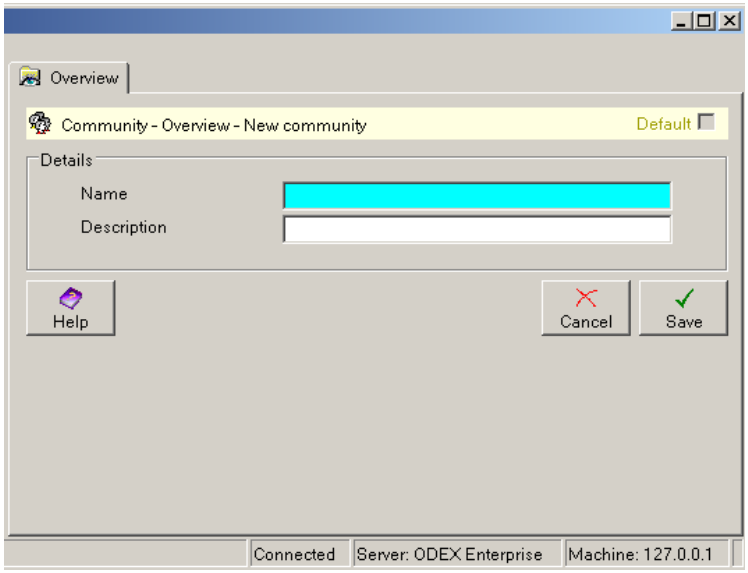


As you can see, it has a single tab, the overview tab. This is described below.

Overview

Before editing the Communities section, please refer to the section entitled "User Security", in order to understand what users, user groups and communities are all about.

This page allows you to add the details of a new community in ODEX, or change the details of an existing community.



The fields and buttons on this page are as follows:

Details – Name

Type in this field a name for the community

Details – Description

Type in this field a description for the community. This field is optional.

Help

If you need more information about the fields on the Overview page and how to fill them in, click on the **Help** button.

Cancel

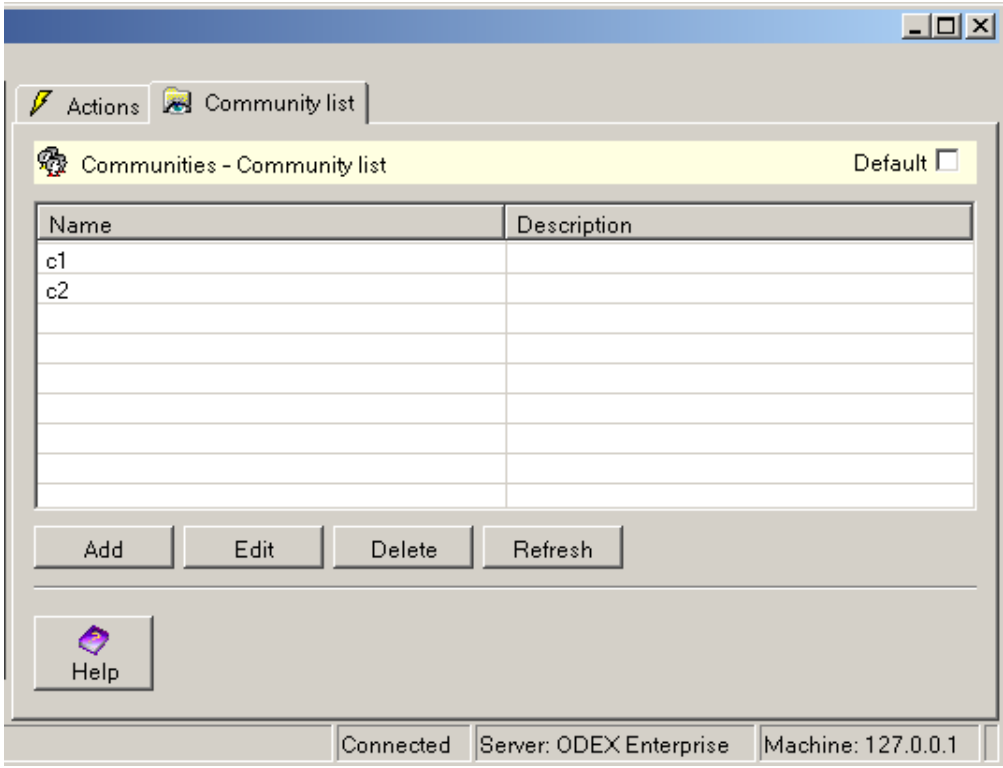
If you do not want to save changes you have made, click the **Cancel** button to discard your changes.

Save

To save all the changes you have made on the Overview page, click the **Save** button.

View Community List

When you click the **View** button to see a list of all ODEX communities, you will then see a page which looks like the one shown below.



The main part of this page consists of a window with two columns: Name, and Description. This window lists all the ODEX communities that are currently profiled, showing their name and their description, if they have one.

This page also has five buttons: **Add**, **Edit**, **Delete**, **Refresh**, and **Help**. Let's have a look at each one in turn and find out what they do.

Add

Click on the **Add** button if you want to add a new community to the community list.

Edit

Highlight a community in the list and click on the **Edit** button if you want to amend the details for the selected community. This will bring up the set of pages described in the section entitled "Adding a new user community".

Delete

Highlight a community in the list and click on the **Delete** button if you want to delete the selected community from the list.

Refresh

Click on the **Refresh** button to refresh the details on this page e.g. if a change you have just made is not reflected in the details you can see.

Help

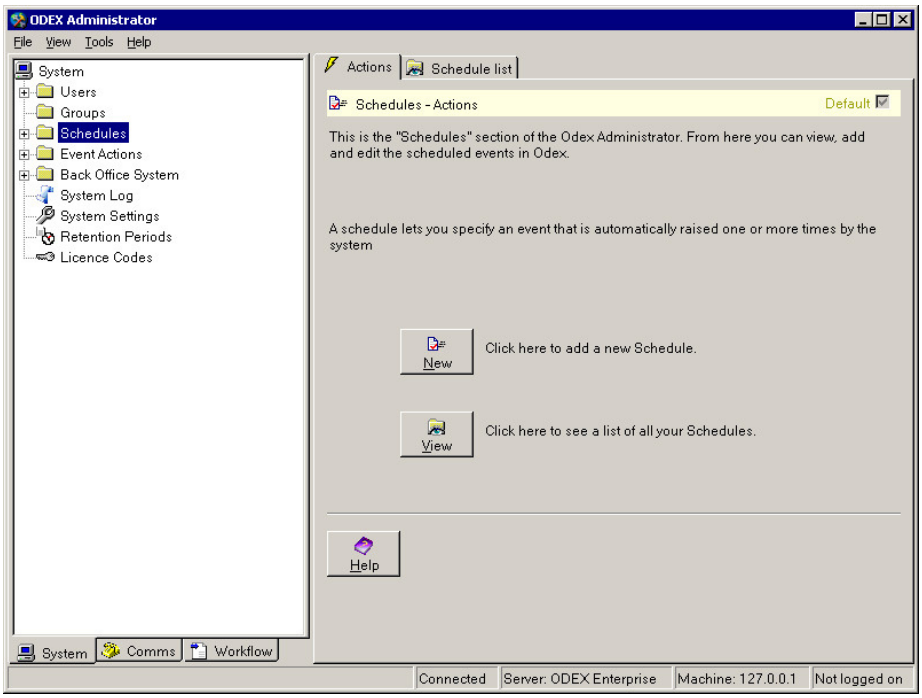
If you need more information about the User list page and how to use it, click on the **Help** button.

Schedules

This section of the System Administrator allows you to view, add and edit the schedules in ODEX.

Before continuing with this section, please ensure that you are familiar with the concept of schedules by reading the section entitled "Schedules and Event Actions".

Click on the name Schedules in the Navigation Panel to see the default page for the Schedules section, as shown below. This is the Schedules – Actions page.



The Schedules section allows you to add, view and edit the schedules in ODEX.

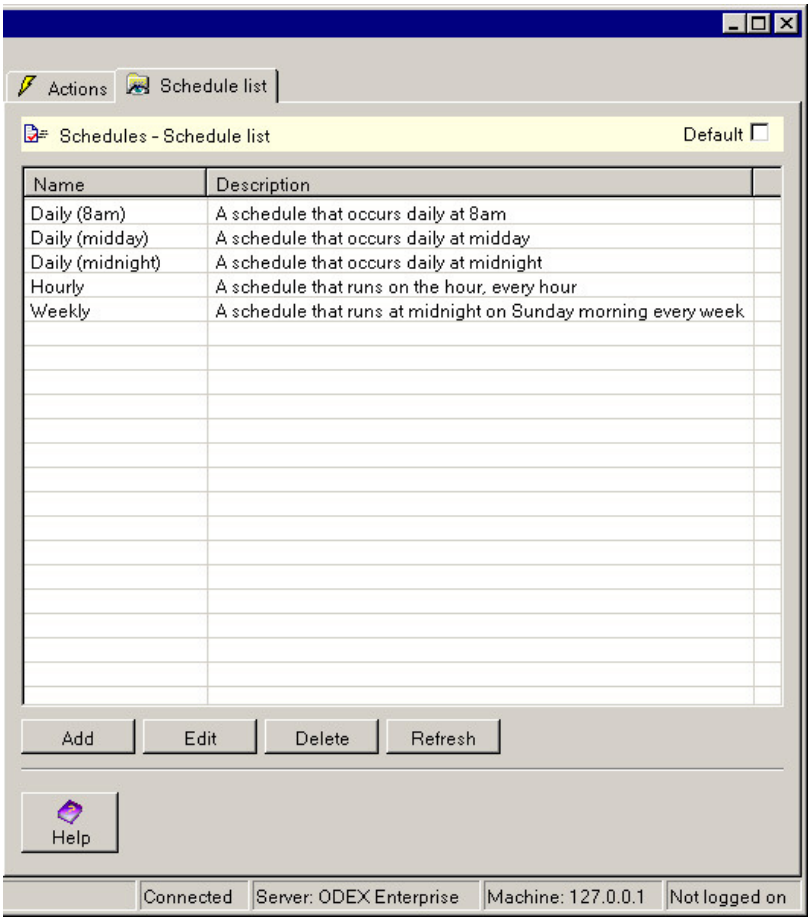
As you can see, there are two page tabs on the Information Panel (Actions and Schedule list) and two buttons, labelled **New** and **View**. The **New** button allows you to add a new schedule. The **View** button allows you to see a list of all the existing schedules, from where you can edit their details, add new entries or delete existing entries.

Viewing all your schedules

If you wish to see a list of all the schedules currently in the ODEX database, you can either click the **View** button on the Schedules – Actions page or click the Schedules list tab. Both have the same result, as in the example below.

As you can see, five schedules have already been defined for you.

You may edit the details of any of these pre-defined schedules if you wish.



The Information Panel now shows the Schedule list page. This is divided into two columns, showing the Schedule Name and its description.

The actions that can be taken from this page are as follows:

Add

New schedules may be added to the list by using the **Add** button. If this button is clicked, it will bring up the set of pages described below under the heading "Adding/Editing Schedules".

Edit

You may edit the details of existing schedules by using the **Edit** button. If this button is clicked, it will bring up the same set of pages described below under the heading "Adding/Editing Schedules".

Delete

If you wish to delete a schedule from the list, highlight the line that you wish to delete, then click on the **Delete** button. ODEX will bring up a dialog box, asking if you are sure you want to delete the selected items. This is to safeguard against accidentally deleting the wrong item. Click **Yes** to delete or **No** to keep the item in the list.

Refresh

Click this button to refresh the details on this page, for example if you have just made some changes which have not yet appeared on this page.

Help

If you need more information about the fields and buttons on this page, click on the **Help** button.

Adding/Editing Schedules

If you wish to add a new schedule, click the **New** button on the Schedules – Actions page. You can also add a new schedule by clicking on the **Add** button on the Schedule list page of the Schedules section.

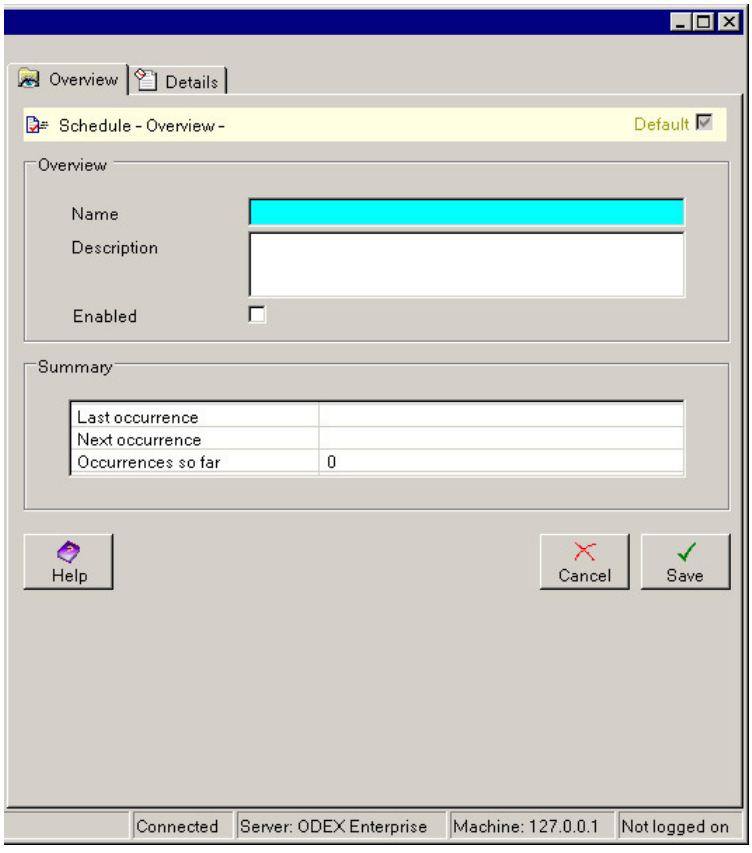
To edit an existing schedule, open the Schedule list page, select the schedule to be edited, and click the **Edit** button. Alternatively, double-click on the Schedules node in the tree view, then click once on the schedule to be edited.

Whichever route you choose, you will be presented with the following set of pages, enabling you to add or edit details of a schedule. There are two pages associated with schedules, so let's go through them and find out what information is required.

One point to remember – each of the **Save** and **Cancel** buttons in the Schedules section work for both Schedules pages, so you do not need to click the **Save** button until you have entered data on both pages. You can click the **Cancel** button at any point to undo changes that you have made.

Schedule – Overview

The Overview page is where you must provide a name for the new schedule and where a summary of the schedule occurrences is displayed. The Overview page looks like the example below.



Overview – Name

This field requires a name for the schedule.

Overview – Description

You may provide a description in this field if you wish.

Overview – Enabled

Select this tickbox if you want this schedule to be enabled.

Summary – Last occurrence

This field shows you when this schedule last occurred.

Summary – Next occurrence

This field shows you when this schedule is next due to occur.

Summary – Occurrences so far

This field shows you how many times this schedule has occurred so far.

Schedule – Details

The Details page is where you provide all the details for the schedule. The dialog contents will change according to which option you select in the Style field.

If you are not sure which style to choose, or how to fill in the field values, it may be helpful to have a look at the settings used for one or more of the schedules that have been provided for you (Daily, Hourly, Weekly).

Recurrence style – Style

This field allows you to select how often you want the schedule to occur. Choose from:

Occur once – the event will be run once only

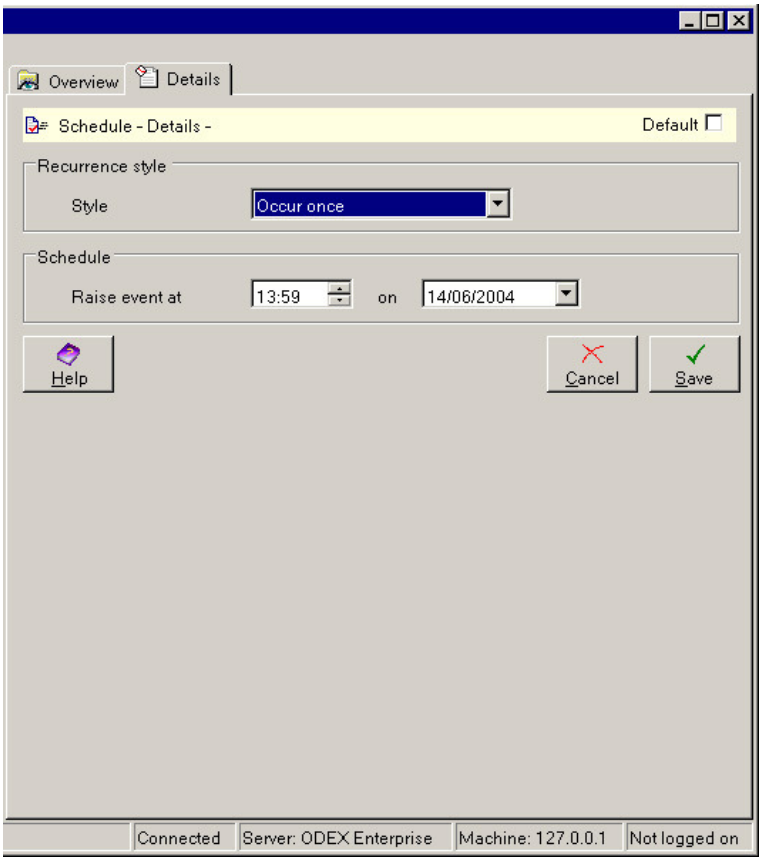
Recur X times – the event will run for the given number of times only

Recur until – the event will run at the specified interval until the specified date and time arrives

Recur forever – the event will run at the specified interval forever. If you want to stop it running for any reason, you can deselect the 'Enabled' tickbox on the Overview page.

Occur once

If you select Occur once in the Style field, the dialog will change to look like the one shown below.



Schedule – Raise event at

Select the time at which you want this schedule to operate.

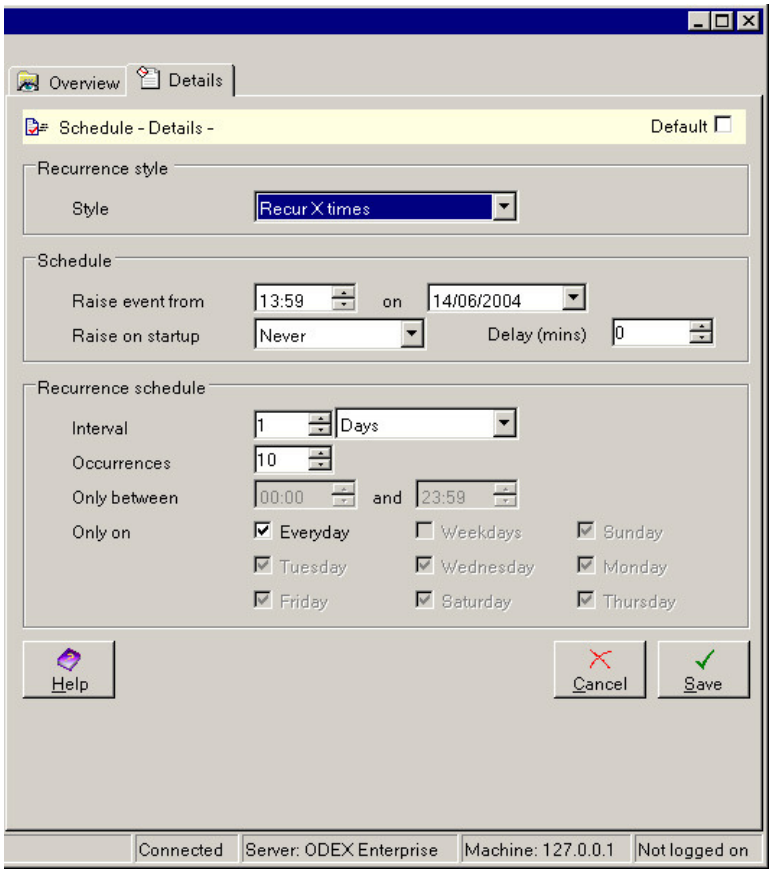
Schedule – on

Select the date on which you want this schedule to operate.

The date and time must be in the future, otherwise the schedule cannot take effect.

Recur X times

If you select Recur X times in the Style field, the dialog will change to look like the one shown below.



Schedule – Raise event from

Select the time at which you want this schedule to begin. This does not necessarily mean that the event will occur at this time. This will depend on the other settings you choose.

Schedule – on

Select the date on which you want this schedule to begin. This does not necessarily mean that the event will occur on this date. This will depend on the other settings you choose.

Schedule – Raise on startup

Startup means when the ODEX Server is started. The three available settings for this field are: Always, If missed and Never. Their meanings are described below.

- Always – always run this event when the ODEX Server is started.
- If missed – only run this event if the ODEX Server is started after the time at which the event should have run.
- Never – never run this event when the ODEX Server is started.

Schedule – Delay (mins)

This field is used in conjunction with the Raise on startup field. If you select "Always" or "If missed" in that field, ODEX will run this event when the ODEX Server is started, but after a delay of the selected number of minutes.

Recurrence schedule – Interval

This field allows you to choose how often (at what interval) the event is to be run. Select a number of Minutes, Hours, Days or Weeks.

Recurrence schedule – Occurrences

Use the dropdown arrow to select how many times you want this event to occur.

Recurrence schedule – Only between

This field will only be enabled if you select Minutes or Hours in the Interval field.

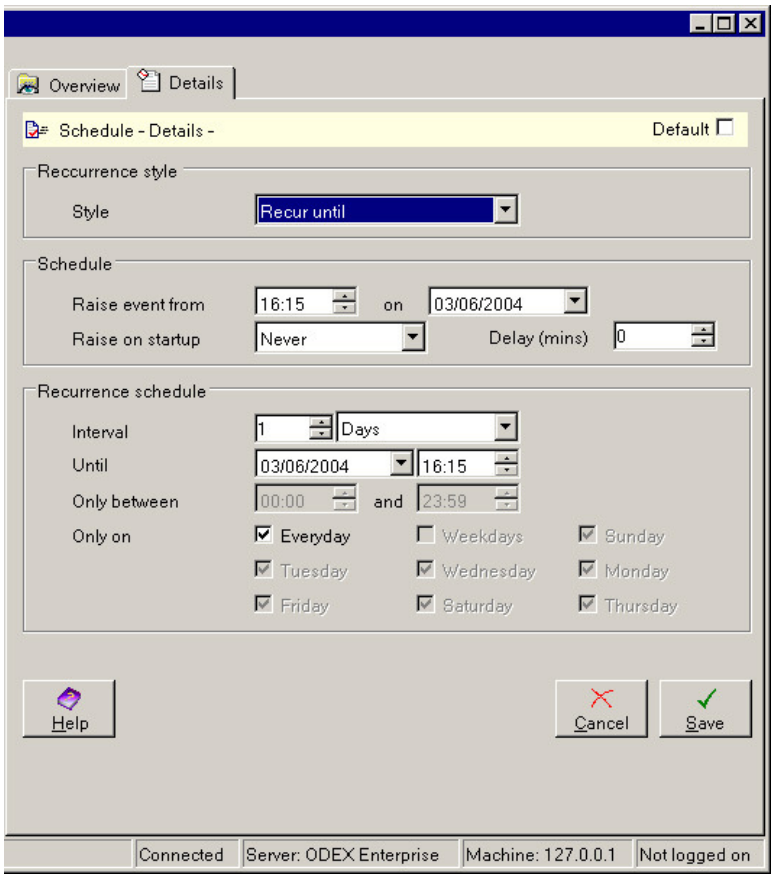
This field allows you to restrict the hours between which the event will run. For 24-hour availability, leave the settings as 00:00 and 23:59.

Recurrence schedule – Only on

By default the 'Everyday' tickbox is selected. To select one or more of the other options, first deselect the 'Everyday' tickbox to enable the others.

Recur until

If you select Recur until in the Style field, the dialog will change to look like the one shown below.



Schedule – Raise event from

Select the time at which you want this schedule to begin. This does not necessarily mean that the event will occur at this time. This will depend on the other settings you choose.

Schedule – on

Select the date on which you want this schedule to begin. This does not necessarily mean that the event will occur on this date. This will depend on the other settings you choose.

Schedule – Raise on startup

Startup means when the ODEX Server is started. The three available settings for this field are: Always, If missed and Never. Their meanings are described below.

- Always – always run this event when the ODEX Server is started.
- If missed – only run this event if the ODEX Server is started after the time at which the event should have run.
- Never – never run this event when the ODEX Server is started.

Schedule – Delay (mins)

This field is used in conjunction with the Raise on startup field. If you select Always or If missed in that field, ODEX will run this event when the ODEX Server is started, but after a delay of the selected number of minutes.

Recurrence schedule – Interval

This field allows you to choose how often (at what interval) the event is to be run. Select a number of Minutes, Hours, Days or Weeks.

Recurrence schedule – Until

Use the dropdown arrow to select the date and time at which you want this schedule to stop operating.

Recurrence schedule – Only between

This field will only be enabled if you select Minutes or Hours in the Interval field.

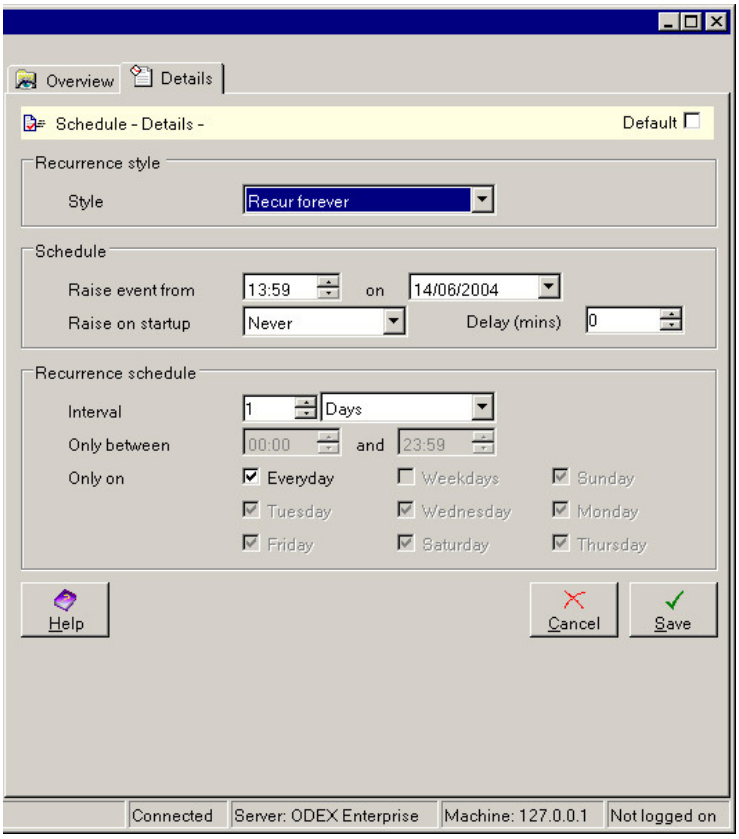
This field allows you to restrict the hours between which the event will run. For 24-hour availability, leave the settings as 00:00 and 23:59.

Recurrence schedule – Only on

By default the 'Everyday' tickbox is selected. To select one or more of the other options, first deselect the 'Everyday' tickbox to enable the others.

Recur forever

If you select Recur forever until in the Style field, the dialog will change to look like the one shown below.



Schedule – Raise event from

Select the time at which you want this schedule to begin. This does not necessarily mean that the event will occur at this time. This will depend on the other settings you choose.

Schedule – on

Select the date on which you want this schedule to begin. This does not necessarily mean that the event will occur on this date. This will depend on the other settings you choose.

Schedule – Raise on startup

Startup means when the ODEX Server is started. The three available settings for this field are: Always, If missed and Never. Their meanings are described below.

- Always – always run this event when the ODEX Server is started.
- If missed – only run this event if the ODEX Server is started after the time at which the event should have run.
- Never – never run this event when the ODEX Server is started.

Schedule – Delay (mins)

This field is used in conjunction with the Raise on startup field. If you select Always or If missed in that field, ODEX will run this event when the ODEX Server is started, but after a delay of the selected number of minutes.

Recurrence schedule – Interval

This field allows you to choose how often (at what interval) the event is to be run. Select a number of Minutes, Hours, Days or Weeks.

Recurrence schedule – Only between

This field will only be enabled if you select Minutes or Hours in the Interval field.

This field allows you to restrict the hours between which the event will run. For 24-hour availability, leave the settings as 00:00 and 23:59.

Recurrence schedule – Only on

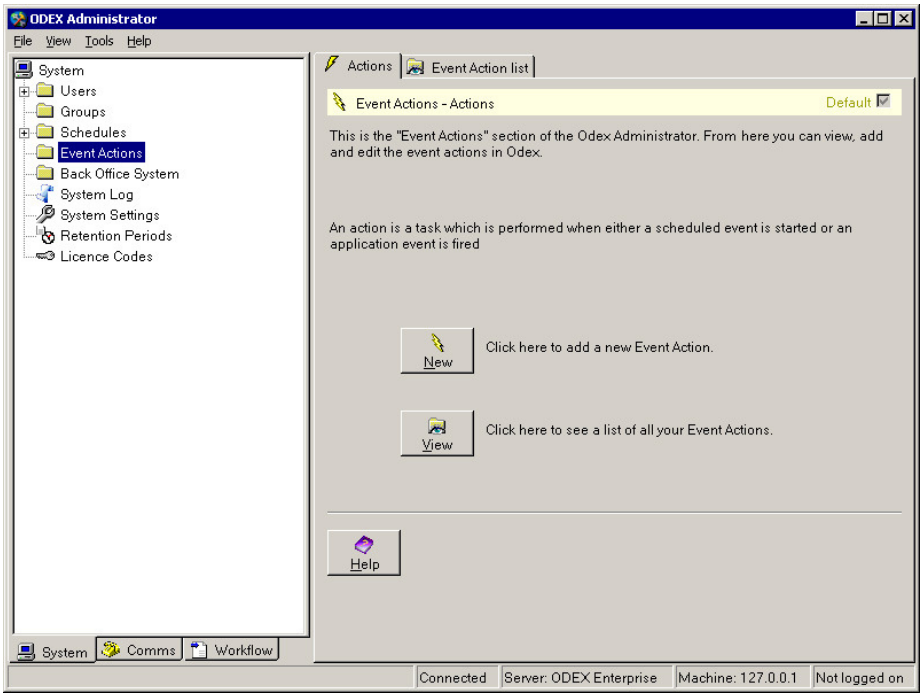
By default the 'Everyday' tickbox is selected. To select one or more of the other options, first deselect the 'Everyday' tickbox to enable the others.

Event Actions

This section of the System Administrator allows you to view, add and edit the event actions in ODEX.

Before continuing with this section, please ensure that you are familiar with the concept of scheduled events and actions by reading the section entitled "Schedules and Event Actions".

Click on the name Event Actions in the Navigation Panel to see the default page for the Event Actions section, as shown below. This is the Event Actions – Actions page.

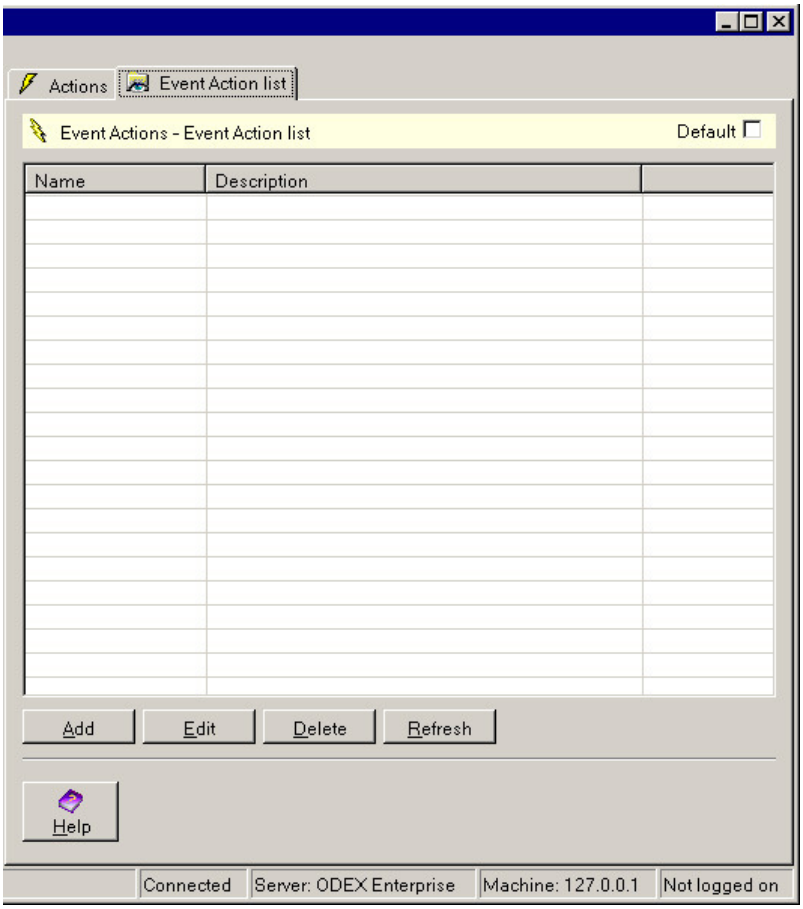


The Event Actions section allows you to add, view and edit the event actions in ODEX.

As you can see, there are two page tabs on the Information Panel (Actions and Event Actions list) and two buttons, labelled **New** and **View**. The **New** button allows you to add a new event action. The **View** button allows you to see a list of all the existing event actions, from where you can edit their details, add new entries or delete existing entries.

Viewing all your event actions

If you wish to see a list of all the event actions currently in the ODEX database, you can either click the **View** button on the Event Actions – Actions page or click the Event Actions list tab. Both have the same result, as in the example below.



The Information Panel now shows the Event Action list page. This is divided into two columns, showing the Event Action Name and its description.

The actions that can be taken from this page are as follows:

Add

New event actions may be added to the list by using the **Add** button. If this button is clicked, it will bring up the set of pages described below under the heading "Adding/Editing Event Actions".

Edit

You may edit the details of existing event actions by using the **Edit** button. If this button is clicked, it will bring up the same set of pages described below under the heading "Adding/Editing Event Actions".

Delete

If you wish to delete an event action from the list, highlight the line that you wish to delete, then click on the **Delete** button. ODEX will bring up a dialog box, asking if you are sure you want to delete the selected items. This is to safeguard against accidentally deleting the wrong item. Click **Yes** to delete or **No** to keep the item in the list.

Refresh

Click this button to refresh the details on this page, for example if you have just made some changes which have not yet appeared on this page.

Help

If you need more information about the fields and buttons on this page, click on the **Help** button.

Adding/Editing Event Actions

If you wish to add a new event action, click the **New** button on the Event Actions – Actions page. You can also add a new event action by clicking on the **Add** button on the Event Action list page of the Event Actions section.

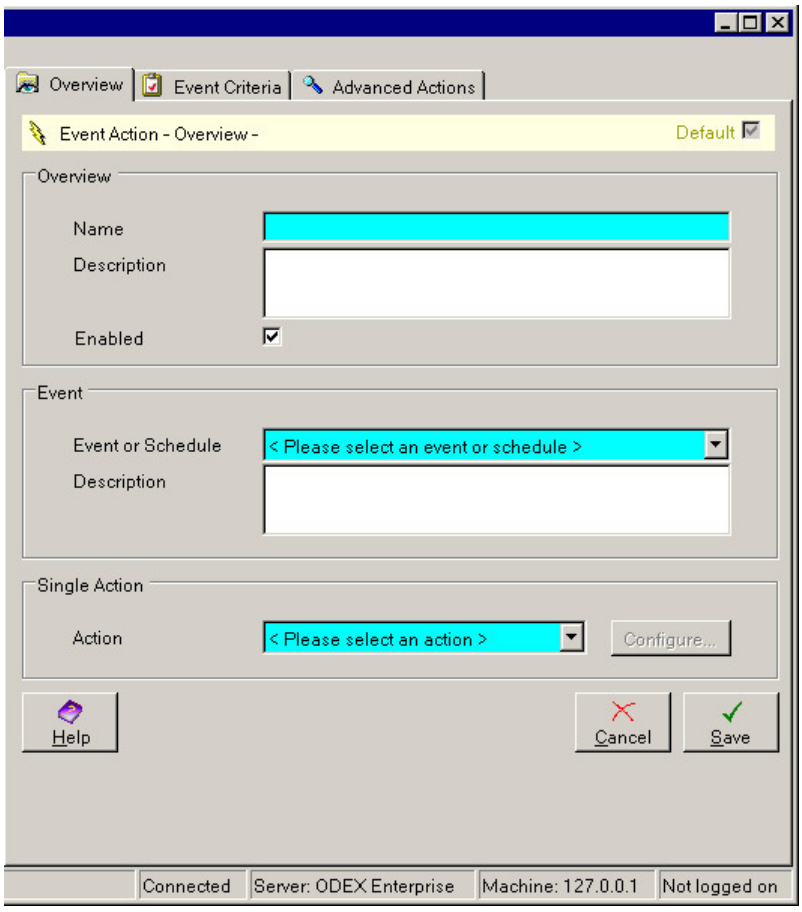
To edit an existing event action, open the Event Action list page, select the event action to be edited, and click the **Edit** button. Alternatively, double-click on the Event Actions node in the tree view, then click once on the event action to be edited.

Whichever route you choose, you will be presented with the following set of pages, enabling you to add or edit details of an event action. There are three pages associated with event actions, so let's go through them and find out what information is required.

One point to remember – each of the **Save** and **Cancel** buttons in the Event Actions section work for all three Event Actions pages, so you do not need to click the **Save** button until you have finished entering data. You can click the **Cancel** button at any point to undo changes that you have made.

Event Action – Overview

The Overview page is where you must provide a name for the new event action and where you must decide on the type of event action you want to create. The Overview page looks like the example below.



Overview – Name

This field requires a name for the event action.

Overview – Description

You may provide a description in this field if you wish.

Overview – Enabled

Select this tickbox if you want this event action to be enabled.

Event – Event or Schedule

Select an event or schedule from the dropdown list. This is the system event or schedule that you want to trigger one or more actions. For a full list of all the events and their criteria, please refer to the section entitled “Events”.

You should select an event or schedule before selecting the action(s) it will trigger, so that you can take advantage of the placeholder facility when editing the associated parameters. Please note that the available placeholders will differ according to the event or schedule you select. For a full list of placeholders, please see the section entitled “Placeholders”.

Event – Description

This field displays a description of the event or schedule you have selected in the field above.

Single Action – Action

If you want the selected event or schedule to trigger a single action, select the single action from this dropdown list.

If you want the selected event or schedule to trigger more than one action, you must specify these actions on the Advanced Actions page.

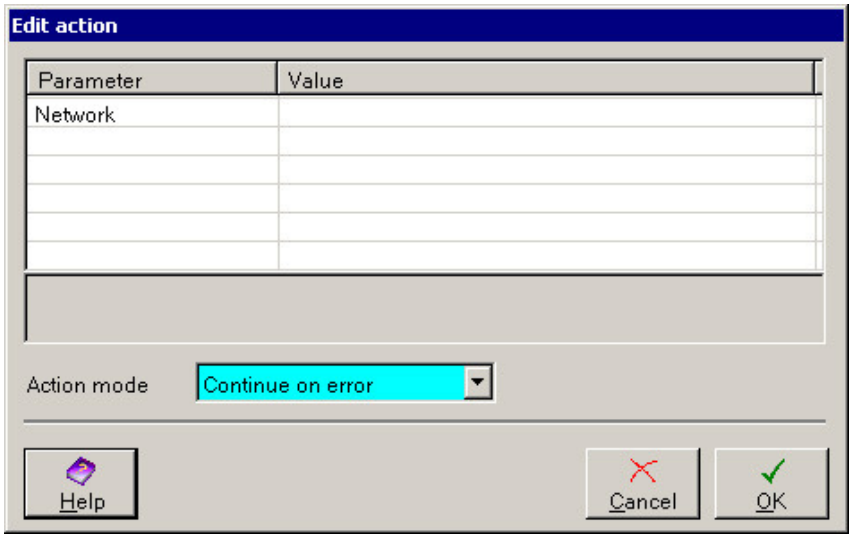
If you use the Advanced Actions page to specify multiple actions, the Single Action section will be disabled.

If you select a single action, you will see the Edit Action dialog appropriate to that action.

For a full list of all the actions and their criteria, please refer to the section entitled “Actions”.

Call Network – Edit Action

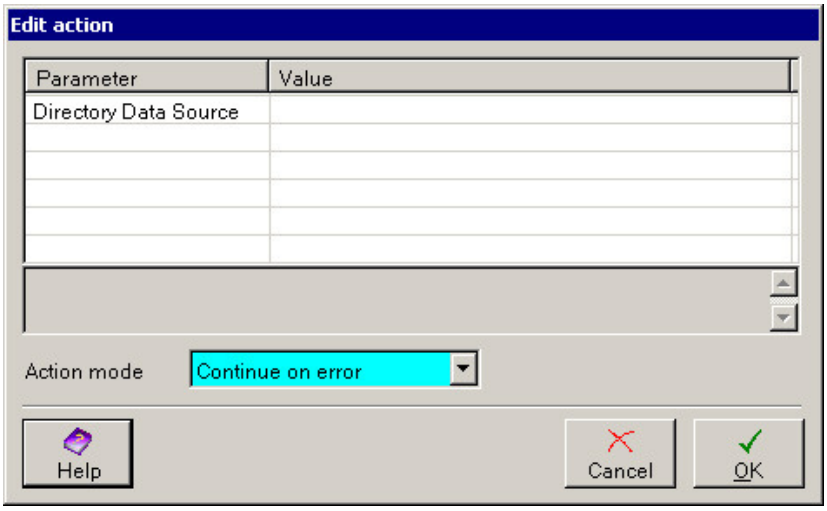
The Edit Action dialog for the Call Network action is shown below.



Double-click on the Network parameter to bring up the associated Edit Parameter dialog, which allows you to edit the value of the Network parameter.

Poll Monitored Directory – Edit Action

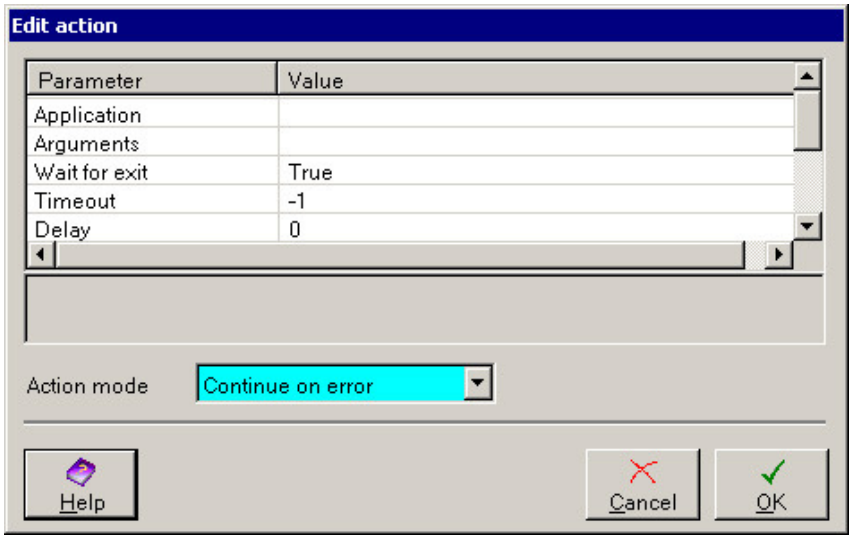
The Edit Action dialog for the Poll Monitored Directory action is shown below.



Double-click on the Directory Data Source parameter to bring up the associated Edit Parameter dialog, which allows you to select a Directory Data Source.

Run Application – Edit Action

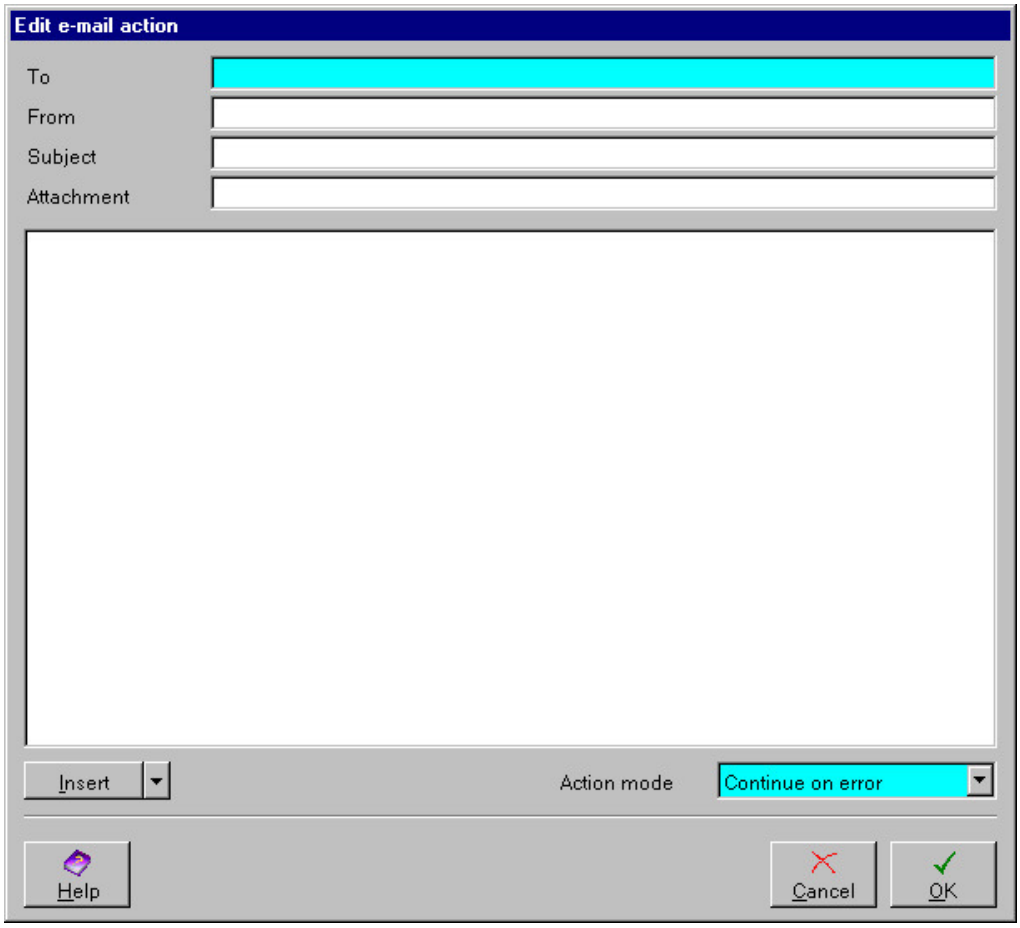
The Edit Action dialog for the Run Application action is shown below.



To edit the value of any parameter, double click on the parameter you want to edit. For a parameter whose value is 'True' or 'False', double-clicking will toggle between the two values. For all other settings, double-clicking will bring up the associated Edit Parameter dialog.

Send E-mail – Edit Action

The Edit Action dialog for the Send E-mail action is shown below.



To – Fill in the To field with the e-mail address of the intended recipient of the e-mail.

From – The From field should be filled in with your e-mail address.

Subject – The Subject field may be filled in with whatever you wish. You may also use the **Insert** button to insert placeholders that will be replaced at run time with the appropriate value.

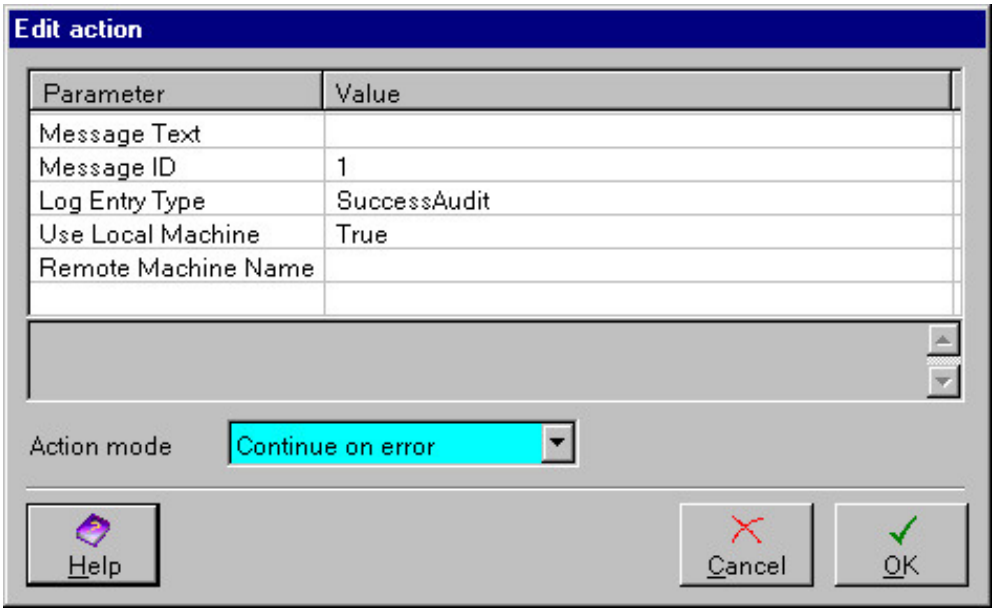
Attachment – You may type in this field the full filepath of any files you wish to send as attachments. Separate each filepath by a semi-colon.

Body – You can write whatever you wish in the body of the e-mail. You may also use the **Insert** button to insert placeholders that will be replaced at run time with the appropriate value.

For a full list of available placeholders, please see the section entitled “Placeholders”.

Windows Application Log – Edit Action

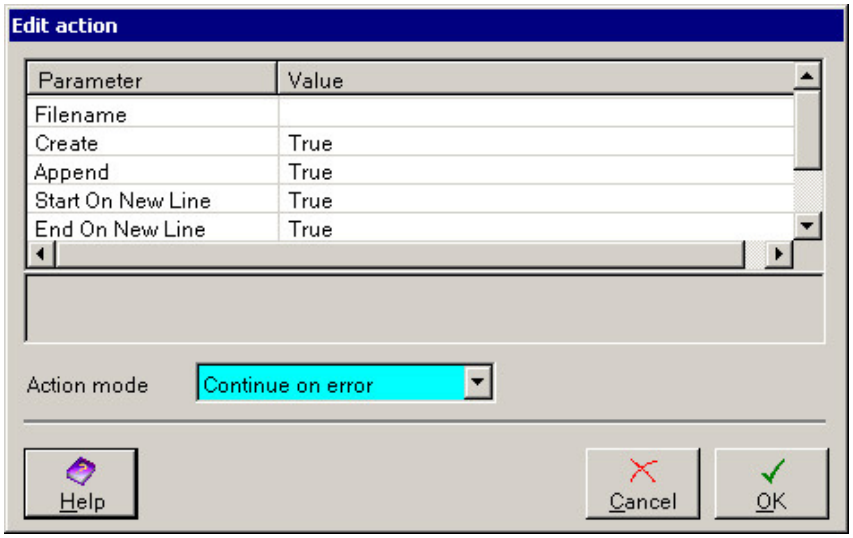
The Edit Action dialog for the Windows Application action is shown below.



To edit the value of any parameter, double click on the parameter you want to edit. For a parameter whose value is 'True' or 'False', double-clicking will toggle between the two values. For all other settings, double-clicking will bring up the associated Edit Parameter dialog.

Write File – Edit Action

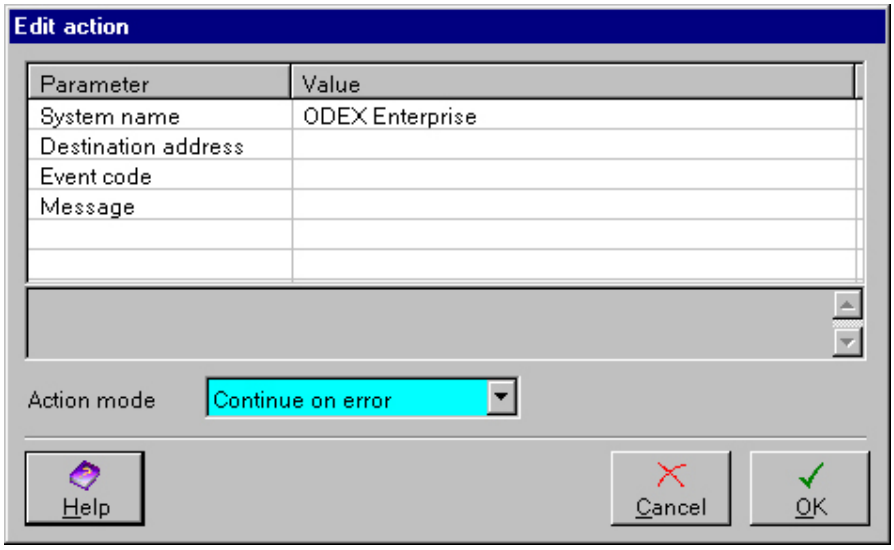
The Edit Action dialog for the Write File action is shown below.



To edit the value of any parameter, double click on the parameter you want to edit. For a parameter whose value is 'True' or 'False', double-clicking will toggle between the two values. For all other settings, double-clicking will bring up the associated Edit Parameter dialog.

Send SNMP Trap – Edit Action

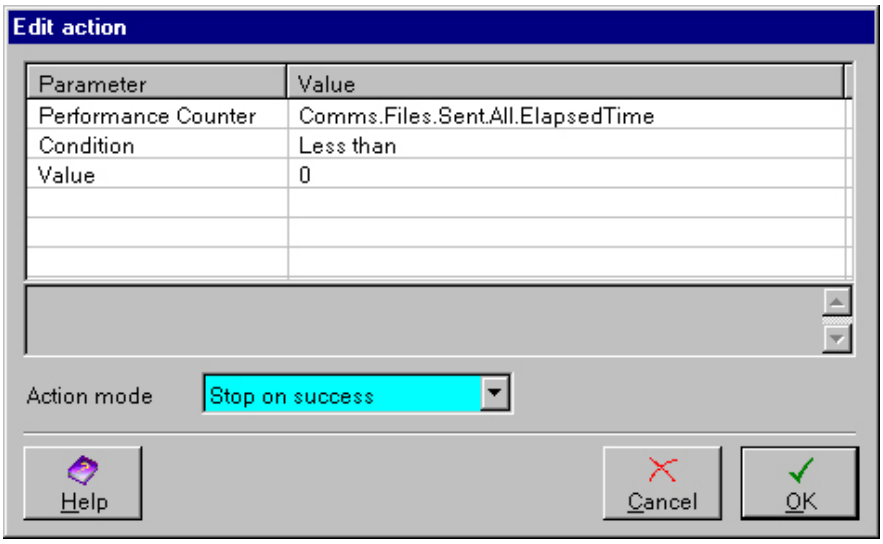
The Edit Action dialog for the Send SNMP Trap action is shown below.



To edit the value of any parameter, double click on the parameter you want to edit. Double-clicking will bring up the associated Edit Parameter dialog. The dialog displayed for editing the Message parameter offers the option to include placeholders in the text.

Check Performance Counter – Edit Action

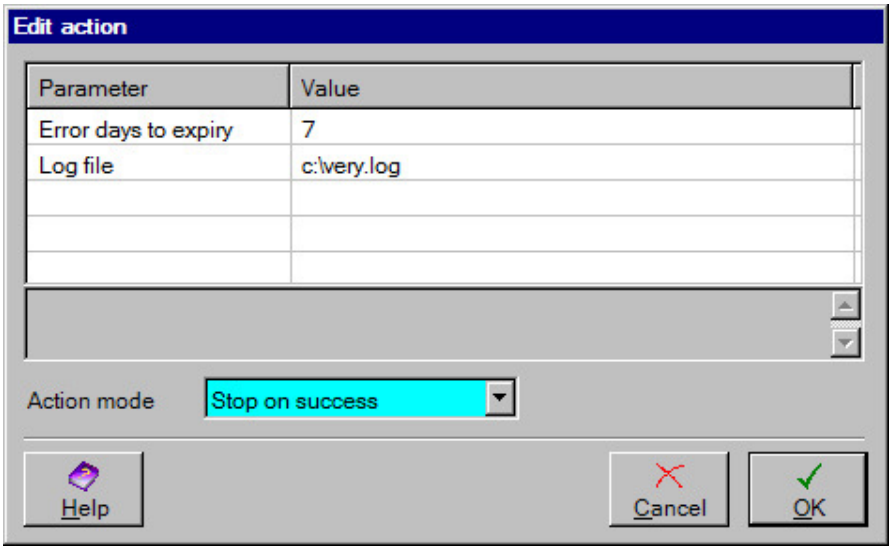
The Edit Action dialog for the Check Performance Counter action is shown below:



To edit the value of any parameter, double click on the parameter you want to edit. Double-clicking will bring up the associated Edit Parameter dialog. The dialog displayed for editing the Performance Counter parameter allows you to select a defined counter from a list (the counter must already have been defined in the System Settings view).

Check Certificates – Edit Action

The Edit Action dialog for the Check Certificates action is shown below:



To edit the value of any parameter, double click on the parameter you want to edit. Double-clicking will bring up the associated Edit Parameter dialog. The 'Error days to expiry' parameter is used to specify that the action should result in an error if any certificate is the given number of days or fewer from its expiry date. The 'Log file' parameter allows you to specify a log file to which the action will write a summary of the checks it performed.

Single Action – Configure

The **Configure** button allows you to edit the settings you have selected for the single action. Clicking this button will bring up the Edit Action dialog, as described above. The parameters listed will differ according to which action you have selected.

Once you have completed all your editing, click **OK** to save your changes and return to the previous dialog. Or click **Cancel** to return to the previous dialog without saving your changes.

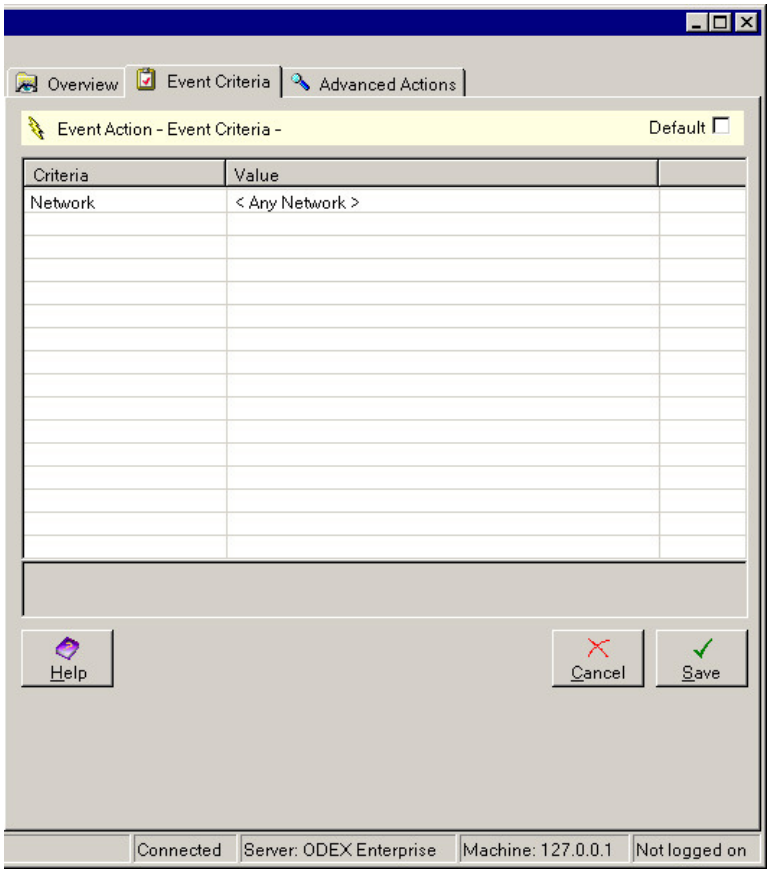
Single Action – Action Mode

This field appears on each of the Edit Action dialogs.

For a single action, the Action Mode on the Edit Action dialog is immaterial. There is only one action to be taken, so it does not matter which option you choose.

Event Criteria

This page allows you to specify criteria values for the selected event. It is not applicable to schedules, the Unhandled Workflow Error event or the Server events.



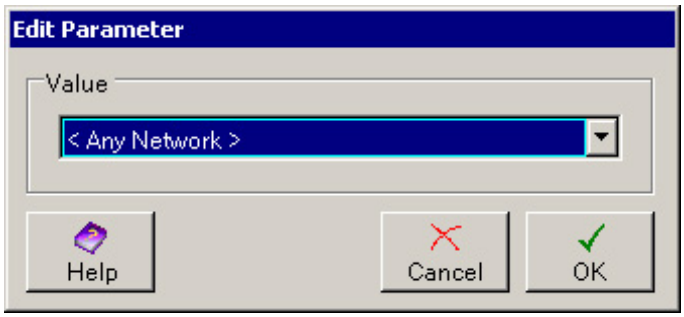
You must select an Event on the Overview page before you can use the Event Criteria page. The example above shows the Event Criteria page for the Call Failed event.

When you open the Event Criteria page you will see the criteria associated with the selected event, with its default value if applicable. There are several criteria (Network, Call Direction, Protocol, Connection Type, Mailbox, Source and SAP System), associated with the events as follows:

- **Network** – Call Ended, Call Failed, Call Retry Limit, Call Started, Connection Failed, Primary Connection Failed, Unexpected Receipt Received
- **Call Direction** – Call Ended, Call Started, Unexpected Receipt Received
- **Protocol** – Call Ended, Call Started, Unexpected Receipt Received
- **Connection Type** – Call Ended, Call Started, Unexpected Receipt Received
- **Mailbox** – File Not Sent, File Retry Limit
- **Source** – General System Error
- **SAP System** – SAP Export Failed

This page allows you to be selective about the criteria you want the action to be valid for. Alternatively you can leave the criteria set to <Any Network>, <Any Mailbox> or <Any SAP System>.

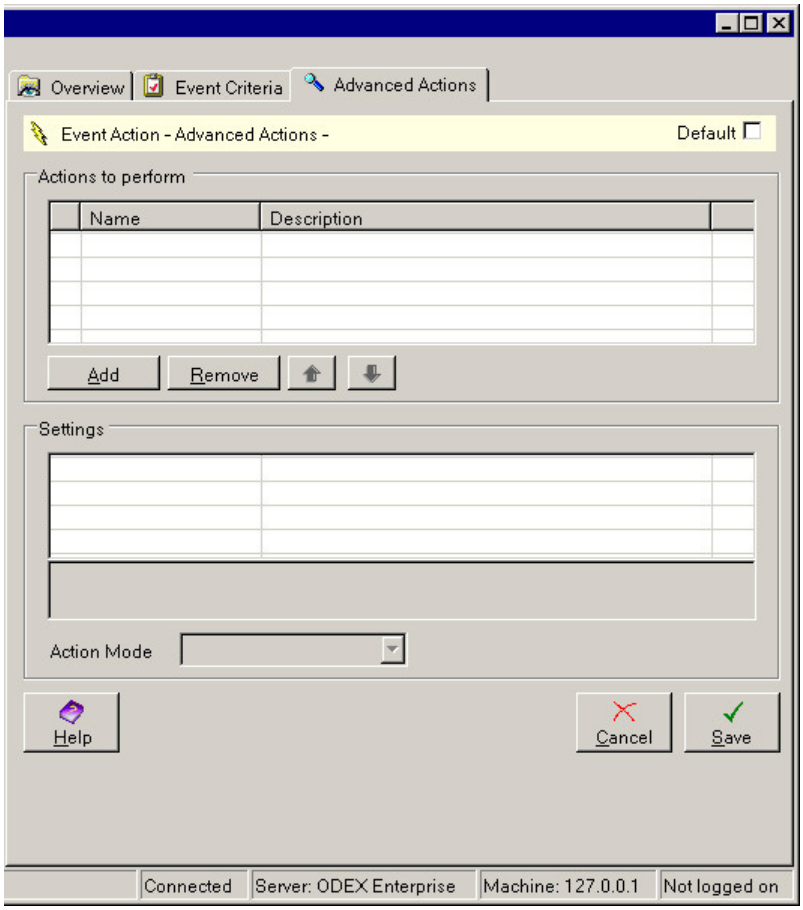
To edit the value for a criterion, double click on the appropriate line and the Edit Parameter dialog will appear.



For General System Errors, you can either type in a specific error code or leave the value blank so that the action will be valid for all errors.

Advanced Actions

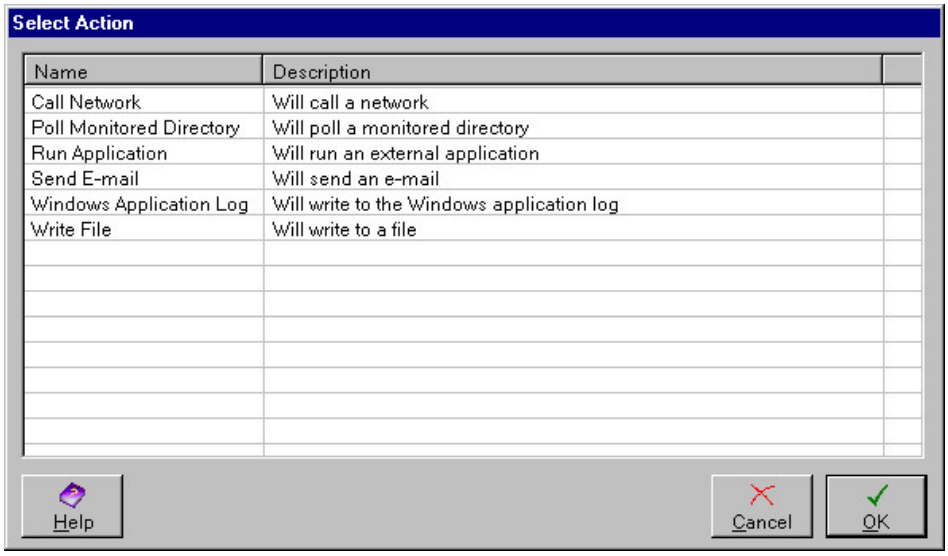
Use this page if you want to specify more than one action to be triggered by the selected event or schedule.



This page is divided into two sections – Actions to perform and Settings.

Actions to perform

Use the **Add** button to add actions to the list to be performed. This will bring up the Select Action dialog, shown below.



The actions listed here are the same as those in the Single Action section of the Overview page. Highlight one or more Actions then click the **OK** button to add them to the list of actions to perform.

For a full list of all the actions and their criteria, please refer to the section entitled “Actions”.

To remove an action from the list of actions to perform, highlight the action to be removed then click the **Remove** button.

The order in which the actions will be performed is indicated by the number in the first column. To change the order, select an action and move it up or down in the list by clicking the Up or Down arrow respectively.

Settings

As you highlight an entry in the list of actions to perform, the settings for that entry will be displayed in the Settings section.

To edit the settings for any entry, double click on the settings line you want to edit. For a setting whose value is ‘True’ or ‘False’, double-clicking will toggle between the two values. For all other settings, double-clicking will bring up the appropriate Edit Parameter dialog.

Action Mode

The Action Mode should be set for each action separately. Highlight each action in turn and select the appropriate action mode for that action. For the last action in the list, it does not matter which action mode you choose.

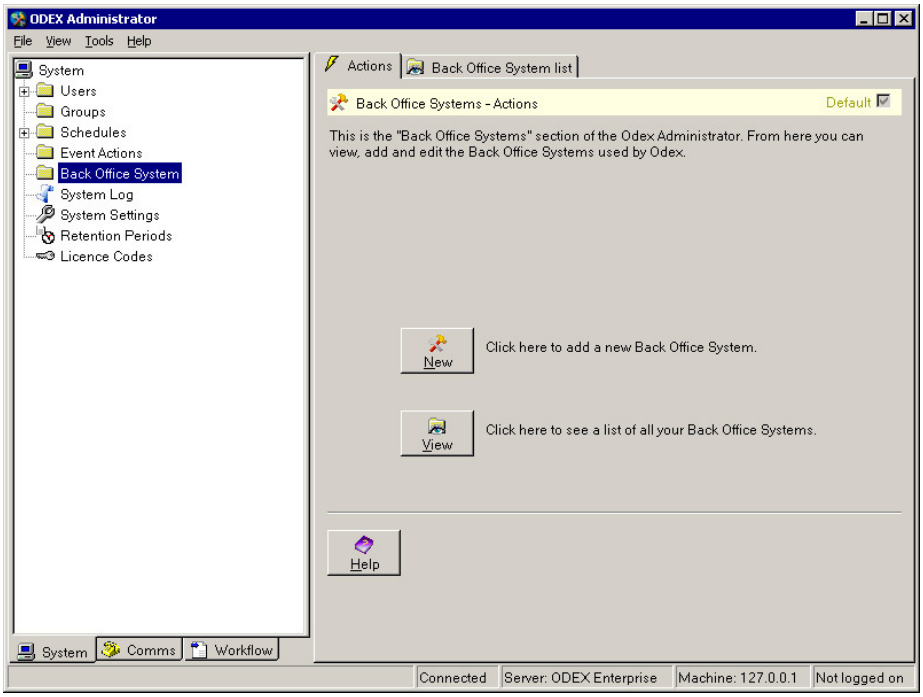
Your choices for each action are:

- Continue on error – if an error occurs during this action, continue on to the next action in the list
- Stop on error – if an error occurs during this action, do not go on to the next action in the list
- Stop on success – if the action is successful, do not go on to the next action in the list

Back Office Systems

This section of the System Administrator allows you to view, add and edit details of the back office systems used by ODEX.

Click on the name Back Office Systems in the Navigation Panel to see the default page for the Back Office Systems section, as shown below. This is the Back Office Systems – Actions page.

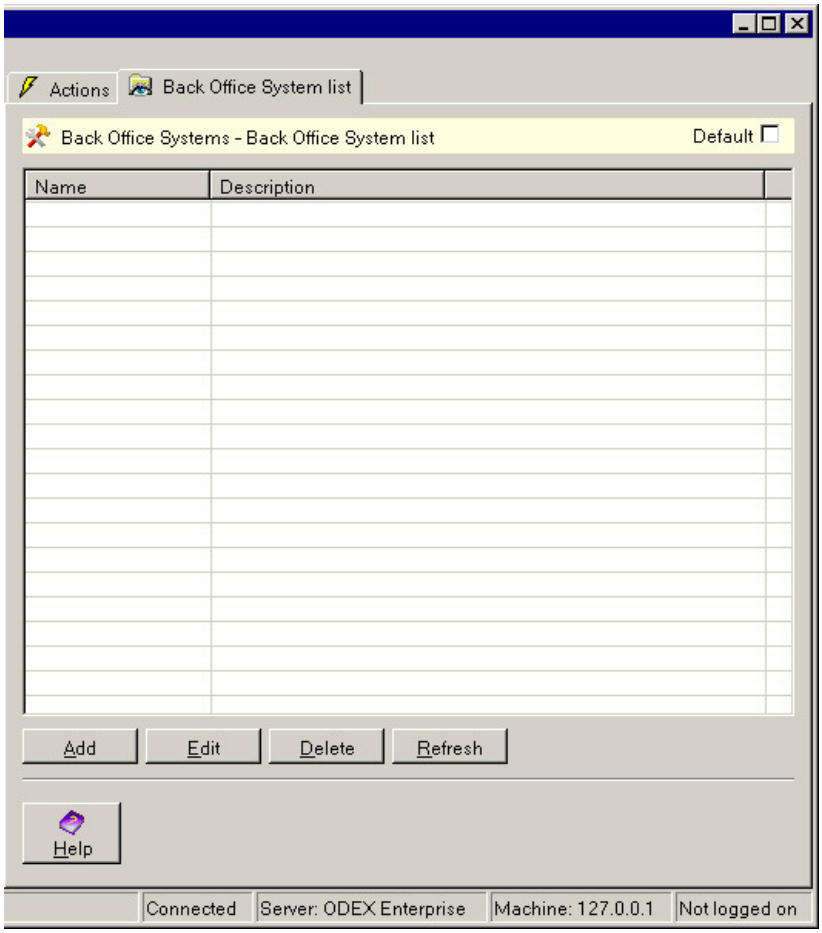


The Back Office Systems section allows you to add, view and edit details of the back office systems used by ODEX.

As you can see, there are two page tabs on the Information Panel (Actions and Back Office System list) and two buttons, labelled **New** and **View**. The **New** button allows you to add details of a new back office system. The **View** button allows you to see a list of all the existing back office systems, from where you can edit their details, add new entries or delete existing entries.

Viewing all your back office systems

If you wish to see a list of all the back office systems currently defined in ODEX, you can either click the **View** button on the Back Office Systems – Actions page or click the Back Office System list tab. Both have the same result, as in the example below.



The Information Panel now shows the Back Office System list page. This is divided into two columns, showing the Back Office System Name and its description.

The actions that can be taken from this page are as follows:

Add

New back office system details may be added to the list by using the **Add** button. If this button is clicked, it will bring up the set of pages described below under the heading "Back Office Systems".

Edit

You may edit the details of existing back office systems by using the **Edit** button. If this button is clicked, it will bring up the same set of pages described below under the heading "Back Office Systems".

Delete

If you wish to delete a back office system from the list, highlight the line that you wish to delete, then click on the **Delete** button. ODEX will bring up a dialog box, asking if you are sure you want to delete the selected items. This is to safeguard against accidentally deleting the wrong item. Click **Yes** to delete or **No** to keep the item in the list.

Refresh

Click this button to refresh the details on this page, for example if you have just made some changes which have not yet appeared on this page.

Help

If you need more information about the fields and buttons on this page, click on the **Help** button.

Adding/Editing SAP Back Office Systems

If you wish to add details of a new SAP back office system, click the **New** button on the Back Office Systems – Actions page. You can also add a new SAP back office system by clicking on the **Add** button on the Back Office System list page of the Back Office Systems section.

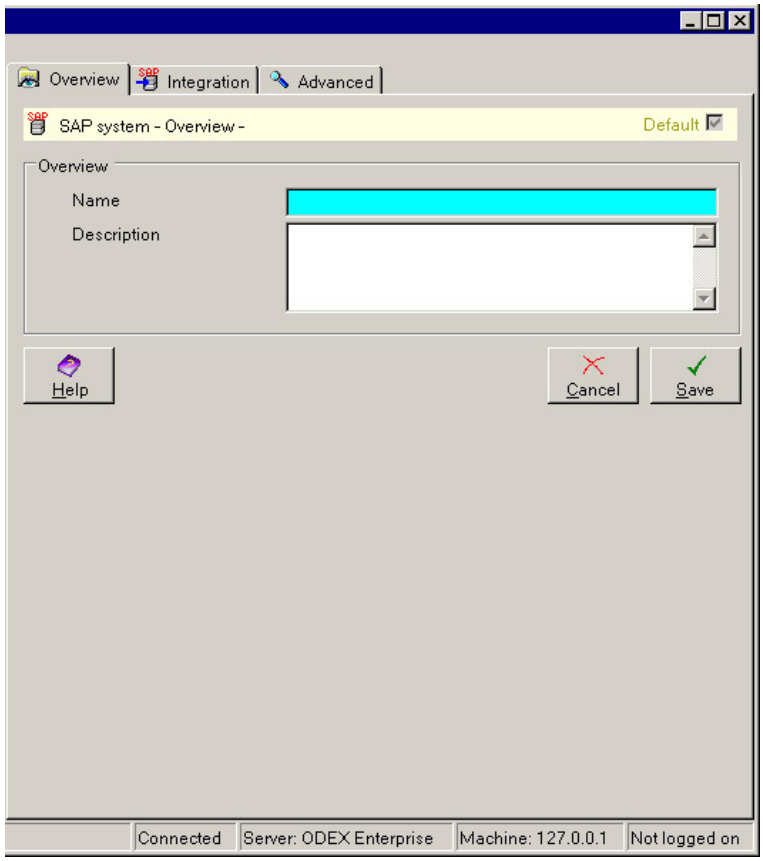
To edit an existing SAP back office system, open the Back Office System list page, select the back office system to be edited, and click the **Edit** button. Alternatively, double-click on the SAP Back Office Systems node in the tree view, then click once on the back office system to be edited.

Whichever route you choose, you will be presented with the following set of pages, enabling you to add or edit details of a back office system. There are three pages associated with back office systems, so let's go through them and find out what information is required.

One point to remember – each of the **Save** and **Cancel** buttons in the SAP Back Office System section work for all three SAP Back Office System pages, so you do not need to click the **Save** button until you have finished entering data. You can click the **Cancel** button at any point to undo changes that you have made.

SAP Back Office System – Overview

The Overview page is where you must provide a name for the new SAP back office system. The Overview page looks like the example below.



Overview – Name

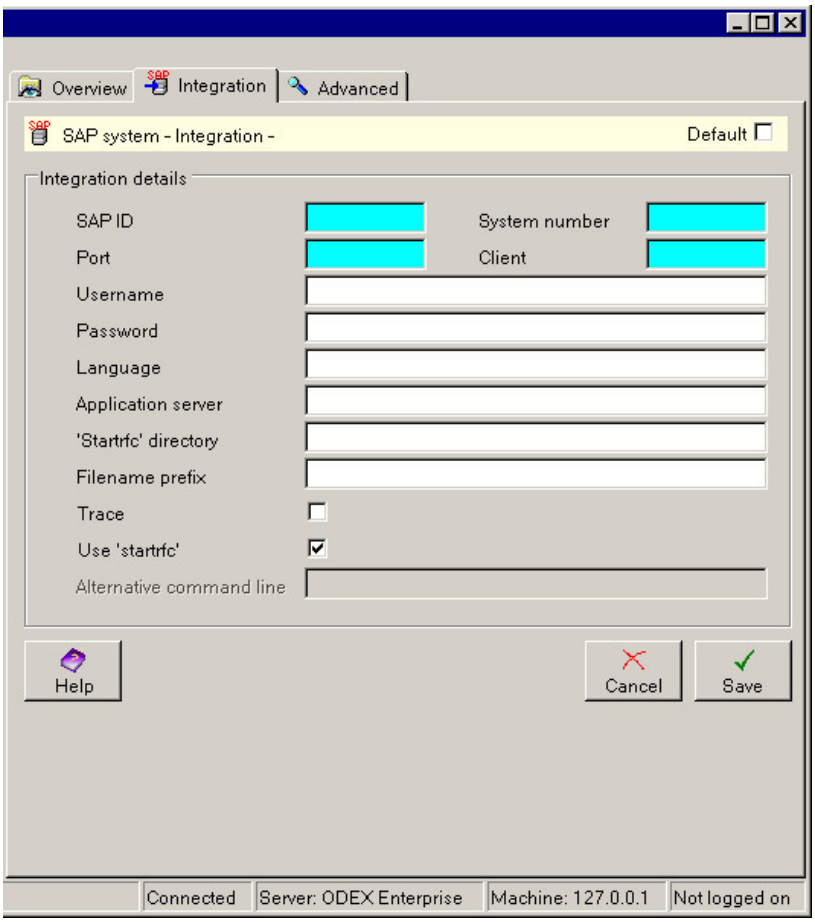
This field requires a name for the SAP back office system, as you will refer to it in ODEX.

Overview – Description

You may provide a description for the SAP back office system in this field if you wish.

SAP Back Office System – Integration

The Integration page is where you must provide the main details of the new SAP back office system. The Integration page looks like the example below.



SAP ID

A 3-character identifier assigned to your SAP instance. You can determine this by looking at the status bar on your SAP screen.

System number

A 2-digit system number. Use the SAP transaction SM51 to display the application servers. The last two digits in the application server name provide the value for the system number.

Port

The name of the port within the SAP system to which files will be passed. The port name may be up to 10 characters long.

Client

The name of the SAP client.

Username

The ID used to log on to the SAP system. This user should be a background user or a CPI-C user, and should have SAPALL permission.

Password

The password for the logon ID used to logon to the system.

Language

The language of the logon ID.

Application server

The server to which the user will log on, in order to connect to the SAP system.

'Startrfc' directory

The directory in which the 'startrfc' program is held.

Filename prefix

The prefix to be attached to files that are submitted to SAP.

Trace

If you select this tickbox, a trace file named dev_rfc will be created in the current directory.

Use 'startrfc'

Select this tickbox if you want to use the 'startrfc' command with the SAP system. This is the default option. (Startrfc is a generic program supplied by SAP, which is used to trigger the SAP system from the EDI subsystem i.e. ODEX in this case).

If you deselect this tickbox, all other fields on this page will be disabled, with the exception of the 'Alternative command line' field below.

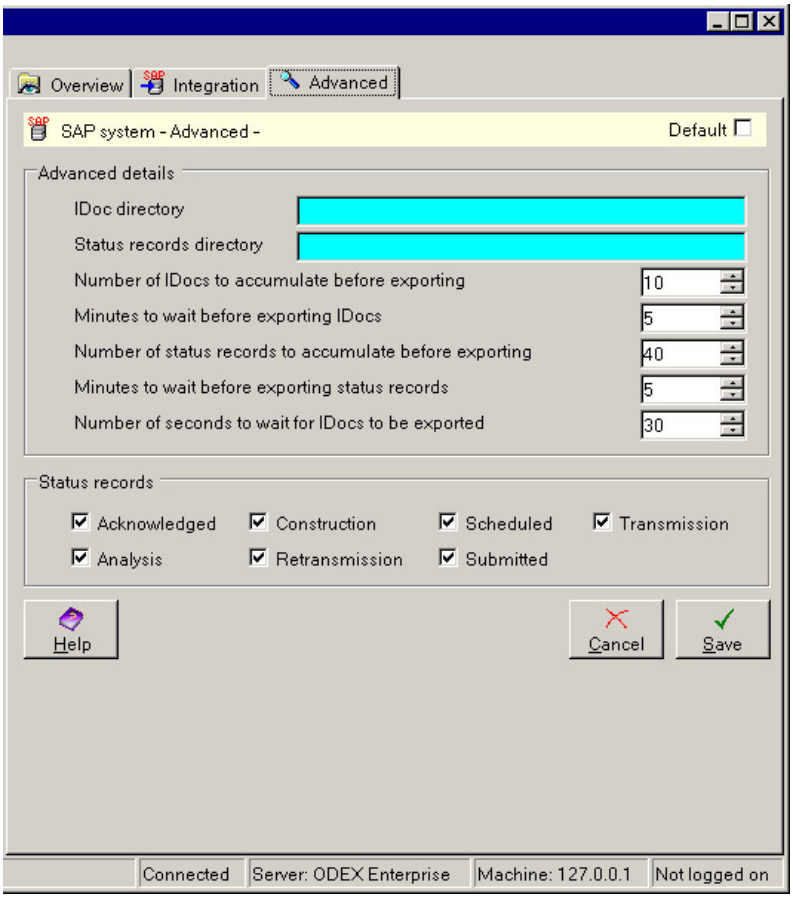
Alternative command line

This field will only be enabled if you deselect the 'Use startrfc' tickbox.

You must provide the full directory filepath of the .exe or batch file (or other means) to be used instead of startrfc, together with any switches, arguments etc that are required.

SAP Back Office System – Advanced

The Advanced page is where you must provide the details of how IDocs and status records will be exported to your SAP system. The Advanced page looks like the example below.



Advanced details

This section allows you to control the way in which IDocs and status records are exported to your SAP system.

IDoc directory

Type in here the directory in which the IDocs will be placed for exporting to the SAP system.

Status records directory

Type in here the directory in which the status records will be placed for exporting to the SAP system.

Number of IDocs to accumulate before exporting

This field allows you to specify how many IDocs you want to accumulate before exporting them. This is simply a way to make the exporting of IDocs as efficient as possible, by sending several at once.

Minutes to wait before exporting IDocs

This field works in conjunction with the field above. If there are any IDocs that have not been exported after the number of minutes specified, then they will be sent even if the "Number of IDocs to accumulate before exporting" has not been reached.

Number of status records to accumulate before exporting

This field allows you to specify how many status records you want to accumulate before exporting them. This is simply a way to make the exporting of status records as efficient as possible, by sending several at once.

Minutes to wait before exporting status records

This field works in conjunction with the field above. If there are any status records that have not been exported after the number of minutes specified, then they will be sent even if the "Number of status records to accumulate before exporting" has not been reached.

Number of seconds to wait for IDocs to be exported

This field provides a way of checking that IDocs and status records have been exported successfully, since SAP does not give any indication whether files have been received. Thirty seconds is the default value for both types of file. After this time, if a file has not been exported successfully (i.e. it is still in the export directory), an error condition will be triggered.

Status records

This section allows you to choose which types of status records are to be transmitted to the SAP system. By default, all are selected. You may deselect any that are not required by your SAP system. Their meanings are as follows:

Acknowledged – an acknowledgement (e.g. EERP for OFTP) has been received from the trading partner to whom an EDI message (originating from a SAP IDoc) was sent.

Construction – the SAP IDoc has been successfully constructed (using Xlate) or mapped (using Xe) into an EDI message

Scheduled – the EDI message has been scheduled to the trading partner

Transmission – the EDI message has been sent to the trading partner

Analysis – the IDoc file received from SAP has been analysed

Retransmission – the EDI message has been sent to the trading partner following a previous failure in transmission

Submitted – the IDoc has arrived in the ODEX system (i.e. the SAP (Associate) job has completed)

Adding/Editing MQ Back Office Systems

If you wish to add details of a new MQ back office system, click the **New** button on the Back Office Systems – Actions page. You can also add a new MQ back office system by clicking on the **Add** button on the Back Office System list page of the Back Office Systems section.

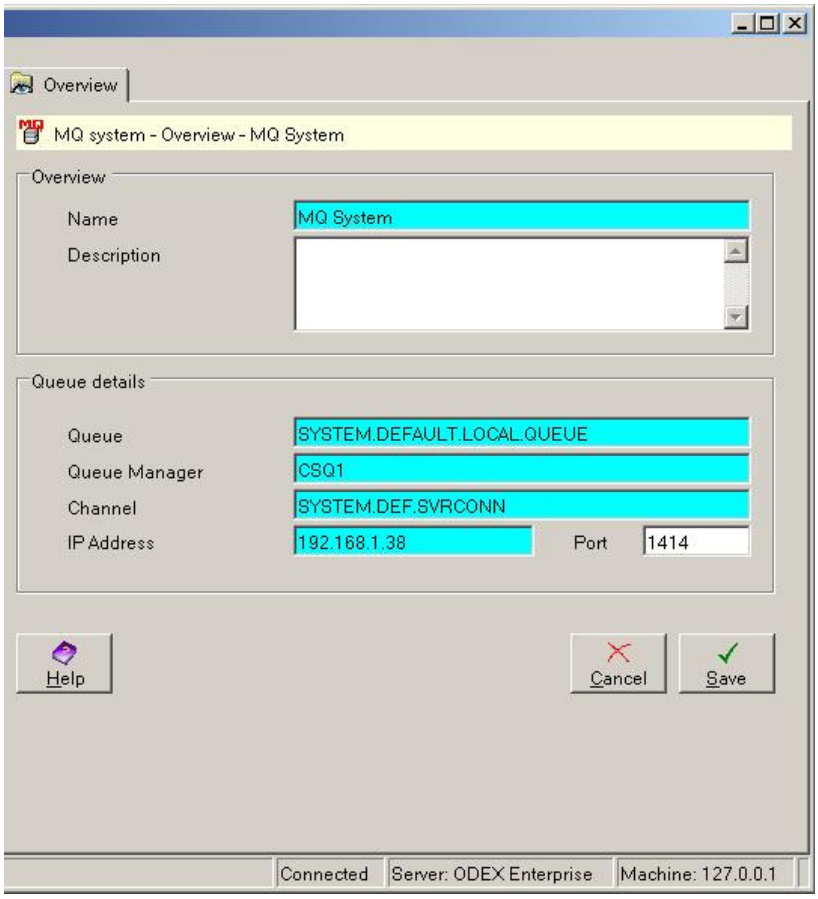
To edit an existing MQ back office system, open the Back Office System list page, select the back office system to be edited, and click the **Edit** button. Alternatively, double-click on the MQ Back Office Systems node in the tree view, then click once on the back office system to be edited.

Whichever route you choose, you will be presented with the following set of pages, enabling you to add or edit details of a back office system. There are three pages associated with back office systems, so let's go through them and find out what information is required.

One point to remember – each of the **Save** and **Cancel** buttons in the MQ Back Office System section work for all three MQ Back Office System pages, so you do not need to click the **Save** button until you have finished entering data. You can click the **Cancel** button at any point to undo changes that you have made.

The settings here are the settings of the queue you wish to poll/write to. If you do not know these settings you will need to contact your System Administrator.

The Overview page is where you must provide a name for the new MQ back office system. The Overview page looks like the example below.



Overview – Name

This field requires a name for the MQ back office system, as you will refer to it in ODEX.

Overview – Description

You may provide a description for the MQ back office system in this field if you wish.

Overview – Queue

This required field is the name of the queue that you wish to use.

Overview – Queue Manager

This required field is the name of the queue manager that manages the queue you have selected.

Overview – Channel

This required field is the name of the channel that establishes the link to the queue manager.

Overview – IP Address

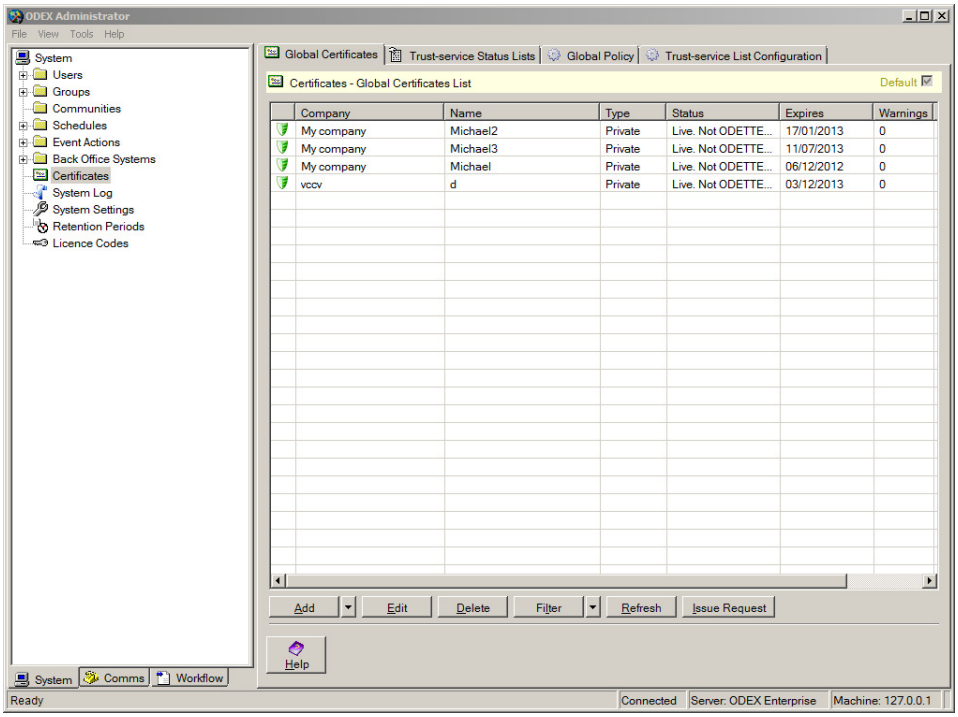
This required field is the IP address of the machine that maintains the queue.

Overview – Port

This field is the port that the machine maintaining the queue is listening on. If no value is entered this defaults to 1414.

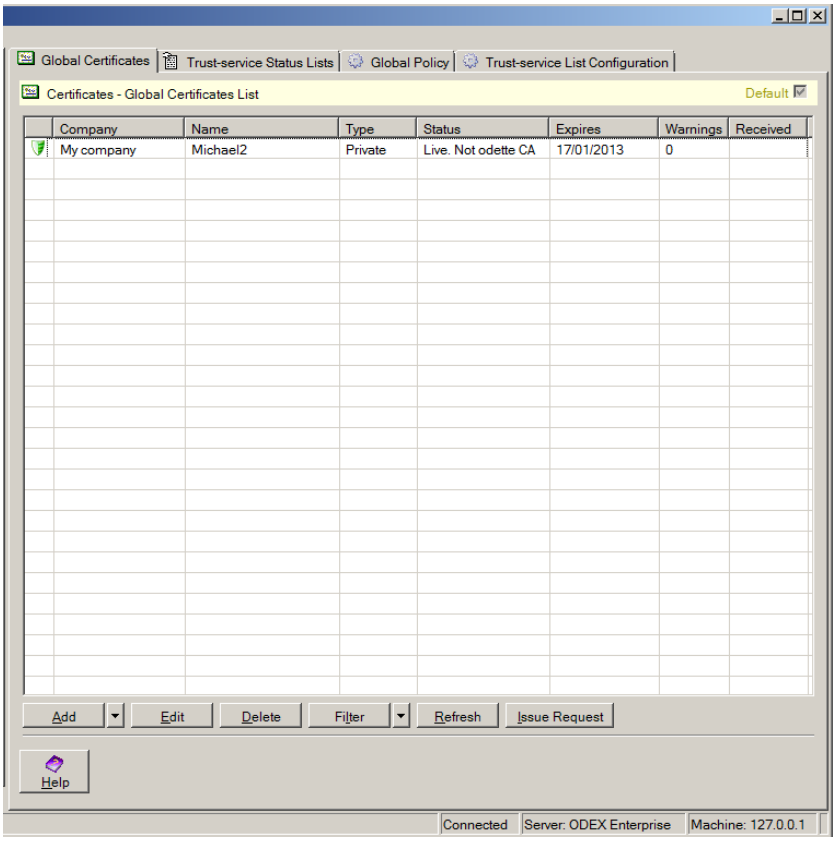
Certificates

The Certificates area comprises – Global Certificates, Trusted-service Status Lists, Global Policy, and Trusted-service List Configuration pages, as shown below.



Certificates

The Certificates page allows you to manage certificates in the ODEX certificate store for use in communications. The page looks like the example below.



This page is divided into a list of all certificates in the ODEX store and a collection of buttons for performing actions with certificates.

Use the **Add** button to add a new certificate into the ODEX store. You will be presented with the following sub-options:

- Import certificates from a file on disk – see 'Import certificate from file'
- Import certificates from the windows certificate store – see 'Import certificate from windows'
- Create a new self-signed certificate in the ODEX store – see 'Create Certificate Dialog'
- Register identification data for a certificate you are expecting to receive through certificate exchange – see 'Register Identification Data'

Use the **Edit** button to change the status of a selected imported certificate or adjust identification data of an expected certificate.

The **Filter** button may be used to filter the list of certificates on chosen criteria based upon the currently selected certificate in the view.

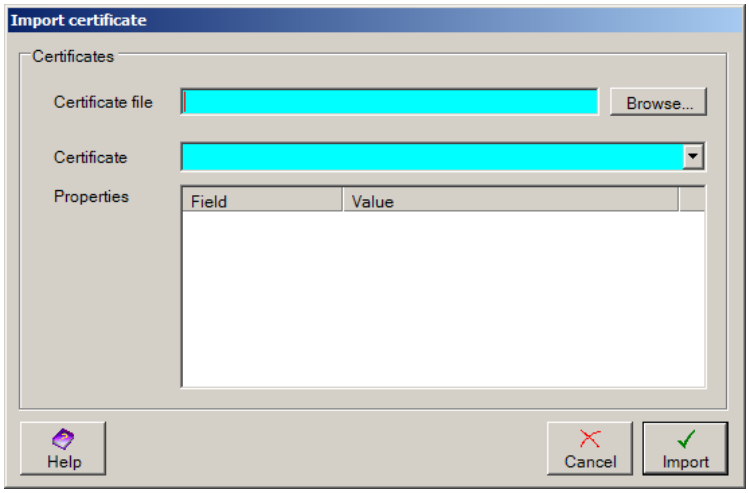
- Filter by Type will filter certificates on the Type column in the view for the currently selected certificate

Import certificate from file

The import certificate dialog allows you to import a certificate from a file into the ODEX certificate store. It is possible to import certificates in any of the following formats,

- PFX: Personal Information Exchange – PKCS#12
- P7B: Cryptographic Message System – PKCS#7
- CER/PEM: Encoded X.509 Certificate

The following dialog allows you to perform the certificate import,



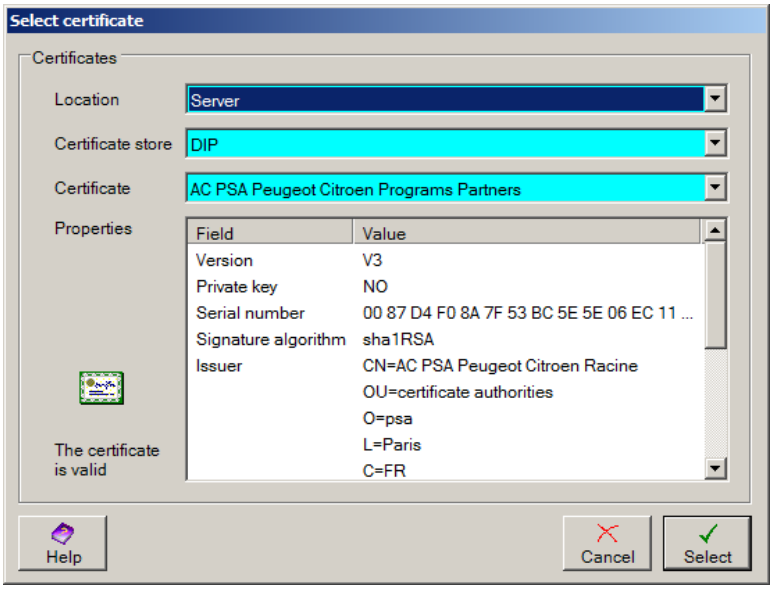
If you know the path of the certificate file you wish to import, then type it into the **Certificate file** field. If you prefer to browse for the file on disk, then click the **Browse** button.

Once you have selected a certificate file, the certificate dropdown list will be populated with a list of certificates that the file contains (in most cases a certificate file contains a single certificate, but sometimes it contains more). Use the dropdown arrow to select the certificate you want from that file. Any properties of that certificate will be displayed in the Properties section.

Click the **Import** button to complete the import process.

Import certificate from windows

The select certificate dialog allows you to select a certificate from Windows to import into the ODEX certificate store.



Use the **Location** dropdown to select the location of the Windows store containing the certificate. This will either be on the ODEX Server machine or on the machine from which you are running the Administrator client application.

Use the **Certificate store** dropdown to select the appropriate certificate store i.e. the store where the certificate you want to use is kept and the **Certificate** dropdown to select the individual certificate you want to use.

The **Properties** section shows the details relating to the selected certificate. Properties include:

- Whether or not the certificate encapsulates a private key
- The signature algorithm
- Issuer details
- Validity dates

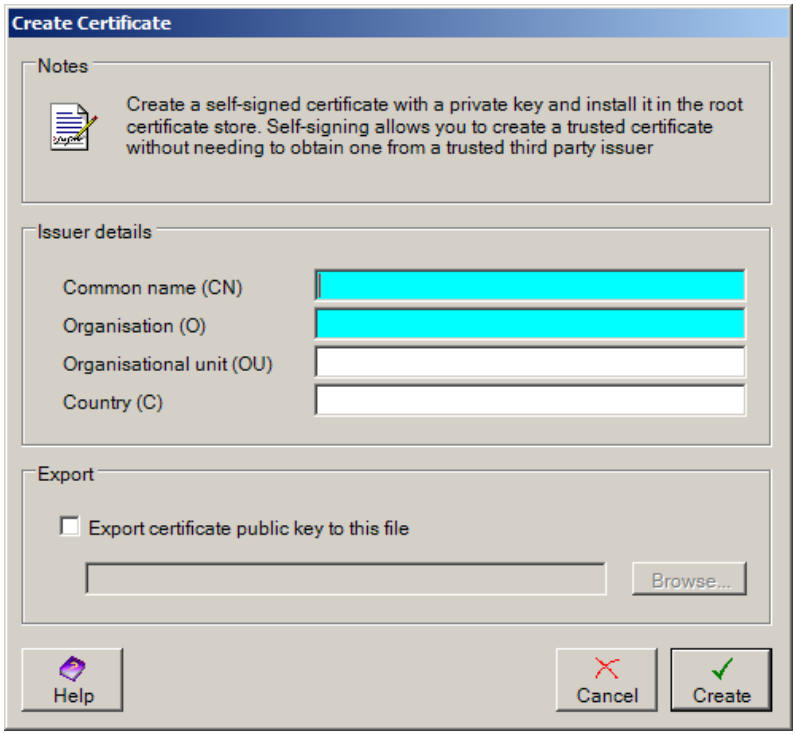
The validity of the certificate will be displayed using one of the following images,

-  The certificate is valid
-  The certificate is invalid

If the certificate is invalid, then the first line of the properties will indicate the failure reason.

Create Certificate Dialog

This dialog allows you to create a self-signed certificate with a private key and install it in the ODEX certificate store. Self-signing allows you to create a trusted certificate without needing to obtain one from a third-party issuer.



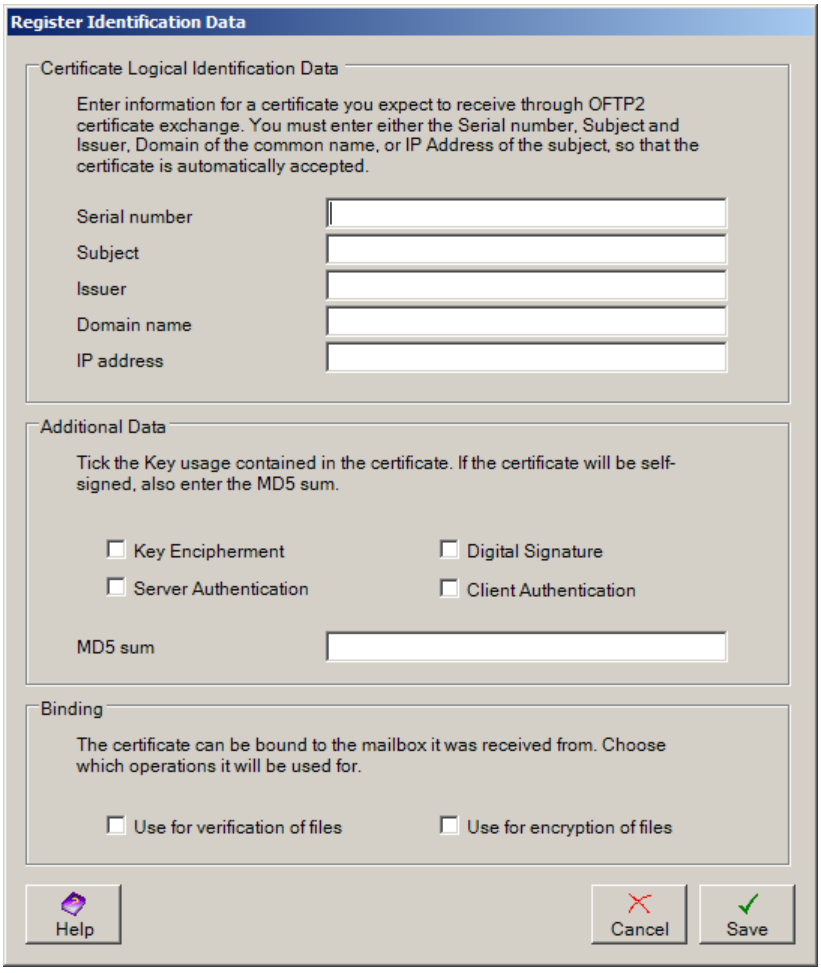
You may specify the details for the Common Name and Organisation which you wish to give to this certificate as well as the Organisation Unit that this certificate is to be associated and the country in which this certificate was issued.

If you wish to export the public key for this certificate to another file, select the Export tickbox and use the **Browse** button to choose the name and location of the file where you want to export it.

Once you have provided the required details, click the **Create** button to create the certificate.

Register Identification Data

This dialog allows you to enter information for identifying and validating a certificate that is later received through certificate exchange. If there is a match, the received certificate will be automatically accepted into the ODEX certificate store.



In the first section of this dialog you need to enter data for identifying the received certificate. The text explains exactly what you need to enter here to aid a successful match. Any extra data you enter here will be used for validation.

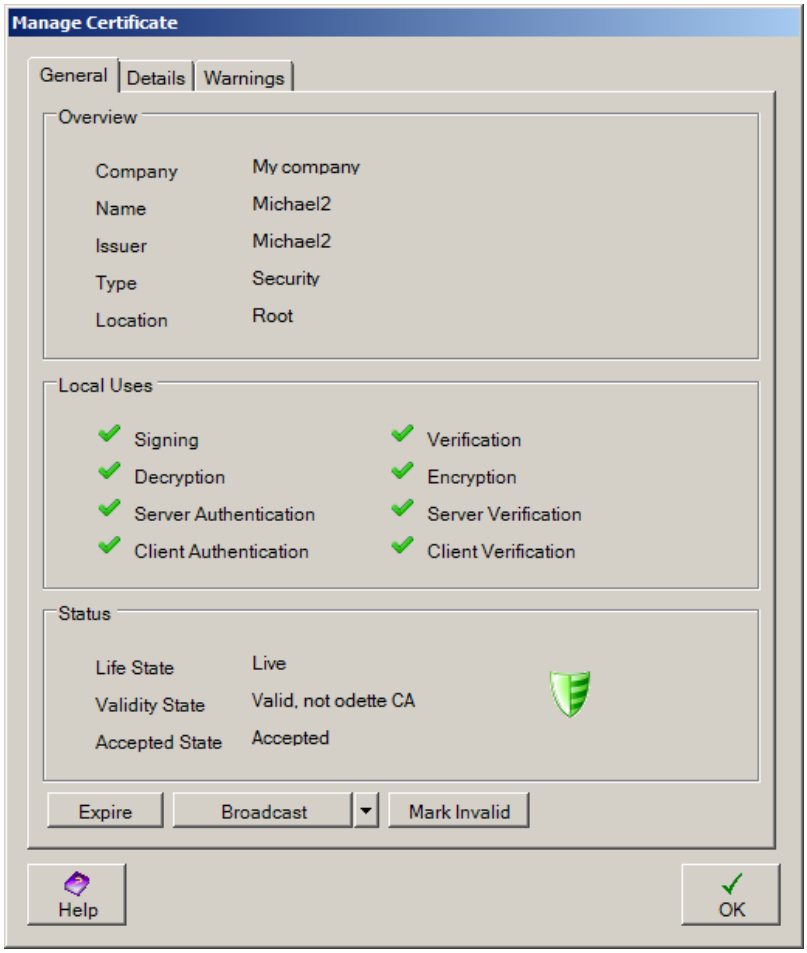
You must tick the key usages you are expecting in the received certificate. This section must exactly match for successful validation. If the received certificate will be self-signed, you are required to enter the MD5 sum of the raw certificate data as an additional validation check.

The final section of this dialog is optional. It is used to bind the received certificate to a particular use against the mailbox from which it was received. If you would rather control the allocation after the certificate has been received, then do not tick any boxes in this section.

When you click the **Save** button the certificate will become a template in the ODEX store and awaiting a match.

Manage Certificate

The Manage Certificate dialog allows you to view all details relating to a certificate in the ODEX store and manage its considered state.



On the **General** page of the dialog you are presented with an overview of the certificate.

The **Overview** section lists some known details of the certificate as it is in the ODEX certificate store. The **Issuer** field references the name of the certificate in the ODEX store that issued this certificate. The **Location** field references the Windows store that contains the certificate.

The **Local Uses** section lists what you can use this certificate for in ODEX. This is determined by a combination of the key usage of the certificate and whether you posses the private key.

Checking **'Ignore Usage Restrictions'** would allow the selected certificate to be used for all purposes other than for those intended for use by the certificate issuer. Odex closely follows the X.509 certificate specifications while using certificates. Checking this option would mean, this certificate could be used for all purposes. If you have enabled this option, ensure that you know what the certificate is supposed to do before using them in ODEX.

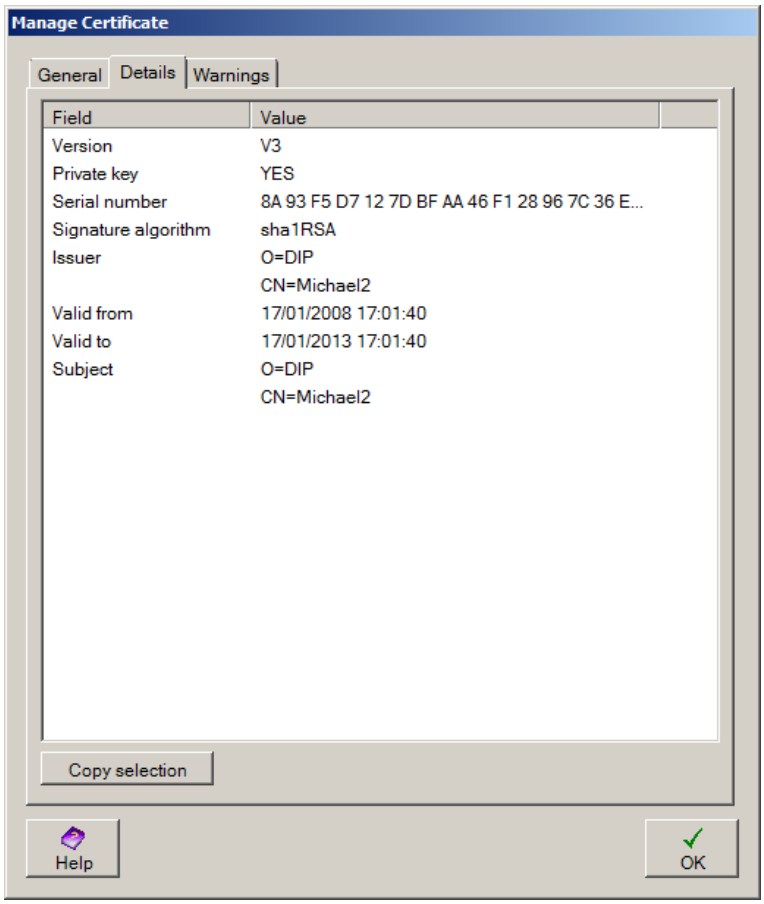
The **Status** section shows the currently considered state of the certificate from view points of whether the certificate is:

- Live (it can be used), New (cannot yet be used), or Expired (life has ended)
- Valid or invalid
- Accepted or rejected in your view point (internal certificates are always accepted)

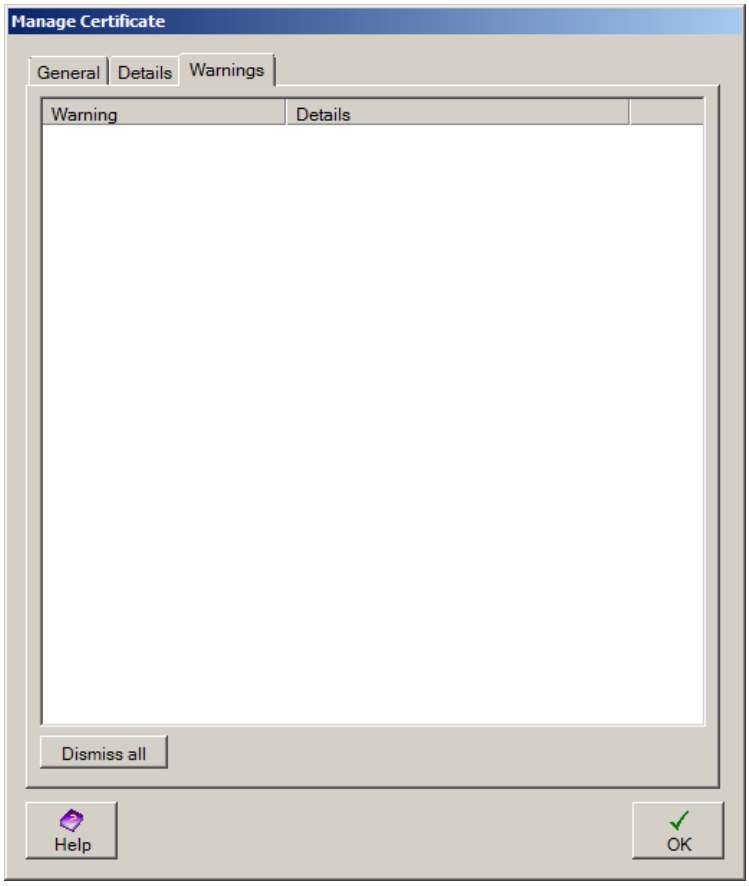
There are a number of action buttons that you can use to manage the state of the certificate, which change depending on the current state and whether the certificate is internal or from a trading partner.

- **Make Live** – bring the certificate into a live state if possible and expire any certificates that it renews.
- **Expire** – send the certificate into an expired state and attempt to find a renewing certificate that can now become live.
- **Request Update** – send a request to the trading partner for a replacement to this certificate.
- **Broadcast** – send this certificate to your trading partners using certificate exchange.
- **Reject** – mark the certificate as rejected in your view point so that it can no longer be used for any purposes.
- **Accept** – mark the certificate as accepted in your view point so that it may be used for security purposes in ODEX.
- **Mark Invalid** – force the certificate into an invalid state. You should do this if you have reason to believe that the certificate has been compromised.

On the **Details** page of the dialog you are presented with a breakdown of the contents of the certificate.



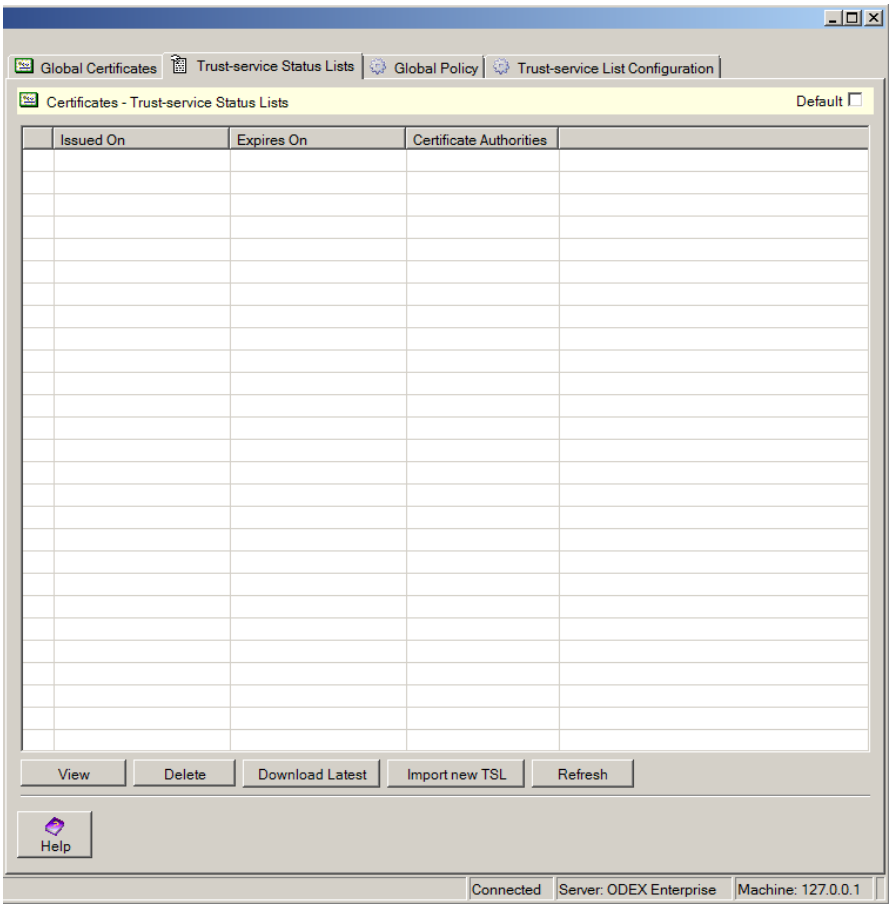
On the **Warnings** page of the dialog you are presented with a list of warnings that ODEX has registered against the certificate because it has found some potential problems.



You can click **Dismiss all** on this page to remove all the current warnings from the certificate. However, if the warnings are serious enough, they may be reissued very soon until you act upon them.

Trusted-service Status Lists

The Trusted-service Status Lists page allows you to manage the trusted-service status lists that are provided by Odette for validation of certificates. The page looks like the example below.



This page is divided into a list of all the TSL files that have been automatically downloaded or manually imported into ODEX and a collection of buttons for performing actions with the TSLs.

The TSL that is currently being used for validation of certificates is marked with a green tick.

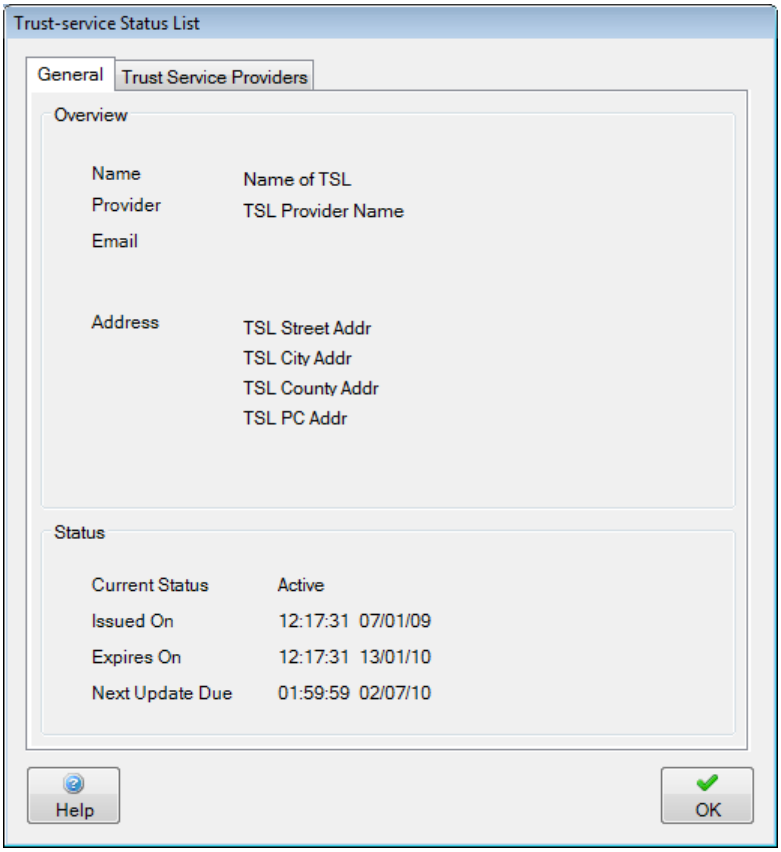
Use the **View** button to show the contents of the currently selected TSL file. See the section entitled 'Trusted-service Status List'.

If you click the **Download Latest** button, ODEX will immediately attempt to download the latest TSL file from Odette. This new TSL will appear in the list if available.

You can manually import a TSL file by clicking the **Import new TSL** button.

Trusted-service Status List

The Trusted-service Status List dialog allows you to view all the details relating to a chosen TSL that is currently stored in ODEX.

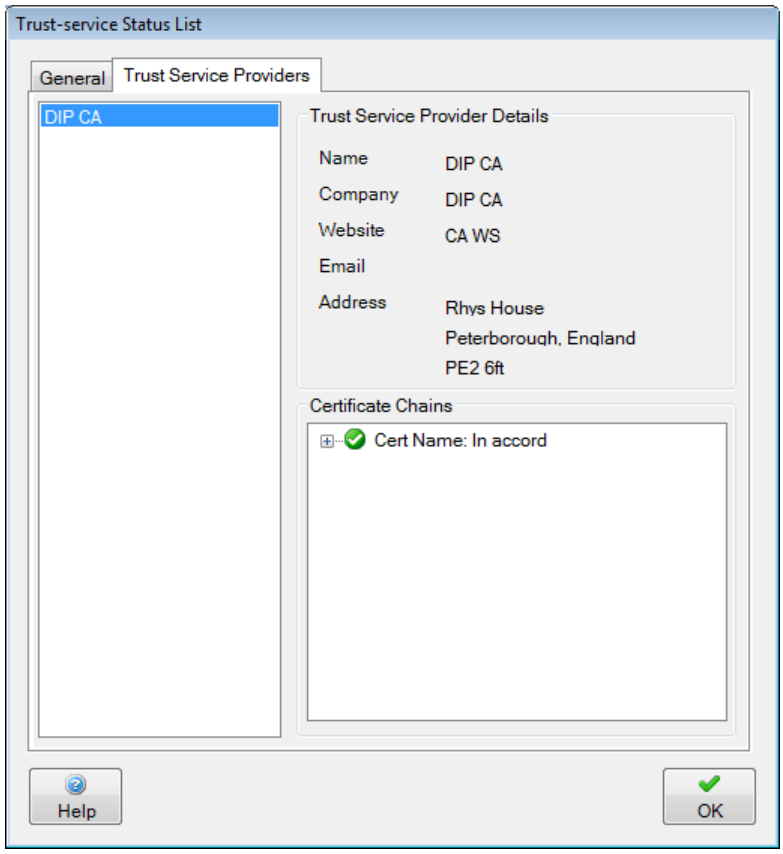


On the **General** page of the dialog you are presented with an overview of the TSL file.

The **Overview** section lists some header details of the TSL.

The **Status** section tells you the period in which this TSL is valid and when you can expect to download a new TSL from Odette.

On the **Trust Service Providers** page of the dialog you can investigate the providers that are listed in the TSL.



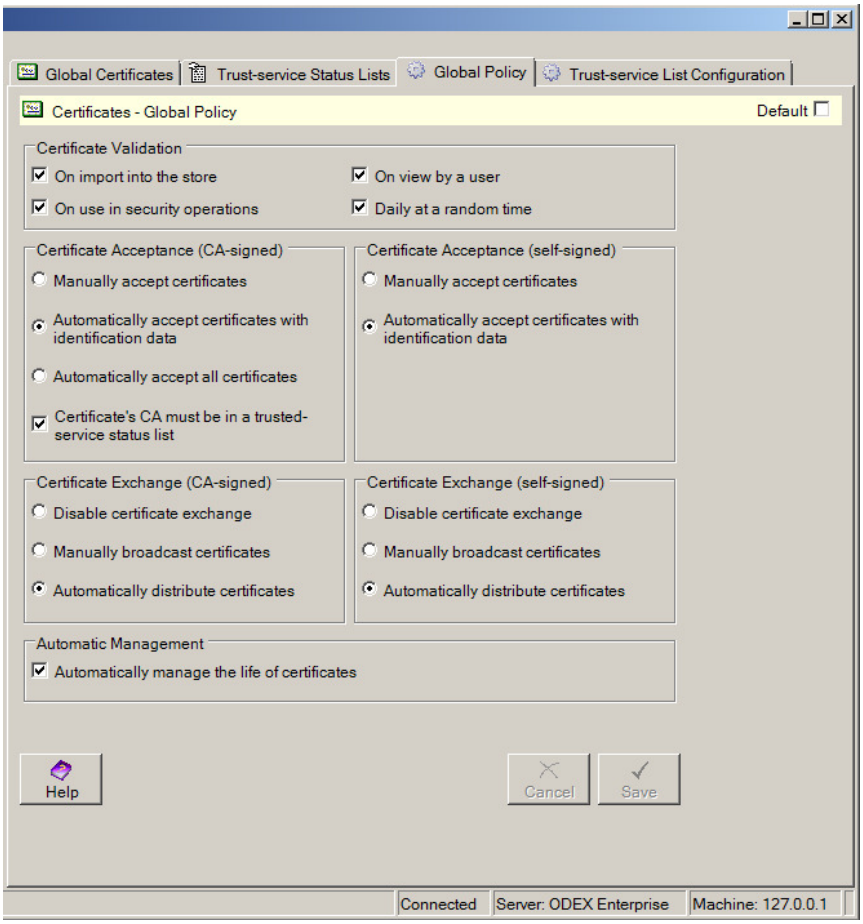
This page lists each provider contained in the TSL on the left-hand-side.

As you click on each provider, the right-hand-side of the page changes to show you the details of the provider and the issuing certificates that they provide. You may view the certificate chains associated with the provider and then double-click to view each certificate in detail.

When a new TSL is downloaded, the providers' certificates are gradually imported into the ODEX certificate store. When you view the certificates from this view you are in fact viewing an Issuer certificate in the store.

Global Certificate Policy

The Global Certificate Policy page is where you can configure the certificate policy defaults for ODEX. The page looks like the example below.



Certificate policy guides ODEX with management of the certificates contained in its certificate store.

Certificate Validation

Here you can configure the situations in which ODEX will check the validity of the certificates contained in its store. By default, all situations are ticked for high security, but you may wish to untick some to increase performance.

Certificate Acceptance

Here you can configure the situations when ODEX will automatically accept certificates that are received from trading partners. A separate policy can be configured for those certificates that the partner has self-signed and those certificates that have been signed by a Certificate Authority.

For a discussion of certificate exchange, please refer to ‘OFTP2 Certificate Exchange’.

Select “Manually accept certificates” if you would like to specifically choose which individual received certificates are accepted into the ODEX certificate store.

Select “Automatically accept certificates with identification data” to permit ODEX to accept received certificates for which you have pre-registered matching identification data.

Select “Automatically accept all certificates” to permit ODEX to accept all received certificates.

There is a further option that opens for some selections that enable you to restrict the automatic acceptance of certificates to those whose CA is in ODETTE’s Trusted-service Status List.

Certificate Exchange

Here you can configure when and if ODEX will distribute the public part of your internal security certificates to your trading partners. A separate policy can be configured for those certificates that you have self-signed and those certificates that you have retrieved from a Certificate Authority.

For a discussion of certificate exchange, please refer to 'OFTP2 Certificate Exchange'.

Select "Automatically distribute certificates" to permit ODEX to decide when and to who your certificates should be broadcast.

Select "Manually broadcast certificates" if you would like to choose exactly when and to who your certificates are broadcast.

Select "Disable certificate exchange" to disable the ability to perform certificate exchange in both directions: broadcast and receipt of certificates.

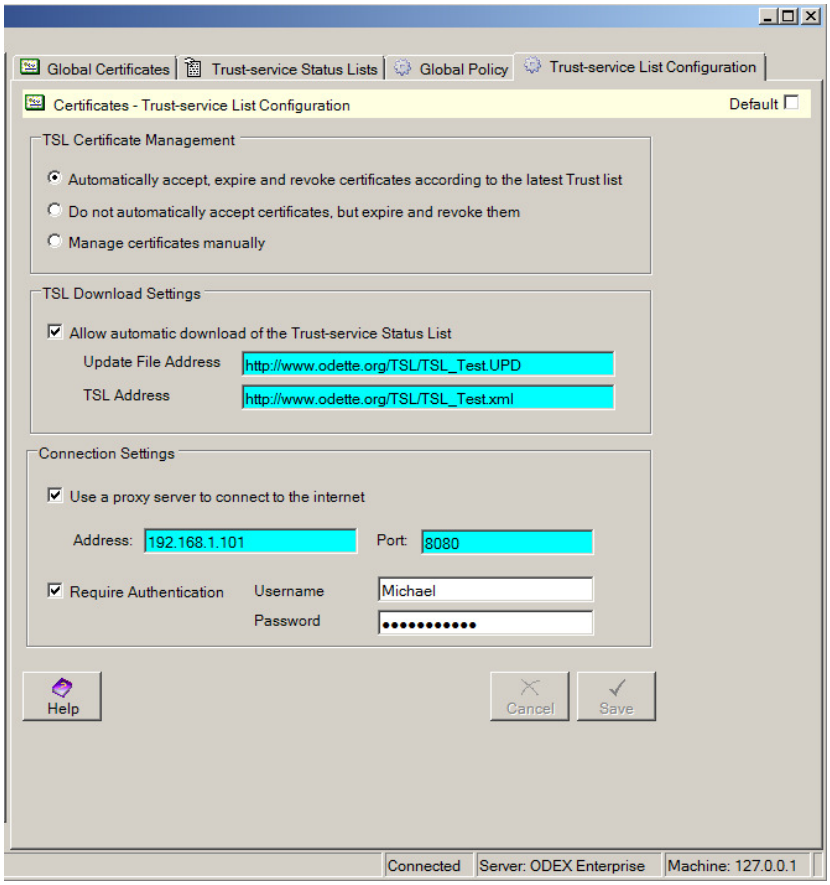
Automatic Management

Tick the single box here to instruct ODEX to automatically manage the life status of certificates, bringing them live and expiring them when appropriate to ensure a slick transition between certificate renewals. When combined with certificate exchange, ODEX will automatically send requests to your trading partners to get their new certificates.

If you untick this box, you will have to manually request certificate exchange and mark certificates as live and expired.

Trusted-service List Configuration

The Trusted-service List Configuration page is where you can configure how ODEX retrieves and uses Trusted-service Status Lists. The page looks like the example below.



TSL Certificate Management

In this section you choose how ODEX should handle the Issuer certificates (of a trust provided) that are distributed with a TSL.

The first option gives ODEX full rights over the Issuer certificates, accepting, rejecting, and expiring them as guided by the latest TSL.

The second option will not automatically accept certificates into the ODEX store but will expire and revoke them if guided to by the latest TSL. This is a compromise between manual oversight and safety as it will always ensure revoked certificates are no longer considered valid.

If you do not want ODEX to automatically manage the Issuer certificates imported from a TSL then choose the final option.

TSL Download Settings

In this section you can choose whether to allow ODEX to automatically download the latest TSL from Odette. If you choose to allow this, you also need to configure the locations that ODEX can find the “Update File” and the “TSL” itself, which are specified by Odette.

Connection Settings

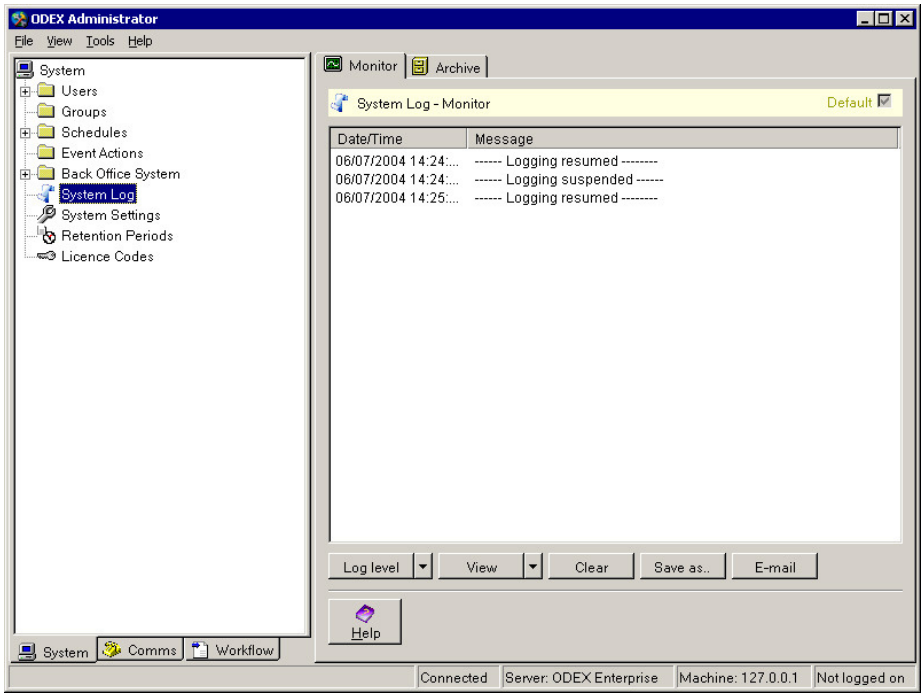
You only need to complete the section if you use a proxy server to connect to the Internet. Enter your proxy server address, port, and the username and password you use to connect to this.

System Log

This section of the System Administrator allows you to configure your log files and view both the current log and archived logs.

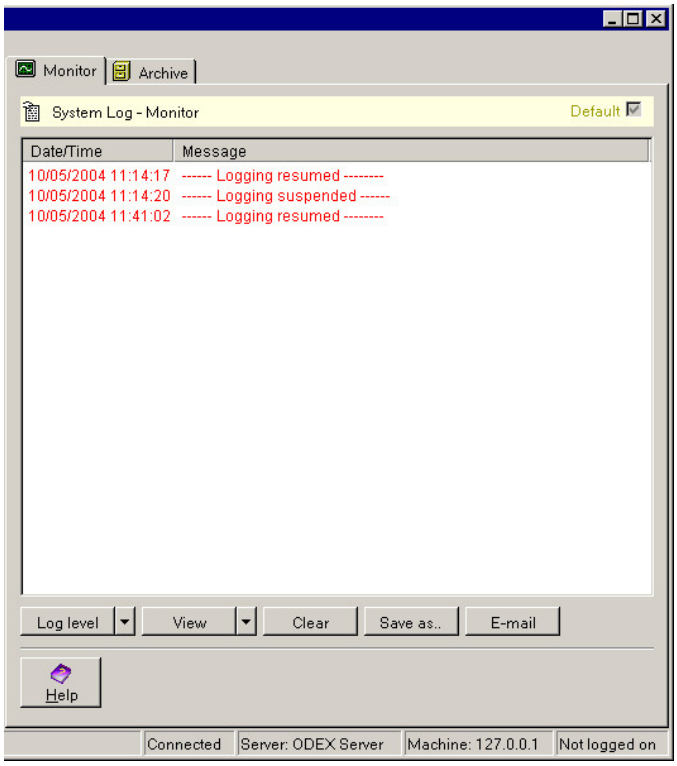
Please note that you do not need to archive any logs yourself as ODEX does this for you automatically. In fact, when you view the current (live) log on the Monitor page, the lines you see are also being written to an archive log.

To see the System Log section, click on the System Log name in the Navigation Panel of the System Administrator. This will bring up the default page of the System Log section, as shown below. There are two pages in the Systems Log section, called Monitor and Archive.



Monitor page

The Monitor page allows you to view your current log. This log is updated in real time, so you will see lines being added to the log while you are looking at it. The first column shows the date and time at which an event occurred, while the second column displays a message informing you of the event that occurred.



Let's have a look at what all the buttons on this page are for.

Log type

The **Log type** button allows you to choose which types of log information you want to see in your system log. We suggest that you keep the default settings just to keep the log uncluttered by too much information. Just click on the button or the dropdown arrow to see the available options. Click on an option to select or deselect it.

View

The **View** button allows you to choose which columns are visible to you in the log. We suggest that you keep the default settings just to keep the log uncluttered by too much information. Just click on the button or the dropdown arrow to see the available options. Click on an option to select or deselect it.

The Active Session Id and the Unique Session Id are only used during ODEX communications sessions.

Type will indicate what type of log information is shown in each line of the log.

Source will indicate the origin of the log message i.e. which source code program has produced the message.

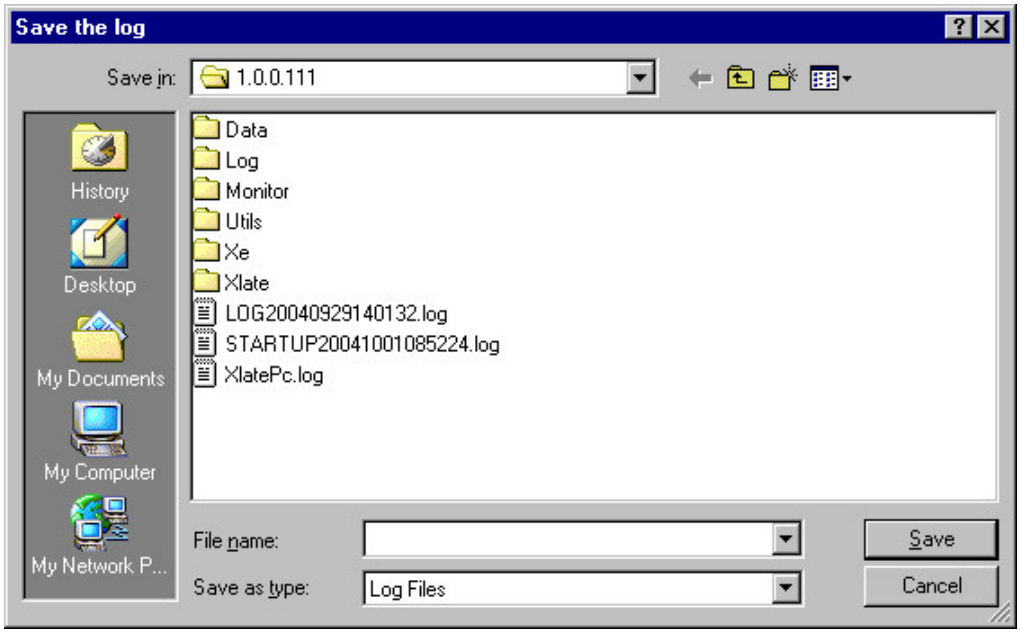
Clear

If you click the **Clear** button, the log lines on this page will be cleared, leaving an empty area on the page. The log file itself will not be affected by the use of this button.

Save as…

The ODEX system logs are automatically saved, when they get to a certain size, in the ODEX Log directory.

However, you may use this button if you also want to save the log file somewhere of your own choosing. If you click on this button you will see the following dialog:



Use it in the same way as you would the Windows File Save dialog i.e. select a directory path and a file name and click the **Save** button.

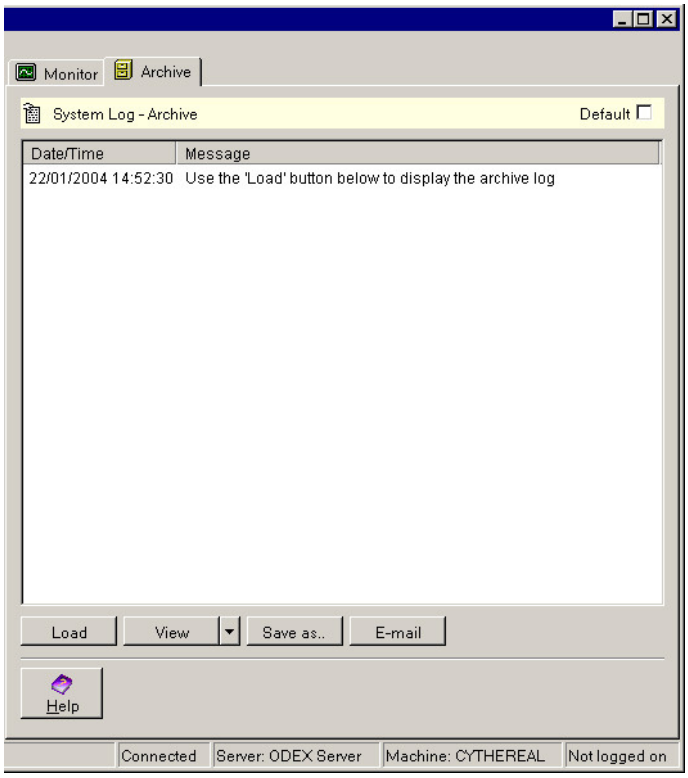
E-mail

Use this button if you want to e-mail the log to somebody (usually this will be our Support department). If you click on this button, it will bring up a new mail message in your default e-mail software, with the e-mail address of our support department and "ODEX Enterprise log" in the subject field. All you have to do is Send it!

The exact behaviour of this function depends on the e-mail system you have installed.

Archive page

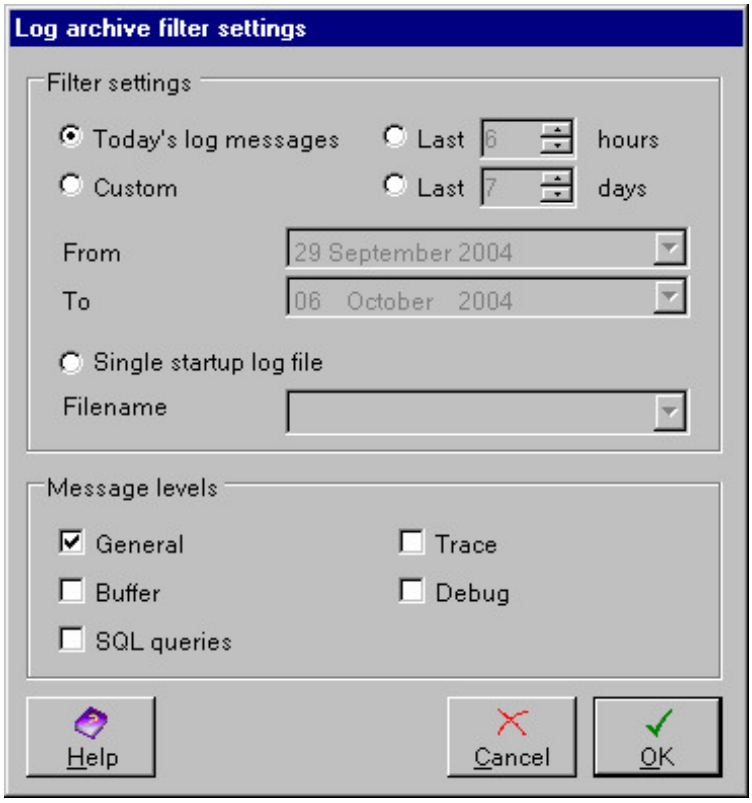
The Archive page allows you to look at previous logs. To do this, you first have to click the **Load** button, as suggested in the message column of this page.



Let's have a look at what all the buttons on this page are for.

Load

If you click the **Load** button, you will see the following dialog.



This filter dialog allows you to select logs from today, or from any range of hours or days.

Alternatively, you can select a particular startup log file. To do this, select the Single startup log file radio button, then use the dropdown arrow alongside the Filename field to select the required startup log file.

The Message Levels section at the bottom of this dialog allows you to choose the level of log information to be included in the loaded log.

View

The **View** button allows you to choose which columns are visible to you in the log. We suggest that you keep the default settings just to keep the log uncluttered by too much information. Just click on the button or the dropdown arrow to see the available options. Click on an option to select or deselect it.

The Active Session Id and the Unique Session Id are only used during ODEX communications sessions.

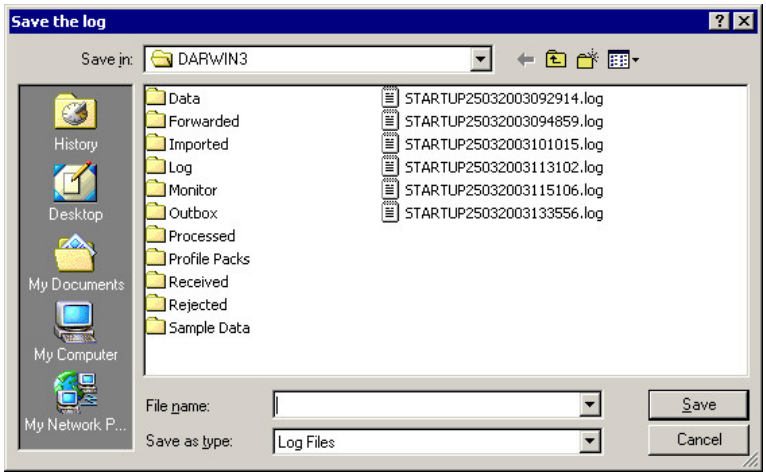
Type will indicate what type of log information is shown in each line of the log.

Source will indicate the origin of the log message i.e. which source code program has produced the message.

Save as…

The ODEX system logs are automatically saved, when they get to a certain size, in the ODEX Log directory.

However, you may use this button if you also want to save the log file somewhere of your own choosing. If you click on this button you will see the following dialog:



Use it in the same way as you would the Windows File Save dialog i.e. select a directory path and a file name and click the **Save** button.

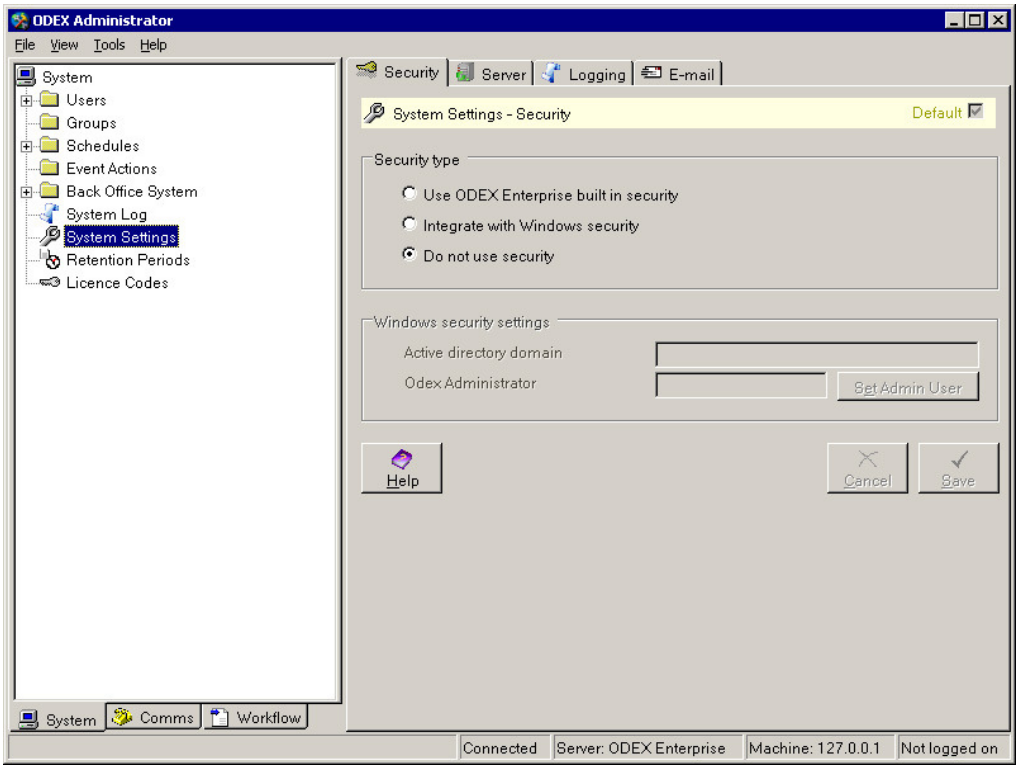
E-mail

Use this button if you want to e-mail the log to somebody (usually this will be our Support department). If you click on this button, it will bring up a new mail message in your default e-mail software, with the e-mail address of our support department and "ODEX Enterprise log" in the subject field. All you have to do is Send it!

The exact behaviour of this function depends on the e-mail system you have installed.

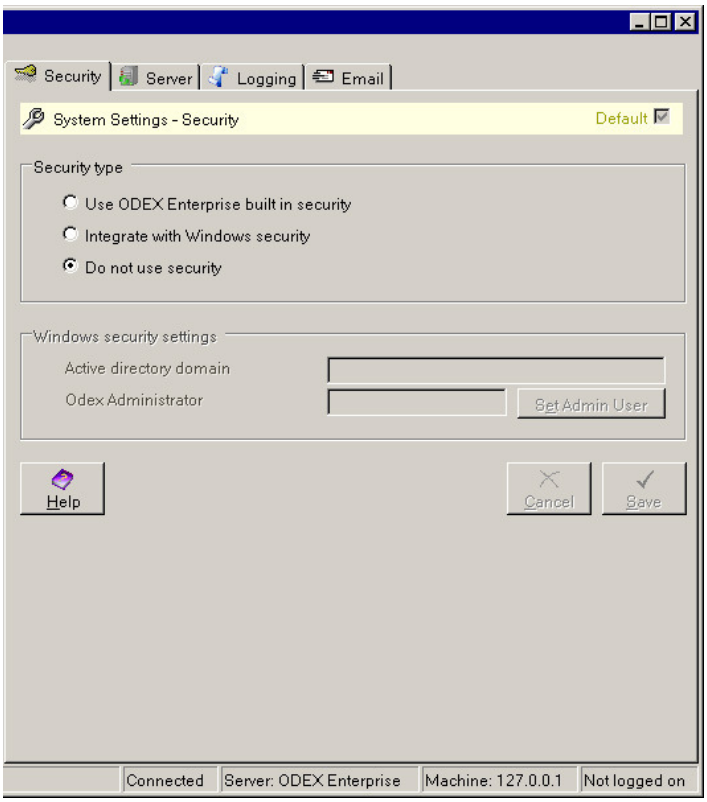
System Settings

The System Settings area comprises four pages – Security, Server, Logging and E-mail, as shown below.



Security page

You will only need to use this page once, in order to select the type of security you want ODEX to have. Click on the Security page tab to see this page, as shown below.



The Security page allows you to select the type of security you want to use in ODEX. You have the choice of:

- ODEX's own security
- Windows NT security
- Using no security

By default, security is switched off when you first use ODEX. You will probably want to take a little time to consider how to organise your user groups before you dive in and switch security on. Of course, you may decide not to enforce any security at all.

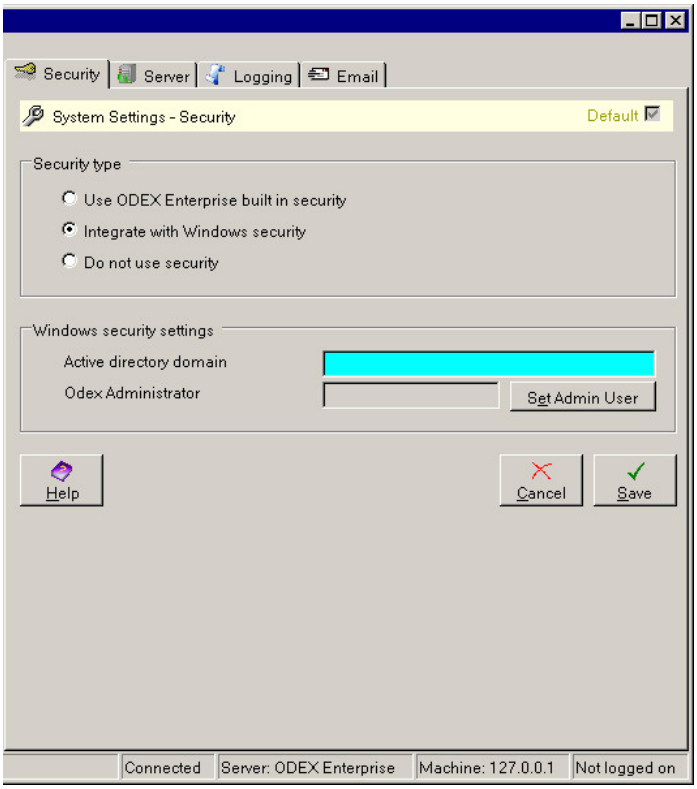
Click **Save** to keep the changes you have made, or click **Cancel** to discard the changes.

ODEX's own security

If you select ODEX built-in security, you cannot edit anything else on this page. Click **Save** to keep the changes you have made, or click **Cancel** to discard the changes. Please continue reading from the section entitled "ODEX users, user groups".

Windows security

If you select Integration with Windows security, you will see that the Windows security settings section becomes enabled, as shown below.



Active directory domain

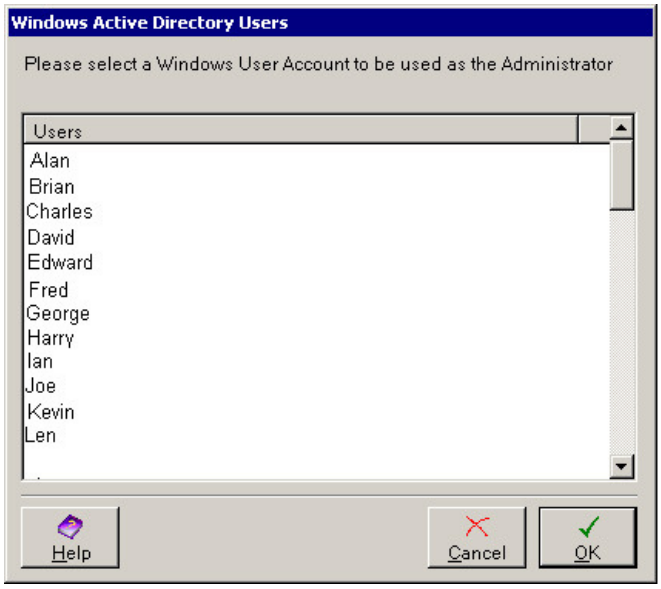
You must type a Windows domain in the Active directory domain field if you are going to use Windows security.

The Windows Active Directory is a catalogue of everything on your network, including users, user groups, computers, and printers. ODEX can utilise the list of users and user groups in the active directory so that you can use existing Windows identities to govern people's use of ODEX.

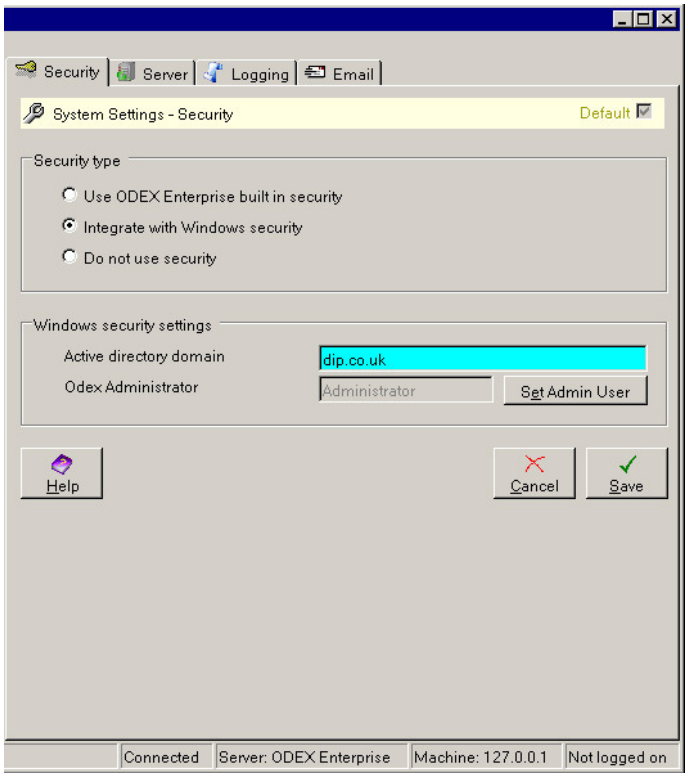
Set Admin User

Having selected the active directory domain, you must now select a user from that domain to be the Admin user. You should choose a responsible, technical person, such as the IT manager, the network administrator or whoever is in charge of ODEX.

To choose an Admin user, click on the **Set Admin User** button to bring up the following dialog.



Highlight the appropriate user to be the Admin user and click **OK**. This will return you to the Security Settings page, which will now display the selected user in the ODEX Administrator field, as shown below.



Click **Save** to keep the changes you have made, or click **Cancel** to discard the changes.

After saving

Once you have clicked the **Save** button on this page, you will see a message box telling you that the server must be restarted for the security changes to take effect. You should do this straight away, otherwise any subsequent changes you make in the User Security area may be lost when you do eventually restart the Server

Using ODEX's own security, once you have re-started the server, the next time you or anyone else tries to start an application, ODEX will require a username and, optionally, a password to be entered.

Using Windows NT security, once you have re-started the server, Windows security will check the identity of any user against a user account before allowing them to use an application.

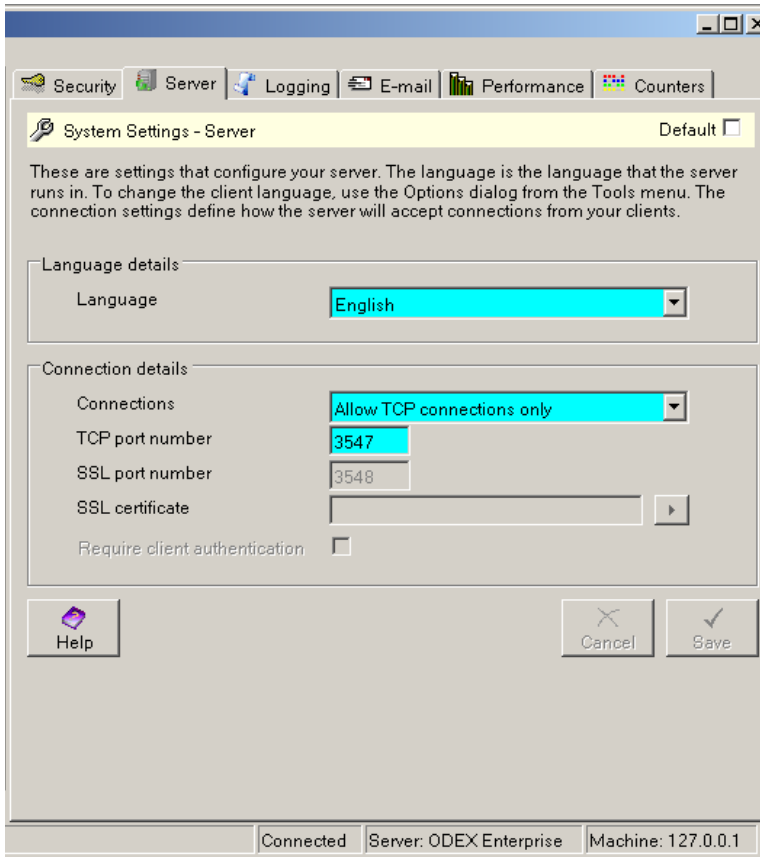
Important!

If the new ODEX Admin user is a different person from the one logged on to this machine (i.e. the machine where the ODEX Administrator application is installed), when you restart the Server you will not be able to log back on to ODEX unless you logoff Windows and logon again as the person you have designated to be the Admin user. Once you have restarted the Server and logged on to ODEX, you can then add further users.

If you selected ODEX or Windows security you can now go ahead and start to add your users and user groups using the buttons on the Actions page or the tree view in the Navigation Panel.

Server page

The Server page allows you to configure the language and specify how clients connect to the server.



Server details – Language

Use the dropdown arrow to select which language you want the server to run in.

Currently available languages are English, German (Deutsch), Spanish (Español), French (Français) and Chinese (Simplified).

If you select a different language and click the **Save** button, you will see a message box telling you that the Server must be restarted for the change to take effect.

N.B. This Language setting only affects the server. To change the language used by any of the clients, use the Options dialog from the Tools menu of the appropriate client.

Connection details – Connections

The connections list allows you to specify whether clients must authenticate with SSL when they connect to the server. You can select 'Allow TCP connections only', which will not allow SSL connections, 'Allow SSL connections', which will only allow clients authenticated with SSL to connect, or TCP and SSL connections can be enabled.

Connection details – Port Number

The port number is the port on which the server listens for clients. The default port number should be usable by most servers, but, if necessary, type in a different port number to be used by the ODEX Server.

Where both TCP and SSL connections are in use, separate port numbers are required for each connection

Connection details – SSL certificate

Select the button next to this field to select a certificate that will be used for authentication. For more details on certificates see the section entitled 'Select certificate dialog'.

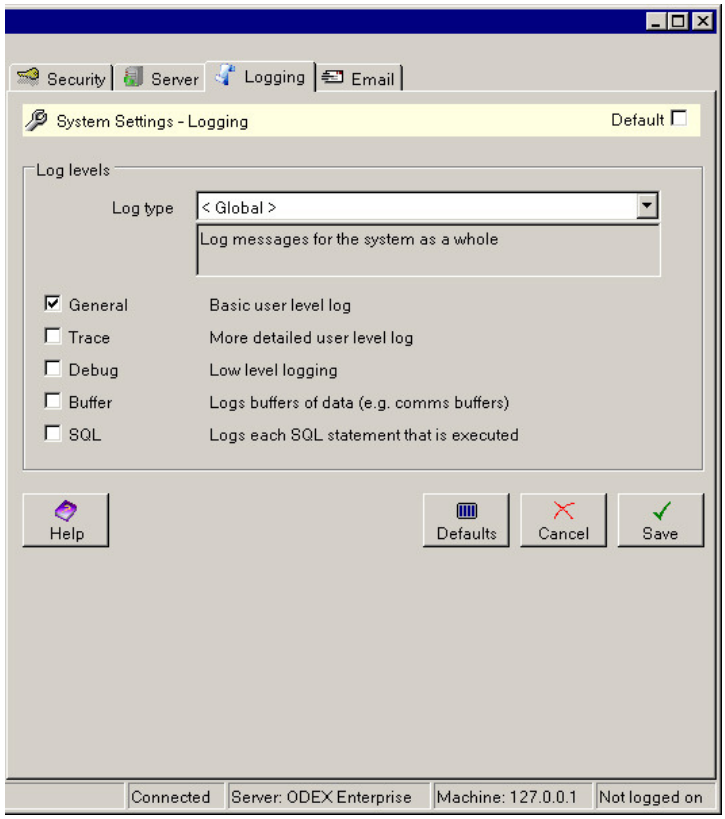
Connection details – Client authentication

Select this check box if you additionally require the server to authenticate with the client.

Logging page

The Logging page is where you can choose what type of information you want to be written to the various ODEX logs. Please be aware that, even though information is written to the log, you can still choose not to see it when you browse the log. This means that you can write information to the log that may be useful for Support purposes, but keep much of it out of your everyday view of the log.

In general you should keep logging to a minimum.



Log type

There are many different types of logging within ODEX, listed in the Log type dropdown list. By default, all are configured to include only General log messages.

As you select any log type, a description will be displayed in the grey box below the Log type field.

The <Global> entry in the Log type field indicates that all log types will contain log messages of whatever types are selected on the dialog above (in this example, just General log messages).

You can override this for individual log types, if necessary, by choosing an entry from the dropdown list and selecting more log message types for that entry.

You can deselect and reselect options at any time.

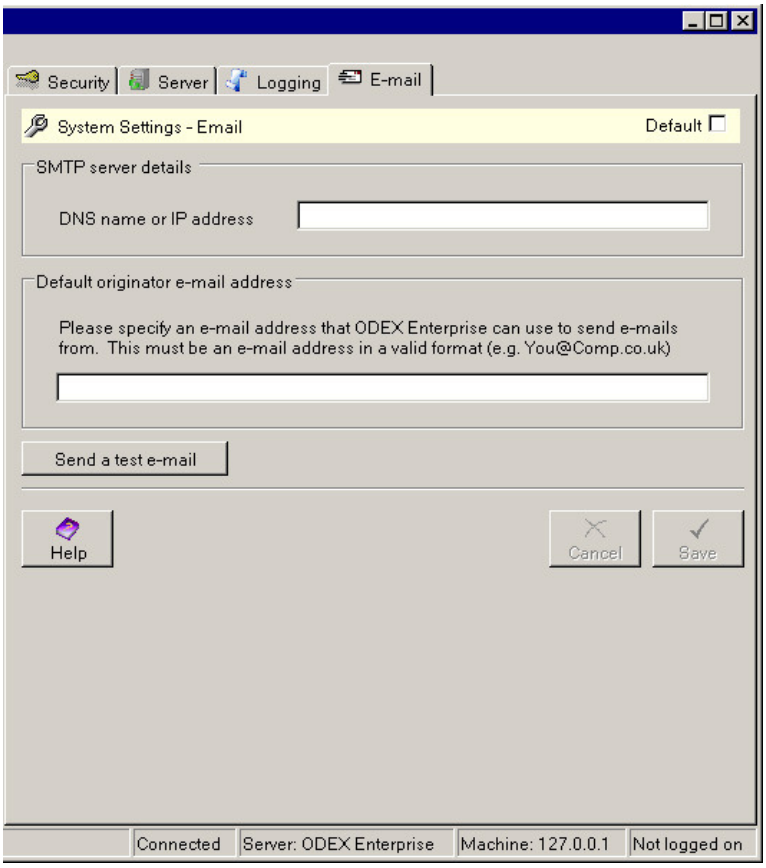
Each log message type is described briefly on the Logging page, to help you make your choices. Under normal circumstances, General log messages should be adequate for most purposes, with Trace messages being used occasionally for extra information. Debug, Buffer and SQL messages are mostly for support purposes only.

If you make any changes on this page, you must click the **Save** button to save the changes, or click the **Cancel** button to discard the changes.

If you want to reset to ODEX's original logging settings, click the **Defaults** button.

E-mail page

The E-mail page is designed to be used in conjunction with ODEX automation and/or Workflows. Once you have set up one or more automated events, or if you use the E-mail job in a workflow, the sending of e-mails can be triggered automatically. The details you set on this page will be used for those e-mails.



You do not need to provide any details on this page unless you want to use e-mails in your ODEX automation and/or workflows.

If you do provide any details on this page, you will not be able to save the details until you have tested them successfully using the **Send a test e-mail** button. First, however, you need to ensure that the mailserver allows internal relaying from the IP address of the ODEX machine. If this is not the case, you will not be able to send e-mails using ODEX at all.

SMTP server details – DNS name or IP address

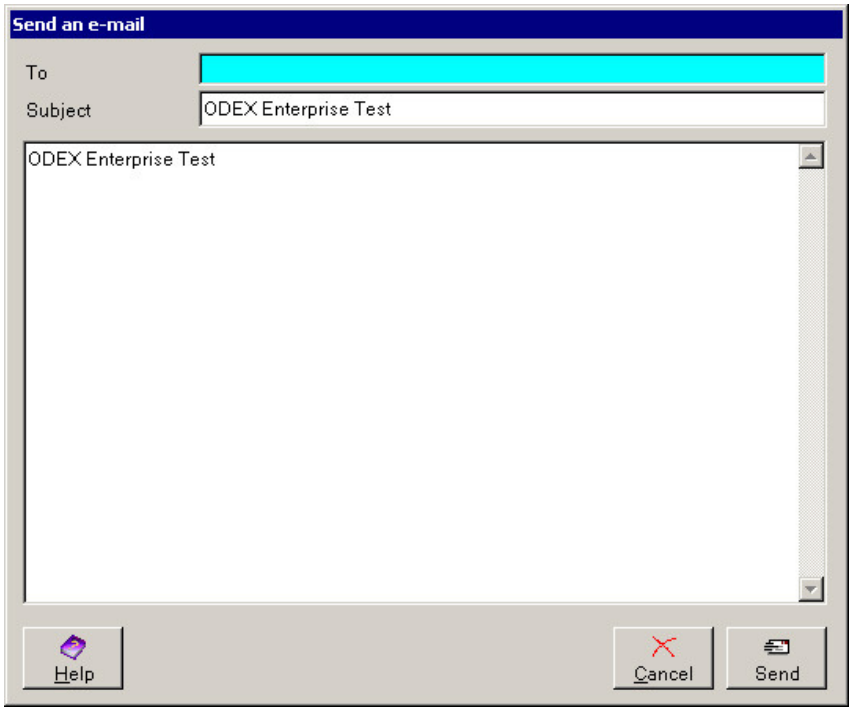
Type in this field the DNS name or IP address of your network.

Default originator e-mail address

Type in this field the address of the e-mail originator (usually yourself). This address will be used by ODEX as the From address when creating and sending e-mails triggered by automated events or workflows. Please ensure that the address is in a valid e-mail address format and that the address is known to your network.

Send a test e-mail

You must use this button to test that the e-mail settings work before you will be allowed to save them.



Type the e-mail address of the intended recipient in the To field.

The Subject field will already be filled in, but you may change the contents if you wish.

The main body of the e-mail will already be filled in, but you may change the contents if you wish.

To send the test e-mail, click the **Send** button. Otherwise click the **Cancel** button. You will be returned to the System Settings – E-mail page.

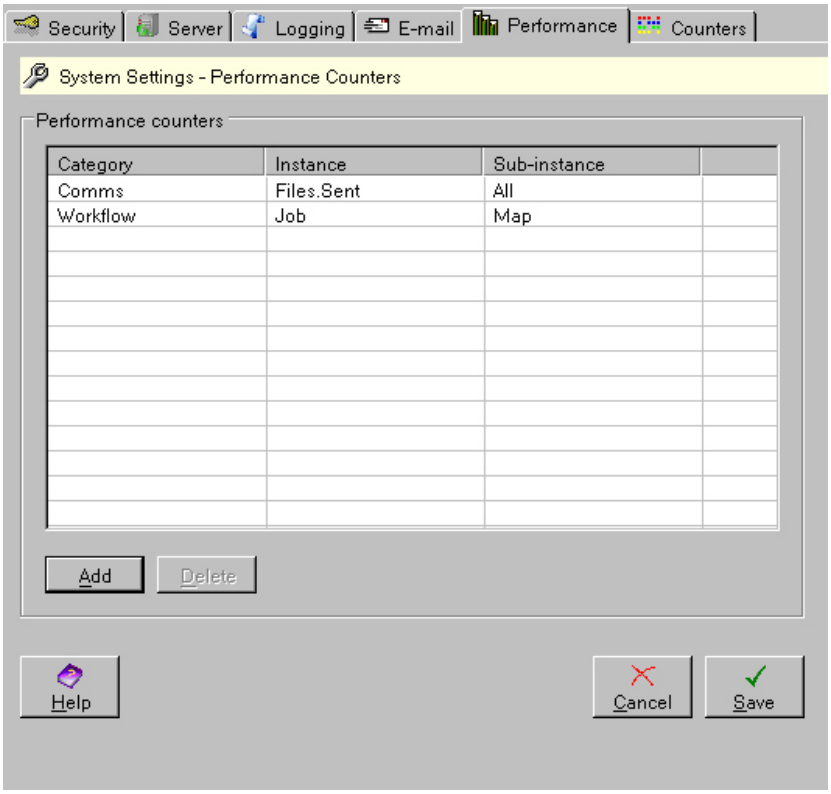
Failure of test e-mail

If your attempt to send a test e-mail fails, it may be because of the configuration of your mail server. If you are trying to send to an internal address there should be no problem. However, if you are trying to send to an external address, you must configure your system to allow relaying on your mail server for your ODEX Server DNS name or IP address.

Performance Page

Performance counters may prove useful in Just-In-Time supply environments where the receipt of files is critical. For example counters may be can be set up to monitor the time since a file was last received, or how many file are sent per hour. An event action can be set up to monitor counters and when they fall below a certain level perform some other action to notify the user such as send an email.

The Performance Page displays a list of performance counters that will be exposed to Windows, and allows you to add new ones, or delete counters already defined:



The list shows the following data:

Category - This is the name of the performance counter category.

Instance - This is the instance name of the counter.

Sub-instance - This is the sub-division of counter instance.

These categories are described more fully below.

Windows Performance Counters

ODEX Enterprise can expose a number of different performance counters to the operating system. Counters are defined to Windows using these four parameters:

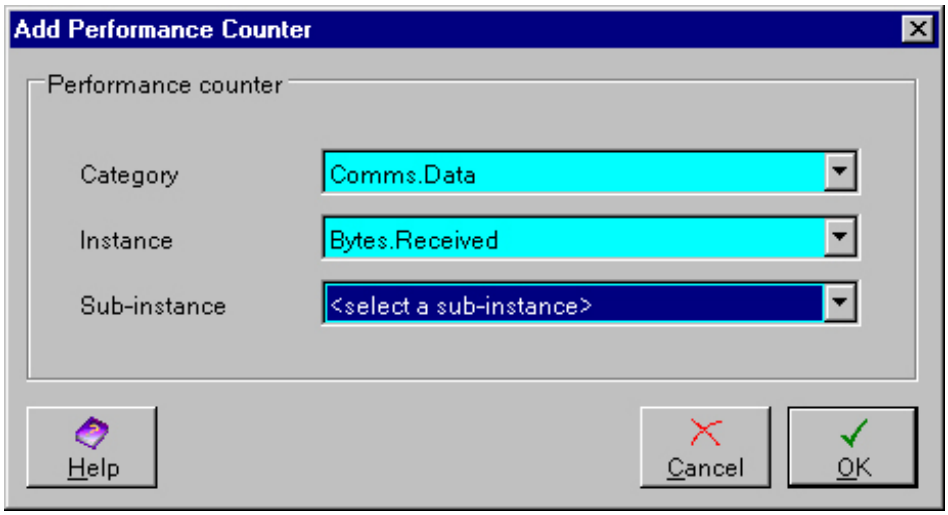
- Machine name – you cannot change this as it will always be the machine that is running the ODEX Enterprise server application (or system service).
- Category (or performance object) – represents the system or application object that will be monitored; for ODEX these will be:
    - Workflow
    - Comms
    - Comms.Data
- Counter name – represents the metric; for ODEX these will be:
    - For all categories except ODEXEnterprise.Comms.Data:
        - ItemsPerHour – number of items processed per hour
        - ItemsPerMinute – number of items processed per minute
        - ElapsedTime – number of seconds since last item processed
    - For the ODEXEnterprise.Comms.Data category:

        - BytesPerMinute – average number of bytes per minute.
- Counter instance (and sub-instance) – the instance for which the metric is collected; for ODEX these will be:
    - For the ODEXEnterprise.Workflow category:
        - Channel.All – instance updated when file completes processing on any channel
        - Channel.NAME – instance updated when file completes processing on named channel
        - Job.All – instance updated when any job completes
        - Job.NAME – instance updated when named job completes
        - DataSource.All – instance updated when any data source is matched to a channel
        - DataSource.NAME – instance updated when named data source is matched to a channel
    - For the ODEXEnterprise.Comms category:
        - Files.Scheduled.All – instance updated when a file is scheduled
        - Files.Scheduled.NAME – instance updated when a file is scheduled to the named trading partner network
        - Files.Sent.All – instance updated when a file is sent
        - Files.Sent.NAME – instance updated when a file is sent to the named trading partner network
        - Files.Received.All – instance updated when a file is received
        - Files.Received.NAME – instance updated when a file is received from the named trading partner network
        - Acks.Sent.All – instance updated when an acknowledgement is sent
        - Acks.Sent.NAME – instance updated when an acknowledgement is sent to the named trading partner
        - Acks.Received.All – instance updated when an acknowledgement is received
        - Acks.Received.NAME – instance updated when an acknowledgement is received from the named trading partner
    - For the ODEXEnterprise.Comms.Data category:
        - Bytes.Sent.All – instance updated with file size when a file is sent
        - Bytes.Sent.NAME – instance updated with file size when a file is sent to the named trading partner network
        - Bytes.Received.All – instance updated with file size when a file is received
        - Bytes.Received.NAME – instance updated with file size when a file is received from the named trading partner network.

Editing Performance Counters

To remove a performance counter that has already been defined, highlight the item in the list and click the **Delete** button.

To define a new performance counter and expose it to windows, click the **Add** button. The following dialog is displayed.

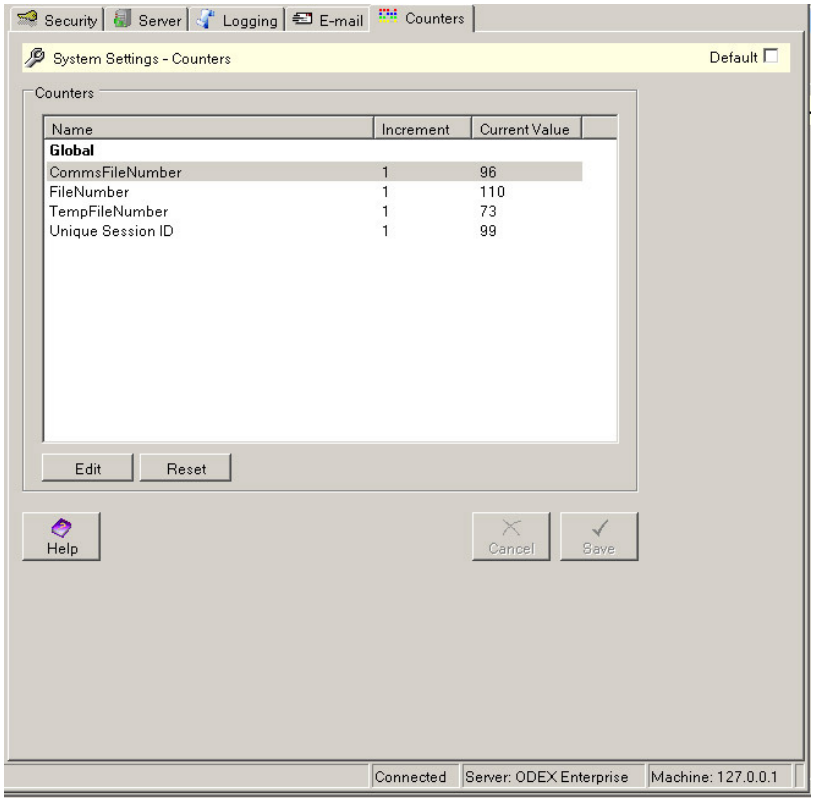


Select the required category, instance and sub-instance from the drop-down lists shown and click OK to add the counter. When you select an entry in the category drop-down list, the instance drop-down list will display the instances available for that category only. When you select an entry in the instance drop-down list, the sub-instance drop-down list will show entries for that instance only. For example. If you select the 'Workflow' category, the instances available will be 'Channel', 'Data Source' and 'Job'. If you then select the 'Channel' instance, the sub-instances available will be 'All', along with the names of the channels defined in the Workflow section of the Administrator.

A counter can only be added once. For instance, if the counter whose full designation is 'ODEXEnterprise.Comms.Files.Sent.All' has been added to the main list, the 'All' option will not be available in the sub-instance drop-down when the category selected is 'Comms' and the instance selected is 'Files.Sent'.

Counters Page

The Counters Page displays the current values of the files associated with ODEX Workstation. The counters page looks like the one below,



These are broken down into the following individual counters,

CommsFileNumber – The number of files that have been sent and received.

FileNumber – The total number of files that have been processed.

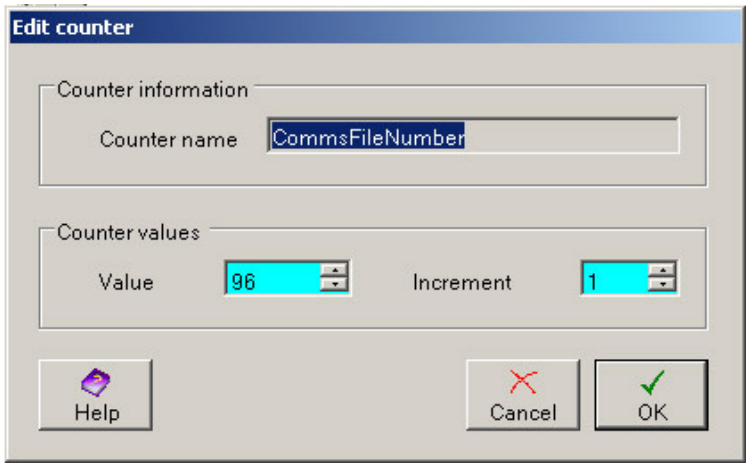
TempFileNumber – The total number of temporary files.

Unique Session ID – The current session ID.

There are two buttons associated with the counters, edit and reset.

Edit

Clicking on Edit displays the dialog as shown below,



This allows the user to change the current value of the counter. Once changed the count will increase from this newly set value. The other option is to adjust the incremental value. This has the effect of increasing the current value by a set amount, rather than the default value of 1.

Reset

Reset simply resets the current value back to zero.

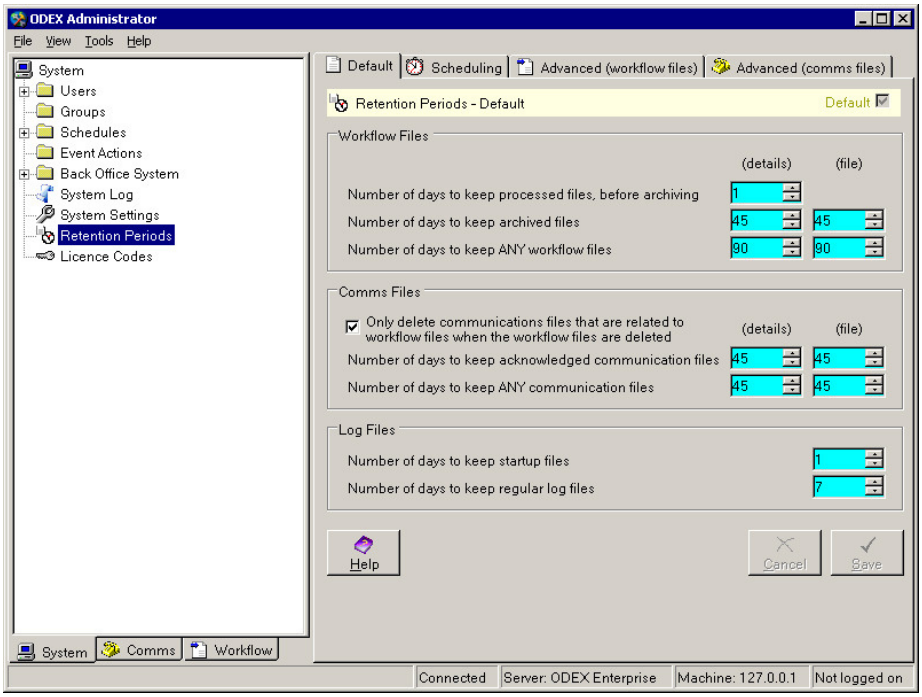
Retention Periods

This section of the ODEX Administrator allows you to specify the length of time for which workflow files, comms files and log files are to be kept in your system before being deleted.

ODEX stores a lot of information. Each new comms file, workflow file and log file means that the amount of data that ODEX has to maintain is increased. There will come a time when the data that ODEX is storing is no longer needed by you. To allow you to decide how long you keep data for, ODEX uses retention periods. These are periods of time associated with certain types of data, that indicate how long you wish to keep that type of data for.

When using this section, if you do change any values, the **Cancel** and **Save** buttons will become enabled. Click **Save** to keep the changes you have made, or click **Cancel** to discard the changes.

To see the Retention Periods section, click on the Retention Periods name in the Navigation Panel of the ODEX Administrator. This will bring up the Default page of the Retention Periods section, as shown below.



The Retention Periods section has four pages: Default, Scheduling, Advanced (workflow files) and Advanced (comms files). A description of each page can be seen below.

Default

The Default page comprises three sections: Workflow Files, Comms Files and Log Files. The Workflow Files and Comms Files sections allow you to specify how long the actual files should be kept (indicated in the file column), and also how long the database details of those files should be kept (indicated in the details column). This allows you to delete disk files while still retaining their information in your database.

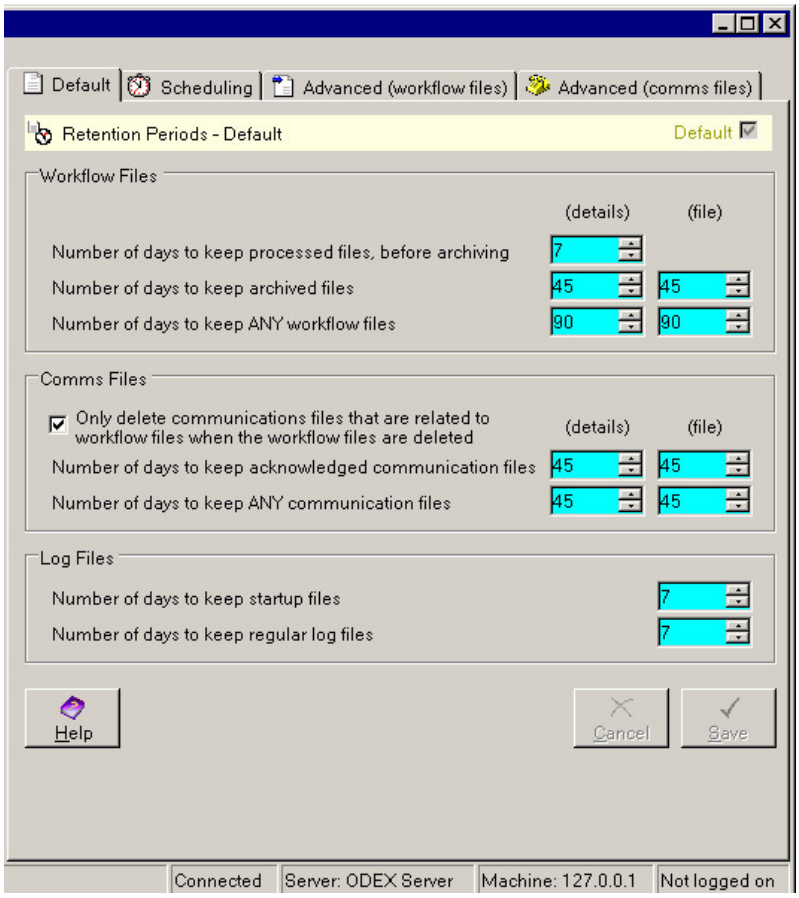
Please note that, for any individual retention period, you cannot set the value in the file column to be greater than that in the details column. This avoids the situation where a disk file exists without its corresponding details in the database.

Similarly, you cannot set the retention period for archived files (details or file) to be greater than that for "ANY" workflow files (details or file).

Likewise, you cannot set the retention period for acknowledged comms files (details or file) to be greater than that for "ANY" comms files (details or file).

The maximum value for any retention period is 10000 days. This value should be used if you want to ensure that a file or its details are never archived/deleted.

You can either type in a value or use the up and down arrows to select a value from the list.



Workflow Files

This section relates to files that have been processed by the ODEX workflow administrator.

When ODEX receives a file to be processed, a copy is taken, on which the processing will be performed. This copy is the file referred to here.

Database details of files whose processing is complete will be kept for the number of days specified in the first line (default is 7 days). The countdown will begin on the date on which the file is imported into ODEX.

Once a file has been archived, it will be kept for the number of days specified in the second line (default is 45 days).

'ANY' workflow files refers to both archived and unarchived files. Files will not be subject to retention periods until they have been processed.

Comms Files

If you want to ensure that comms files are not deleted until their related workflow files have been deleted, select the tickbox in this section.

Acknowledged communication files are outgoing files for which an EERP has been received, and incoming files for which an EERP has been sent.

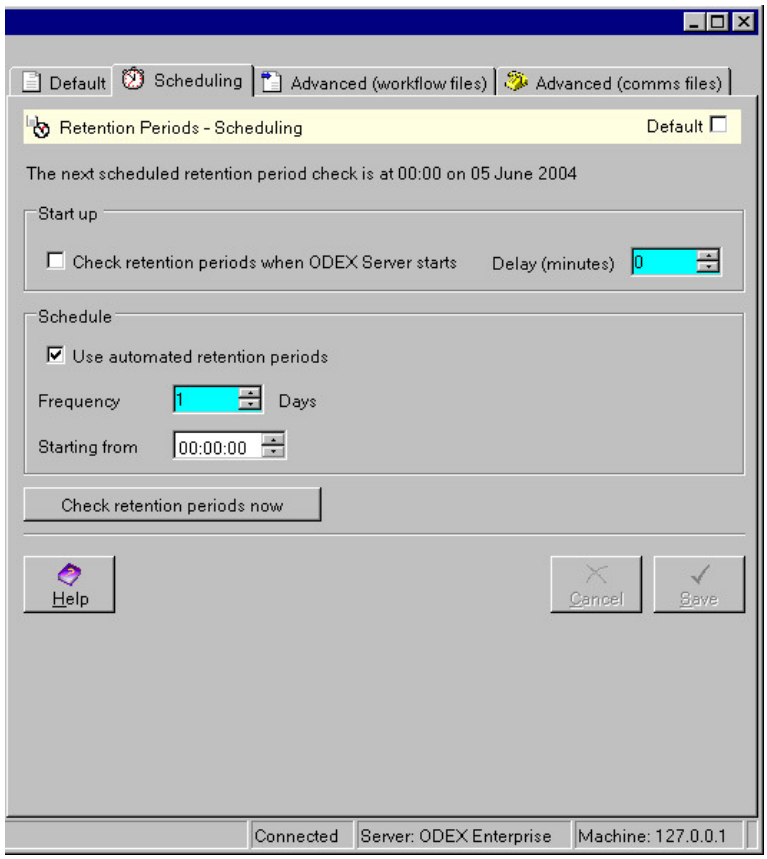
'ANY' communication files includes files for which an EERP has been received/sent and those for which an EERP has not been received/sent.

Log Files

This section allows you to choose different retention periods for startup logs and 'regular' logs. The default retention period for both is 7 days.

Scheduling

The scheduling page comprises two sections: Start up and Schedule.



This page can be used to automate the retention period sweep and to initiate a sweep manually.

An information line below the page tab banner tells you when the next scheduled retention period check is due. By default this will be at midnight of the current day.

Start up

The Start up section allows you to initiate a retention period sweep automatically when ODEX Enterprise is started. You can delay the sweep by a number of minutes if required, up to a maximum of 10000. The default delay is 0 minutes.

Schedule

The "Use automated retention periods" tickbox is selected by default. You can use the Frequency field to select how often you want the sweep to be run (1 = every day, 2 = every other day, and so on). You can also select a time for the automated sweep to begin.

If you deselect the "Use automated retention periods" tickbox, the Frequency and Starting From fields will be disabled.

Whether you select the "Use automated retention periods" tickbox or not, you can run a sweep manually at any time by clicking on the **Check retention periods now** button.

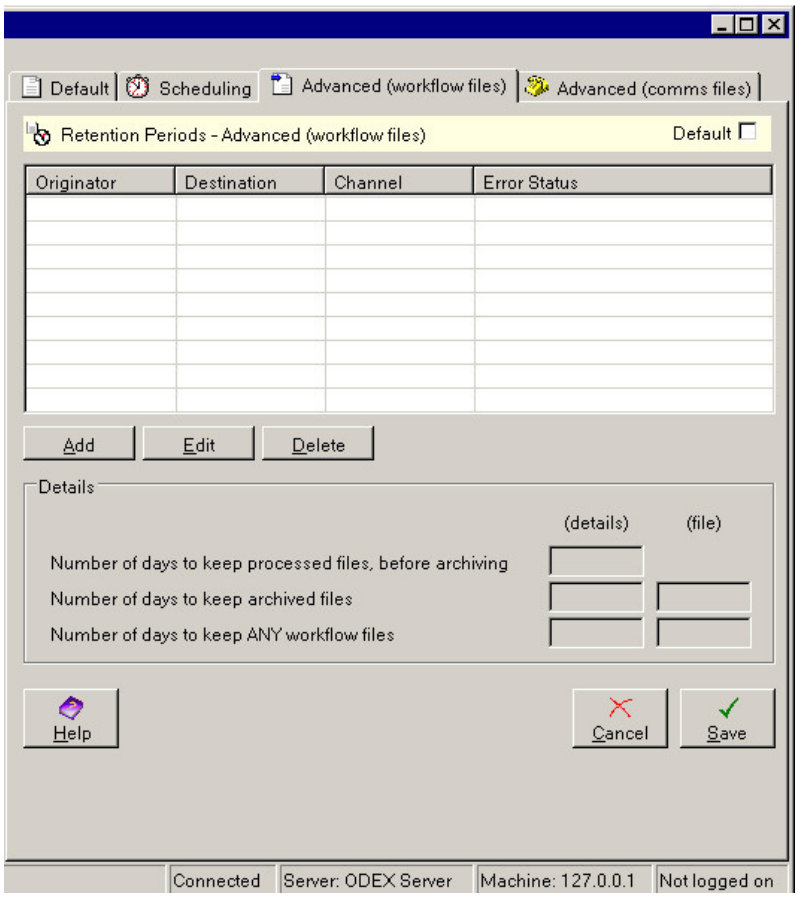
Advanced (workflow files)

This page allows you to add, edit or delete specific retention period details for specific workflow files.

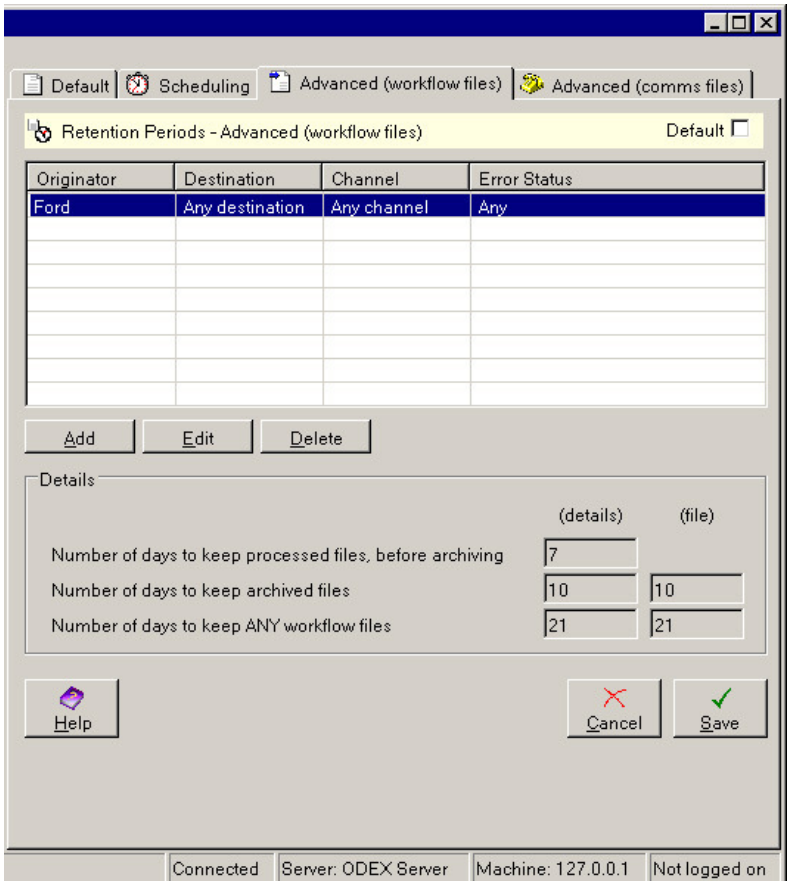
Use the **Add** button to add new details for a specific workflow file.

Use the **Edit** button to change the details of an existing entry (highlight the entry you want to edit).

Use the **Delete** button to delete an existing entry (highlight the entry you want to delete).



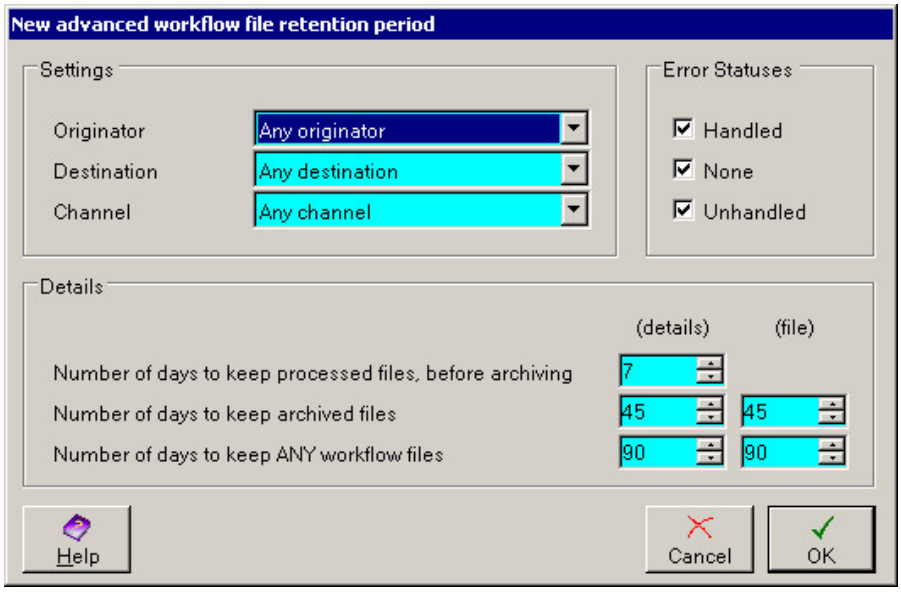
The four columns on this page (Originator, Destination, Channel and Error Status) show the details that you have already set up for specific workflow files. If you highlight one of the entries in the list, the corresponding retention period details will be displayed in the fields in the lower half of the page, as illustrated below.



Advanced workflow file retention period dialog

This is the dialog you will see if you select the **Add** or **Edit** button from the Advanced (workflow files) page.

This dialog is intended to provide specific retention period details for specific workflow files. Therefore you should change at least one of the Originator, Destination and Channel field settings as well as the values in the Details section. Otherwise the effect of this page will be to override the retention period details on the Default page (if the values here are lower than there) or to have no effect at all (if the values here are greater than there).



Settings

Use the dropdown arrows to select the required Originator and Destination trading partners.

Use the dropdown arrow to select the required Channel.

It is your responsibility to ensure that the selected settings are compatible.

Error Statuses

You must select at least one type of error status. If you select all three types, this will appear on the Advanced (workflow files) page as "Any".

Details

The fields in this section are the same as those in the **Workflow Files** section of the Default page. Please refer to those sections for further details.

Click **OK** to save your changes, or **Cancel** to quit this dialog without saving your changes.

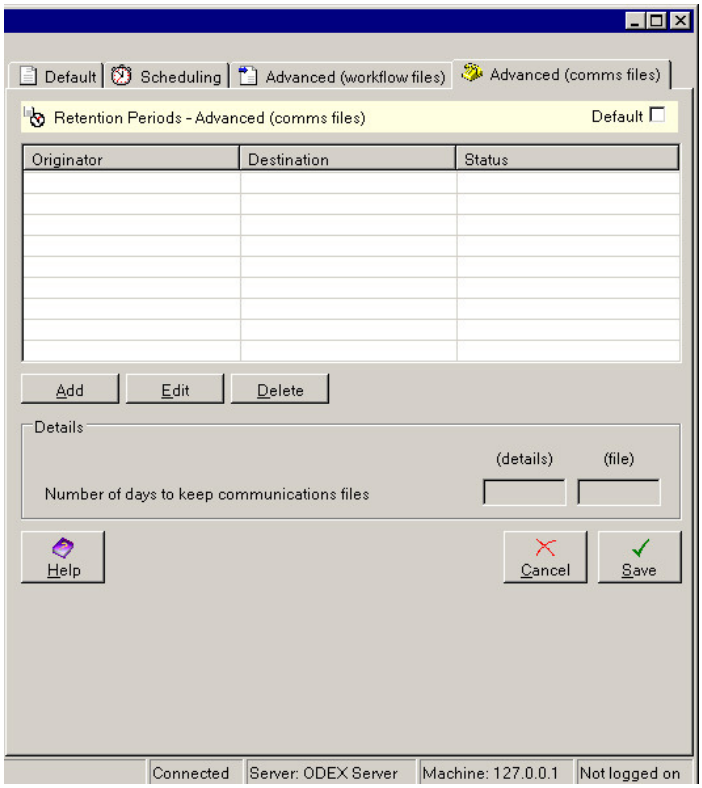
Advanced (comms files)

This page allows you to add, edit or delete specific retention period details for specific comms files.

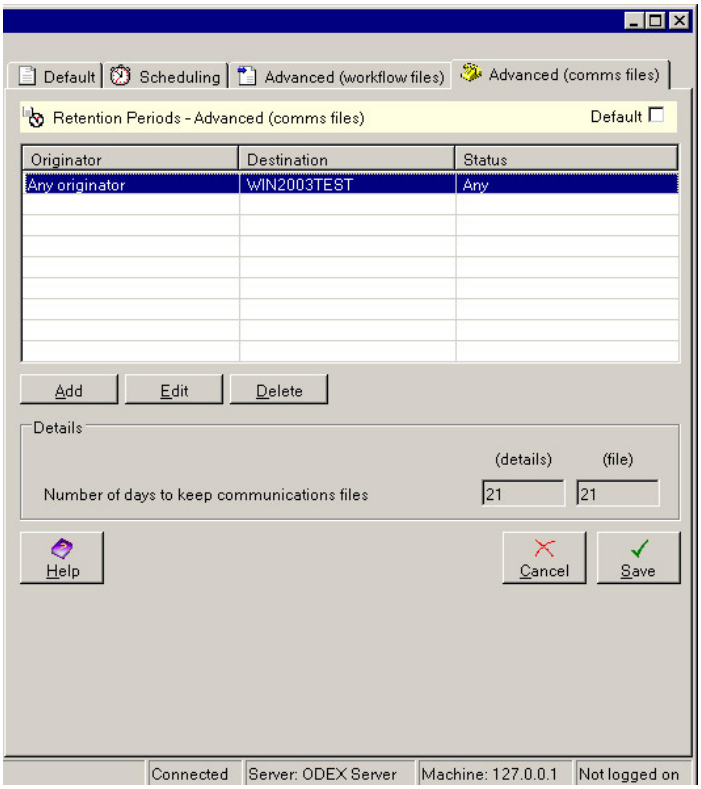
Use the **Add** button to add new details for a specific comms file.

Use the **Edit** button to change the details of an existing entry (highlight the entry you want to edit).

Use the **Delete** button to delete an existing entry (highlight the entry you want to delete).



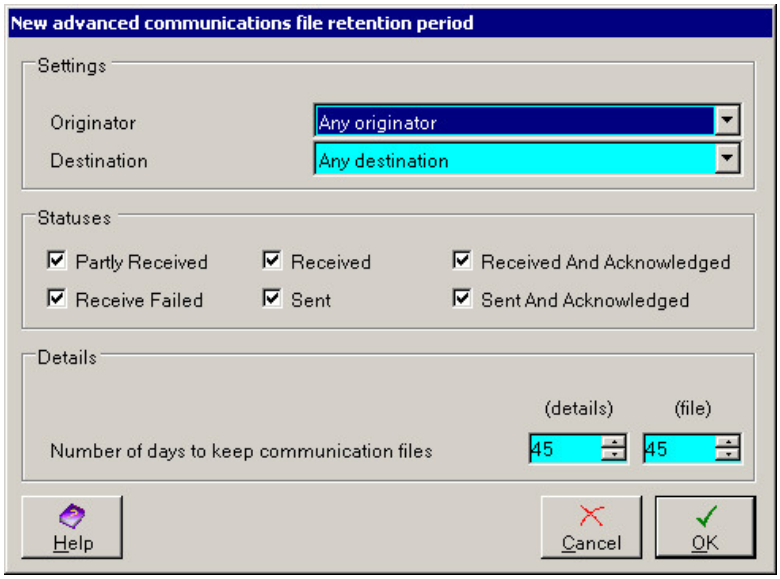
The three columns on this page (Originator, Destination and Status) show the details that you have already set up for specific comms files. If you highlight one of the entries in the list, the corresponding retention period details will be displayed in the fields in the lower half of the page, as illustrated below.



Advanced communications file retention period dialog

This is the dialog you will see if you select the **Add** or **Edit** button from the Advanced (comms files) page.

This dialog is intended to provide specific retention period details for specific comms files. Therefore you should change at least one of the Originator and Destination settings as well as the values in the Statuses section and Details section. Otherwise the effect of this page will be to override the retention period details on the Default page (if the values here are lower than there) or to have no effect at all (if the values here are greater than there).



Settings

Use the dropdown arrows to select the required Originator and Destination mailboxes.

It is your responsibility to ensure that the selected settings are compatible.

Statuses

You must select at least one type of status. If you select all six types, this will appear on the Advanced (comms files) page as "Any".

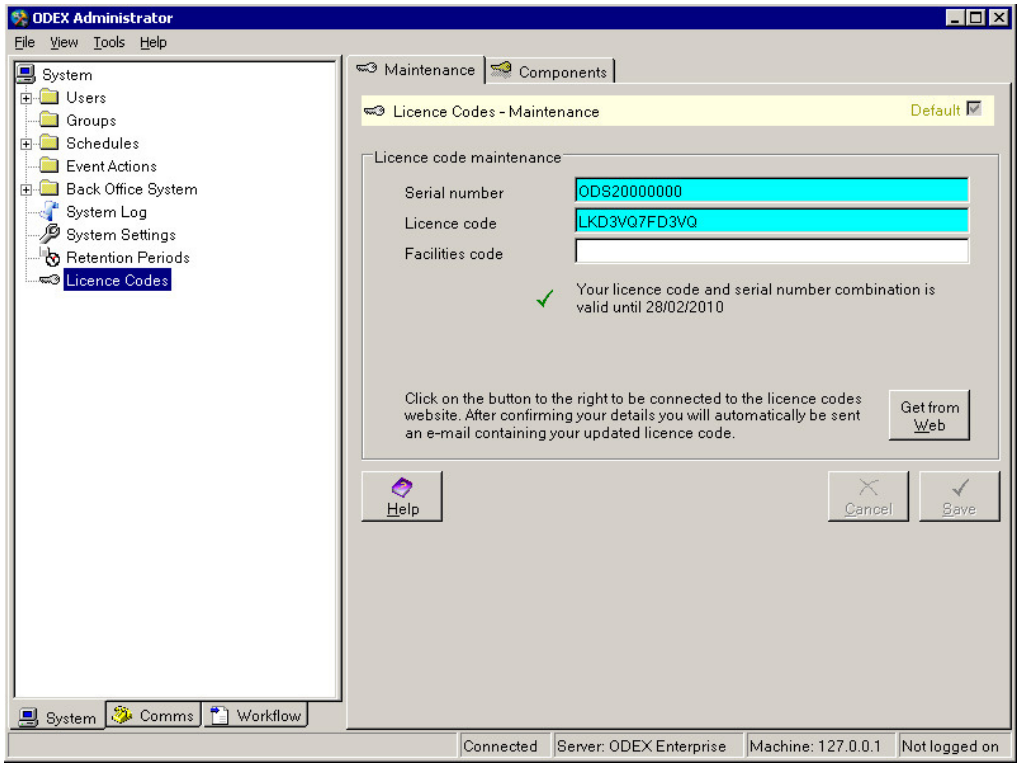
Details

You can type in a value or use the up and down arrows to select a value for the comms files retention periods.

Click **OK** to save your changes, or **Cancel** to quit this dialog without saving your changes.

Licence Codes

To see the Licence Codes section, click on the Licence Codes name in the Navigation Panel of the System Administrator. This will bring up the Licence Codes – Maintenance page, as shown below.



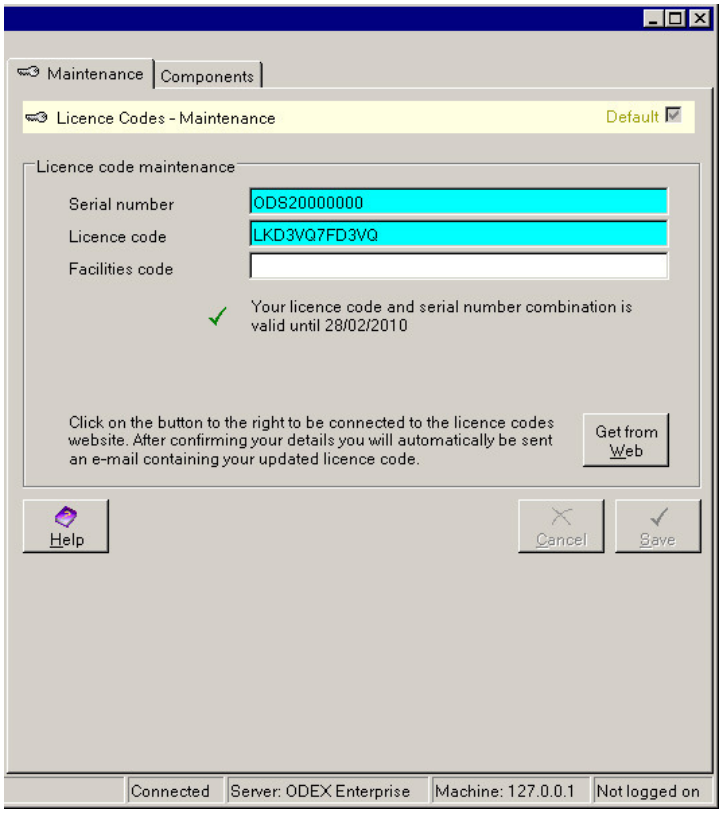
A valid and current licence code is required in order for you to use ODEX. When you first take delivery of ODEX, you will be provided with a licence code and a serial number for your copy of ODEX. These must be entered the first time you start to use ODEX after the installation process.

Some users may have been given an installation code instead of a licence code. In this case you will not be able to use ODEX until you have upgraded the installation code to a full licence code. These users should refer to the section below entitled "Installation Codes".

The serial number is a unique number allocated to your copy of ODEX. It should be quoted in all correspondence relating to ODEX.

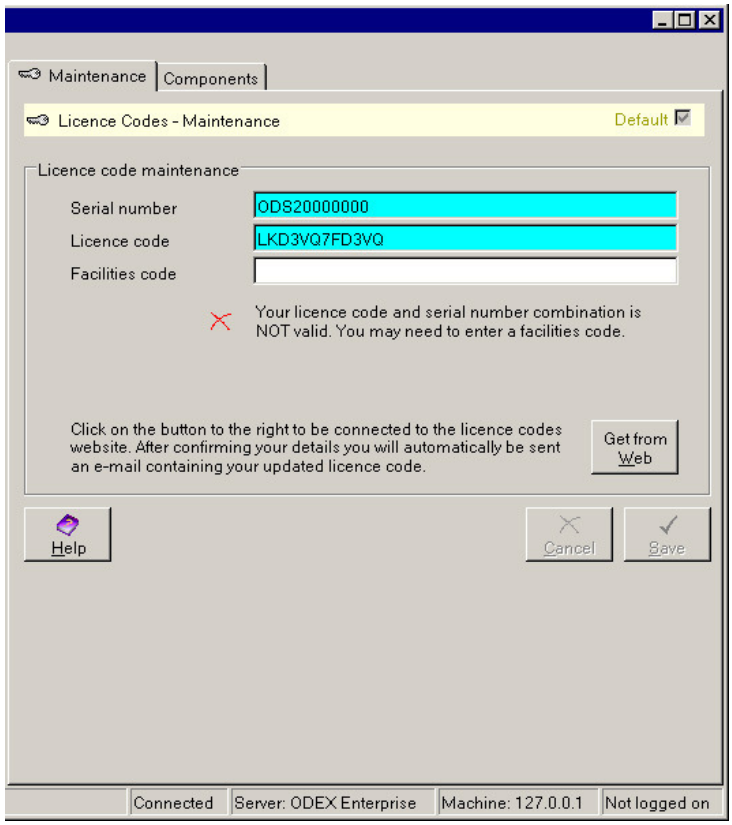
The licence code belongs uniquely to the serial number, but has an expiry date. This means that, usually once a year, you must update your licence code in order to continue using ODEX. The place to do that is here, on the Licence Codes page of the ODEX System Administrator.

The default page in the Licence Codes section is the Maintenance page, as shown below.



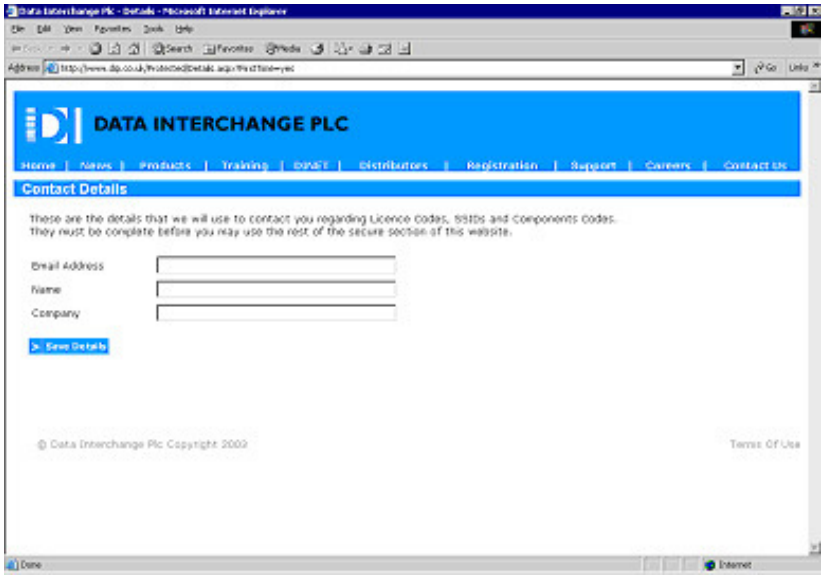
During the validity of your licence code, if you open this page you will see a message telling you that your licence code and serial number combination is valid. This is further indicated by a green tick alongside the message. It also tells you the expiry date of the licence code.

When the licence code expires, the message will change to say that your licence code and serial number combination is NOT valid. This is further indicated by a red cross alongside the message, as shown below.



In this case, you will not be able to use ODEX again until you have inserted a valid and current licence code.

To obtain an updated licence code, click on the **Get from Web** button. This will take you to the Data Interchange Plc website, where you will be able to obtain your new licence code. If this is the first time you have used it, the website page looks like the one shown below:

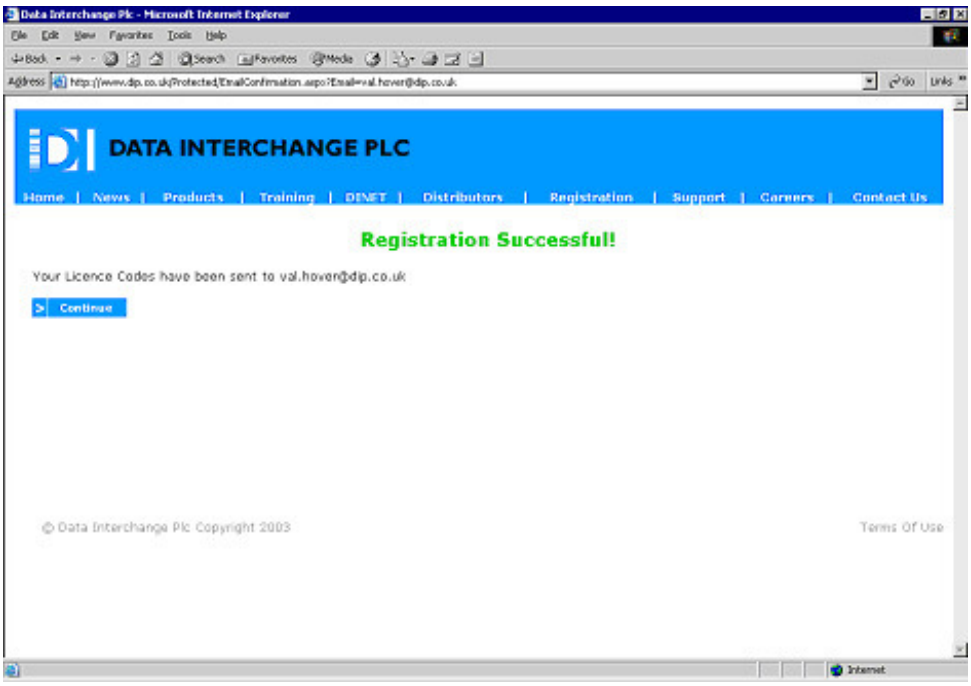


You should fill in your e-mail address, name and company name in the boxes provided, so that a new licence code can be sent to you.

If you have previously accessed this page of the website, these details will already be filled in. Please check the details shown on this screen, and change them if necessary.

In either case, it is important that we have the correct contact name and e-mail address, so that we can send the new licence code to you.

Click the **Save Details** button to send us the details, and you should then see the following screen:



The new code will be e-mailed to you, using the e-mail address shown on this screen. When you have the new code, return to the Licence Codes page of the System Admin section of the ODEX Administrator and copy it into the Licence code field.

> *If you choose to type the code in, please be very careful not to confuse the letter I with the number 1 and the letter O with the number 0.*

When the red cross has changed to a green tick, click the **Save** button. You may now leave the Licence Codes page.

Components

ODEX comes with six extra components: the SAP component, the Xe component, the XLATE component, the ENGDAT Component, the OFTP2 component and the SFTP component. You will need to unlock one or more of these if you intend to use any of the following Jobs in the Workflows section of the Administrator:

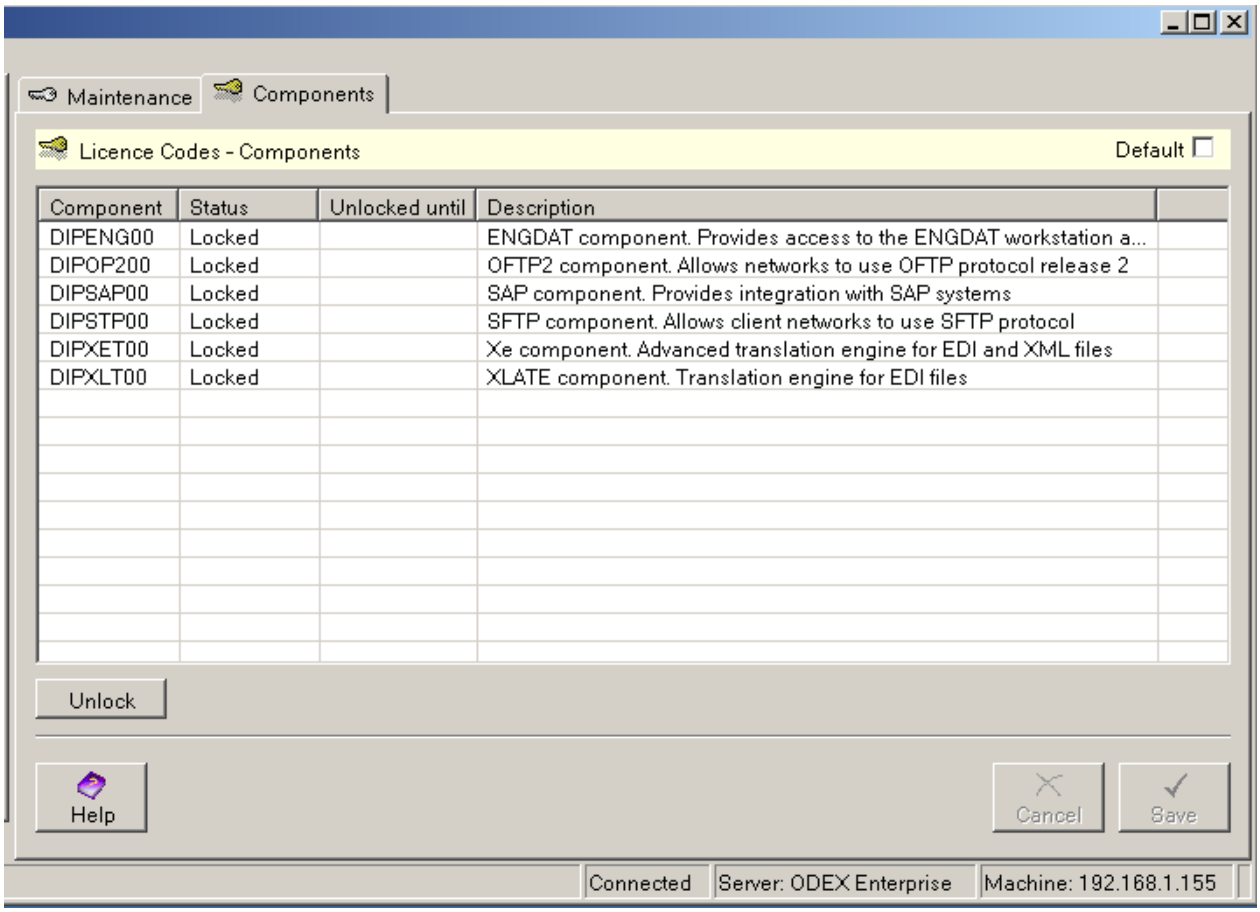
- Construct – uses XLATE
- Translate – uses XLATE
- Map – uses Xe
- SAP (Associate) – uses SAP
- SAP (Export) – uses SAP

You will need to use these Jobs if you want to integrate ODEX with a SAP system and/or transform files of one format into files of another format.

OFTP2 component which when unlocked opens up OFTP2 to be used in ODEX.

SFTP component which when unlocked allows connection to a FTP server using SFTP protocol.

Click on the Components page tab to see the Licence Codes Components page, shown below.



This page has three columns, displaying all the available components, their status and their description. Components currently available are:

DIPENG00 – the ENGDAT component

DIPSAP00 – the SAP component

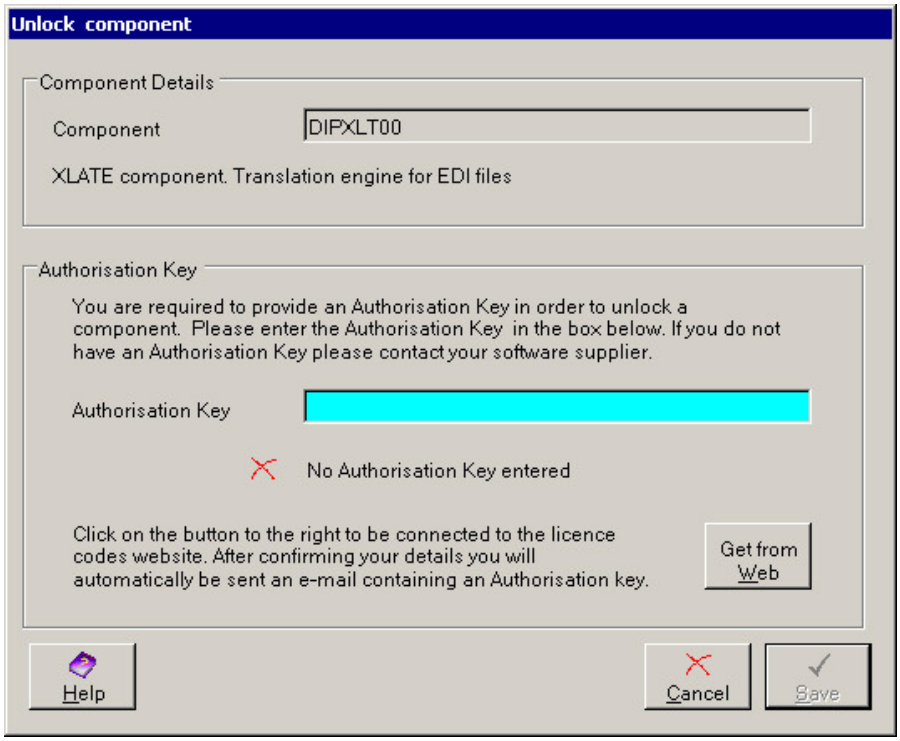
DIPXET00 – the XE component

DIPXLT00 – the XLATE component

DIPOP200 – the OFTP 2 component

DIPSTP00 – the SFTP component

To unlock a component, highlight the component in the list and click the **Unlock** button. This will bring up the dialog shown below.



The selected component is shown at the top of the dialog, with a brief description below it.

In the Authorisation Key section, please enter your authorisation key for this component in the field provided.

> *If you do not yet have an authorisation key, please contact your software supplier or click the **Get from Web** button on the dialog.*

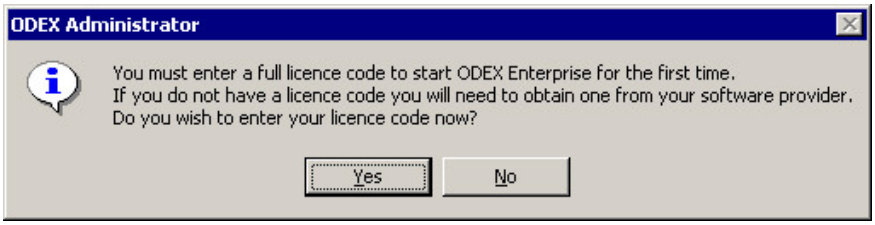
If the authorisation key is valid, click the **Save** button, which will now be enabled. If the **Save** button is not enabled, please check that you have used the correct authorisation key for the selected component.

After saving, you will be returned to the Components page, where you will see that the Status of the component has changed to "Unlocked". Click the **Save** button on this page and the component is now available to use.

Installation Codes

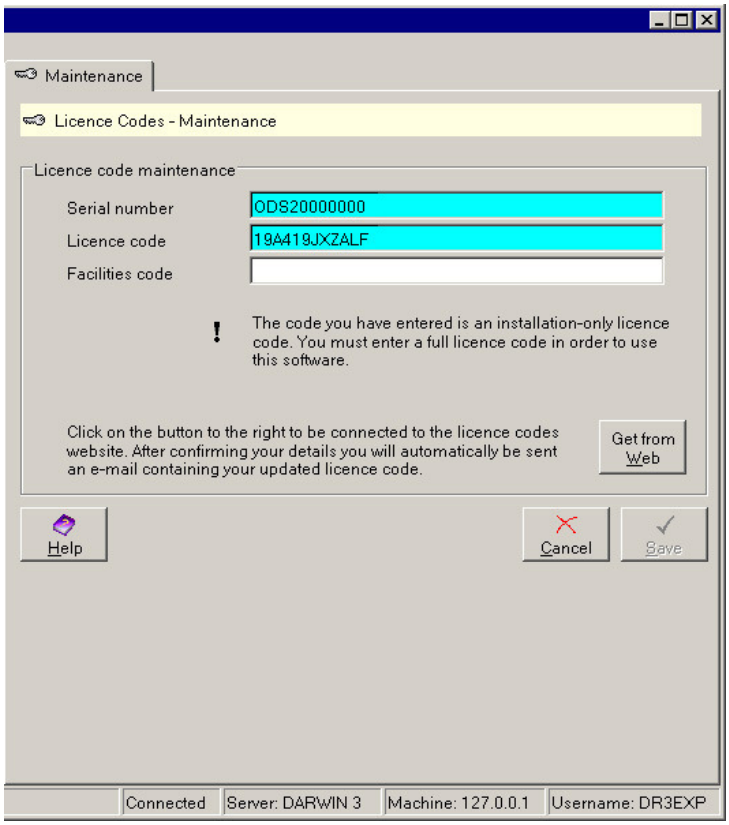
If you have been given an installation code, you will not be able to use ODEX until you have exchanged the installation code for a full licence code.

When you start the ODEX Administrator for the first time you will see the following message box:



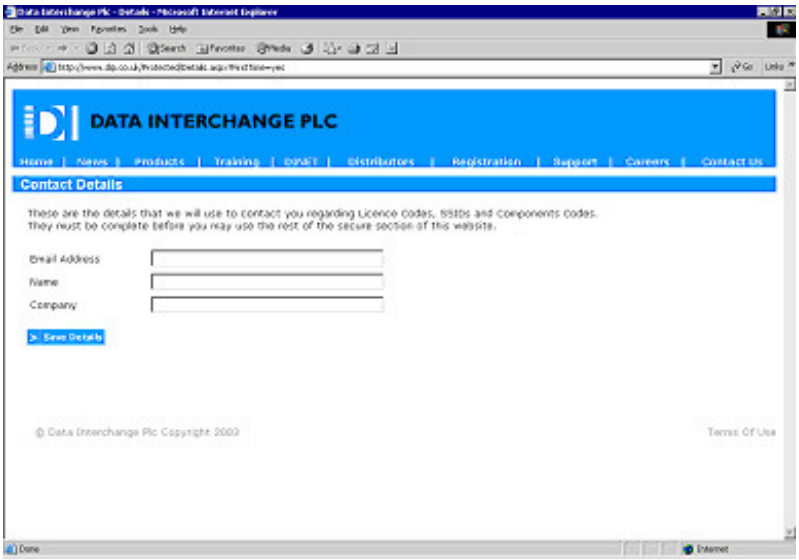
If you choose **No**, the ODEX Administrator will close. If you choose **Yes**, you will be taken straight to the Licence Codes page, so that you can upgrade your installation code to a full licence code.

The Licence Codes page will initially look like the one shown below:



You will see a black exclamation mark, indicating that the code you have entered is an installation-only licence code.

Click on the **Get From Web** button to gain access to the Data Interchange Plc website, where you will be able to obtain your full licence code. The website page will look like the one shown below:

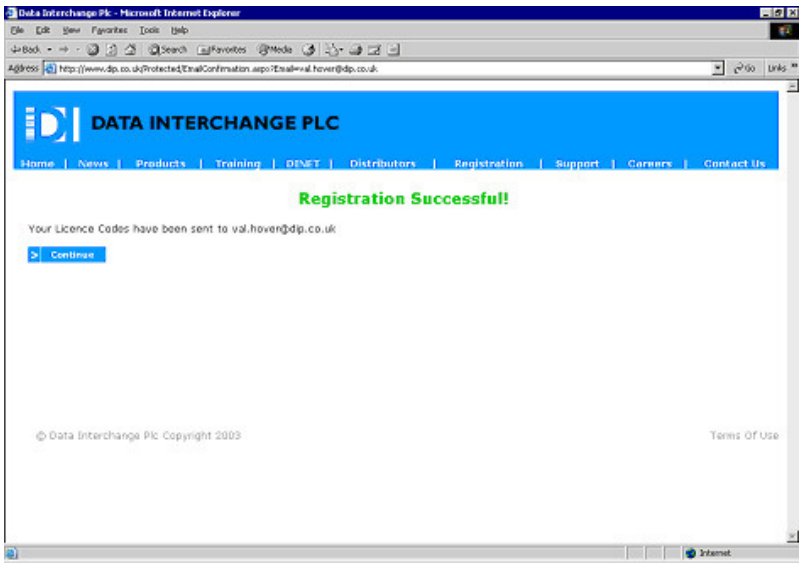


You should fill in your e-mail address, name and company name in the boxes provided, so that a new licence code can be sent to you.

If you have previously accessed this page of the website, these details will already be filled in. Please check the details shown on this screen, and change them if necessary.

In either case, it is important that we have the correct contact name and e-mail address, so that we can send the new licence code to you.

Click the **Save Details** button to send us the details, and you should then see the following screen:



The new code will be e-mailed to you, using the e-mail address shown on this screen. When you have the code, return to the Licence Codes page of the System Admin section of the ODEX Administrator and copy it into the Licence code field.

> *If you choose to type the code in, please be very careful not to confuse the letter I with the number 1 and the letter O with the number 0.*

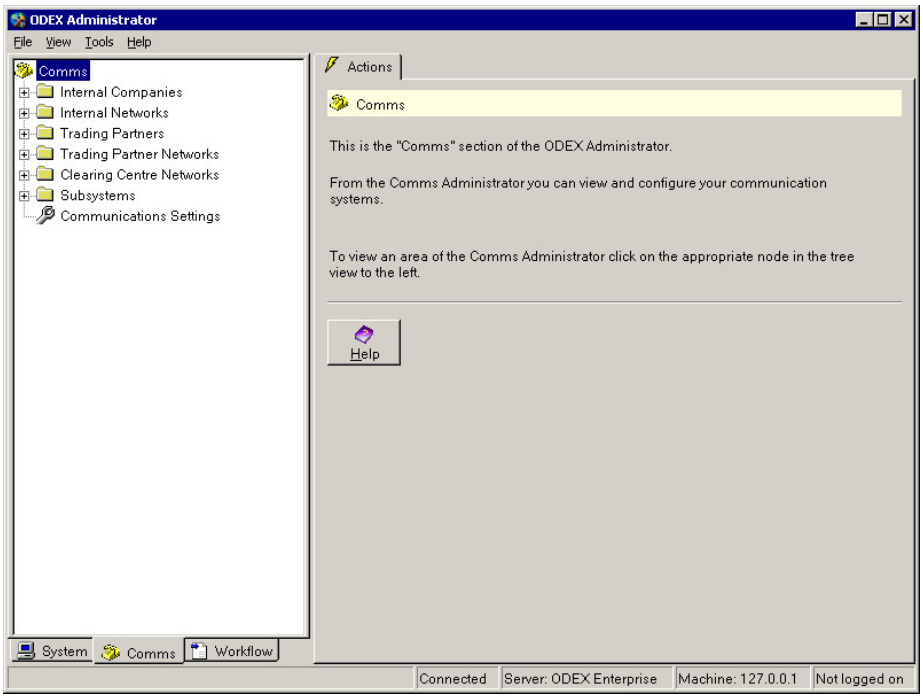
When the black exclamation mark has changed to a green tick, click the **Save** button. You may now leave the Licence Codes page.

Comms Administrator

Introduction

You only need to configure this section if you are using ODEX as your communications system.

The first time you click on the Comms page tab of the ODEX Administrator, you will see the following screen.

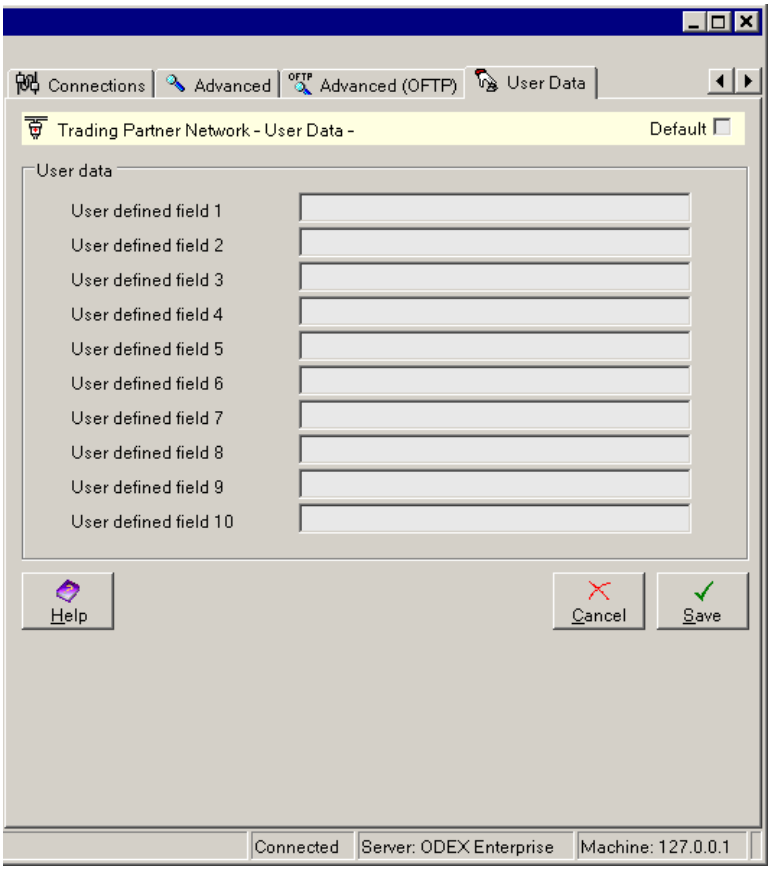


This is the Comms section of the ODEX Administrator. From here you can view and configure your trading partners and communication systems. To view an area of the Comms Administrator, click on the appropriate node in the tree view to the left.

The Comms section comprises seven areas, shown in the tree list in the Navigation Panel. These are: Internal Companies, Internal Networks, Trading Partners, Trading Partner Networks, Clearing Centre Networks, Subsystems and Communication Settings.

User Data

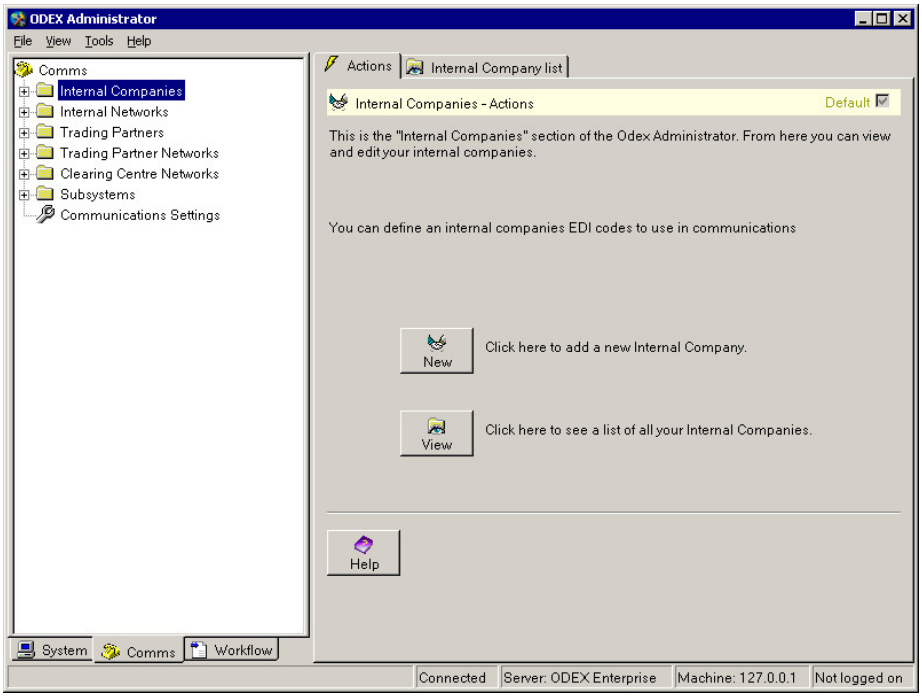
A page for configuring user data is available for all companies, networks and mailboxes. User Data pages allows you to provide a number of fields that can be used throughout Odex. For example, you can set up a User Data field against each Network to specify a different email subject for each one. Then, if a workflow is set up to send you an email whenever a file is received, you can use a placeholder to specify the networks User Data should be used for the email subject. Using this technique you can tailor your emails to be network specific, without having a number of channels/workflows defined.



Simply edit the fields you wish to use and they can then be accessed using placeholders in jobs and actions (see the Placeholders section for more details).

Internal Companies

Click on the name Internal Companies in the Navigation Panel to see the default page for the Internal Companies section, as shown below. This is the Internal Companies – Actions page.

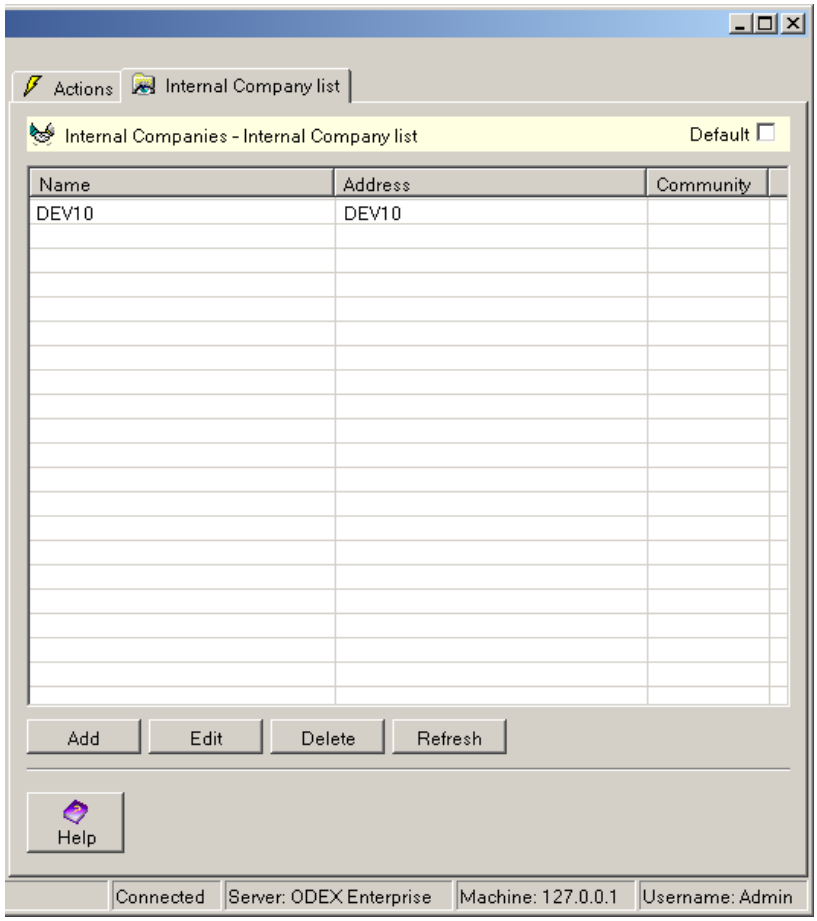


The Internal Companies section allows you to add, view and edit your internal company details.

As you can see, there are two page tabs on the Information Panel (Actions and Internal Company list) and two buttons, labelled **New** and **View**. The **New** button allows you to add a new internal company. The **View** button allows you to see a list of all the existing internal companies, from where you can edit their details, add new entries or delete existing entries.

Viewing all your internal companies

If you wish to see a list of all the internal companies currently in the ODEX database, you can either click the **View** button on the Internal Companies – Actions page or click the Internal Company list tab. Both have the same result, as in the example below.



The Information Panel now shows the Internal Company list page. Depending on your system configuration, this is divided into two or three columns. If you are not using communities, the list will have two columns, showing the Internal Company Name and its Address. If security is enabled and you are using communities, an additional column will be displayed showing the community that each internal company is associated with.

The actions that can be taken from this page are as follows:

Add

New internal companies may be added to the list by using the **Add** button. If this button is clicked, it will bring up the set of pages described below under the heading "Internal Company – Overview ".

Edit

You may edit the details of existing internal companies by using the **Edit** button. If this button is clicked, it will bring up the same set of pages described below under the heading "Internal Company – Overview ".

Delete

If you wish to delete an internal company from the list, highlight the line that you wish to delete, then click on the **Delete** button. ODEX will bring up a dialog box, asking if you are sure you want to delete the selected items. This is to safeguard against accidentally deleting the wrong item. Click **Yes** to delete or **No** to keep the item in the list.

Refresh

Click this button to refresh the details on this page, for example if you have just made some changes which have not yet appeared on this page.

Help

If you need more information about the fields and buttons on this page, click on the **Help** button.

Adding/Editing Internal Companies

If you wish to add a new internal company, click the **New** button on the Internal Companies – Actions page. You can also add a new internal company by clicking on the **Add** button on the Internal Company list page of the Internal Companies section.

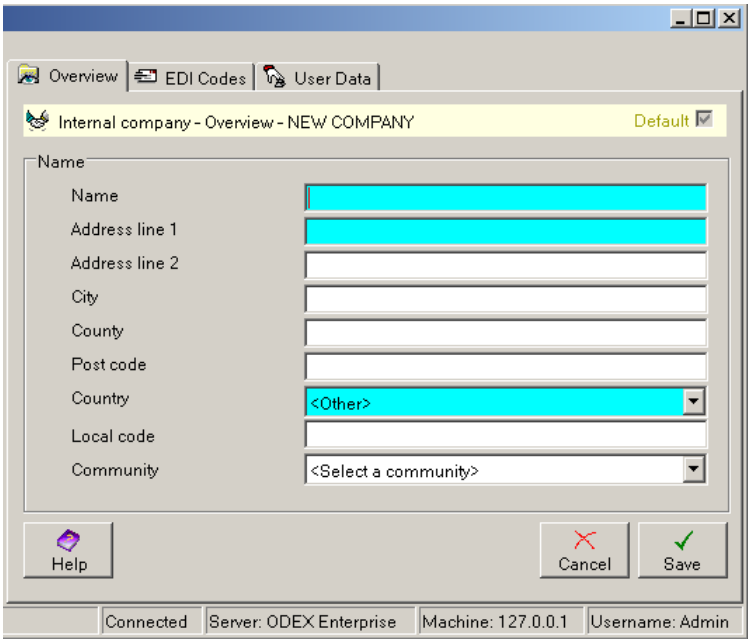
To edit an existing internal company, open the Internal Company list page, select the company to be edited, and click the **Edit** button. Alternatively, double-click on the Internal Companies node in the tree view, then click once on the company to be edited.

Whichever route you choose, you will be presented with the following set of pages, enabling you to add or edit details of an internal company. There are two pages associated with internal companies in addition to the user data page, so let's go through them and find out what information is required. For information on User Data, see the section entitled ‘User Data’.

One point to remember – each of the **Save** and **Cancel** buttons in the Internal Companies section work for both Internal Companies pages, so you do not need to click the **Save** button until you have entered data on both pages. You can click the **Cancel** button at any point to undo changes that you have made.

Internal Company – Overview

The Overview page is where mandatory information about each internal company must be provided. The Overview page looks like the example below.



Name – Name

This is the trading name of the company.

Name – Address line 1

This is the first line of the company address. It must not be left blank.

Name – other fields

If you wish to provide the full company address, please type the remaining address details into the appropriate fields.

Name – Country

This is the country where the company is based. Use the dropdown arrow to select the appropriate country.

Name – Local code

This is an optional field, included for compatibility with other systems. Most users can ignore this field. The local code is simply a unique code designated by you and used to identify the company in a shorthand form, instead of having to remember their EDI code. It is a code internally used by ODEX and will never be seen by your trading partners.

Name – Community

This field will only be visible if you are using communities and you are logged on as a user that is a member of multiple communities or a user that is not a member of any communities, e.g. the admin user.

If you are using communities and you are logged on as a user that is a member of one community, the field is hidden because the company will be created and associated with your community automatically.

Select a community if you wish to associate this network with a community. The network will then only be visible to users that are a member of the selected community, or users that are a member of a group that is a member of the selected community.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

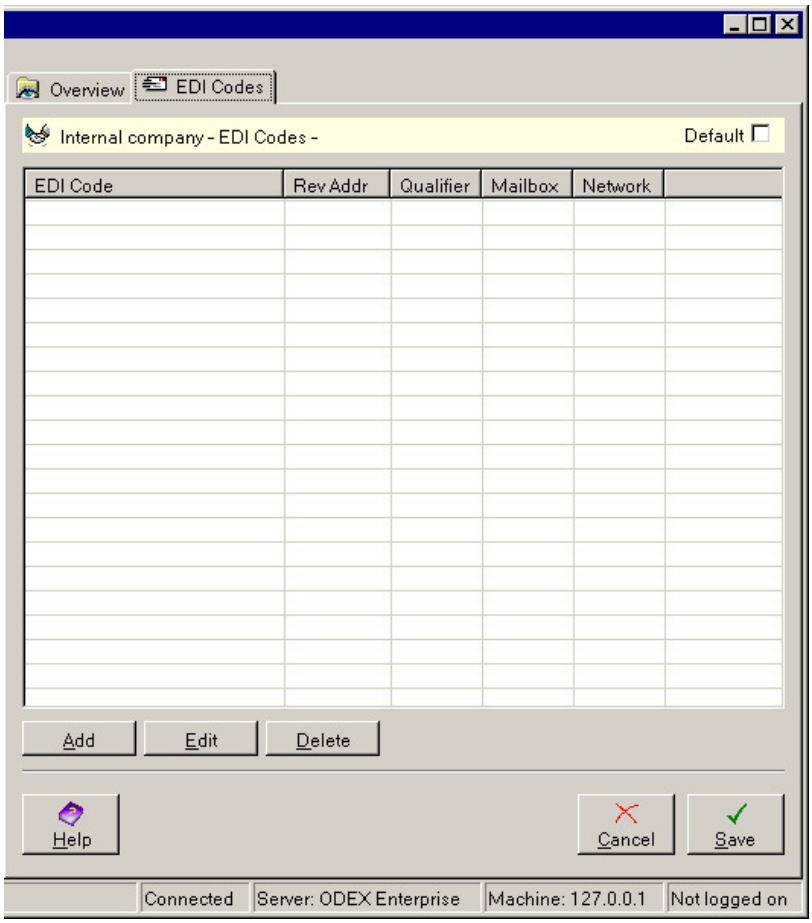
If you want to discard all the changes you have made on the Overview page, click the **Cancel** button.

Save

To save all the changes you have made on the Overview page, click the **Save** button.

Internal Company – EDI Codes

The EDI Codes page allows you to provide details of each internal company's EDI code and related details. The EDI Codes page looks like the example below.

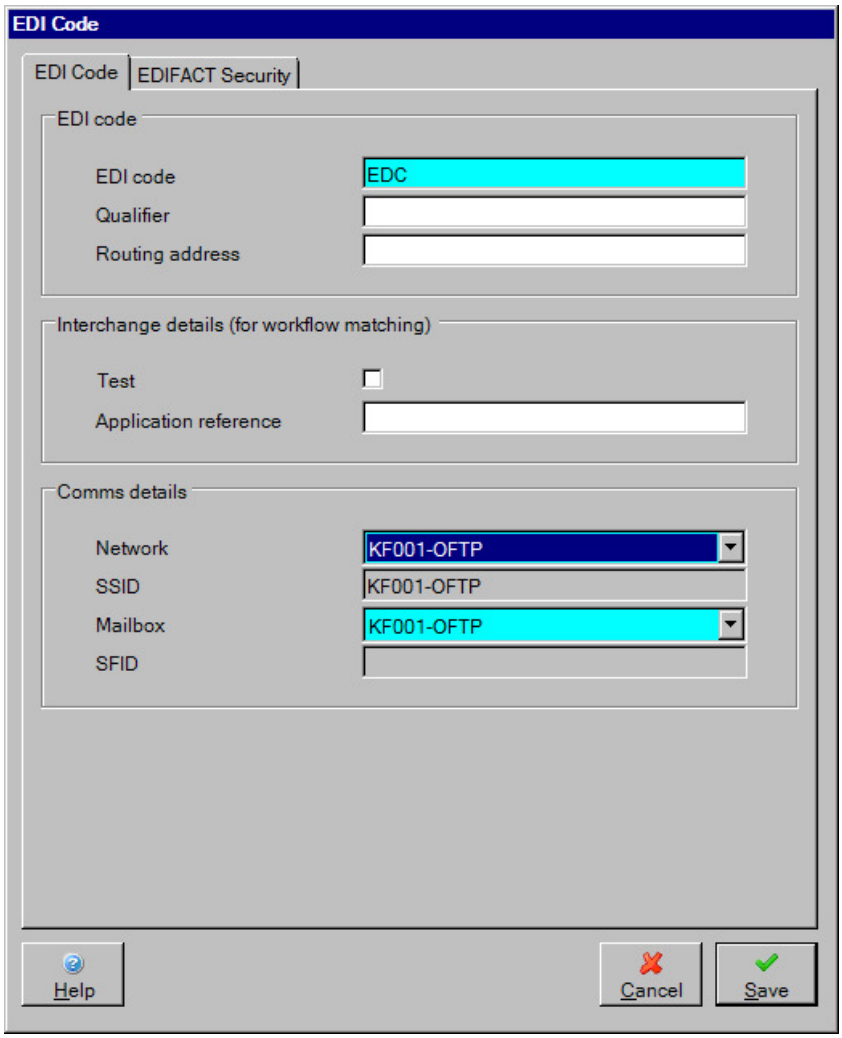


This shows a list of all the EDI codes you have already defined for the current internal company.

Add/Edit

Use the **Add** or **Edit** button to add or edit an EDI code for this internal company.

You will see the EDI Code dialog, shown below.



There is an additional tab used for specifying EDIFACT security information. Details can be found in the section ”EDIFACT Security Settings”.

The tab page shown is divided into three sections: EDI code, Interchange details and Comms details.

EDI Code – EDI code

Type in this field the EDI code of this internal company.

EDI Code – Qualifier

You only need to provide a value in this field if your trading partners require it.

EDI Code – Reverse routing address

You only need to provide a value in this field if your trading partners require it.

Interchange details – Test

Specify whether this is a test EDI code (affects the processing of inbound files when matching to a channel).

Interchange details – Application reference

Specify the application reference from the interchange segment (affects the processing of inbound files when matching to a channel).

Comms details – Network

How you handle this field depends on how you want to use ODEX.

If you want to use the auto-detect facility when scheduling EDI files or if you want to validate the EDI code in received EDI messages, you should select the appropriate network for this internal company from the dropdown list.

Otherwise you may leave the value in this field set to <None>.

If the network you require is not in the list, you must first add it in the Internal Networks section.

Comms details – ID

This field is not editable.

The caption of this field will change according to the value selected in the Network field.

If Network is <None>, the caption is 'ID'.

If the selected Network is an OFTP network, the caption is 'SSID'.

If the selected Network is an AS2 network, the caption is 'AS2 identifier'.

If the selected Network is an FTP network, the caption is 'Local code'.

Once you have selected a network in the field above, the associated SSID, Local code or AS2 identifier will appear in this field.

Comms details – Mailbox

This field will only be enabled if you have selected an OFTP network in the field above.

Select the appropriate mailbox for this internal company from the dropdown list. If the mailbox you require is not in the list, you must first add it in the Internal Networks section.

Comms details – SFID

This field is not editable.

Once you have selected a mailbox in the field above, the associated SFID will appear in this field.

Internal Companies – Locations

This page allows you to view all your different company locations (if you have more than one), to add new locations, and to edit or delete existing locations.

This page will always show the name and address line of the company from the Overview page, with the Location name of Head Office.

You only need to enter further company locations here if you want to use the addresses in ENGDAT messages. The three columns show you the following details:

Name

The name of the company location.

1st Address line

The first line of the company location address.

Add

To add a new location, click on the **Add** button at the bottom of the page.

Edit

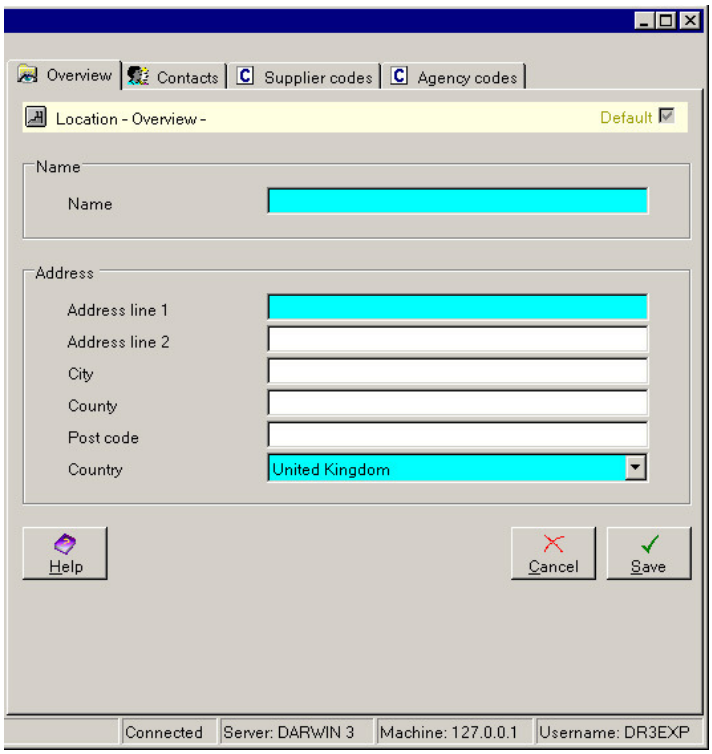
To edit an existing location, highlight the location in the list and click on the **Edit** button.

Delete

To remove an existing location from the list, highlight the location in the list and click on the **Delete** button. You will see a message box, asking if you are sure you want to delete the selected location. Click **Yes** to delete the location. Click **No** to leave the location in the list.

Locations - Adding a new location

The **Add** button brings up four new pages, labelled Overview, Contacts, Supplier codes and Agency codes, as shown in the example below.



Let's have a look at these pages and see what information is required.

Location Overview

This page requires a name for the location, one address line of the location and the country in which the location is based.

Name – Name

Type in here the name you use to refer to the location.

Address – Address line 1

This is the first line of your location address. It must not be left blank.

Address details – other fields

If you wish to provide your full location address, please type the remaining address details into the appropriate fields.

Address details – Country

Use the dropdown arrow to select the country where your location is based.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

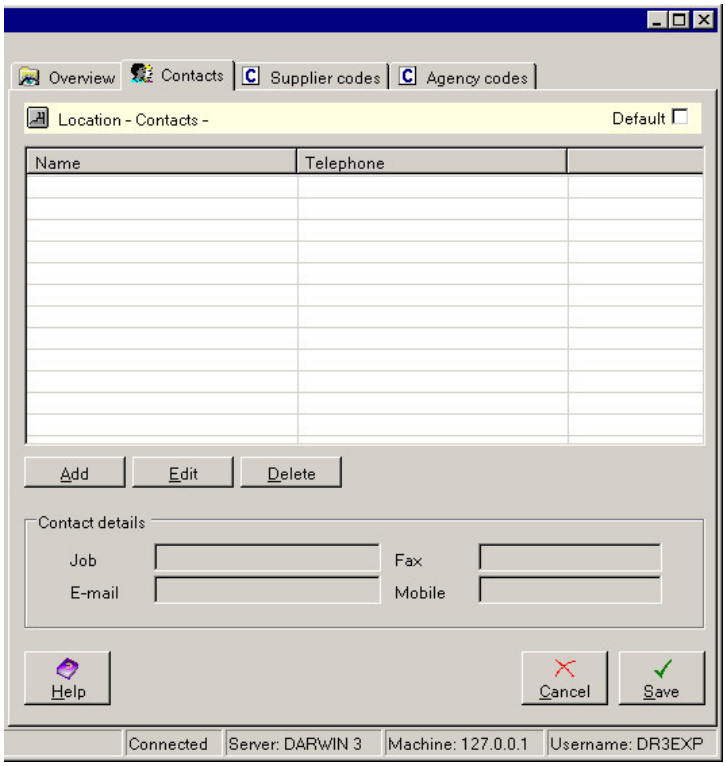
If you want to discard all the changes you have made on the Location Overview page, click the **Cancel** button.

Save

To save all the changes you have made on the Location Overview page, click the **Save** button.

Location - Location Contacts

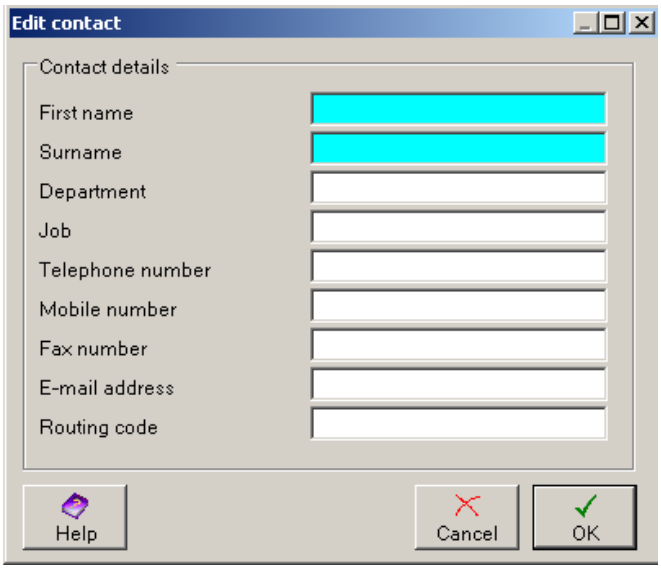
This page allows you to add a contact for the new location, if you so wish. The Contacts page looks like the example below:



If you have added details for a new location on the Overview page, you will see that the yellow title banner on the Contacts page shows the name of that location.

Locations – Location Contacts - Adding a new internal location contact

You do not have to provide contact details for new locations, but if you want to you should click the **Add** button on this page. This will bring up the following dialog:



It contains the following fields:

Contact details – Name

If you supply any contact details at all, you must provide a name. This should be the full name of the contact e.g. Mr Leslie Smith, to avoid any ambiguity.

Contact details – Other details

It will be most useful to include at least one contact number or address for the person, but none of these fields is mandatory.

Help

If you need more information about the fields on this dialog and how to fill them in, click on the **Help** button.

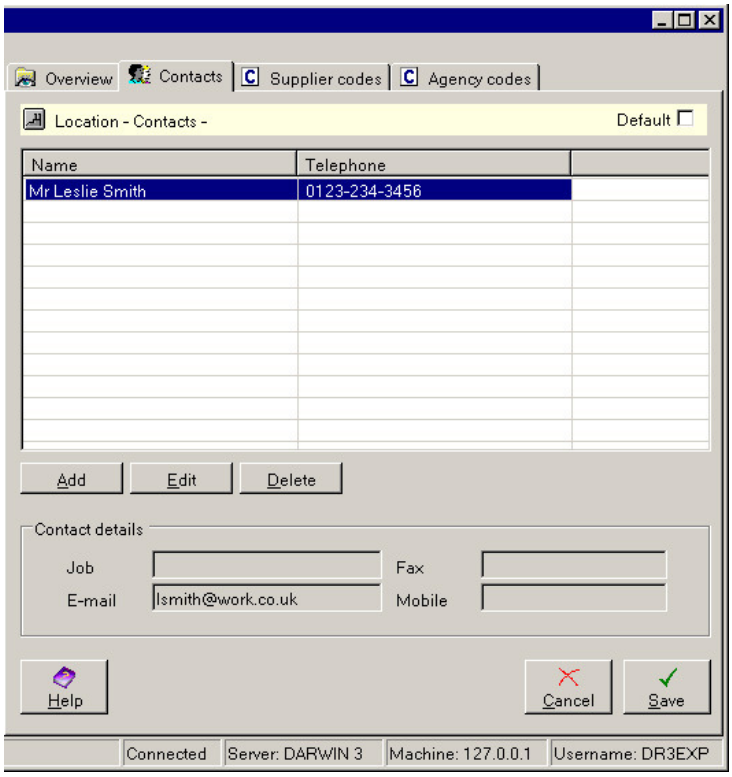
Cancel

If you want to discard all the changes you have made on the New contact dialog, click the **Cancel** button.

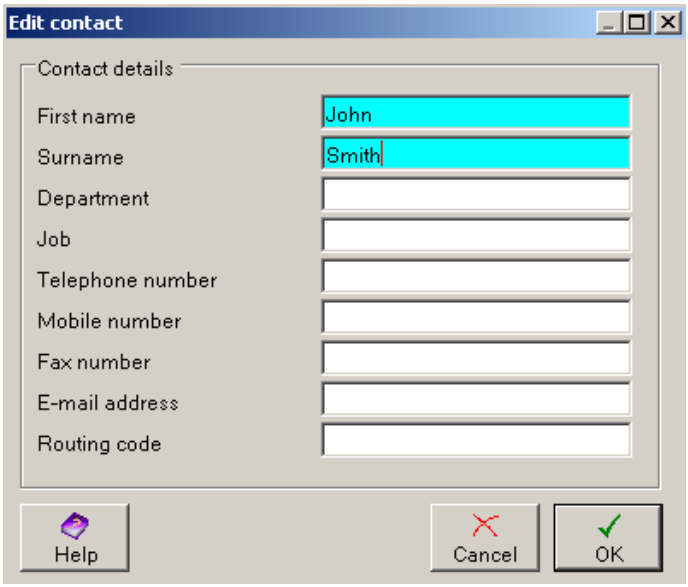
OK

To save all the changes you have made on the New contact dialog, click the **OK** button.

On returning to the Contacts page, you will see that the details you supplied on the New contact dialog are now visible, as illustrated by the example below, where just the email address and telephone number were added. The telephone number is shown alongside the contact name, and, if you highlight the contact name, the remaining details are shown in the Contact details section at the bottom of the page:



If you want to edit the contact details, highlight the appropriate contact in the list and click the **Edit** button. You will see a dialog similar to the following:



The Edit contact dialog is just the same as the New contact dialog, except that data is already in the fields. You should make any changes you need to make then either click the **Cancel** button to discard your changes or click **OK** to save your changes and return to the Contacts page.

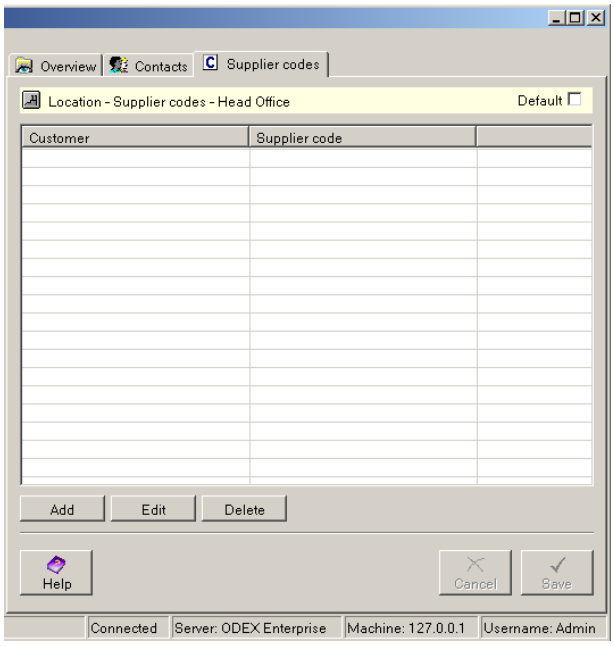
Supplier codes

This page allows you to add one or more supplier codes for the new location. Supplier codes can be used in ENGDAT messages. If you do not use ENGDAT, you do not need to enter any information on this page.

Please refer to the following sections for more information on ENGDAT

XXX

The Supplier codes page looks like the example below:



This page allows you to view all the different supplier codes by which your customers or trading partners know you, to add new codes, and to edit or delete existing codes. The two columns show you the following details:

Customer

The name of the trading partner / customer

Supplier code

The supplier code that the trading partner / customer has designated to this location of your company.

Add

To add a new supplier code, click on the **Add** button at the bottom of the page.

Edit

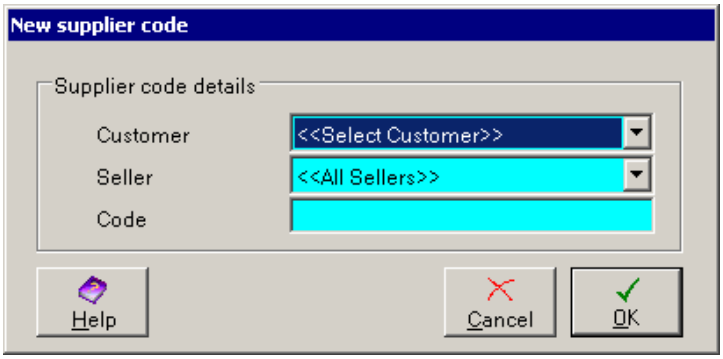
To edit an existing supplier code, highlight the supplier code in the list and click on the **Edit** button.

Delete

To remove an existing supplier code from the list, highlight the supplier code in the list and click on the **Delete** button. You will see a message box, asking if you are sure you want to delete the selected supplier code. Select **Yes** to delete the code or **No** to leave the code in the list.

Supplier codes - Adding a new supplier code

If you wish to add a new supplier code, click the **Add** button on the Location – Supplier codes page. You will then see the New supplier code dialog. The New supplier code dialog has three fields, labelled Customer, Seller and Code, as shown in the diagram below.



You should add a supplier code for this location of your company, as designated by each customer in your system. To do this, click on the dropdown arrow alongside the Customer field and choose a trading partner / customer from the list. If you have different codes for this trading partner / customer, depending on the Seller, select the Seller as well. For most codes, the Seller should be left as All Sellers. Then type into the Code field your supplier code as designated to this location by this trading partner / customer.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

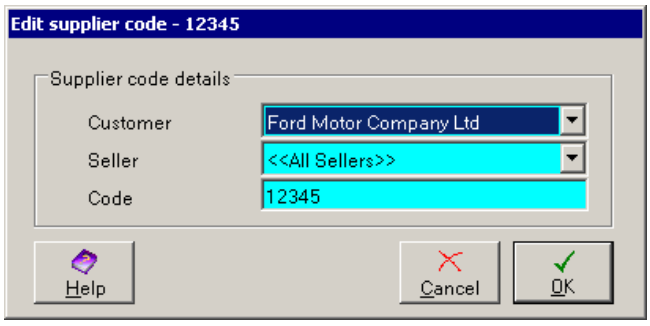
If you want to discard the details you have added on the New supplier code dialog, click the **Cancel** button. You will be returned to the Supplier codes page.

OK

To save the details you have added on the New supplier code dialog, click the **OK** button. You will be returned to the Supplier codes page, where you will see that the new code has been added to the list.

Supplier Codes - Editing a supplier code

If you wish to edit an existing supplier code, highlight the entry you want to edit, then click the **Edit** button on the Location – Supplier codes page. You will then see the Edit supplier code dialog. There are three fields on the Edit supplier code dialog, labelled Customer, Seller and Code.



You can either choose a different customer or seller to be associated with this code, or amend the code that is associated with this customer and seller.

Help

If you need more information about the fields on this dialog and how to fill them in, click on the **Help** button.

Cancel

If you want to discard the changes you have made on the Edit supplier code dialog, click the **Cancel** button. You will be returned to the Supplier codes page.

OK

To save the changes you have made on the Edit supplier code dialog, click the **OK** button. You will be returned to the Supplier codes page, where you will see that your changes have taken effect.

Help

If you need more information about the fields on the Supplier codes page and how to fill them in, click on the **Help** button.

Cancel

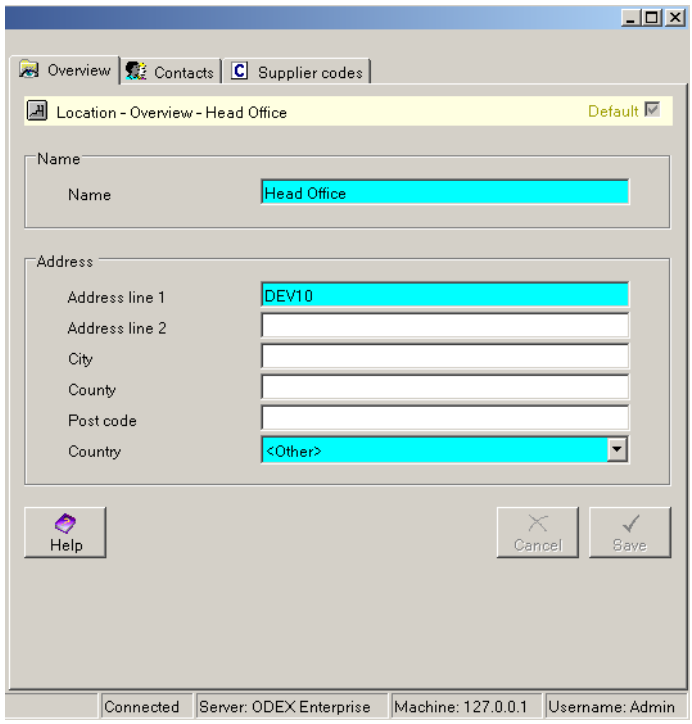
If you want to discard all the changes you have made on the Supplier codes page, click the **Cancel** button.

Save

To save all the changes you have made on the Supplier codes page, click the **Save** button.

Editing a location

The Edit button brings up three pages, labelled Overview, Contacts and Supplier codes, as shown in the example below. We are looking at an existing location, so the fields are already filled in.



Let's have a look at these pages and see what information is on them.

Overview

This page requires a name for the location, one address line of the location and the country where the location is based.

Name – Name

This is the name you use to refer to the location.

Address – Address line 1

This is the first line of your location address.

Address – other fields

If you wish to provide your full location address, please type the remaining address details into the appropriate fields.

Address – Country

This is the country where your location is based.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

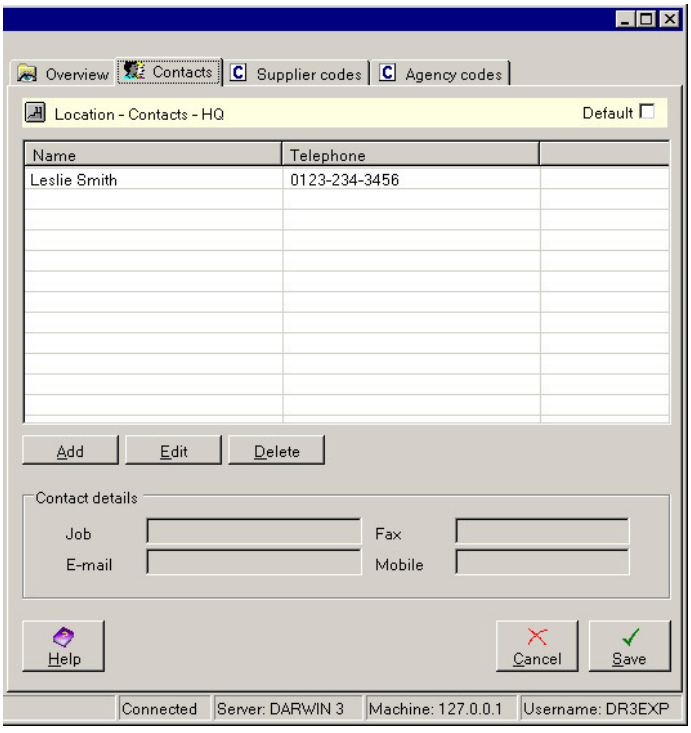
If you want to discard all the changes you have made on the Overview page, click the **Cancel** button.

Save

To save all the changes you have made on the Overview page, click the **Save** button.

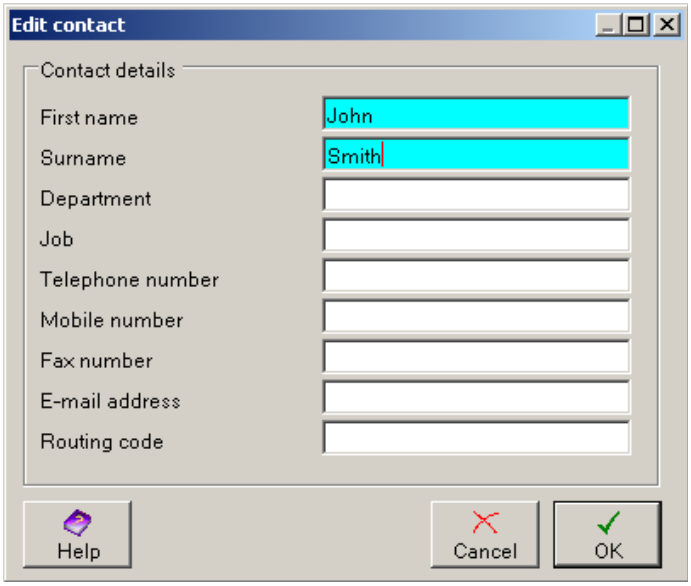
Contacts

This page allows you to add a new contact, edit an existing contact or delete an existing contact. The Contacts page looks like the example below:



As you can see, the yellow title banner shows the name of the location we are currently editing details for.

If you want to edit any existing contact details you should highlight the appropriate line and click the **Edit** button on this page. This will bring up a dialog similar to the following:



Simply edit whichever fields you need to, then click **Cancel** or **OK**.

Help

If you need more information about the fields on this dialog and how to fill them in, click on the **Help** button.

Cancel

If you want to discard all the changes you have made on the Edit contact dialog, click the **Cancel** button.

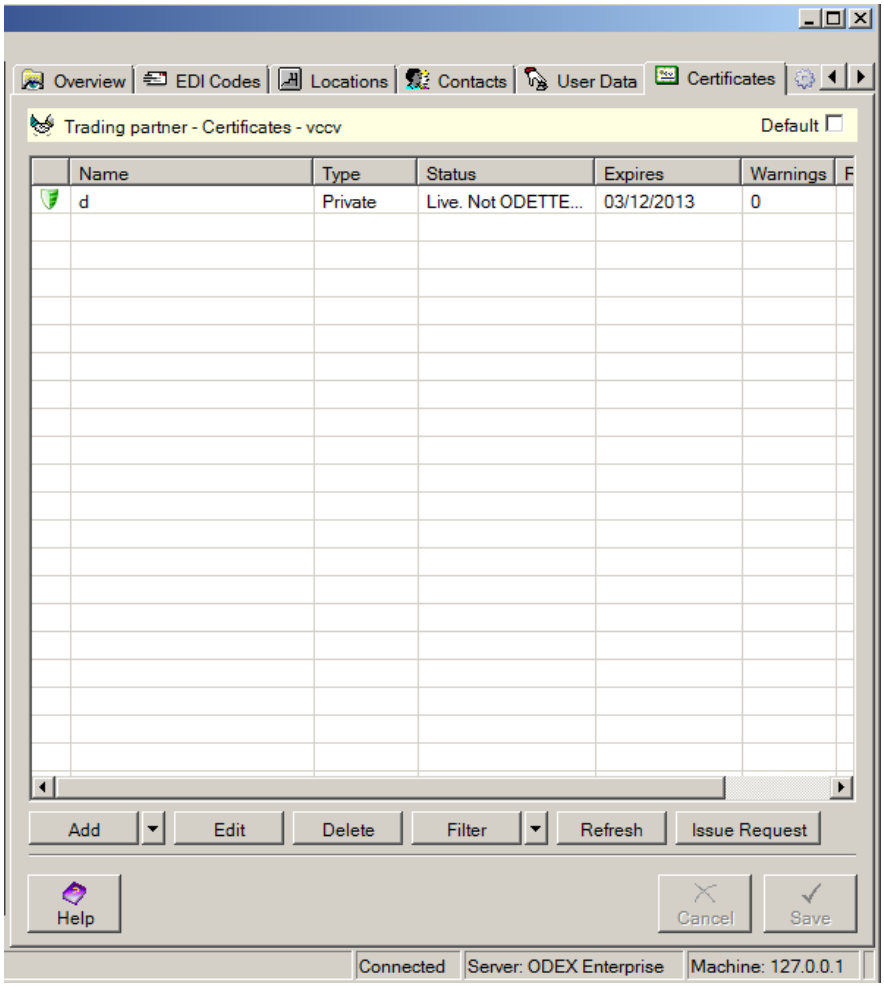
OK

To save all the changes you have made on the Edit contact dialog, click the **OK** button.

When you return to the Contacts page, if you want to keep the changes you have made, click **Save** to return to the Locations page of the supplier company view. If you want to discard the changes you have made, click **Cancel** to return to the Locations page of the supplier company view.

Internal Company – Certificates

The Certificates page allows you to manage the security certificates associated with your internal company, for use in communications. The page looks like the example below.

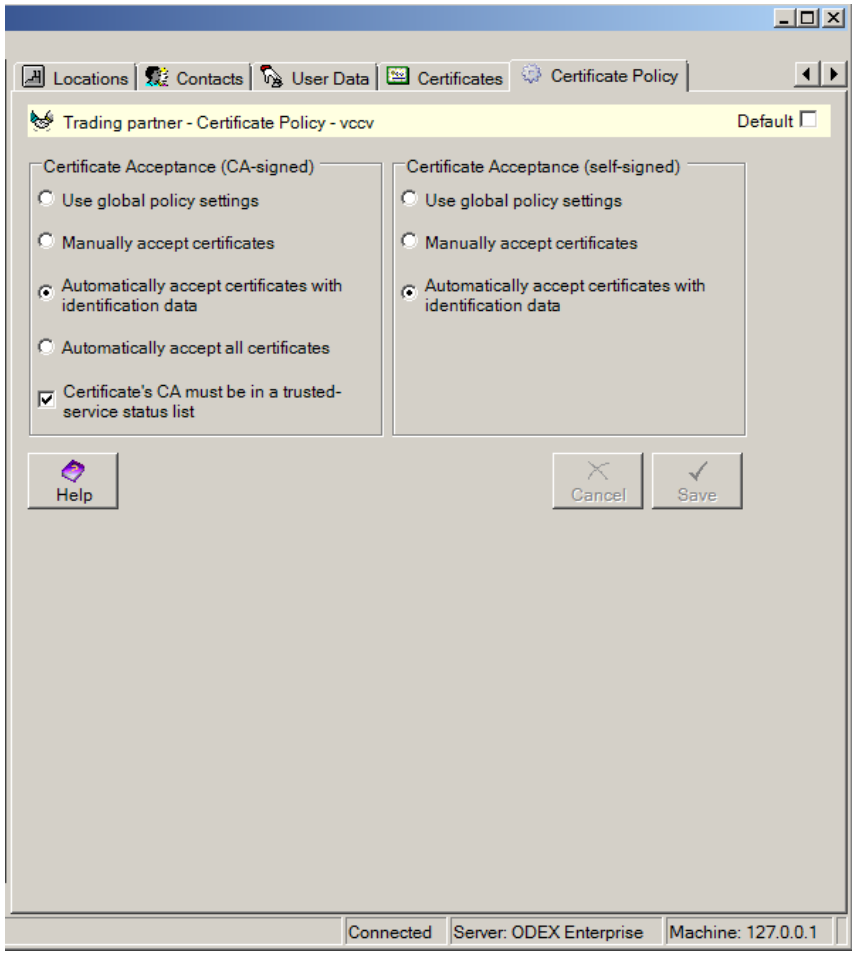


This page is divided into a list of all certificates belonging to your internal company and a collection of buttons for performing actions with certificates.

Management of certificates from this page is a subset of management that can be performed at a global level, discussed in the section entitled ‘Certificates’.

Internal Company – Certificate Policy

The Certificate Policy page is where you can configure the certificate policy of your internal company. The page looks like the example below.



Certificate policy guides ODEX with management of your certificates. Options configured here override global certificate policy (see the section entitled 'Global Certificate Policy').

Certificate Exchange

Here you can configure when and if ODEX will distribute the public part of your security certificates to your trading partners. By default, global certificate policy is used, but you can override the global settings with specific settings for distributing the certificates belonging to this internal company. A separate policy can be configured for those certificates that you have self-signed and those certificates that you have retrieved from a Certificate Authority.

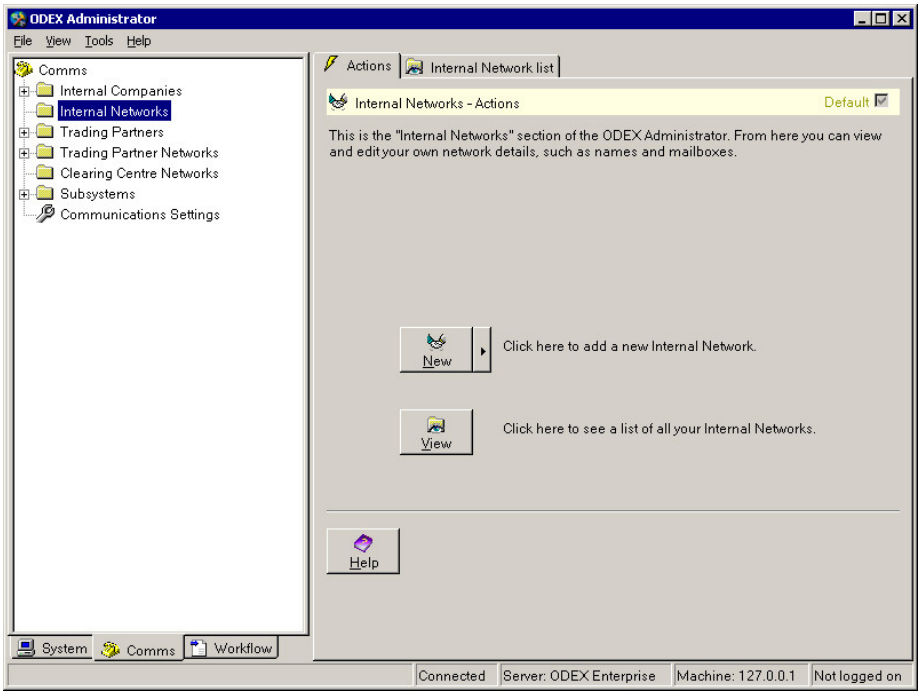
For a discussion of certificate exchange, please refer to 'OFTP2 Certificate Exchange'.

Select "Manually broadcast certificates" if you would like to choose exactly when and to who your certificates are broadcast.

Select "Automatically distribute certificates" to permit ODEX to decide when and to who your certificates should be broadcast.

Internal Networks

Click on the name Internal Networks in the Navigation Panel to see the default page for the Internal Networks section, as shown below. This is the Internal Networks – Actions page.



The Internal Networks section allows you to add, view and edit your own network details.

As you can see, there are two page tabs on the Information Panel (Actions and Internal Network list) and two buttons, labelled **New** and **View**. The **New** button allows you to add a new internal network. The **View** button allows you to see a list of all the existing internal networks, from where you can edit their details, add new entries or delete existing entries.

The Default Page tickbox is ticked, indicating that this is the page you will see first when you open the Internal Networks view. Once you are familiar with ODEX you will probably choose the Internal Network list page as your default page in this section.

There are currently four different types of internal network you can use within ODEX. These are:

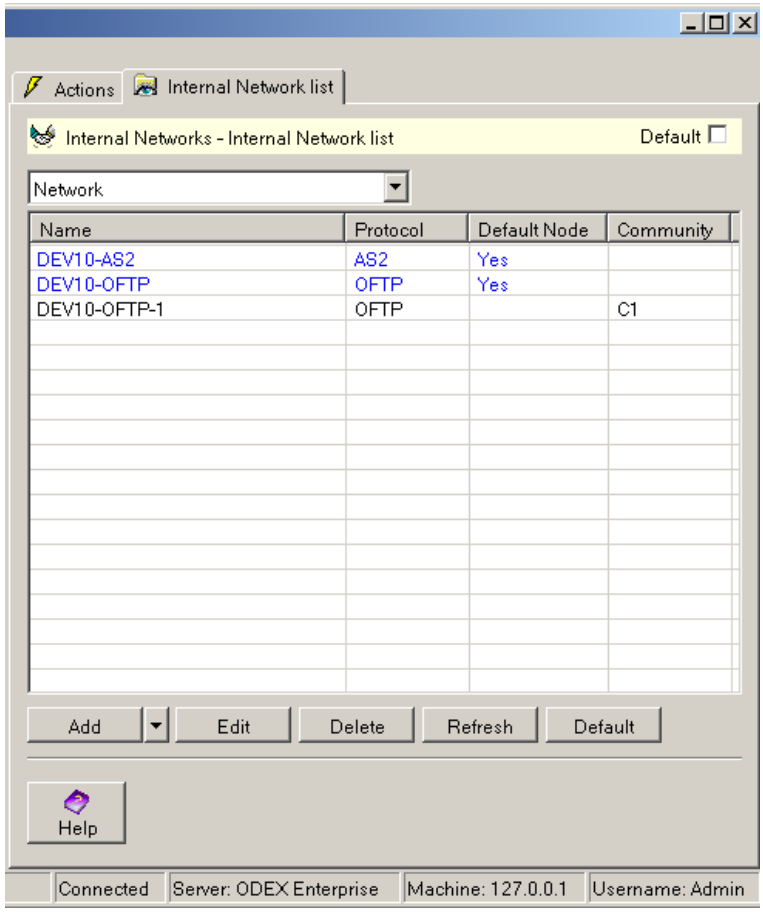
- OFTP
- AS2
- FTP client
- FTP server

Select the type you want to add from the arrow alongside the **New** button.

Viewing all your internal networks

Networks

If you wish to see a list of all the internal networks currently in the ODEX database, you can either click the **View** button on the Internal Network – Actions page or click the Internal Network list tab. Both have the same result, as in the example below. You may also view all of the mailboxes or EDI codes associated with internal networks by selecting ‘Mailbox’ or ‘EDI code’ from the drop-down list at the top of the page.



When ‘Network’ is selected from the drop-down list, the Information Panel shows the Internal Network list page. This page lists all the internal networks you currently have defined in your system. Depending on your system configuration, the page is divided into three or four columns. If you are not using communities, the list shows the Internal Network Name, its associated Protocol and whether it is the Default Node or not. If you are using communities, an additional column is displayed showing the community that each network is associated with.

The Protocol column will show "OFTP", "AS2", “FTP server” or “FTP client”.

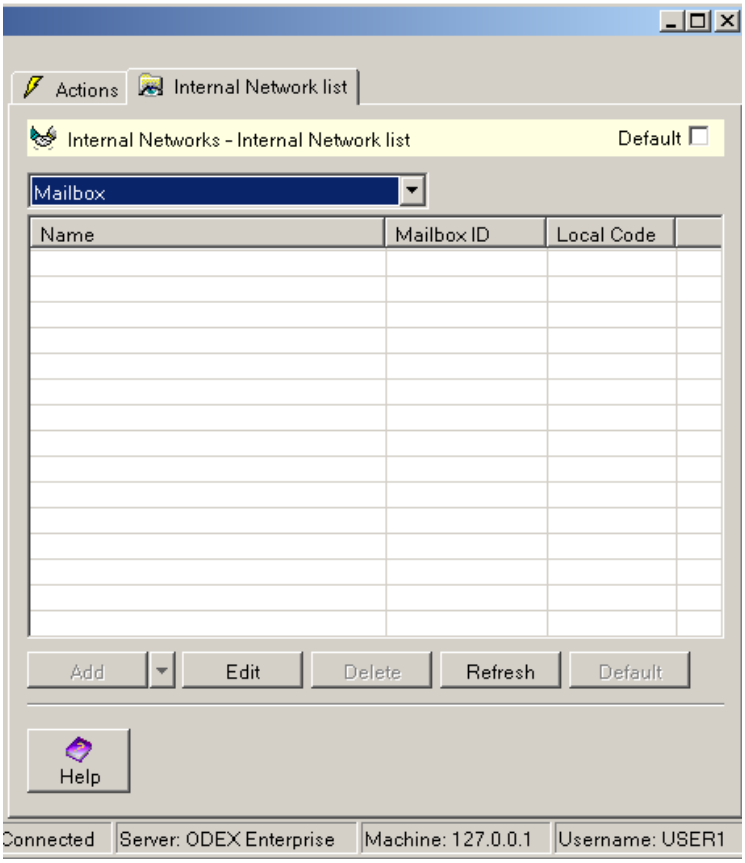
The Default Node column will either show “Yes” or it will be blank. In addition, the default internal network is always displayed in blue.

You can change the default internal network by selecting a different network and clicking the **Default** button (this will not be permitted if you already have files scheduled from the old default internal network).

New internal networks may be added to the list by using the **Add** button. There are four options available – New OFTP Network, New AS2 Network, New FTP Server Network and New FTP Client Network. For details of how to view or edit a network, see the sections entitled "Adding/Editing an Internal OFTP Network", "Adding/Editing an Internal AS2 Network", “Adding/Editing an Internal FTP client Network” and ”Adding/Editing an Internal FTP server Network” respectively.

Mailboxes

You may view all the mailboxes associated with your internal networks by selecting ‘Mailbox’ from the drop-down list at the top of the page. The page will then be displayed as in the example below:



The page is divided into three columns – Name, Mailbox ID and Local Code.

The list will contain an entry for each mailbox profiled against each of your internal OFTP networks and FTP client networks. For each internal AS2 network and FTP server network profiled on your system, there will be one mailbox displayed in the list, since these network types do not allow additional mailboxes to be added to them.

The Mailbox ID column will display the SFID for OFTP mailboxes. For FTP client mailboxes, the mailbox ID is the same as the name of the mailbox. For FTP server mailboxes, the mailbox ID is the same as the network local code. For AS2 mailboxes, the mailbox ID is the AS2 identifier of the AS2 network.

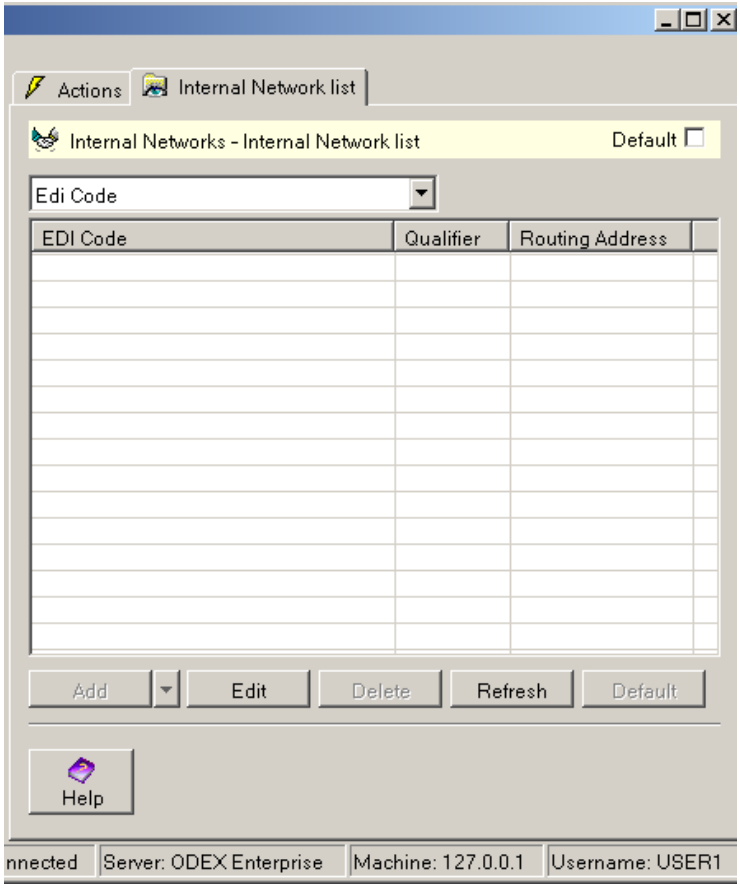
The **Add, Delete** and **Default** buttons are disabled when viewing the list of mailboxes, as these buttons are only applicable to networks. To add a mailbox to a network, or delete a mailbox from a network you must first view the details of the associated network.

You can view or edit the details of the network associated with a mailbox by double-clicking the mailbox entry in the list, or selecting the mailbox and clicking the **Edit** button.

For details of how to view or edit a network, see the sections entitled "Adding/Editing an Internal OFTP Network", "Adding/Editing an Internal AS2 Network", “Adding/Editing an Internal FTP client Network” and ”Adding/Editing an Internal FTP server Network” respectively.

EDI Codes

You may view all of the EDI codes associated with your internal networks by selecting ‘EDI Code’ from the drop-down list at the top of the page. The list will then be displayed as below:



The list will now be divided into three columns – EDI Code, Qualifier and routing address.

The **Add, Delete** and **Default** buttons are disabled when viewing all of the internal EDI codes, as these buttons are only applicable to networks. To add an EDI code to a network, or remove an EDI code from a network, you must first view the network associated with the EDI code.

You can view or edit the details of the network associated with an EDI code by double-clicking an entry in the list or selecting an entry and clicking the **Edit** button.

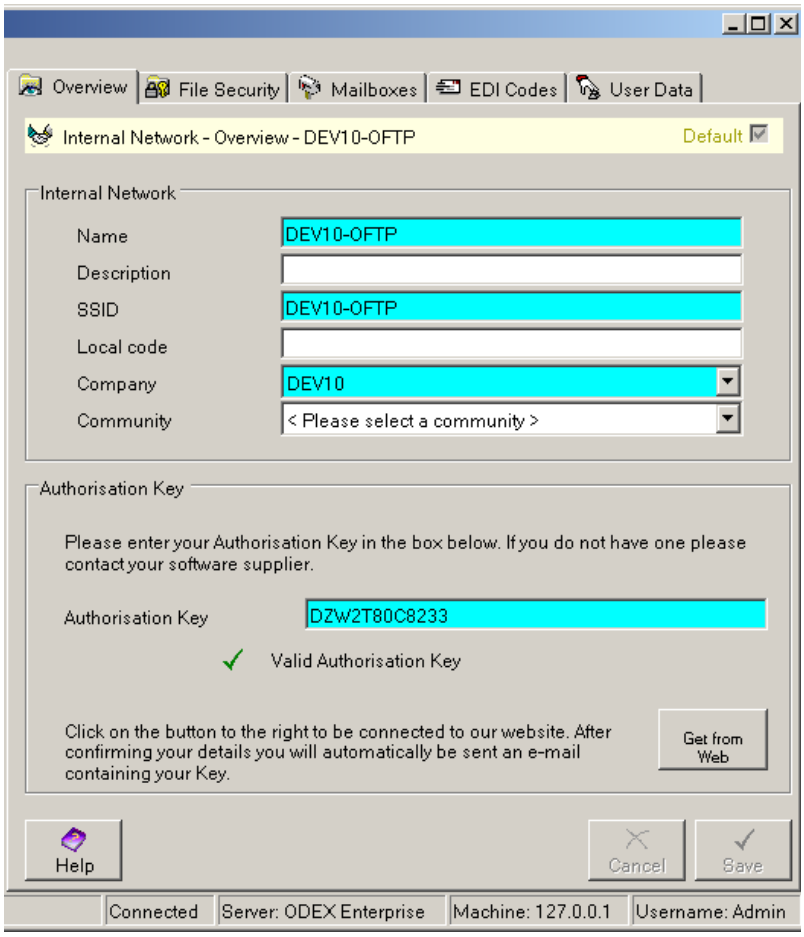
For details of how to view or edit a network, see the sections entitled "Adding/Editing an Internal OFTP Network", "Adding/Editing an Internal AS2 Network", “Adding/Editing an Internal FTP client Network” and ”Adding/Editing an Internal FTP server Network” respectively.

Adding/Editing an Internal OFTP Network

There are five pages associated with an internal OFTP network, so let's go through them and find out what information is required. The User Data page is described in the section entitled ‘User Data’.

Internal OFTP Network – Overview

The Overview page is where mandatory information has to be provided for each new internal OFTP network node. The Overview page looks like the example below.



Internal Network – Name

Type in this field a name for the internal network. This name must be unique among your other internal networks, but it can be whatever you want it to be. The name is a unique identifier, enabling you to recognise it easily when you want to use this internal network.

Internal Network – Description

You may give a brief description of the internal network in this field if you wish. You can simply repeat the name of the internal network if you like, or include any other information that helps you to recognise it. The description is intended to help you remember what the internal network is for.

Internal Network – SSID

This field requires the SSID for this internal network. The SSID is used for addressing purposes with an OFTP network.

Internal Network – Local code

This field is provided for compatibility with the systems of users who have upgraded from ODEX Professional and who wish to use the Batch Interface. Other users should ignore it.

The local code is simply a unique code designated by you and used to identify the company in a shorthand form, instead of having to remember their EDI code. It is a code internally used by ODEX and will never be seen by your trading partners.

Internal Network – Community

This field will only be visible if you are using communities and you are logged on as a user that is a member of multiple communities or a user that is not a member of any communities, e.g. the admin user.

If you are using communities and you are logged on as a user that is a member of one community, the field is hidden because the company will be created and associated with your community automatically.

Select a community if you wish to associate this network with a community. The network will then only be visible to users that are a member of the selected community, or users that are a member of a group that is a member of the selected community.

Internal Network – Company

If you have defined more than one internal company, use the dropdown arrow to select the appropriate internal company with which this network is to be associated.

Authorisation Key

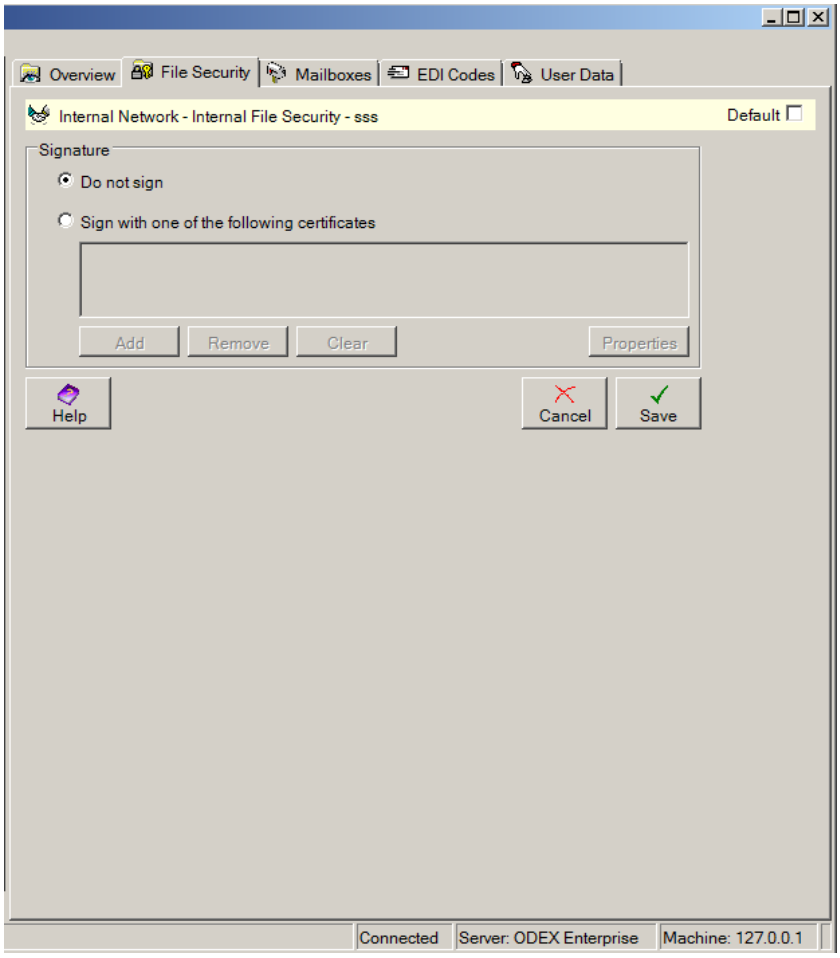
You are required to provide an authorisation key for each internal network you define. If you have the authorisation key, type it in this field. Otherwise, please click on the **Get from Web** button to be connected to the Licence Codes website. After confirming your details you will automatically be sent an e-mail containing an authorisation key.

As soon as you have provided a valid authorisation key in this field, the "No SSID code entered" or "Invalid key" message will change to "Valid key".

Internal OFTP Network – File Security

You need to enter data on the File Security page only if you want to use OFTP2 data security.

The File Security page looks like the example below.



The File Security page is where you can provide the default security details for files that you send from this internal network. You can specify the private key certificate (if any) that will be used to sign data sent by you to your trading partners.

These default settings will be used by all the mailboxes defined against this network, sending files to all your OFTP trading partners. You can, however, choose different settings for any mailbox on the Security page of that mailbox. You can also override these settings for sending files to individual trading partners as explained in the section entitled ‘Network – Security’.

For a fuller explanation of encryption, decryption, signatures, certificates and public and private keys, please refer to ‘Data Security’.

Signature

Select “Do not sign” if none of your trading partners expect you to send them signed data.

If you need to sign the files that you send and you select "Do not sign", this means you do not want to configure a primary or default private key certificate to use when signing outgoing data. If a trading partner communicating with this internal network wants you to sign files that you send to him, you will need to configure your signing certificate against either your internal mailbox or his external network.

Select “Sign with one of the following certificates” to specify the certificate(s) to use for signing files sent from this internal network. Action buttons are enabled for you to choose the certificate(s). See the section entitled ‘Dynamic Certificate Selection’.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

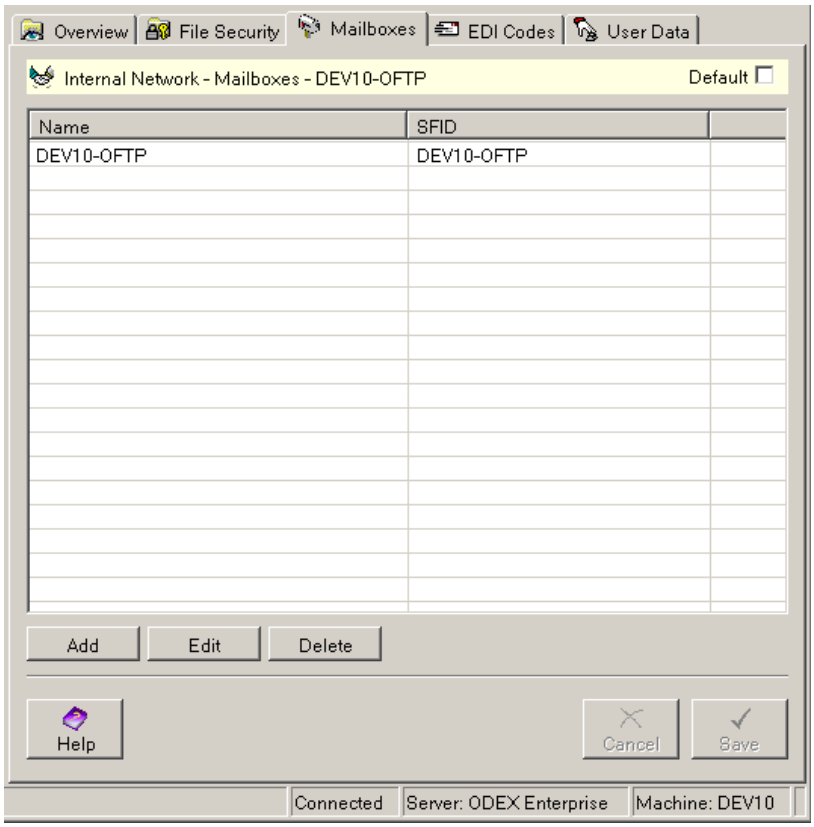
If you want to discard all the changes you have made, click the **Cancel** button.

Save

To save any changes you have made in the File Security section, click the **Save** button.

Internal OFTP Network – Mailboxes

The Mailboxes page looks like the example below, and shows a list of all mailboxes currently defined for this internal network.



Use the **Add**, **Edit** and **Delete** buttons to add new mailboxes, and edit and delete existing mailboxes.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

If you want to discard all the changes you have made, click the **Cancel** button.

Save

To save any changes you have made in the Mailboxes section, click the **Save** button.

Mailboxes – Add/Edit

Use the **Add** or **Edit** button to add or edit a mailbox for this internal network.

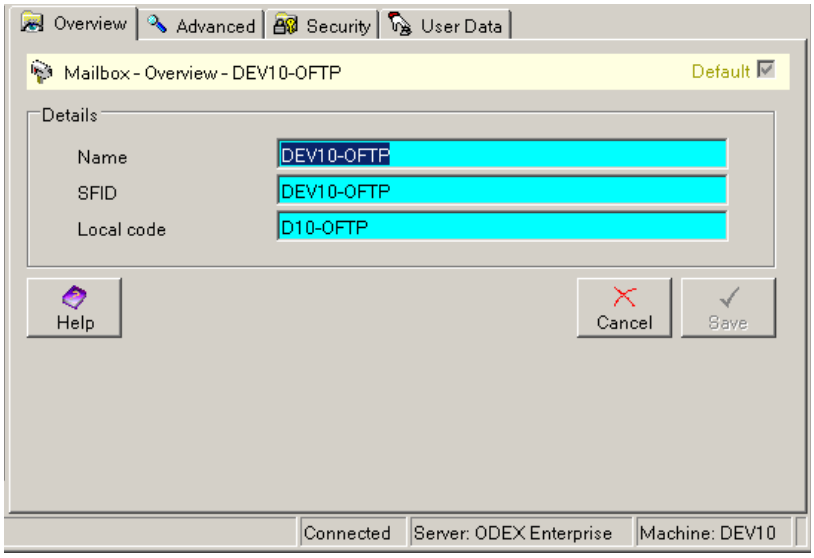
Mailboxes – Delete

To delete an entry from the list on the Mailboxes page, select the mailbox you want to delete and click the **Delete** button. You will see a message box asking if you are sure you want to delete the selected mailbox. Click **Yes** to delete the mailbox, or **No** to keep the mailbox in the list.

There are four pages associated with an internal OFTP mailbox, so let's go through them and find out what information is required. The User Data page is described in the section entitled 'User Data'.

Internal OFTP Mailbox – Overview

The Overview page is where mandatory information has to be provided for each new internal OFTP mailbox. The Overview page looks like the example below.



Details – Name

Type in here a name for the mailbox. This name is just for your own use within ODEX.

Details – SFID

Type in here the SFID of the mailbox.

Details – Local code

This field is provided for compatibility with the systems of users who have upgraded from ODEX Professional and who wish to use the Batch Interface. Other users should ignore it.

The local code is simply a unique code designated by you and used to identify the company in a shorthand form, instead of having to remember their EDI code. It is a code internally used by ODEX and will never be seen by your trading partners.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

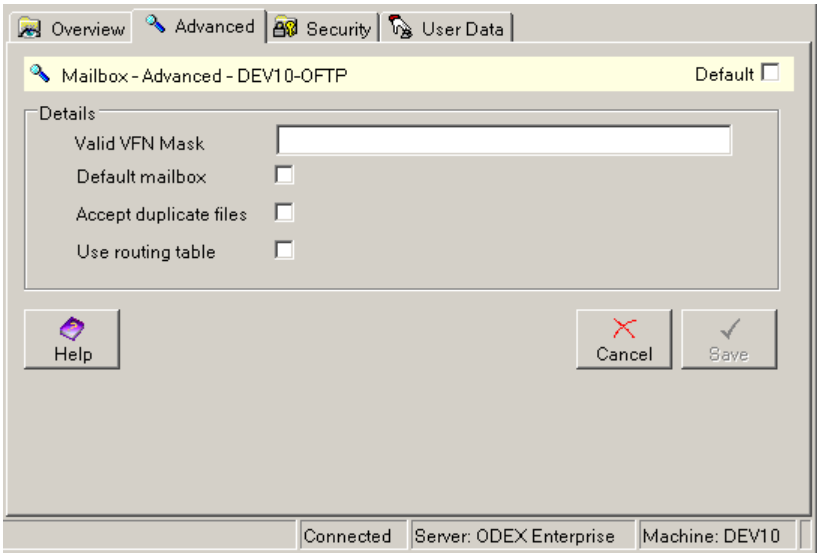
If you want to discard all the changes you have made, click the **Cancel** button.

SAVE

To save details of the new mailbox, click the **SAVE** button.

Internal OFTP Mailbox – Advanced

The advanced page allows optional settings to be defined. The advanced page looks like the example below:



Details – Valid VFN Mask

This field allows you to provide a VFN (virtual filename) mask to be matched against files received from this trading partner network. If the VFN of the received file does not match the mask, the file will be rejected.

You may use the asterisk character (*) to signify one or more unspecified characters. You may use the question mark character (?) to signify one unspecified character.

Taking the Ford VFN format as an example, you could use one of the following filename masks to achieve different results:

FORD.S* – accept all Ford files

FORD.SABC12* – accept all Ford messages for the Supplier code ABC12

FORD.S*RE – accept all Ford Release messages for any Supplier code

FORD.S?????ST – accept all Ford DCI messages for any Supplier code (five question marks are more precise than the asterisk but would have the same effect)

Details – Default mailbox

This field allows you to specify that this is the default mailbox for the network. A default mailbox is a mailbox that will be used to receive files when the SFID associated with a received file does not match the SFID of any other mailbox defined on this network.

Details – Accept duplicate files

This allows you to specify that ODEX should accept files sent to this mailbox, regardless of whether another file has been received with the same virtual filename and virtual date/time. When the check box is not checked, ODEX will reject files with a duplicate virtual filename and virtual date/time.

Details – Use routing table

This field allows you to specify that when forwarding files received through this mailbox, the routing table must be used to route the file to its destination.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

If you want to discard all the changes you have made, click the **Cancel** button.

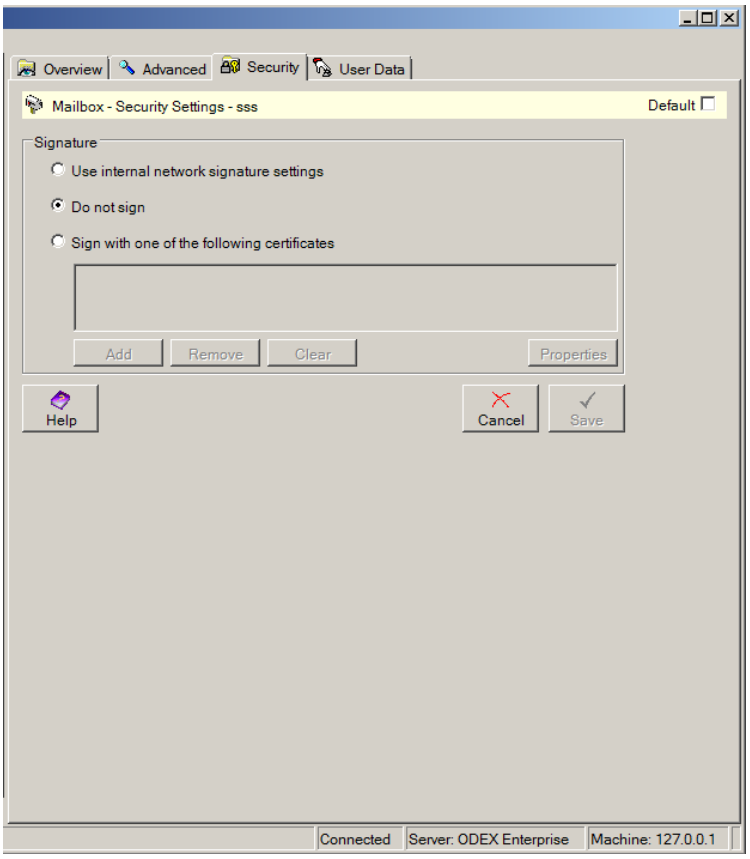
SAVE

To save details of the new mailbox, click the **SAVE** button.

Internal OFTP Mailbox – Security

You need to enter data on the File Security page only if you want to override the values you have set for the network.

The Security page looks like the example below.



The Security page is where you can provide the default security details for files that you send from this internal mailbox. You can specify the private key certificate (if any) that will be used to sign data sent by you to your trading partners.

These default settings will be used for sending files to all your OFTP trading partners from this mailbox. You can, however, override these settings for sending files to individual trading partners as explained in the section entitled 'Network – Security'.

For a fuller explanation of encryption, decryption, signatures, certificates and public and private keys, please refer to 'Data Security'.

Signature

Select “Use internal network signature settings” if you don’t want to override the values set on the internal network.

Select “Do not sign” if none of your trading partners expect you to send them signed data from this mailbox.

If you need to sign the files that you send and you select "Do not sign", this means you do not want to configure a primary or default private key certificate to use when signing outgoing data. If a trading partner communicating with this internal mailbox wants you to sign files that you send to him, you will need to configure your signing certificate against his external network.

Select “Sign with one of the following certificates” to specify the certificate(s) to use for signing files sent from this internal mailbox. Action buttons are enabled for you to choose the certificate(s). See the section entitled ‘Dynamic Certificate Selection’.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

If you want to discard all the changes you have made, click the **Cancel** button.

Save

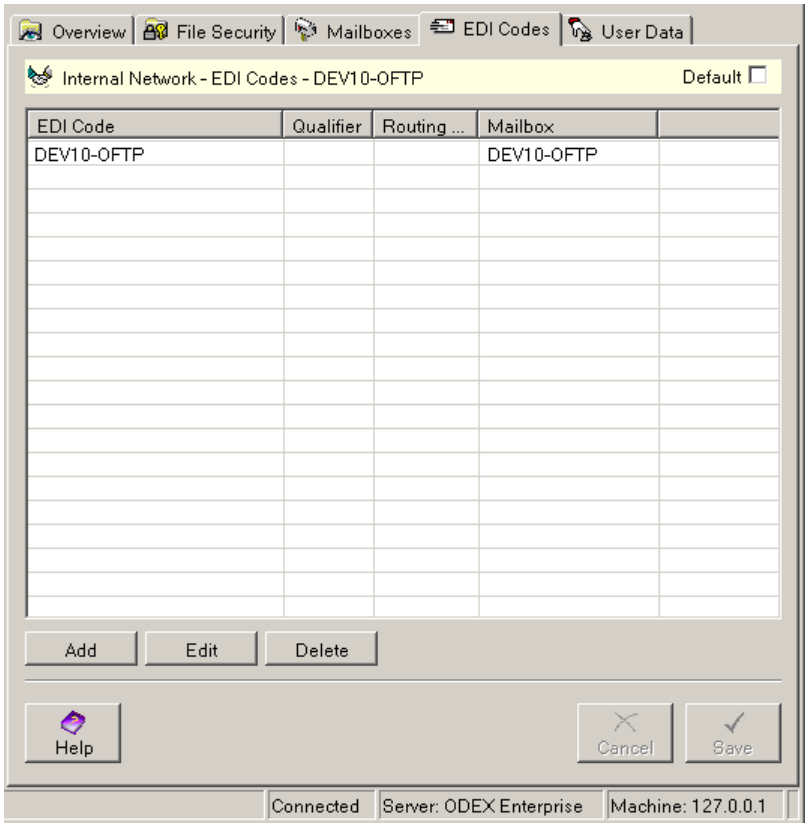
To save any changes you have made in the Security section, click the **Save** button.

Internal OFTP Mailbox – User Data

See the section entitled

Internal OFTP Network – EDI Codes

The EDI Codes page is where you can provide the EDI addressing details for each of your internal companies that use this network. The EDI Codes page looks like the example below and shows a list of all EDI codes currently defined for this internal network.



Use the **Add**, **Edit** and **Delete** buttons to add new EDI codes, and edit and delete existing EDI codes.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

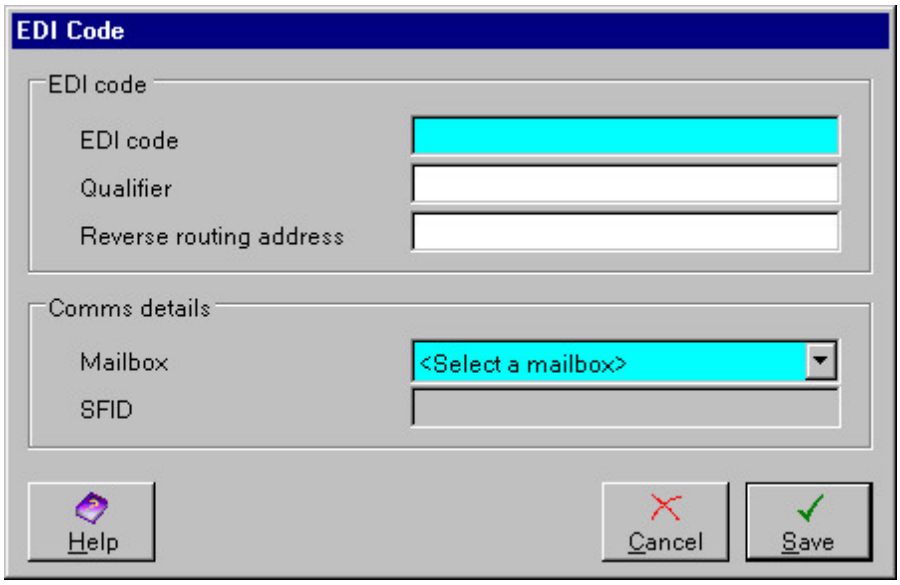
If you want to discard all the changes you have made, click the **Cancel** button.

Save

To save any changes you have made in the EDI codes section, click the **Save** button.

EDI codes – Add/Edit

Use the **Add** or **Edit** button to add or edit an EDI Code for this internal network. This will bring up the following dialog:



EDI code – EDI code

Type in the EDI code for this internal OFTP network.

EDI code – Qualifier

This is a qualifier for the EDI code and is usually only required if you or your trading partner demands it.

EDI code – Reverse routing address

This is an address used for reverse routing of the EDI code and is usually only required if you or your trading partner demands it.

Comms details – Mailbox

Use the dropdown arrow to select the appropriate mailbox for this EDI code. You must define a mailbox on the Mailboxes page tab and save it before you can complete this dialog.

Comms details – SFID

The SFID associated with the selected mailbox will automatically appear in this field.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

If you want to discard all the changes you have made, click the **Cancel** button.

Save

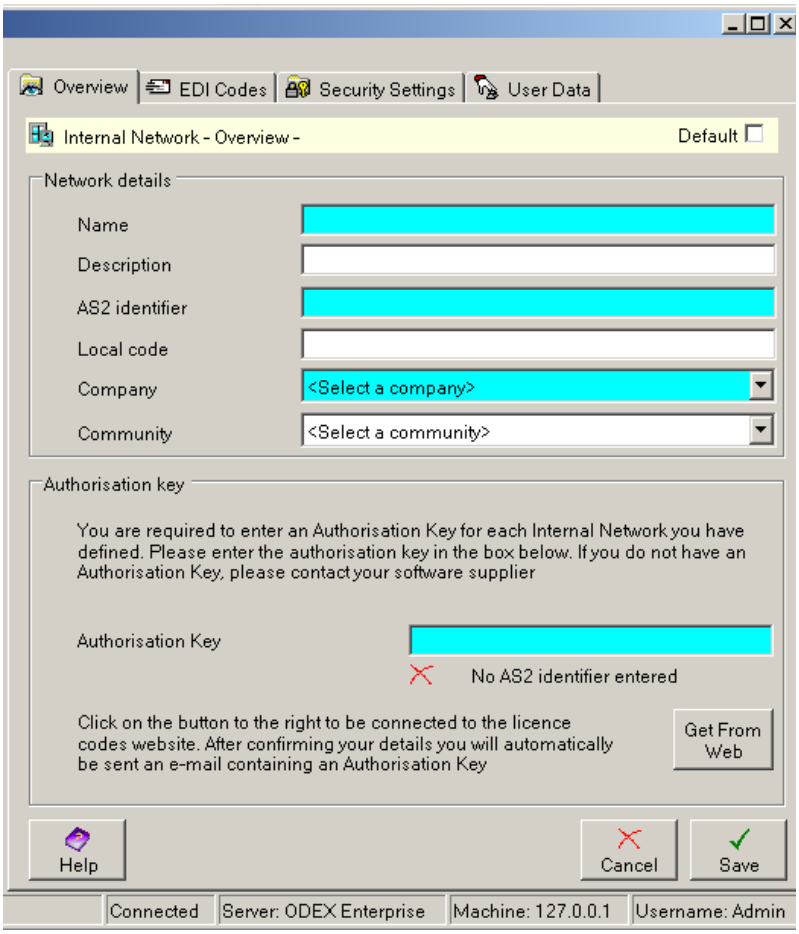
To save the changes you have made on this dialog, click the **Save** button.

Adding/Editing an Internal AS2 Network

There are four pages associated with an internal AS2 network, so let's go through them and find out what information is required. The User Data page is described in the section entitled ‘User Data’.

Internal AS2 Network – Overview

The Overview page is where mandatory information has to be provided for each new internal AS2 network node. The Overview page looks like the example below.



Network details – Name

Fill in the name by which you want this internal AS2 network to be known. This name will only be used internally by ODEX and is intended to help you identify your network easily.

Network details – Description

You may provide a description of the network in this field.

Network details – AS2 identifier

The AS2 identifier is used to identify your company to your AS2 trading partners.

Network details – Local code

This field is provided for compatibility with the systems of users who have upgraded from ODEX Professional and who wish to use the Batch Interface. Other users should ignore it.

The local code is simply a unique code designated by you and used to identify the company in a shorthand form, instead of having to remember their EDI code. It is a code internally used by ODEX and will never be seen by your trading partners.

Network details – Company

If you have defined more than one internal company, use the dropdown arrow to select the appropriate internal company for this network.

Network details – Community

This field will only be visible if you are using communities and you are logged on as a user that is a member of multiple communities or a user that is not a member of any communities, e.g. the admin user.

If you are using communities and you are logged on as a user that is a member of one community, the field is hidden because the company will be created and associated with your community automatically.

Select a community if you wish to associate this network with a community. The network will then only be visible to users that are a member of the selected community, or users that are a member of a group that is a member of the selected community.

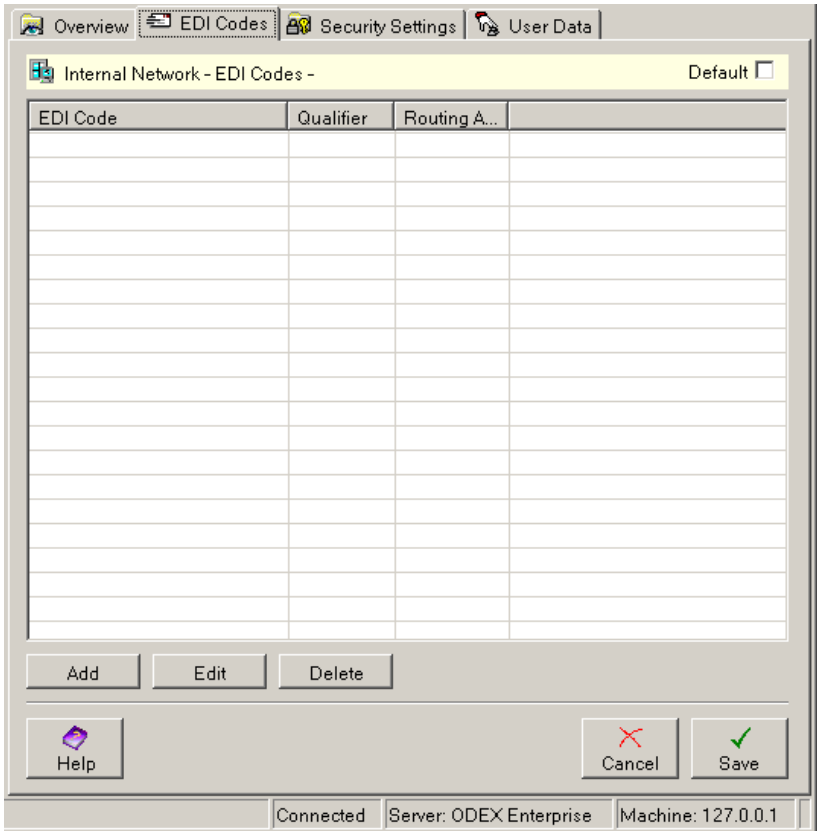
Authorisation Key

You are required to provide an authorisation key for each internal network you define. If you have the authorisation key, type it in this field. Otherwise, please click on the **Get from Web** button to be connected to the Licence Codes website. After confirming your details you will automatically be sent an e-mail containing an authorisation key.

As soon as you have provided a valid authorisation key in this field, the "No AS2 identifier entered" or "Invalid key" message will change to "Valid key".

Internal AS2 Network – EDI Codes

The EDI Codes page is where you can provide the EDI addressing details for each of your internal companies that use this network. The EDI Codes page looks like the example below and shows a list of all EDI codes currently defined for this internal network.



Use the **Add**, **Edit** and **Delete** buttons to add new EDI codes, and edit and delete existing EDI codes.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

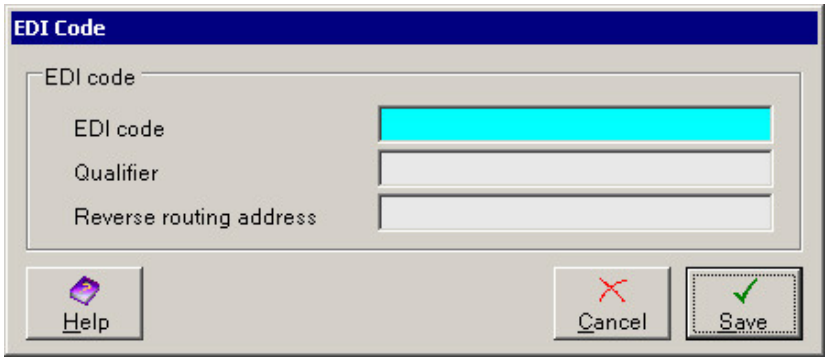
If you want to discard all the changes you have made, click the **Cancel** button.

Save

To save any changes you have made in the EDI codes section, click the **Save** button.

EDI codes – Add/Edit

Use the **Add** or **Edit** button to add or edit an EDI Code for this internal network. This will bring up the following dialog:



EDI code – EDI code

Type in the EDI code for this internal AS2 network.

EDI code – Qualifier

This is a qualifier for the EDI code and is usually only required if you or your trading partner demands it.

EDI code – Reverse routing address

This is an address used for reverse routing of the EDI code and is usually only required if you or your trading partner demands it.

Internal AS2 Network – Security Settings

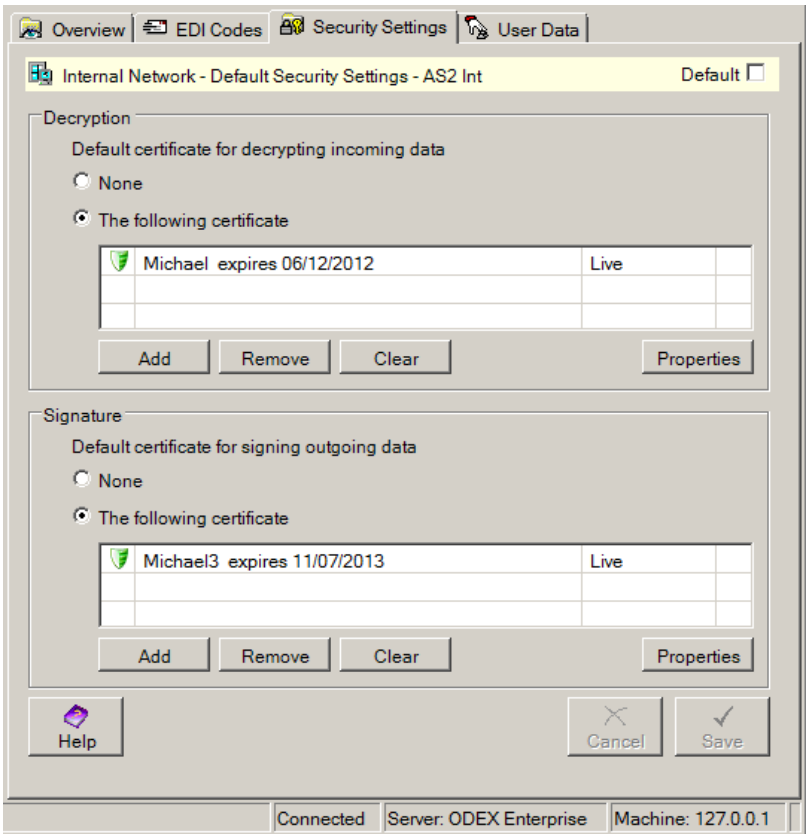
The Security Settings page is where you can provide the default security details for use with your AS2 networks. This page is where you specify the private key certificate (if any) that will be used to decrypt data sent to you by your trading partners and to sign data sent by you to your trading partners.

These default settings will be used by all your AS2 trading partner networks, thus saving you from having to enter the details for each one separately. You can, however, choose different settings for any of your AS2 trading partner networks if you wish to, on the Inbound and Outbound pages of the "Networks (Trading Partner or Clearing Centre)" section.

The two areas of security are decryption and signatures. You are required to configure the details of security to be used. This is not a matter of choice – the configuration must reflect the security arrangement you have agreed with your trading partner.

For a fuller explanation of encryption, decryption, signatures, certificates and public and private keys, please refer to the section entitled “Encryption and signatures”.

The Security Settings page looks like the example below.



Decryption

If you select "None", this means you do not want to configure a primary or default private key certificate to use when decrypting incoming data. If a trading partner communicating with this internal network is going to send encrypted data, you will need to configure your decryption certificate against his external network.

Select “One of the following certificates” to specify the certificate(s) to use for decrypting incoming data. Action buttons are enabled for you to choose the certificate(s). See the section entitled ‘Dynamic Certificate Selection’.

Signature

Certificates are also used for signing outgoing data.

If you select "None", this means you do not want to configure a primary or default private key certificate to use when signing outgoing data. If a trading partner communicating with this internal network wants you to sign files that you send to him, you will need to configure your signing certificate against his external network.

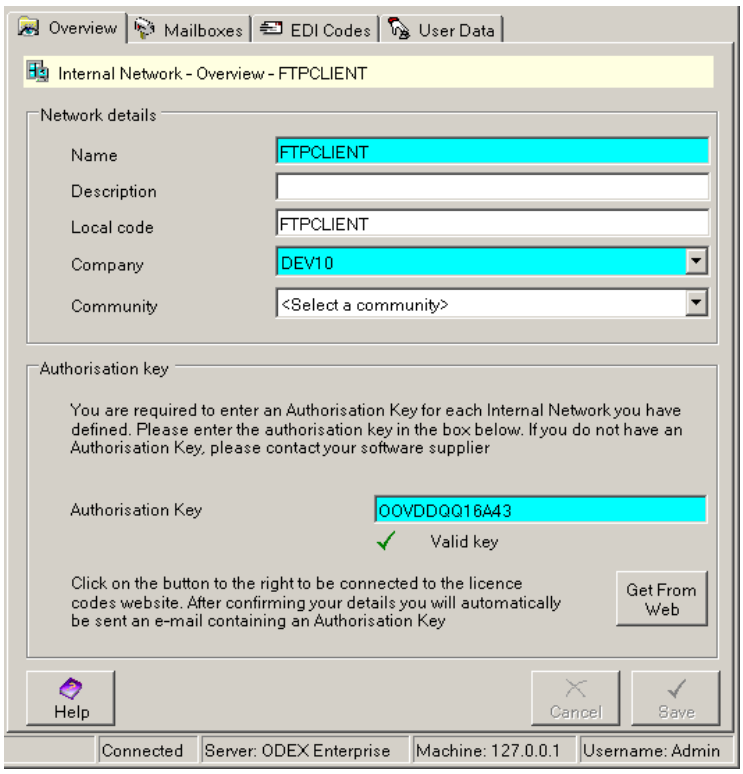
Select “One of the following certificates” to specify the certificate(s) to use for signing outbound data. Action buttons are enabled for you to choose the certificate(s). See the section entitled ‘Dynamic Certificate Selection’.

Adding/Editing an Internal FTP client Network

There are four pages associated with an internal FTP client network, so let's go through them and find out what information is required. The User Data page is described in the section entitled 'User Data'.

Internal FTP client Network – Overview

The Overview page is where mandatory information has to be provided for each new internal FTP client network node. The Overview page looks like the example below.



Network details – Name

Type in this field a name for the internal network. This name must be unique among your other internal networks, but it can be whatever you want it to be. The name is a unique identifier, enabling you to recognise it easily when you want to use this internal network.

Network details – Description

You may give a brief description of the internal network in this field if you wish. You can simply repeat the name of the internal network if you like, or include any other information that helps you to recognise it. The description is intended to help you remember what the internal network is for.

Network details – Local code

This mandatory field is used for licensing an internal network (your authorisation code is valid for only a single specific local code) and for compatibility with users upgraded from ODEX Professional wishing to use the batch interface.

The local code is simply a unique code designated by you and used to identify the company in a shorthand form, instead of having to remember their EDI code. It is a code internally used by ODEX and will never be seen by your trading partners.

Network details – Company

If you have defined more than one internal company, use the dropdown arrow to select the appropriate internal company with which this network is to be associated.

Network details – Community

This field will only be visible if you are using communities and you are logged on as a user that is a member of multiple communities or a user that is not a member of any communities, e.g. the admin user.

If you are using communities and you are logged on as a user that is a member of one community, the field is hidden because the company will be created and associated with your community automatically.

Select a community if you wish to associate this network with a community. The network will then only be visible to users that are a member of the selected community, or users that are a member of a group that is a member of the selected community.

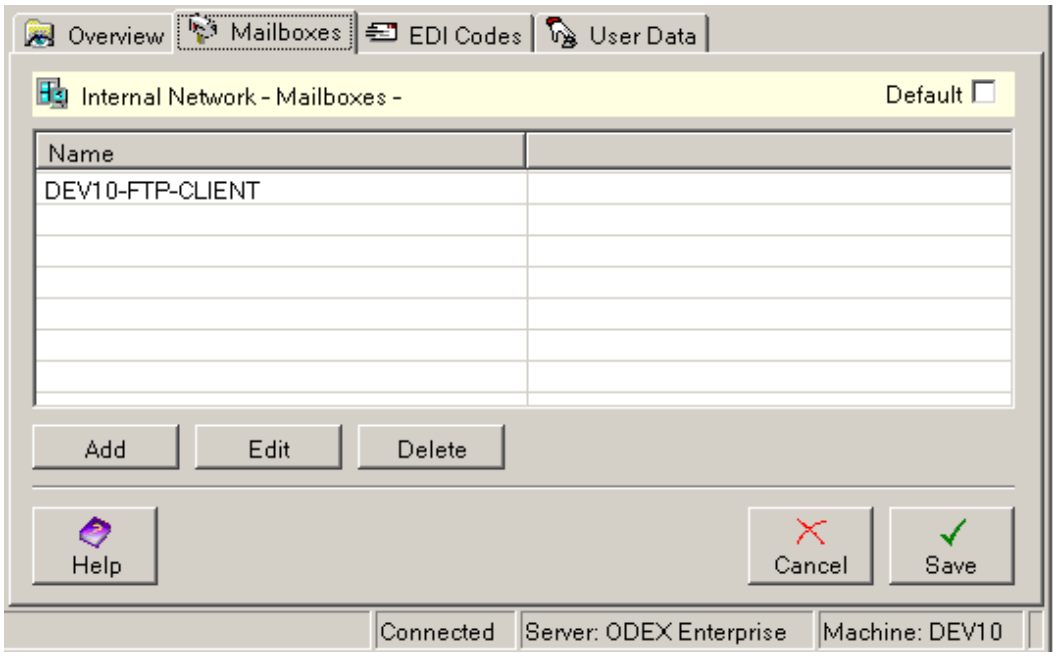
Authorisation Key

You are required to provide an authorisation key for each internal network you define. If you have the authorisation key, type it in this field. Otherwise, please click on the **Get from Web** button to be connected to the Licence Codes website. After confirming your details you will automatically be sent an e-mail containing an authorisation key.

As soon as you have provided a valid authorisation key in this field, the "No local code entered" or "Invalid key" message will change to "Valid key".

Internal FTP client Network – Mailboxes

The Mailboxes page looks like the example below, and shows a list of all mailboxes currently defined for this internal network.



Use the **Add**, **Edit** and **Delete** buttons to add new mailboxes, and edit and delete existing mailboxes.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

If you want to discard all the changes you have made, click the **Cancel** button.

Save

To save any changes you have made in the Mailboxes section, click the **Save** button.

Mailboxes – Add/Edit

Use the **Add** or **Edit** button to add or edit a mailbox for this internal network.

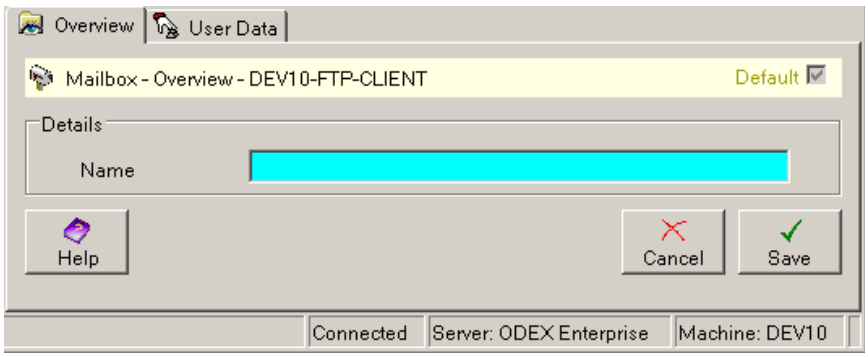
Mailboxes – Delete

To delete an entry from the list on the Mailboxes page, select the mailbox you want to delete and click the **Delete** button. You will see a message box asking if you are sure you want to delete the selected mailbox. Click **Yes** to delete the mailbox, or **No** to keep the mailbox in the list.

There are two pages associated with an internal FTP client mailbox. The User Data page is described in the section entitled 'User Data'.

Internal FTP client Mailbox – Overview

The Overview page is where mandatory information has to be provided for each new internal FTP client mailbox. The Overview page looks like the example below.



Details – Name

Type in here a name for the mailbox. This name is just for your own use within ODEX.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

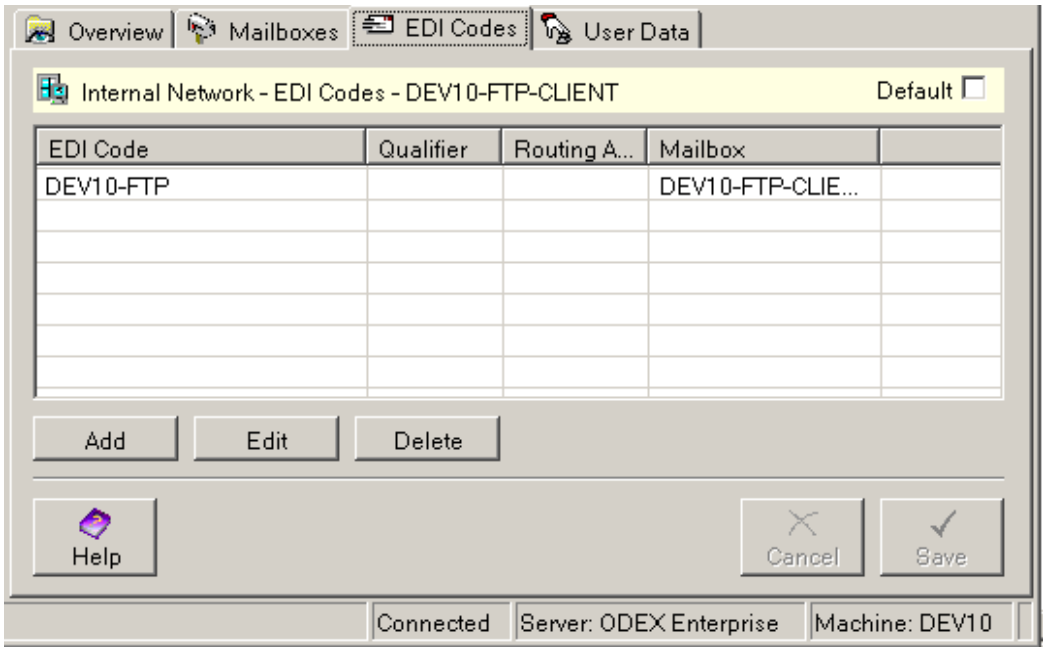
If you want to discard all the changes you have made, click the **Cancel** button.

SAVE

To save details of the new mailbox, click the **SAVE** button.

Internal FTP client Network – EDI Codes

The EDI Codes page is where you can provide the EDI addressing details for each of your internal companies that use this network. The EDI Codes page looks like the example below and shows a list of all EDI codes currently defined for this internal network.



Use the **Add**, **Edit** and **Delete** buttons to add new EDI codes, and edit and delete existing EDI codes.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

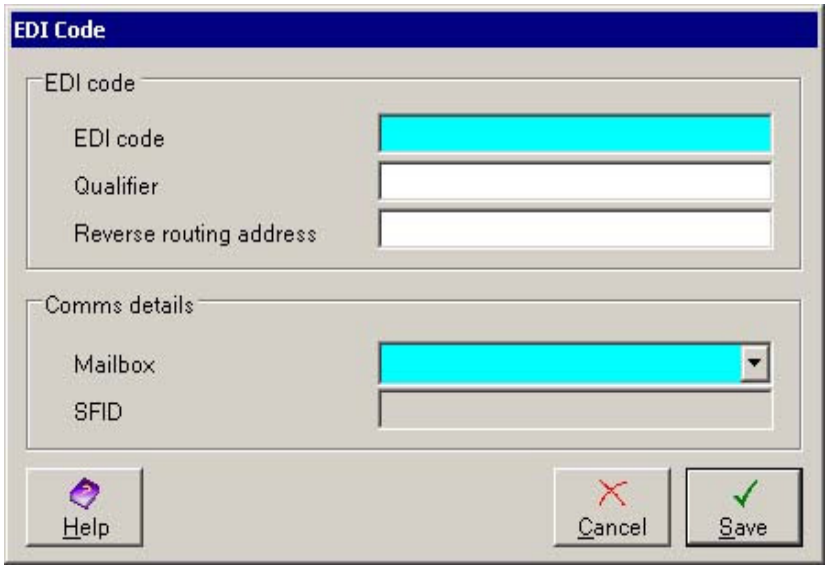
If you want to discard all the changes you have made, click the **Cancel** button.

Save

To save any changes you have made in the EDI codes section, click the **Save** button.

EDI codes – Add/Edit

Use the **Add** or **Edit** button to add or edit an EDI Code for this internal network. This will bring up the following dialog:



EDI code – EDI code

Type in the EDI code for this internal FTP client network.

EDI code – Qualifier

This is a qualifier for the EDI code and is usually only required if you or your trading partner demands it.

EDI code – Reverse routing address

This is an address used for reverse routing of the EDI code and is usually only required if you or your trading partner demands it.

Comms details – Mailbox

Use the dropdown arrow to select the appropriate mailbox for this EDI code. You must define a mailbox on the Mailboxes page tab and save it before you can complete this dialog.

Comms details – SFID

There is no SFID associated with an FTP client mailbox so this field is always greyed out.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

If you want to discard all the changes you have made, click the **Cancel** button.

Save

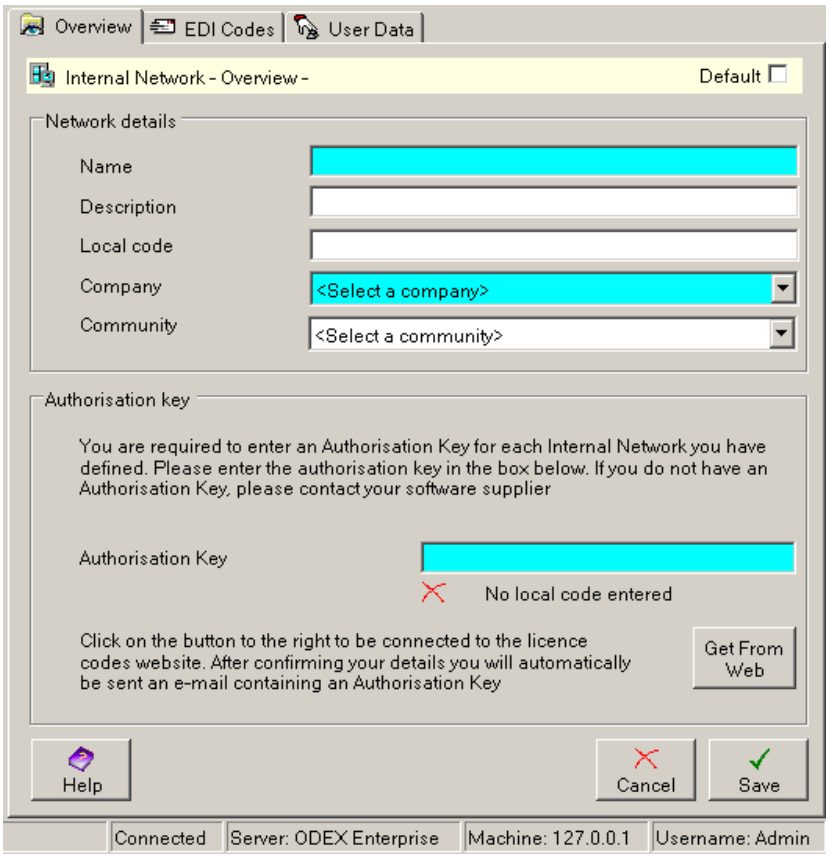
To save the changes you have made on this dialog, click the **Save** button.

Adding/Editing an Internal FTP server Network

There are three pages associated with an internal FTP server network, so let's go through them and find out what information is required. The User Data page is described in the section entitled ‘User Data’.

Internal FTP server Network – Overview

The Overview page is where mandatory information has to be provided for each new internal FTP server network node. The Overview page looks like the example below.



Network details – Name

Type in this field a name for the internal network. This name must be unique among your other internal networks, but it can be whatever you want it to be. The name is a unique identifier, enabling you to recognise it easily when you want to use this internal network.

Network details – Description

You may give a brief description of the internal network in this field if you wish. You can simply repeat the name of the internal network if you like, or include any other information that helps you to recognise it. The description is intended to help you remember what the internal network is for.

Network details – Local code

This mandatory field is used for licensing an internal network (your authorisation code is valid for only a single specific local code) and for compatibility with users upgraded from ODEX Professional wishing to use the batch interface.

The local code is simply a unique code designated by you and used to identify the company in a shorthand form, instead of having to remember their EDI code. It is a code internally used by ODEX and will never be seen by your trading partners.

Network details – Company

If you have defined more than one internal company, use the dropdown arrow to select the appropriate internal company with which this network is to be associated.

Internal Network – Community

This field will only be visible if you are using communities and you are logged on as a user that is a member of multiple communities or a user that is not a member of any communities, e.g. the admin user.

If you are using communities and you are logged on as a user that is a member of one community, the field is hidden because the company will be created and associated with your community automatically.

Select a community if you wish to associate this network with a community. The network will then only be visible to users that are a member of the selected community, or users that are a member of a group that is a member of the selected community.

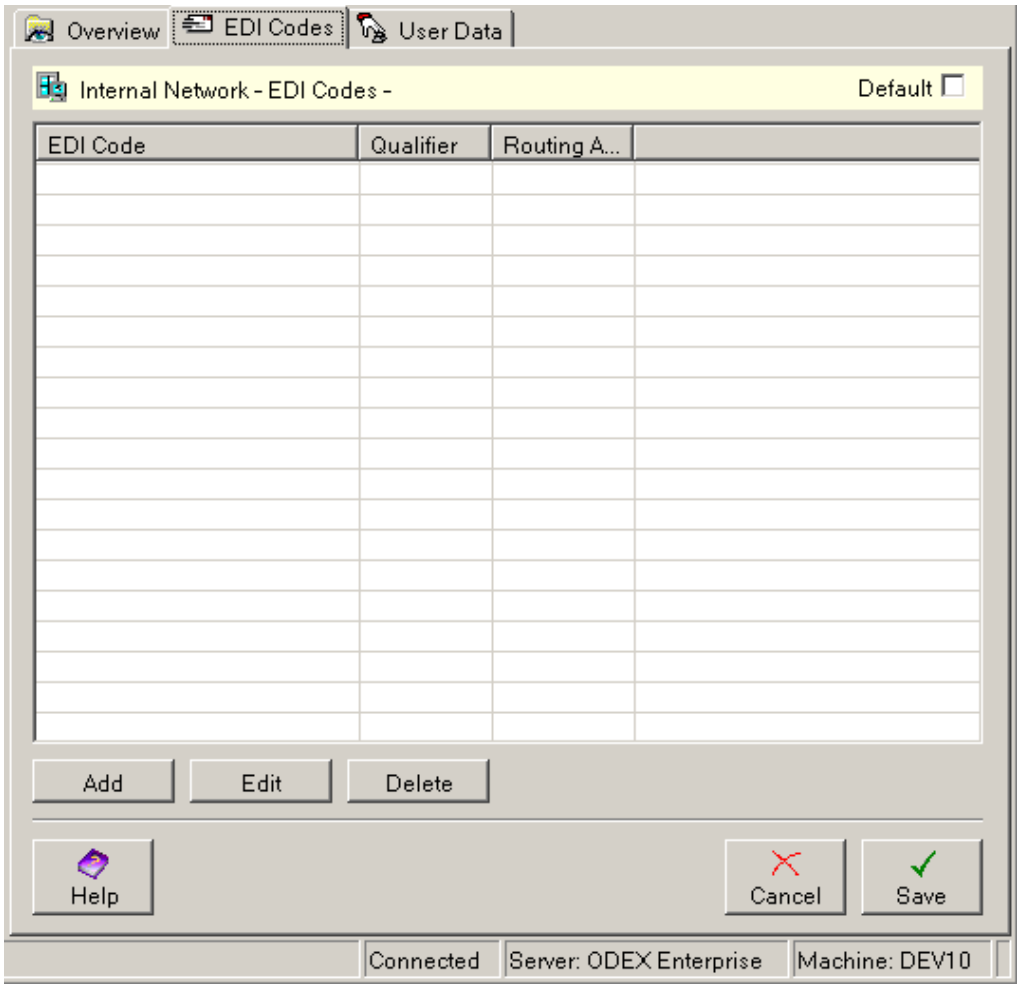
Authorisation Key

You are required to provide an authorisation key for each internal network you define. If you have the authorisation key, type it in this field. Otherwise, please click on the **Get from Web** button to be connected to the Licence Codes website. After confirming your details you will automatically be sent an e-mail containing an authorisation key.

As soon as you have provided a valid authorisation key in this field, the "No local code entered" or "Invalid key" message will change to "Valid key".

Internal FTP server Network – EDI Codes

The EDI Codes page is where you can provide the EDI addressing details for each of your internal companies that use this network. The EDI Codes page looks like the example below and shows a list of all EDI codes currently defined for this internal network.



Use the **Add**, **Edit** and **Delete** buttons to add new EDI codes, and edit and delete existing EDI codes.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

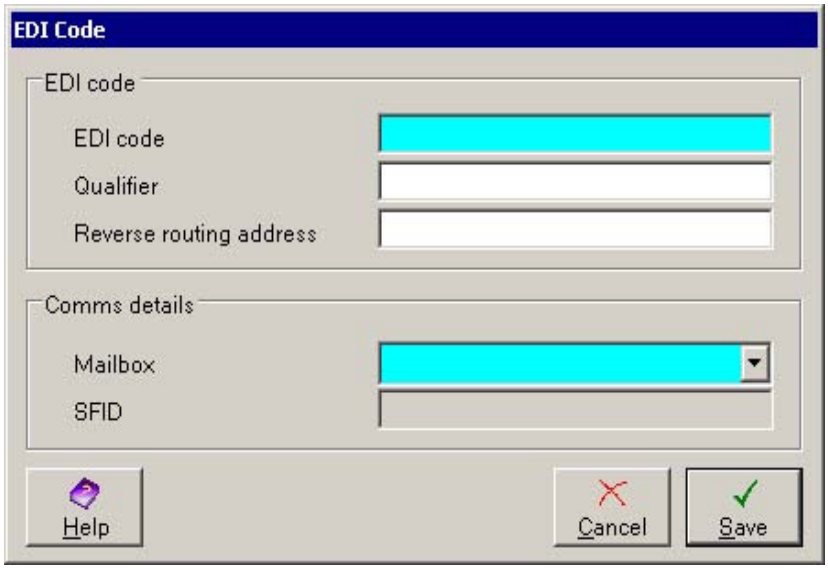
If you want to discard all the changes you have made, click the **Cancel** button.

Save

To save any changes you have made in the EDI codes section, click the **Save** button.

EDI codes – Add/Edit

Use the **Add** or **Edit** button to add or edit an EDI Code for this internal network. This will bring up the following dialog:



EDI code – EDI code

Type in the EDI code for this internal FTP server network.

EDI code – Qualifier

This is a qualifier for the EDI code and is usually only required if you or your trading partner demands it.

EDI code – Reverse routing address

This is an address used for reverse routing of the EDI code and is usually only required if you or your trading partner demands it.

Comms details – Mailbox

Use the dropdown arrow to select the appropriate mailbox for this EDI code. You must define a mailbox on the Mailboxes page tab and save it before you can complete this dialog.

Comms details – SFID

There is no SFID associated with an FTP server mailbox so this field is always greyed out.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

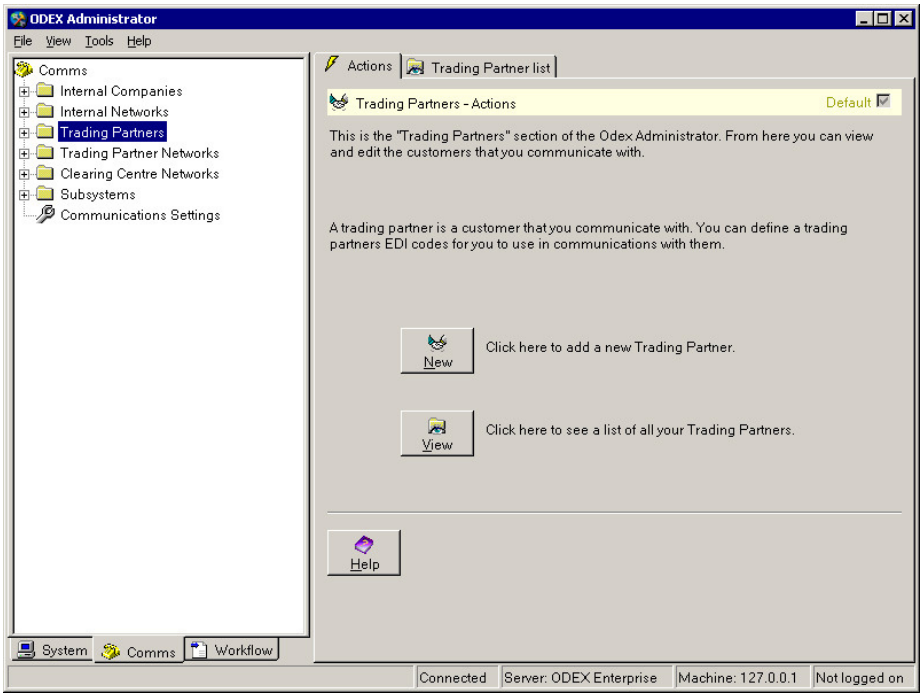
If you want to discard all the changes you have made, click the **Cancel** button.

Save

To save the changes you have made on this dialog, click the Save button.

Trading Partners

Click on the name Trading Partners in the Navigation Panel to see the default page for the Trading Partners section, as shown below. This is the Trading Partners – Actions page.

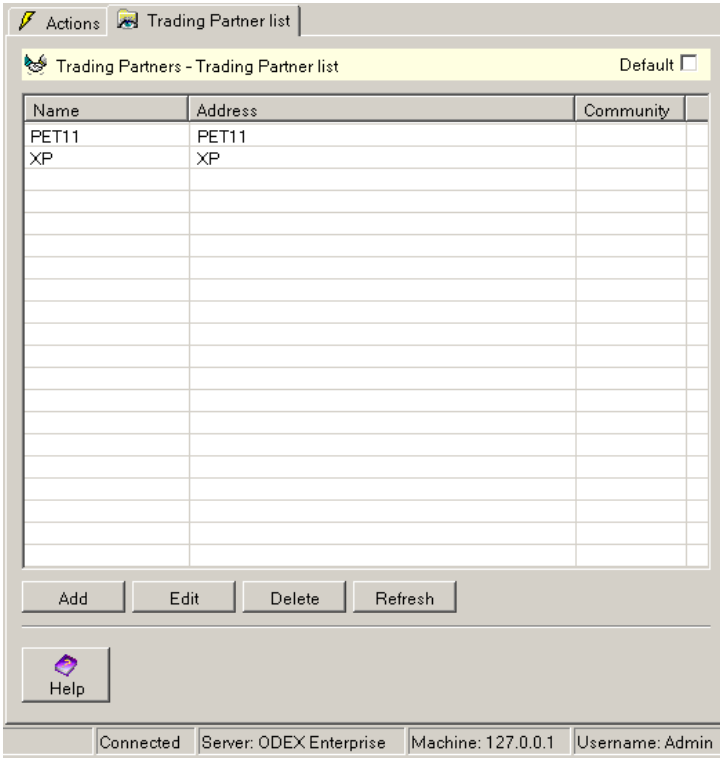


The Trading Partners section allows you to add, view and edit your trading partners' details.

As you can see, there are two page tabs on the Information Panel (Actions and Trading Partner list) and two buttons, labelled **New** and **View**. The **New** button allows you to add a new trading partner. The **View** button allows you to see a list of all the existing trading partners, from where you can edit their details, add new entries or delete existing entries.

Viewing all your trading partners

If you wish to see a list of all the trading partners currently in the ODEX database, you can either click the **View** button on the Trading Partners – Actions page or click the Trading Partner list tab. Both have the same result, as in the example below.



The Information Panel now shows the Trading Partner list page. Depending on your system configuration, this is divided into two or three columns. If you are not using communities, two columns will be displayed showing the Trading Partner Name and Address. If you are using communities, an additional column will be present for the community associated with each trading partner.

The actions that can be taken from this page are as follows:

Add

New trading partners may be added to the list by using the **Add** button. If this button is clicked, it will bring up the set of pages described below under the heading "Trading Partner – Overview".

Edit

You may edit the details of existing trading partners by using the **Edit** button. If this button is clicked, it will bring up the same set of pages described below under the heading "Trading Partner – Overview".

Delete

If you wish to delete a trading partner from the list, highlight the line that you wish to delete, then click on the **Delete** button. ODEX will bring up a dialog box, asking if you are sure you want to delete the selected items. This is to safeguard against accidentally deleting the wrong item. Click **Yes** to delete or **No** to keep the item in the list.

Refresh

Click this button to refresh the details on this page, for example if you have just made some changes which have not yet appeared on this page.

Help

If you need more information about the fields and buttons on this page, click on the **Help** button.

Adding/Editing Trading partners

If you wish to add a new trading partner, click the **New** button on the Trading Partners – Actions page. You can also add a new trading partner by clicking on the **Add** button on the Trading Partners list page of the Trading Partners section.

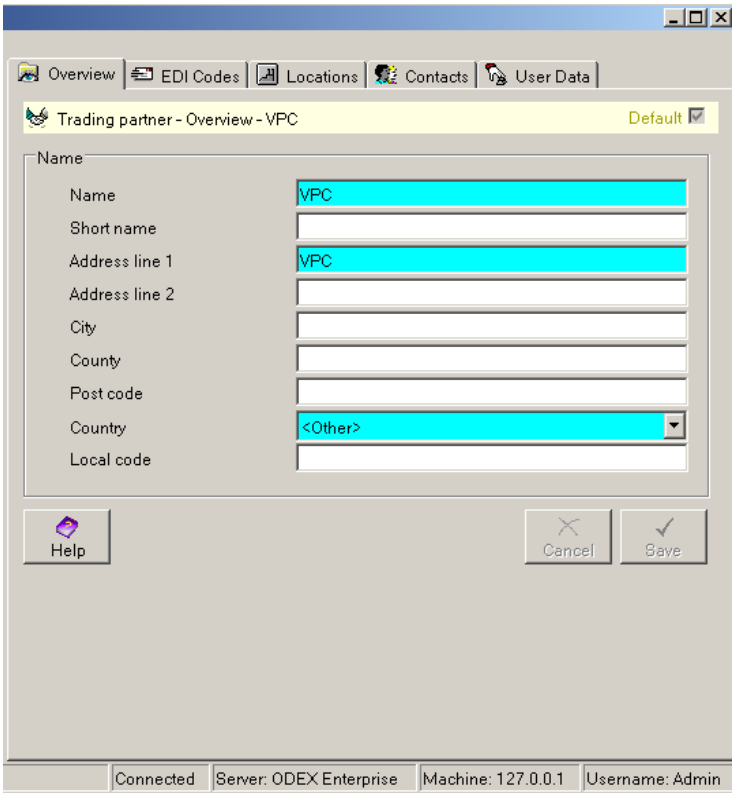
To edit an existing trading partner, open the Trading Partners list page, select the partner to be edited, and click the **Edit** button. Alternatively, double-click on the Trading Partners node in the tree view, then click once on the partner to be edited.

Whichever route you choose, you will be presented with the following set of pages, enabling you to add or edit details of a trading partner. There are three pages associated with trading partners, so let's go through them and find out what information is required. The User Data page is described in the section entitled ‘User Data’.

One point to remember – each of the **Save** and **Cancel** buttons in the Trading Partners section work for both Trading Partners pages, so you do not need to click the **Save** button until you have entered data on both pages. You can click the **Cancel** button at any point to undo changes that you have made.

Trading Partner – Overview

The Overview page is where mandatory information about each trading partner must be provided. The Overview page looks like the example below.



Name – Name

This is the trading name of the company.

Name – Short name

This is a shortened company name. This company name can be used in ENGDAT messages (see XXX for further details). If you do not use ENGDAT, this field can be ignored.

Name – Address line 1

This is the first line of the company address. It must not be left blank.

Name – other fields

If you wish to provide the full company address, please type the remaining address details into the appropriate fields.

Name – Country

This is the country where the company is based. Use the dropdown arrow to select the appropriate country.

Name – Local code

This is an optional field, included for compatibility with other systems. Most users can ignore this field. The local code is simply a unique code designated by you and used to identify the company in a shorthand form, instead of having to remember their EDI code. It is a code internally used by ODEX and will never be seen by your trading partners.

Name – Community

This field will only be visible if you are using communities and you are logged on as a user that is a member of multiple communities or a user that is not a member of any communities, e.g. the admin user.

If you are using communities and you are logged on as a user that is a member of one community, the field is hidden because the company will be created and associated with your community automatically.

Select a community if you wish to associate this company with a community. The company and any data associated with it will then only be visible to users that are a member of the selected community, users that are a member of a group that is a member of the selected community and users that are not a member of any communities, such as the admin user.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

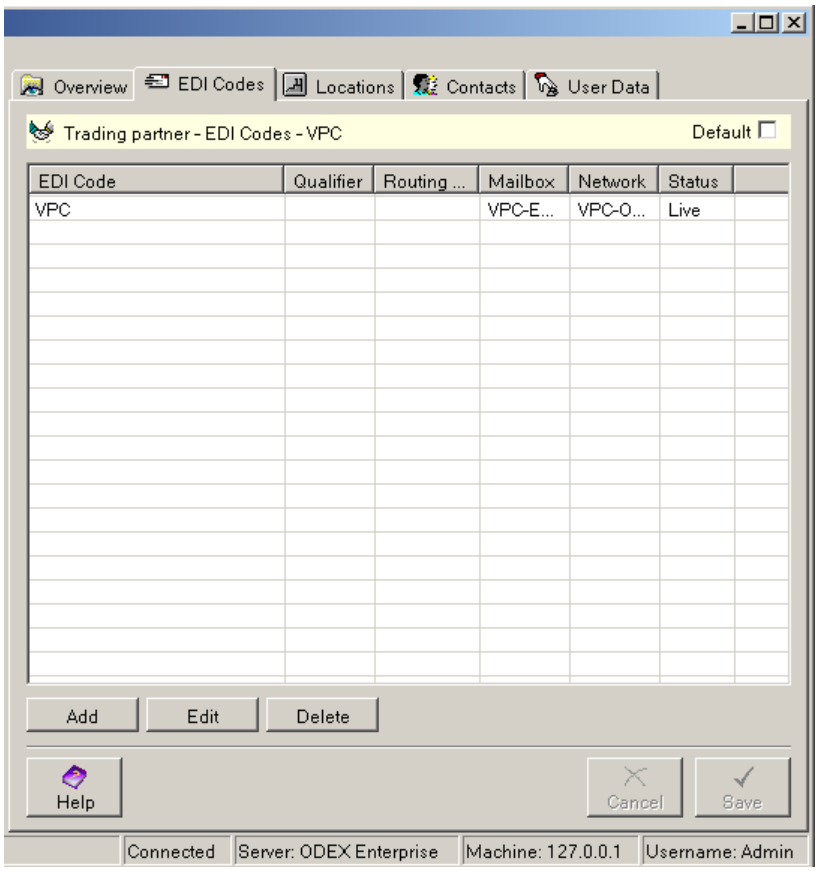
If you want to discard all the changes you have made on the Overview page, click the **Cancel** button.

Save

To save all the changes you have made on the Overview page, click the **Save** button.

Trading Partner – EDI Codes

The EDI Codes page allows you to provide details of each trading partner's EDI code and related details. The EDI Codes page looks like the example below.

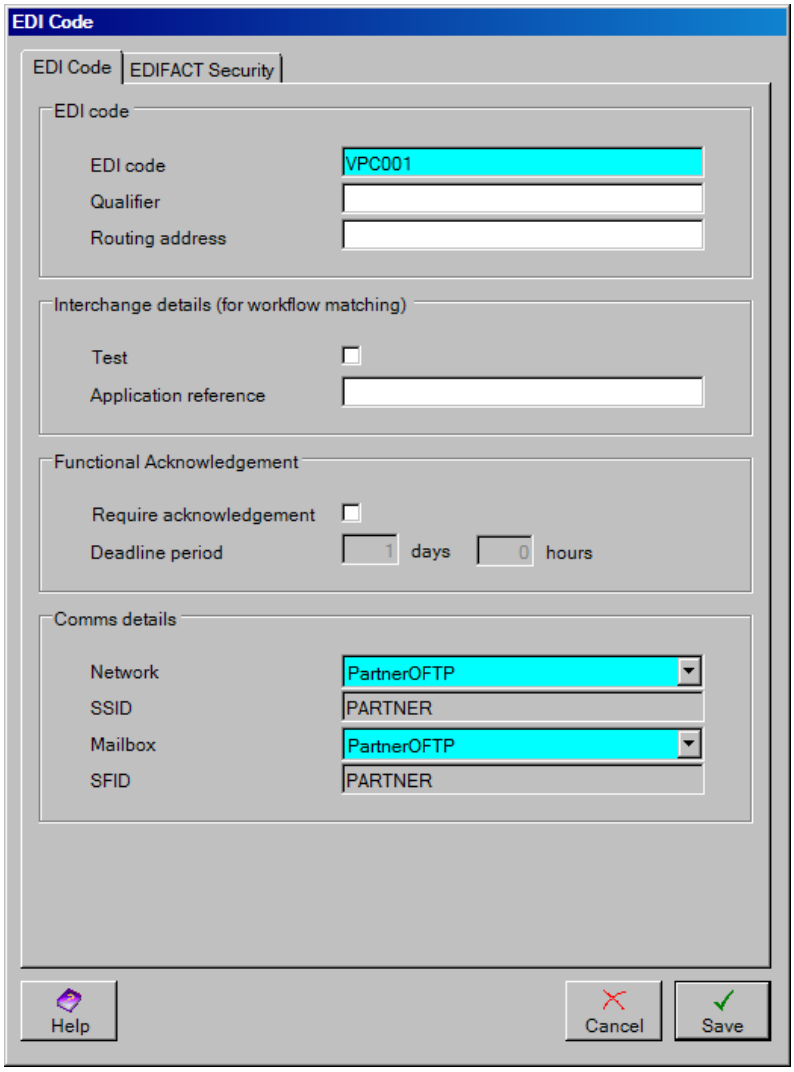


This shows a list of all the EDI codes you have already defined for the current trading partner.

Add/Edit

Use the **Add** or **Edit** button to add or edit an EDI code for this trading partner.

You will see the EDI Code dialog, shown below.



There is an additional tab used for specifying EDIFACT security information. Details can be found in the section ”EDIFACT Security Settings”.

This tab page shown is divided into three sections: EDI code, Interchange Details and Comms details.

The Interchange Details section is only important if you are going to use these details for workflow matching purposes.

EDI Code – EDI code

Type in this field the EDI code of this trading partner.

EDI Code – Qualifier

You only need to provide a value in this field for those trading partners who require it.

EDI Code – Reverse routing address

You only need to provide a value in this field for those trading partners who require it.

Interchange Details – Test

Select this tickbox if you want to treat 'Test' EDI files from this trading partner to be treated differently from 'Live' files.

N.B. A 'Test' EDI file has a special flag set in the EDI message to indicate its Test status. A 'Live' EDI message simply does not have the flag set. For example, in an EDIFACT message, a '1' in element 0035 of the UNB segment indicates a Test message. If this element is blank, the message is Live.

Interchange Details – Application reference

You only need to provide a value in this field if you want to treat messages from this trading partner differently according to the application reference they contain.

The application reference is held in element 0026 of the UNB segment.

Functional Acknowledgement – Require

Select this tickbox if you require EDI functional acknowledgements for files scheduled to this EDI code.

You will also need to flag the schedule job to require a functional acknowledgement for workflow files that it schedules.

Functional Acknowledgement – Deadline period

Enter here the number of days and hours that you allow for an EDI functional acknowledgement to be received. If an acknowledgement is not received within the specified period, the acknowledgement status of the workflow file is marked as Overdue and a system event is raised.

Comms details – Network

How you handle this field depends on how you want to use ODEX.

If you want to use the auto-detect facility when scheduling EDI files or if you want to validate the EDI code in received EDI messages, you should select the appropriate network for this trading partner from the dropdown list.

Otherwise you may leave the value in this field set to <None>.

If the network you require is not in the list, you must first add it in the Trading Partner Networks or Clearing Centre Networks section, as appropriate.

Comms details – ID

This field is not editable.

If you have selected an OFTP network in the field above, the associated SSID will appear in this field (and the field caption will change accordingly).

If you have selected an AS2 network in the field above, the associated AS2 identifier will appear in this field (and the field caption will change accordingly).

Comms details – Mailbox

This field will only be enabled if you have selected an OFTP network in the field above. Select the appropriate mailbox for this trading partner from the dropdown list.

Comms details – SFID

This field is not editable.

Once you have selected an OFTP mailbox in the field above, the associated SFID will appear in this field.

Trading Partner – Locations

This page allows you to view the different company locations (if your trading partner has more than one), to add new locations, and to edit or delete existing locations.

This page will always show the name and address line of the company from the Overview page, with the Location name of Head Office.

You only need to enter further company locations here if you want to use the addresses in ENGDAT messages. The three columns show you the following details:

Name

The name of the company location.

1st Address line

The first line of the company location address.

Code

The code by which the trading partner identifies the location.

Add

To add a new location, click on the **Add** button at the bottom of the page.

Edit

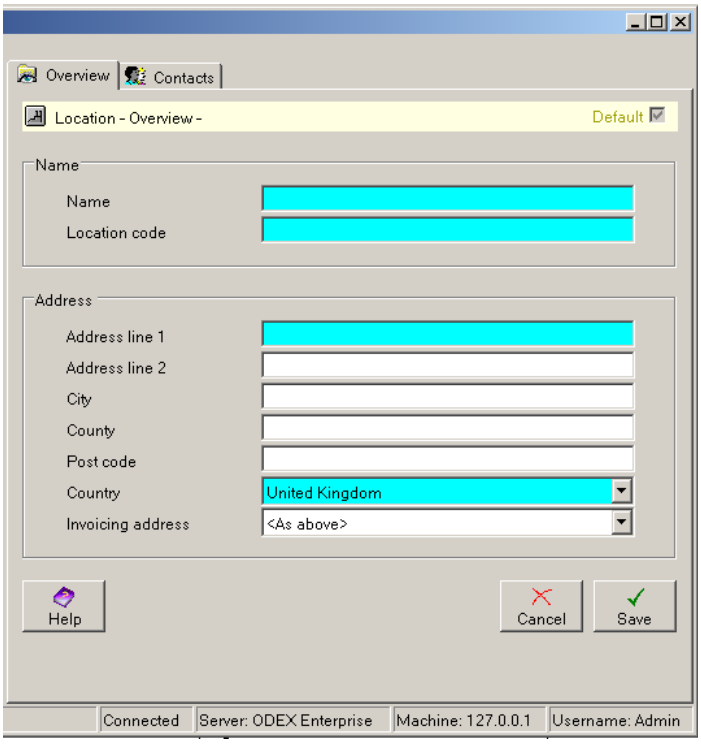
To edit an existing location, highlight the location in the list and click on the **Edit** button.

Delete

To remove an existing location from the list, highlight the location in the list and click on the **Delete** button. You will see a message box, asking if you are sure you want to delete the selected location. Click **Yes** to delete the location. Click **No** to leave the location in the list.

Locations - Adding a new location

The **Add** button brings up two new pages, labelled Overview and Contacts, as shown in the example below.



Let's have a look at these pages and see what information is required.

Location Overview

This page requires a name for the location, one address line of the location and the country in which the location is based.

Name – Name

Type in here the name you use to refer to the location.

Address – Address line 1

This is the first line of your location address. It must not be left blank.

Address details – other fields

If you wish to provide your full location address, please type the remaining address details into the appropriate fields.

Address details – Country

Use the dropdown arrow to select the country where your location is based.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

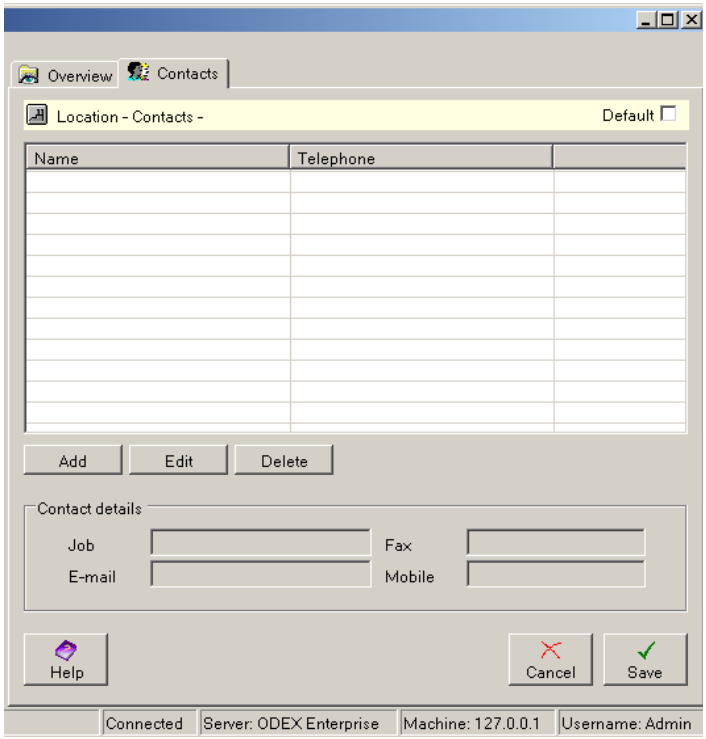
If you want to discard all the changes you have made on the Location Overview page, click the **Cancel** button.

Save

To save all the changes you have made on the Location Overview page, click the **Save** button.

Location - Location Contacts

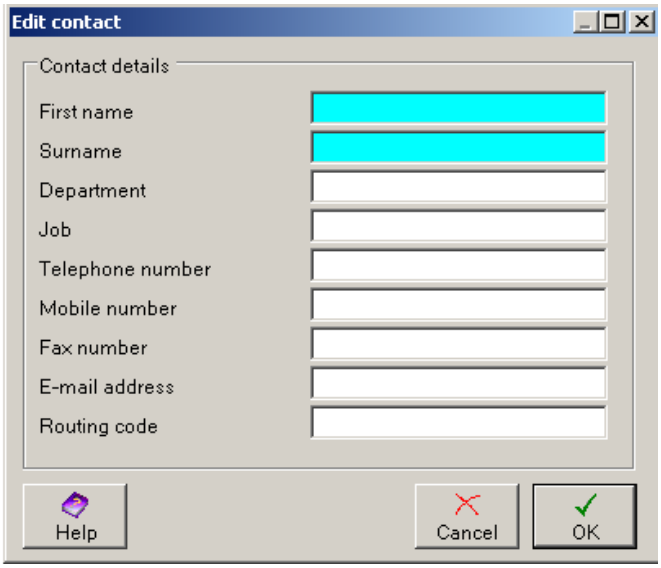
This page allows you to add a contact for the new location, if you so wish. The Contacts page looks like the example below:



If you have added details for a new location on the Overview page, you will see that the yellow title banner on the Contacts page shows the name of that location.

Locations – Location Contacts - Adding a new internal location contact

You do not have to provide contact details for new locations, but if you want to you should click the **Add** button on this page. This will bring up the following dialog:



It contains the following fields:

Contact details – Name

If you supply any contact details at all, you must provide a name. This should be the full name of the contact e.g. Mr Leslie Smith, to avoid any ambiguity.

Contact details – Other details

It will be most useful to include at least one contact number or address for the person, but none of these fields is mandatory.

Help

If you need more information about the fields on this dialog and how to fill them in, click on the **Help** button.

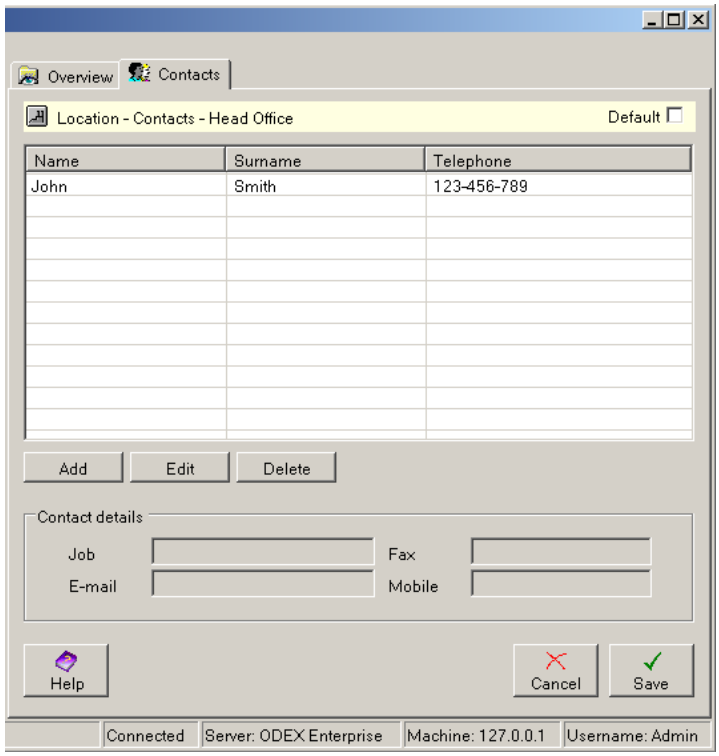
Cancel

If you want to discard all the changes you have made on the New contact dialog, click the **Cancel** button.

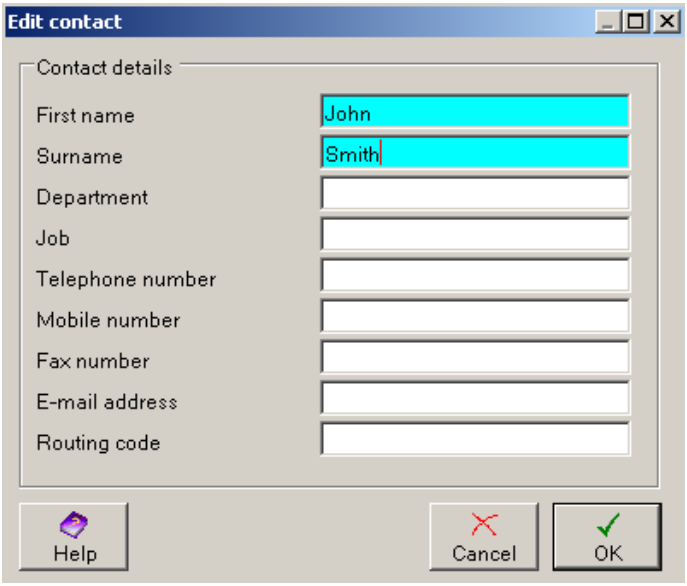
OK

To save all the changes you have made on the New contact dialog, click the **OK** button.

On returning to the Contacts page, you will see that the details you supplied on the New contact dialog are now visible, as illustrated by the example below, where just the email address and telephone number were added. The telephone number is shown alongside the contact name, and, if you highlight the contact name, the remaining details are shown in the Contact details section at the bottom of the page:



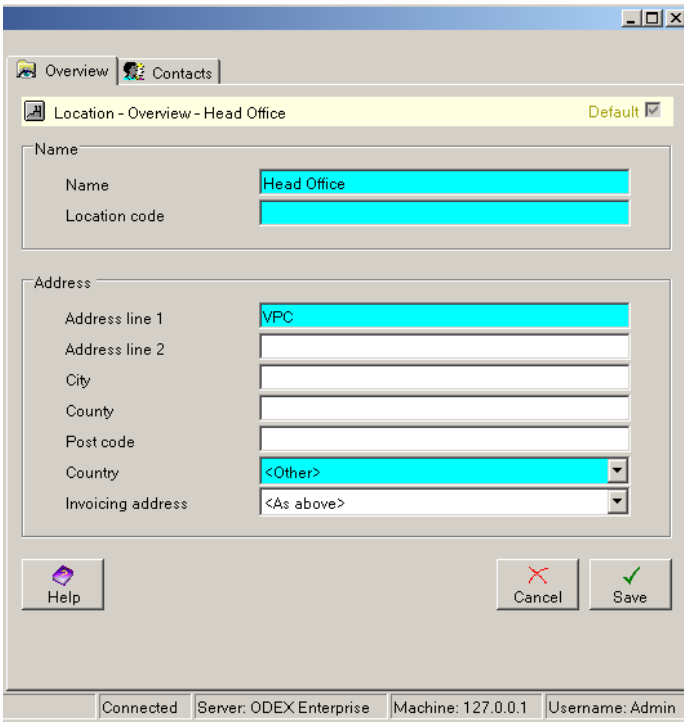
If you want to edit the contact details, highlight the appropriate contact in the list and click the **Edit** button. You will see a dialog similar to the following:



The Edit contact dialog is just the same as the New contact dialog, except that data is already in the fields. You should make any changes you need to make then either click the **Cancel** button to discard your changes or click **OK** to save your changes and return to the Contacts page.

Editing a location

The Edit button brings up two pages, labelled Overview and Contacts, as shown in the example below. We are looking at an existing location, so the fields are already filled in.



Let's have a look at these pages and see what information is on them.

Overview

This page requires a name for the location, one address line of the location and the country where the location is based.

Name – Name

This is the name you use to refer to the location.

Name – Location code

This is the code that the trading partner uses to identify this location.

Address – Address line 1

This is the first line of your location address.

Address – other fields

If you wish to provide your full location address, please type the remaining address details into the appropriate fields.

Address – Country

This is the country where your location is based.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

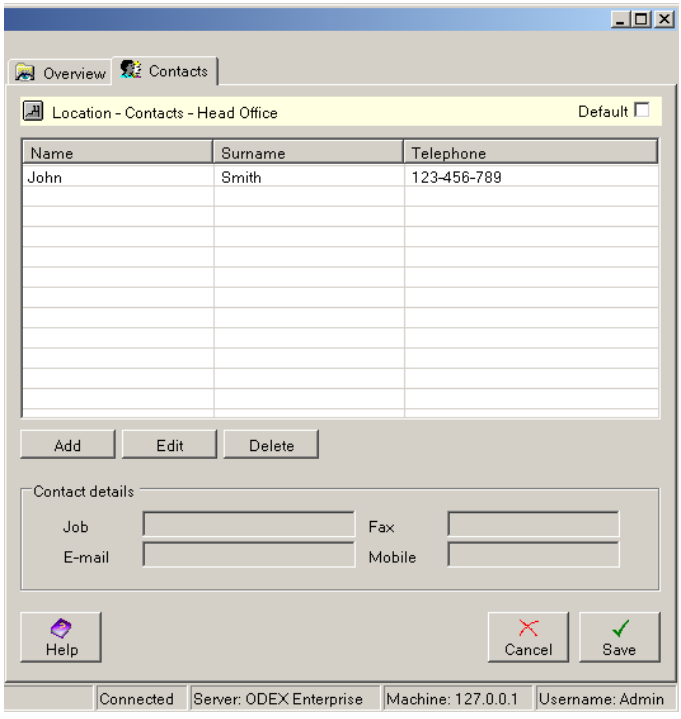
If you want to discard all the changes you have made on the Overview page, click the **Cancel** button.

Save

To save all the changes you have made on the Overview page, click the **Save** button.

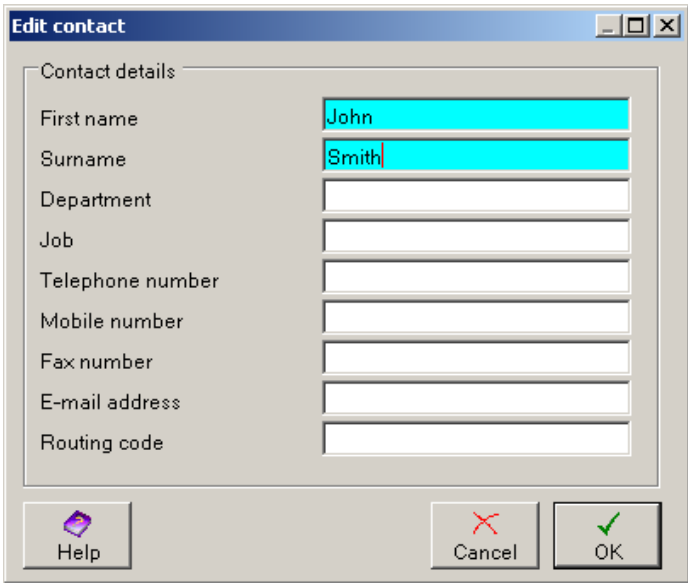
Contacts

This page allows you to add a new contact, edit an existing contact or delete an existing contact. The Contacts page looks like the example below:



As you can see, the yellow title banner shows the name of the location we are currently editing details for.

If you want to edit any existing contact details you should highlight the appropriate line and click the **Edit** button on this page. This will bring up a dialog similar to the following:



Simply edit whichever fields you need to, then click **Cancel** or **OK**.

Help

If you need more information about the fields on this dialog and how to fill them in, click on the **Help** button.

Cancel

If you want to discard all the changes you have made on the Edit contact dialog, click the **Cancel** button.

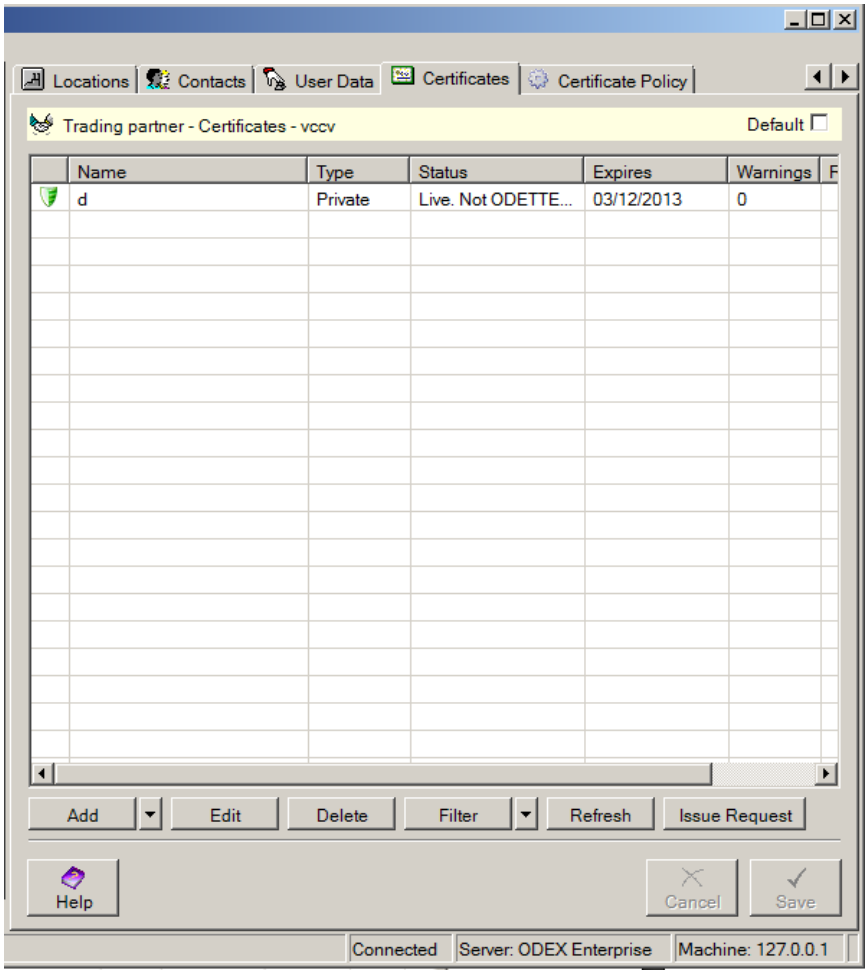
OK

To save all the changes you have made on the Edit contact dialog, click the **OK** button.

When you return to the Contacts page, if you want to keep the changes you have made, click **Save** to return to the Locations page of the supplier company view. If you want to discard the changes you have made, click **Cancel** to return to the Locations page of the supplier company view.

Trading Partner – Certificates

The Certificates page allows you to manage the security certificates associated with your trading partner, for use in communications. The page looks like the example below.

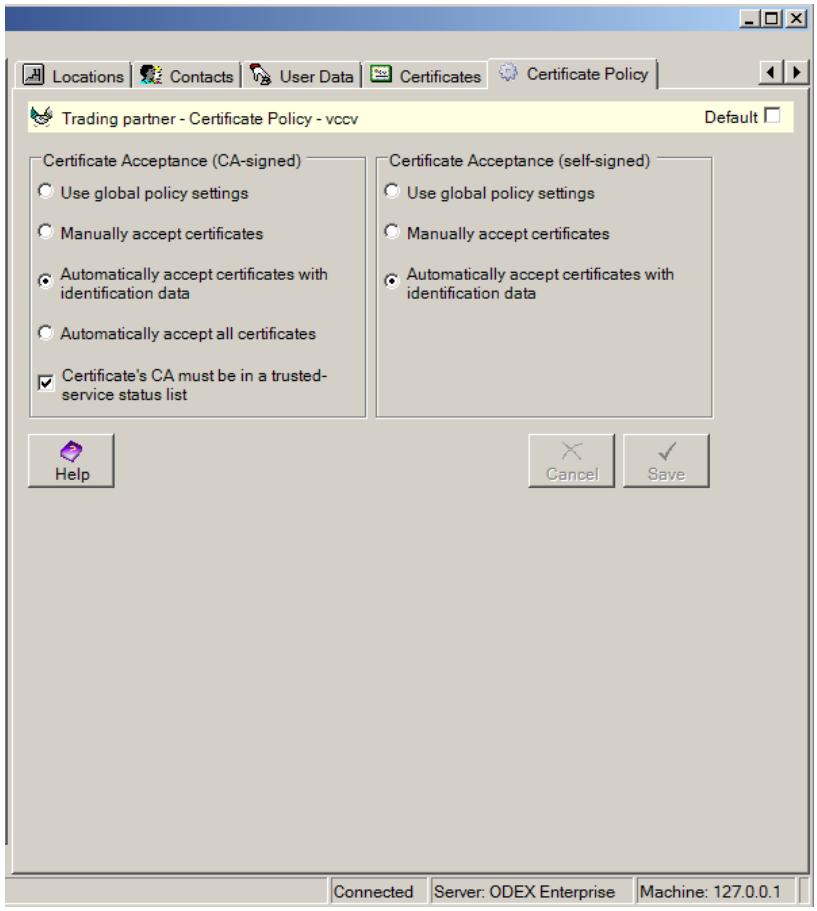


This page is divided into a list of all certificates belonging to your trading partner and a collection of buttons for performing actions with certificates.

Management of certificates from this page is a subset of management that can be performed at a global level, discussed in the section entitled ‘Certificates’.

Trading Partner – Certificate Policy

The Certificate Policy page is where you can configure the certificate policy for your trading partner. The page looks like the example below.



Certificate policy guides ODEX with management of your trading partner's certificates. Options configured here override global certificate policy (see the section entitled 'Global Certificate Policy').

Certificate Acceptance

Here you can configure the situations when ODEX will automatically accept certificates that are received from trading partners. By default, global certificate policy is used, but you can override the global settings with specific settings for accepting the certificates received from this trading partner. A separate policy can be configured for those certificates that the partner has self-signed and those certificates that have been signed by a Certificate Authority.

For a discussion of certificate exchange, please refer to 'OFTP2 Certificate Exchange'.

Select "Manually accept certificates" if you would like to choose which individual received certificates are accepted into the ODEX certificate store.

Select "Automatically accept certificates with identification data" to permit ODEX to accept received certificates for which you have pre-registered matching identification data.

Select "Automatically accept all certificates" to permit ODEX to accept all received certificates.

There is a further option that opens for some selections that enable you to restrict the automatic acceptance of certificates to those who's CA is in ODETTE's Trusted-service Status List.

Networks (Trading Partner or Clearing Centre)

The Trading Partner Networks section of the ODEX Administrator is where you provide the communication details for those customers with whom you communicate directly.

The Clearing Centre Networks section of the ODEX Administrator is where you provide the details of communication for those trading partners with whom you communicate via clearing centre.

These sections also give you the opportunity to automate calls to your trading partners and clearing centres respectively.

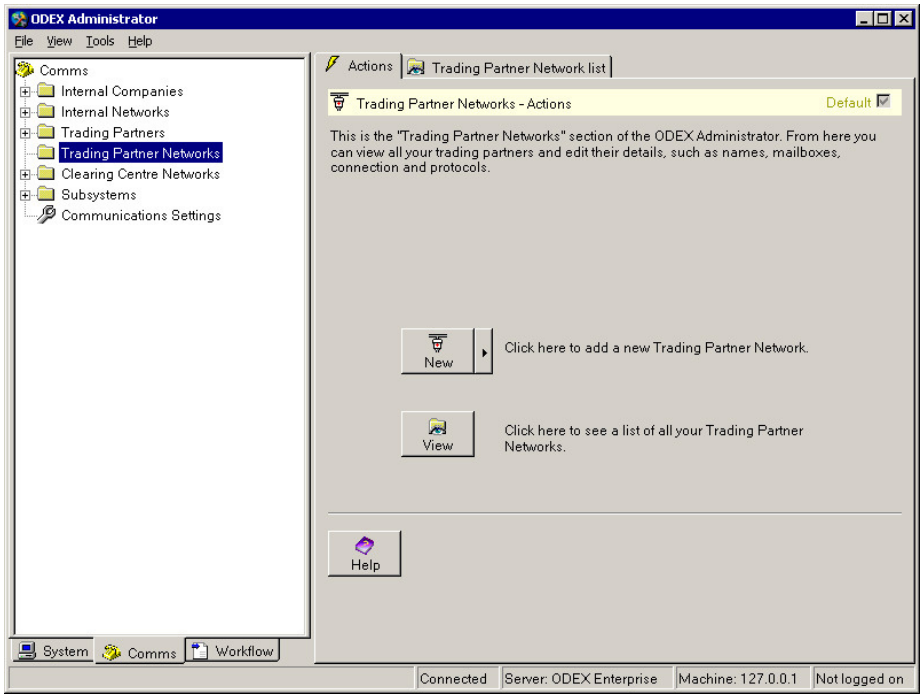
There are currently three types of network available with ODEX – OFTP, FTP and AS2. When you add a new trading partner or clearing centre network you must be sure to select the correct type of network.

Before you begin to add details to these sections you should ensure that you have the following information to hand:

- The SSID code or AS2 identifier of the trading partner or clearing centre
- The IP host address, ISDN number or URL of the trading partner or clearing centre (depending on what type of subsystem you use to connect to them)
- OFTP or FTP passwords if they are used by the trading partner or clearing centre

Since the details required by trading partner and clearing centre networks are almost exactly identical, they are described in a single section. Any differences between the two will be indicated where appropriate.

Click on either the Trading Partner Networks node in the Navigation Panel, or on the Clearing Centre Networks node, to see the default page for the selected Networks section, as shown below. This is the Networks – Actions page.



The Trading Partner Networks section allows you to add, view and edit your trading partner communication details.

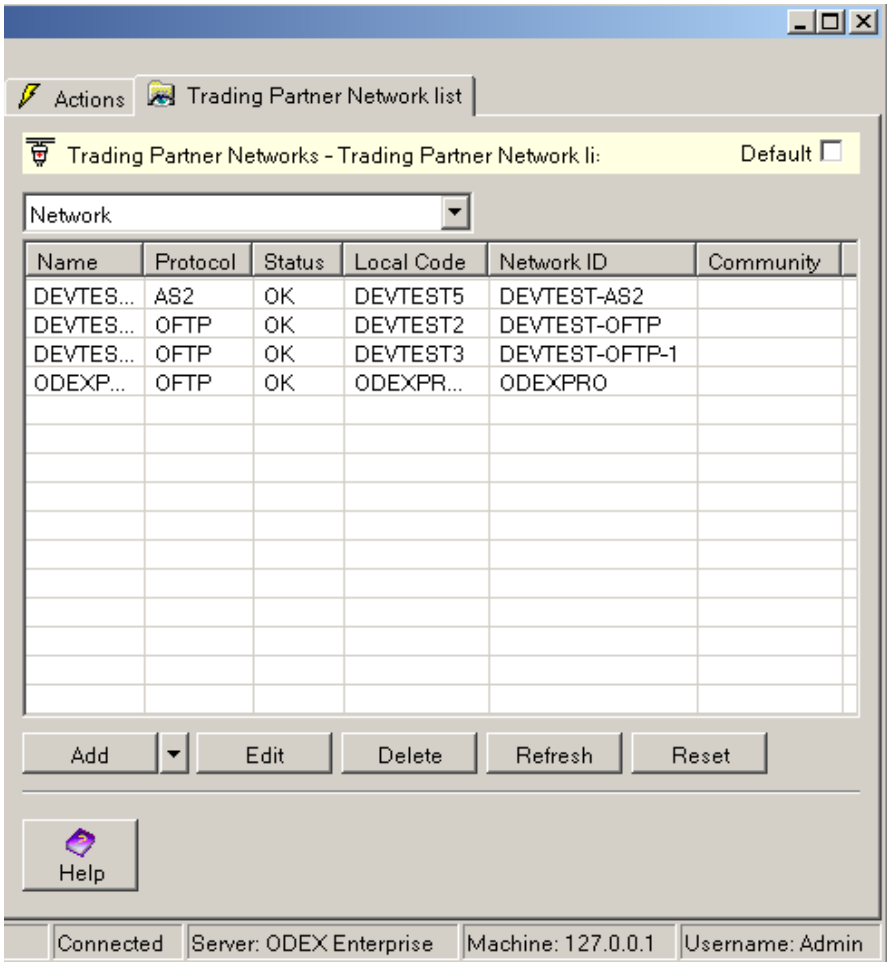
The Clearing Centre Networks section allows you to add, view and edit your clearing centre communication details.

As you can see, there are two page tabs on the Information Panel (Actions and Network list) and two buttons, labelled **New** and **View**. The **New** button has an arrow leading to three further options – **New OFTP Network, New FTP Network** or **New AS2 Network** – which allow you to add a new network of the appropriate kind. The **View** button allows you to see a list of all the existing networks, from where you can edit their details, add new entries or delete existing entries.

The Default Page tickbox is ticked, indicating that this is the page you will see first when you open a Networks view. Once you are familiar with ODEX you will probably choose the Network list page as your default page in this section.

Viewing all your networks (trading partner or clearing centre)

If you wish to see a list of all the networks of all protocols (of the selected type – either Trading Partner or Clearing Centre) currently in the ODEX database, you can either click the **View** button on the Networks – Actions page or click the Network list tab. Both have the same result, as in the example below. You may also view all of the mailboxes or EDI codes associated with your internal networks by selecting 'Mailbox' or 'EDI code' from the drop-down list at the top of the page.



Networks

When 'Network' is selected from the drop-down list, the Information Panel shows the Network list page. Depending on your system configuration, this is divided into five or six columns. If you are not using communities, the columns show the Network Name, its associated Protocol, Status, Local Code and

Network ID. If you are using communities, an additional column will be present, showing the community that each network is associated with.

The actions that can be taken from this page are as follows:

Add

New networks may be added to the list by using the **Add** button. If this button is clicked, it will bring up the set of pages described below under the heading "Adding/Editing Networks".

Edit

You may edit the details of existing networks by using the **Edit** button. If this button is clicked, it will bring up the set of pages described below under the heading "Adding/Editing Networks".

Delete

If you wish to delete a network from the list, highlight the line that you wish to delete, then click on the **Delete** button. ODEX will bring up a dialog box, asking if you are sure you want to delete the selected item. This is to safeguard against accidentally deleting the wrong item. Click **Yes** to delete or **No** to keep the item in the list.

Refresh

Click this button to refresh the details on this page, for example if you have just made some changes which have not yet appeared on this page.

Reset

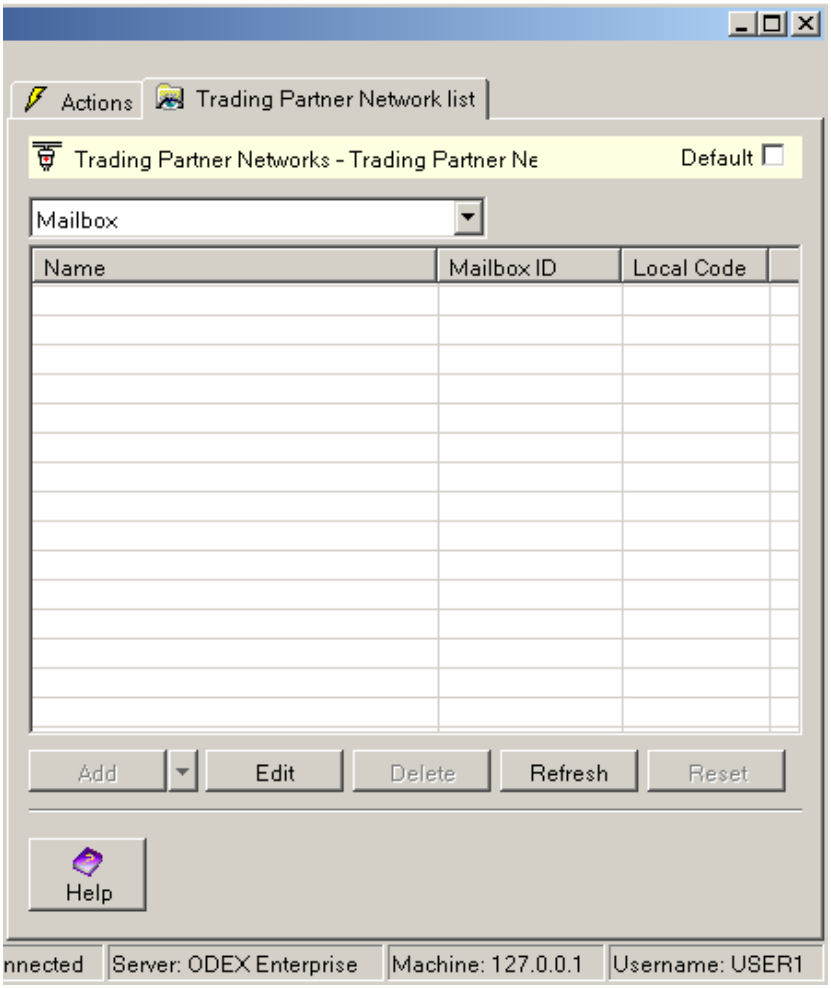
Click the **Reset** button if you wish to reset the status of a selected network. If ODEX has been trying unsuccessfully to send a file to this network (i.e. the status is not OK), you can reset the status to OK with this button. The effect of this will be to allow ODEX to start again with its calls to this network, until it reaches its maximum retry limit.

Help

If you need more information about the fields and buttons on this page, click on the **Help** button.

Mailboxes

You may view all the mailboxes associated with your trading partner or clearing centre networks by selecting ‘Mailbox’ from the drop-down list at the top of the page. The page will then be displayed as in the example below:



The page is divided into three columns – Name, Mailbox ID and Local Code.

The list will contain an entry for each mailbox profiled against each of your OFTP networks and FTP client networks. For each AS2 network and FTP server network profiled on your system, there will be one mailbox displayed in the list, since these network types do not allow additional mailboxes to be added to them.

The Mailbox ID column will display the SFID for OFTP mailboxes. For FTP client mailboxes, the mailbox ID is the same as the name of the mailbox. For FTP server mailboxes, the mailbox ID is the same as the network local code. For AS2 mailboxes, the mailbox ID is the AS2 identifier of the AS2 network.

The **Add, Delete** and **Reset** buttons are disabled when viewing the list of mailboxes, as these buttons are only applicable to networks. To add a mailbox to a network, or delete a mailbox from a network you must first view the details of the network.

The actions that can be taken from this page are as follows:

Edit:

You may view or edit the details of the network associated with a mailbox by double-clicking the mailbox entry in the list, or selecting the mailbox and clicking the **Edit** button. For details of how to view or edit a network, see the section entitled “Adding/Editing Networks”.

Refresh

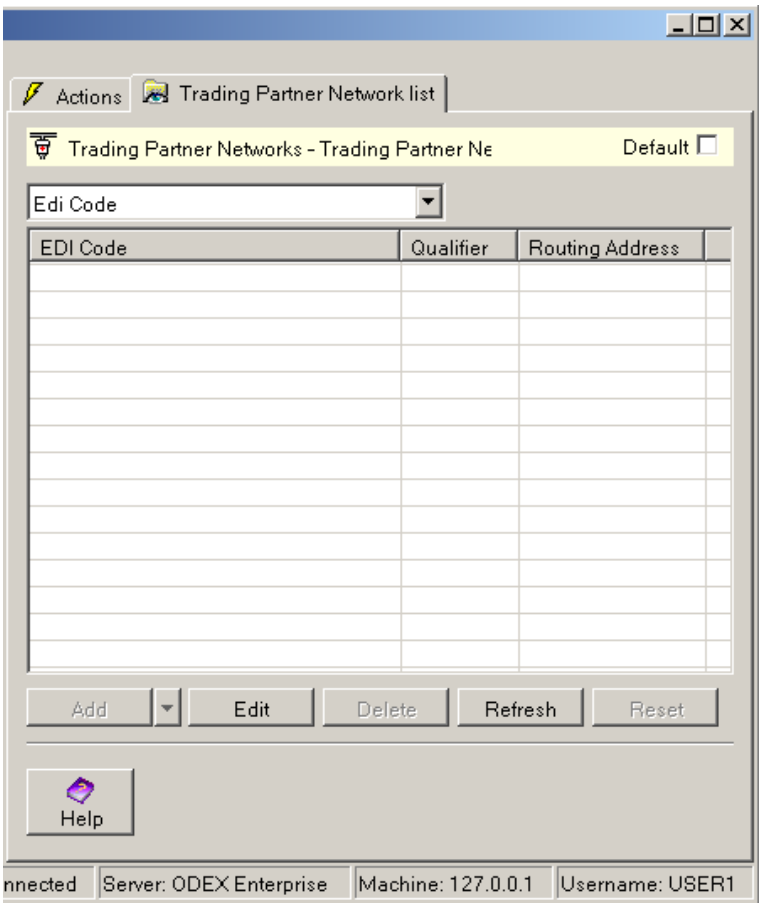
Click this button to refresh the details on this page, for example if you have just made some changes which have not yet appeared on this page.

Help

If you need more information about the fields and buttons on this page, click on the **Help** button.

EDI Codes

You may view all of the EDI codes profiled on each of your internal networks by selecting 'EDI Code' from the drop-down list at the top of the page. The list will then be displayed as below:



The list will now be divided into three columns – EDI Code, Qualifier and routing address.

The **Add, Delete** and **Reset** buttons are disabled when viewing all of the EDI codes, as these buttons are only applicable to networks. To add an EDI code to a network, or remove an EDI code from a network, you must first view the network associated with the EDI code.

The actions that can be taken from this page are as follows:

Edit:

You may view or edit the details of the network associated with an EDI code by double-clicking the EDI code entry in the list, or selecting the EDI code and clicking the **Edit** button. For details of how to view or edit a network, see the section entitled "Adding/Editing Networks".

Refresh

Click this button to refresh the details on this page, for example if you have just made some changes which have not yet appeared on this page.

Help

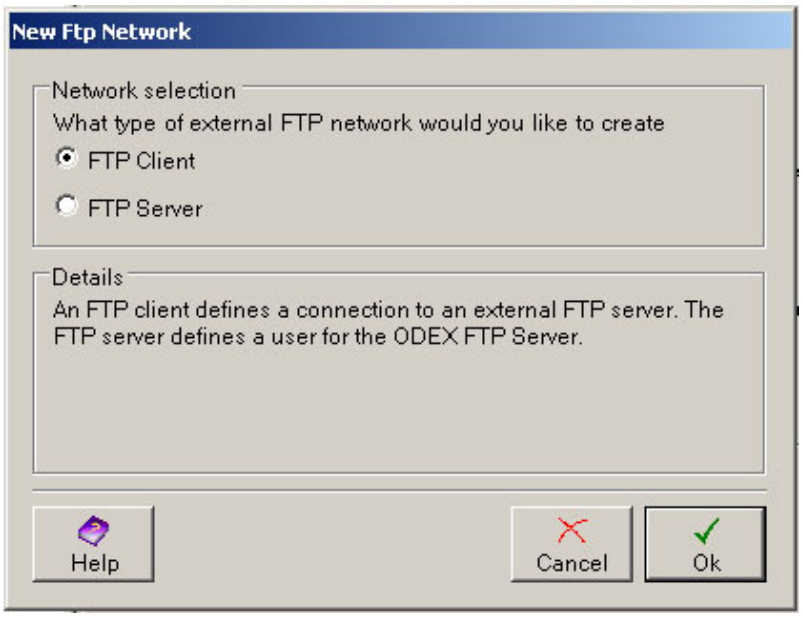
If you need more information about the fields and buttons on this page, click on the **Help** button.

Adding/Editing Networks

If you wish to add a new network, click the **New** button on the Networks – Actions page. You can also add a new network by clicking on the **Add** button on the Network list page of the Networks section.

The **New** and **Add** buttons have an arrow leading to three further options – **New OFTP Network, New AS2 Network or New FTP Network** – which allow you to add a new network of the appropriate kind.

If you select New FTP Network, you will be prompted further to select either an FTP client or an FTP server with the dialog shown below. If you are to function as an FTP client, select FTP client (ODEX configures the trading partner as the complementary FTP server) and if you are to function as an FTP server, select FTP server.



Whichever route you choose, you will be presented with a set of pages, enabling you to add details for the new network. Each type of network has some pages that are specific to that network type and some that are common to all. The User Data pages, common to all networks and mailboxes, are described in the section entitled ‘User Data’. The other pages are described in this section, with an indication as to which network type they relate to. Let's go through them and find out what information is required.

One point to remember – each of the **Save** and **Cancel** buttons in the Networks section work for all Networks pages you are currently editing, so you do not need to click the **Save** button until you have entered data on all applicable pages. You can click the **Cancel** button at any point to undo changes that you have made.

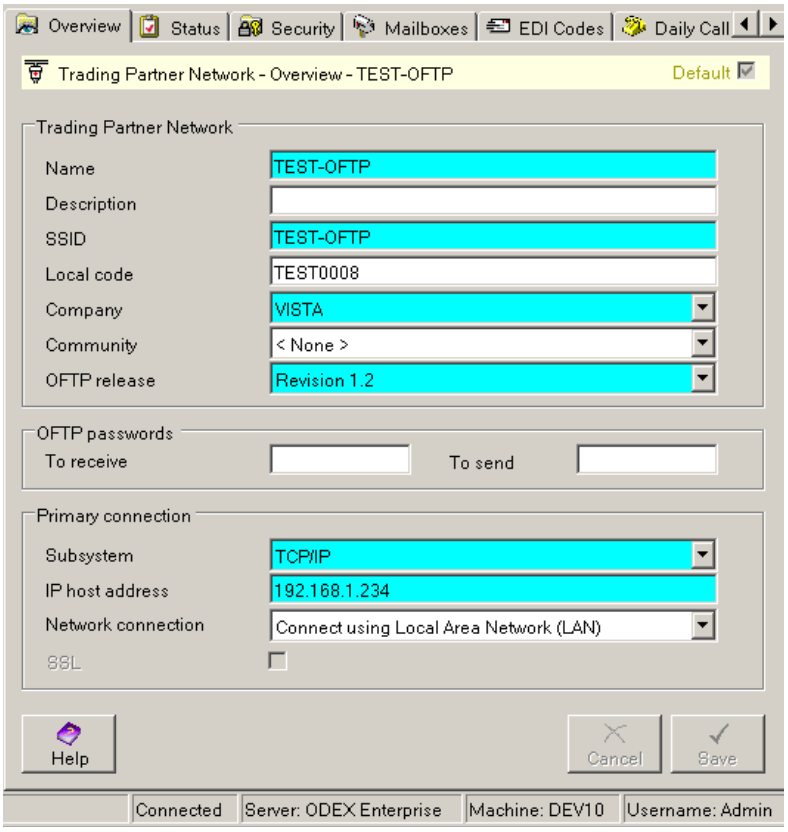
OFTP Network (Trading Partner or Clearing Centre) – Overview

The Overview page requires you to provide mandatory information about the way yoqu are going to communicate with your trading partners or clearing centres.

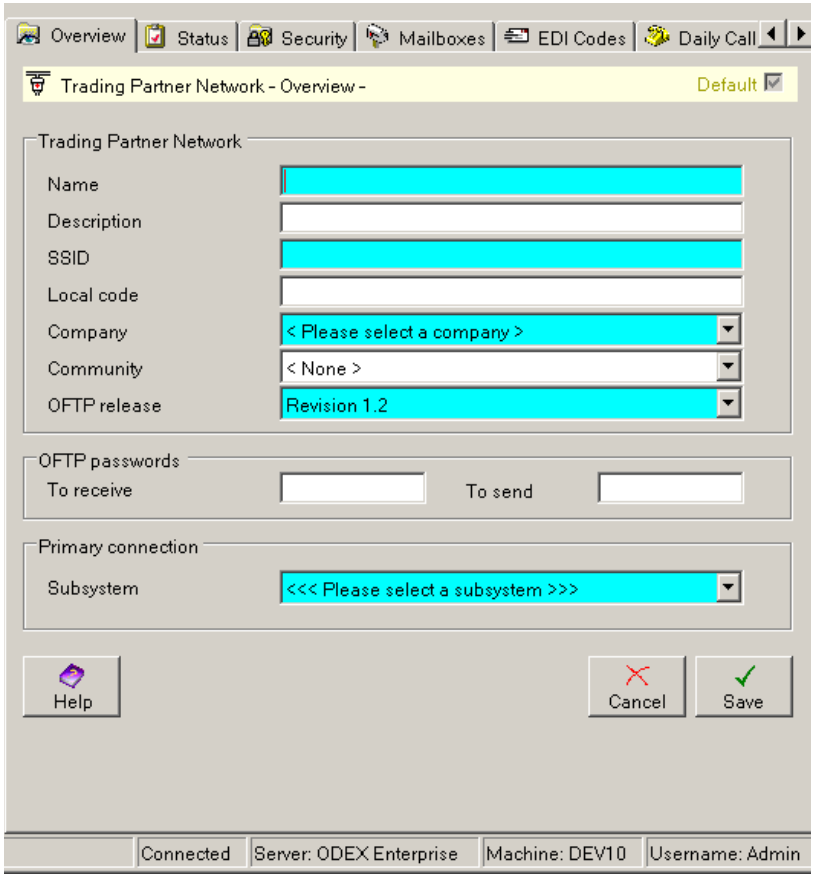
There is one extra piece of information that is required for a trading partner network but not for a clearing centre network. The field where you insert this information is shown on the example page below.

Because ODEX already has a TCP/IP subsystem set up for you, the Overview page will initially look like the example below, where the single subsystem has already been selected.

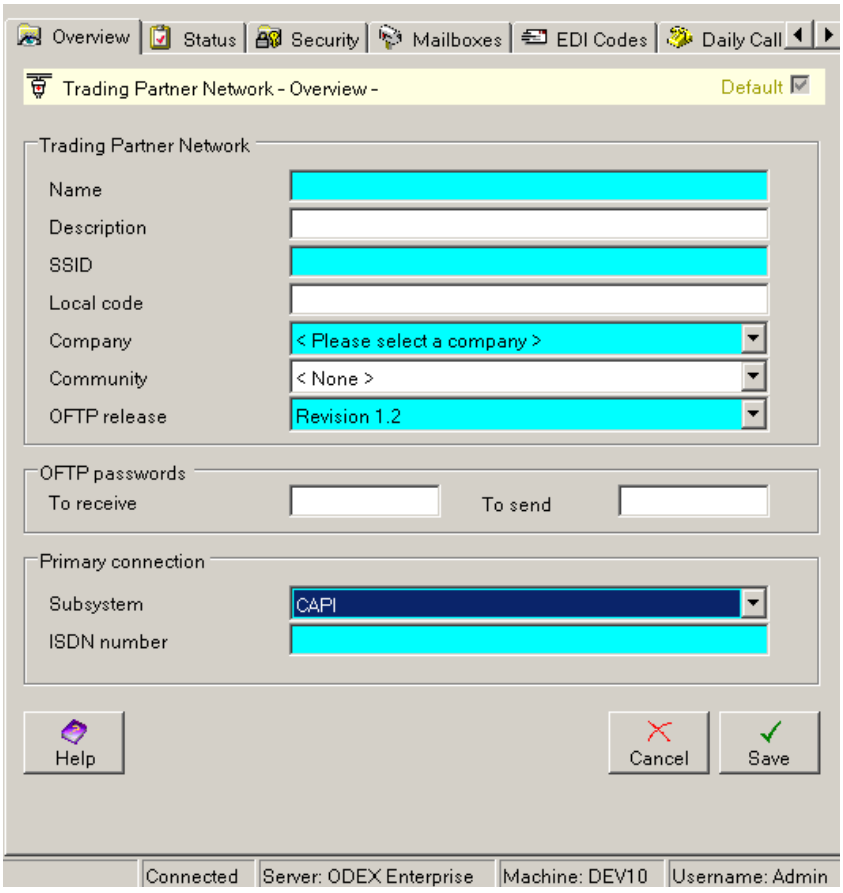
There are three sections on this page: Trading Partner Network (or Clearing Centre), OFTP passwords and Primary connection.



Once you have added further subsystems to the Comms section, ODEX will allow you to choose which subsystem to use for this network, and the Overview page will look like the one shown below.



Once you have selected a subsystem at the bottom of the page, more fields will be revealed in the Primary connection section, as shown in the example below. Please note that the fields shown may differ, according to which subsystem you choose.



Network – Name

Type in this field a name for the network. This name will only be used within ODEX, so you can use any name that will help you recognise which network this is.

Network – Description

You may give a brief description of the network in this field if you wish. You can repeat the name of the network if you like, or include any other information that helps you to recognise it.

Network – SSID

This field requires the SSID of the network. If you do not type it in correctly, your messages will not reach their intended destination.

Network – Local code

This field is provided for compatibility with the systems of users who have upgraded from ODEX Professional and who wish to use the Batch Interface. Other users should ignore it.

The local code is simply a unique code designated by you and used to identify the company in a shorthand form, instead of having to remember their EDI code. It is a code internally used by ODEX and will never be seen by your trading partners.

Network – Company

This field will only be present for Trading Partner Networks, not for Clearing Centre Networks.

Since you are choosing to communicate directly with your trading partner, you must select the appropriate company from the dropdown list in this field.

Network – Community

This field will only be visible if you are using communities and you are logged on as a user that is a member of multiple communities or a user that is not a member of any communities, e.g. the admin user.

If you are using communities and you are logged on as a user that is a member of one community, the field is hidden because the network will be created and associated with your community automatically.

Select a community if you wish to associate this network with a community. The network and any data associated with it will then only be visible to users that are a member of the selected community, users that are a member of a group that is a member of the selected community and users that are not a member of any communities, such as the admin user.

Network – OFTP release

This field allows you to select the highest OFTP protocol release that ODEX will use when communicating with this trading partner. Select OFTP revision 2 to enable OFTP 2 features such as security and advanced compression. These features are disabled when a revision level before OFTP revision 2 is selected.

If the trading partner does not support the selected OFTP release level, a lower release level, supported by both ODEX and the trading partner should automatically be used. However some companies run implementations of the OFTP protocol that are not compliant with the standard in all respects. In

particular they do not negotiate the protocol release level correctly and communication sessions soon fail.

The OFTP standard says that the protocol release level should be negotiated down to the lowest level that both communicating parties support. ODEX supports revision 2 and all earlier revisions of the protocol. If ODEX is configured to use OFTP revision 2 when communicating with a trading partner, ODEX will say 'I want to use revision 2' when calling that trading partner. If the trading partner only supports a lower revision (for example revision 1.2) it should respond with 'but I want to use revision 1.2' and both parties proceed using only features defined for revision 1.2 of the protocol.

Some implementations, wrongly, just echo the release level they are sent even though they may not be able to support that level. ODEX proceeds using higher level features, the trading partner's software can't handle them and communication fails.

The value set here is the highest protocol level ODEX will attempt to use when communicating with this trading partner. If the trading partner negotiates correctly, communications proceed. If communications fail, try setting a lower value and retrying, until communications succeed.

OFTP Passwords – To receive

If this trading partner or clearing centre uses OFTP passwords, you must provide in this field the password that you will receive.

OFTP Passwords – To send

If this trading partner or clearing centre uses OFTP passwords, you must provide in this field the password that you will send.

Primary connection – Subsystem

Use the dropdown list to select the appropriate subsystem for this network.

Primary connection – IP host address

This field will only be present if you select TCP/IP as your subsystem in the Subsystem field.

Here you must provide the IP host address of the trading partner or clearing centre. You should have been informed of this address when you exchanged communications details with the trading partner or clearing centre.

Primary connection – Network connection

This field will only be present if you select TCP/IP as your subsystem in the Subsystem field.

Select the appropriate option using the dropdown list in this field.

The number of options in this field will depend on whether you have the ability to connect to the Internet from your computer using a modem. If you do not have this ability, there will only be one choice available to you:

- Connect using Local Area Network (LAN).

If you have a modem, and have configured dial-up networking connections (to trading partners or to the Internet) there will be additional entries for each dial-up connection configured.

Primary connection – Use SSL

This field will only be present if you select TCP/IP as your subsystem in the Subsystem field. Select this option if your trading partner requires you to connect using SSL (Secure Socket Layer).

SSL may only be used when communicating using OFTP revision 2. If you select an OFTP release level that is lower than revision 2, the SSL checkbox will not be available.

Primary connection – ISDN Number

This field will only be present if you select a local or remote CAPI subsystem in the Subsystem field.

Type the ISDN number of your trading partner or clearing centre in this field.

Primary connection – Remote X.25 NUA

This field will only be present if you select an XOT subsystem in the Subsystem field.

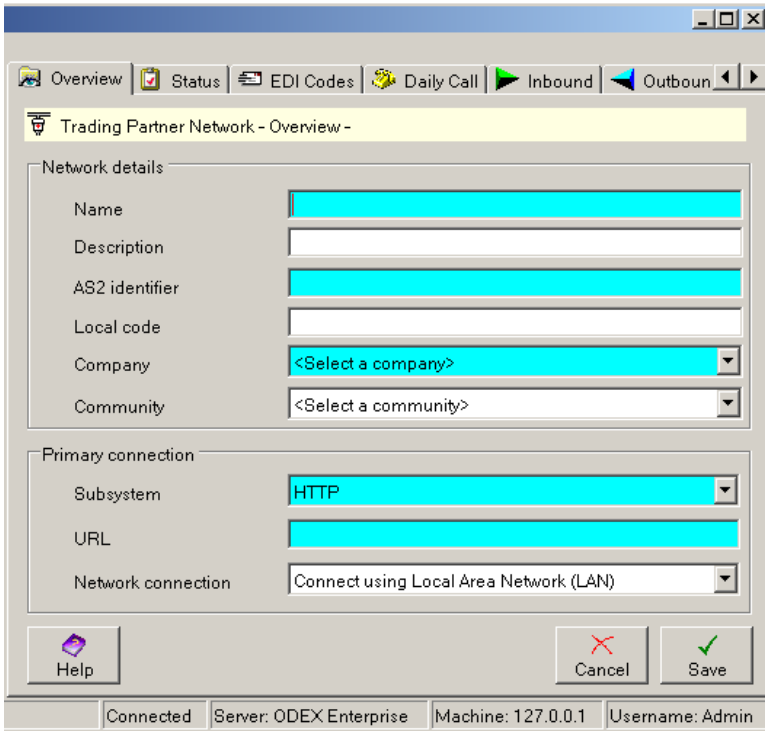
Type the X.25 NUA of your trading partner or clearing centre in this field.

AS2 Network (Trading Partner or Clearing Centre) – Overview

The Overview page requires you to provide mandatory information about the way you are going to communicate with your trading partners or clearing centres.

There is one extra piece of information that is required for a trading partner network but not for a clearing centre network. The field where you insert this information is shown on the example page below.

There are two sections on this page: Network details and Primary connection.



Network – Name

Type in this field a name for the AS2 network. This name will only be used within ODEX, so you can use any name that will help you recognise which network this is.

Network – Description

You may give a brief description of the network in this field if you wish. You can repeat the name of the network if you like, or include any other information that helps you to recognise it.

Network – AS2 identifier

This field requires the AS2 identifier of the network. If you do not type it in correctly, your messages will not reach their intended destination.

Network – Local code

This field is provided for compatibility with the systems of users who have upgraded from ODEX Professional and who wish to use the Batch Interface. Other users should ignore it.

The local code is simply a unique code designated by you and used to identify the company in a shorthand form, instead of having to remember their EDI code. It is a code internally used by ODEX and will never be seen by your trading partners.

Network – Community

This field will only be visible if you are using communities and you are logged on as a user that is a member of multiple communities or a user that is not a member of any communities, e.g. the admin user.

If you are using communities and you are logged on as a user that is a member of one community, the field is hidden because the network will be created and associated with your community automatically.

Select a community if you wish to associate this network with a community. The network and any data associated with it will then only be visible to users that are a member of the selected community, users that are a member of a group that is a member of the selected community and users that are not a member of any communities, such as the admin user.

Network – Company

This field will only be present for Trading Partner Networks, not for Clearing Centre Networks. Since you are choosing to communicate directly with your trading partner, you must select the appropriate company from the dropdown list in this field.

Primary connection – Subsystem

You will only be shown subsystems that are appropriate for an AS2 network i.e. HTTP subsystems.

Primary connection – URL

Here you must provide the URL of the trading partner or clearing centre. You should have been given this when you exchanged communications details with the trading partner or clearing centre.

Primary connection – Network connection

Select the appropriate option using the dropdown list in this field.

The number of options in this field will depend on whether you have the ability to connect to the Internet from your computer using a modem. If you do not have this ability, there will only be one choice available to you:

- Connect using Local Area Network (LAN).

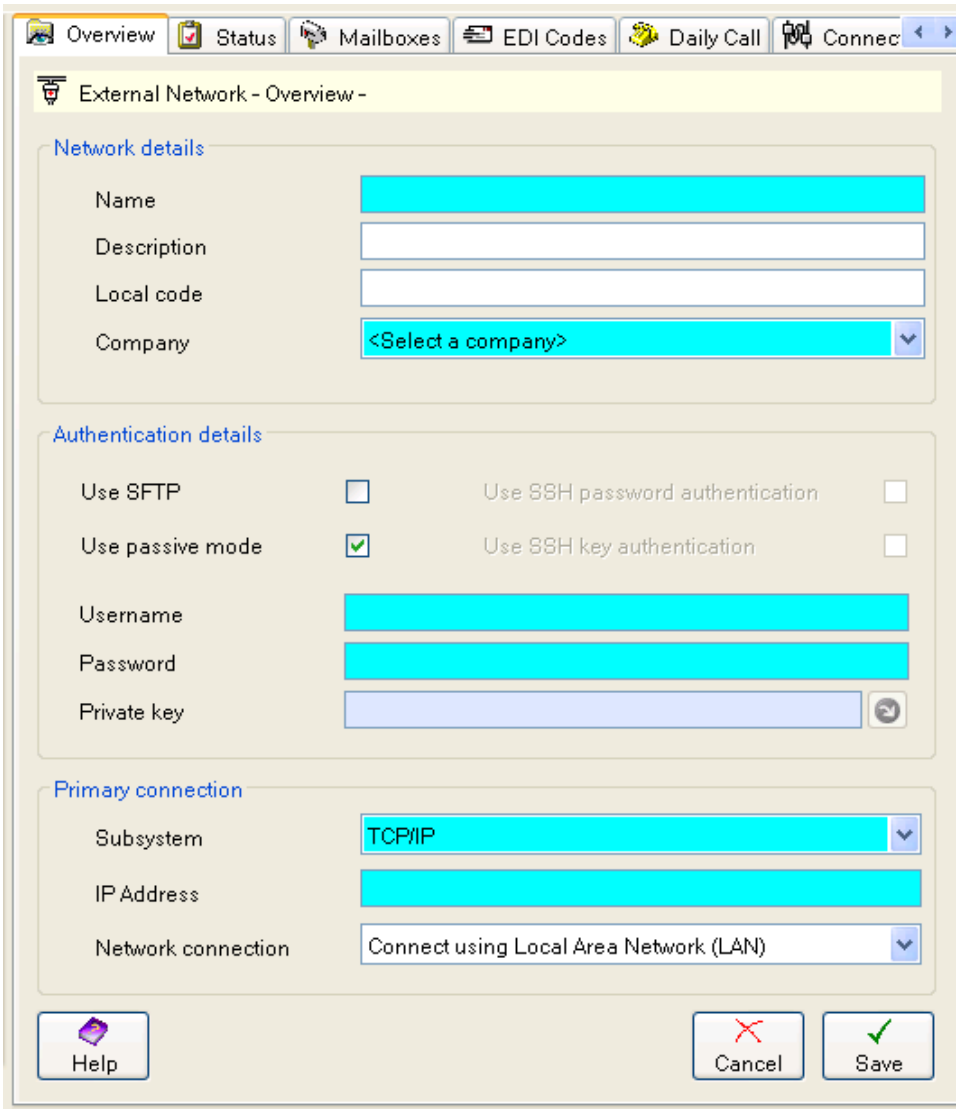
If you have a modem, and have configured dial-up networking connections (to trading partners or to the Internet) there will be additional entries for each dial-up connection configured.

FTP client Network (Trading Partner or Clearing Centre) – Overview

The Overview page requires you to provide mandatory information about the way you are going to communicate with your trading partners or clearing centres.

The only difference between trading partner and clearing centre is that a clearing centre does not have a company selection.

There are three sections on this page: Network Details, Authentication Details and Primary connection.



Network details – Name

Type in this field a name for the network. This name will only be used within ODEX, so you can use any name that will help you recognise which network this is.

Network details – Description

You may give a brief description of the network in this field if you wish. You can repeat the name of the network if you like, or include any other information that helps you to recognise it.

Network details – Local code

This field is provided for compatibility with the systems of users who have upgraded from ODEX Professional and who wish to use the Batch Interface. Other users should ignore it.

The local code is simply a unique code designated by you and used to identify the company in a shorthand form, instead of having to remember their EDI code. It is a code internally used by ODEX and will never be seen by your trading partners.

Network details – Company

This field will only be present for Trading Partner Networks, not for Clearing Centre Networks.

Since you are choosing to communicate directly with your trading partner, you must select the appropriate company from the dropdown list in this field.

Network – Community

This field will only be visible if you are using communities and you are logged on as a user that is a member of multiple communities or a user that is not a member of any communities, e.g. the admin user.

If you are using communities and you are logged on as a user that is a member of one community, the field is hidden because the network will be created and associated with your community automatically.

Select a community if you wish to associate this network with a community. The network and any data associated with it will then only be visible to users that are a member of the selected community, users that are a member of a group that is a member of the selected community and users that are not a member of any communities, such as the admin user.

Authentication Details – Use SFTP

If the FTP server you are connecting to uses SFTP, rather than FTP then check this box. If you do not know, then leave this checkbox unchecked.

By checking this box, the SSH authentication checkboxes become enabled, allowing you to select the type of connection you wish to use (Password or Private Key). The type of authentication will depend on the SFTP server you are connecting to.

Authentication Details – Use SSH Password Authentication

Password authentication requires a username and password to be specified. These details must match those expected by the SFTP server otherwise the connection will be refused.

Password authentication is more commonly used, but is more susceptible to attack as the password is easier to hack than Key authentication.

Checking this box enables the Password textbox.

Authentication Details – Use SSH Key Authentication

Private Key authentication requires a username to be used in conjunction with a public/private key pair. The private key is yours to use and the SFTP server you

are connecting to must have a copy of your public key in order to authenticate the user.

A pair of public/private keys may be generated using a bespoke application such as the “PuTTY Key Generator”.

Checking this box enables the Private Key controls.

Authentication Details – Use Passive Mode

In almost all cases it will not be necessary to change this option.

The FTP client initially attempts to use passive mode and if this is unsupported it uses the normal mode for transfer. However, in rare cases it may be required to not attempt to connect in passive mode, in which case this checkbox can be unchecked and the FTP client will not attempt to use any passive mode transfer.

A full explanation of passive mode is given in the advanced FTP explanation in the Odex Concepts section of this manual.

This option is always enabled when using SFTP.

Authentication Details – Username

To start an FTP session you must first log in to your trading partner or clearing centre In this field enter the user name your trading partner/clearing centre has given you to access his system.

Authentication Details – Password

In this field, enter the password that allows the user name above access to your trading partner/clearing centre.

Authentication Details – Private Key

This field lets you specify your Private Key to be used for key authentication. To add or change your private key, click the button to the side of the textbox.

Primary connection – Subsystem

Since FTP is an Internet protocol, you will only be presented with TCP/IP.

Primary connection – IP address

Here you must provide the IP host address of the trading partner or clearing centre. You should have been informed of this address when you exchanged communications details with the trading partner or clearing centre.

Primary connection – Network connection

Select the appropriate option using the dropdown list in this field.

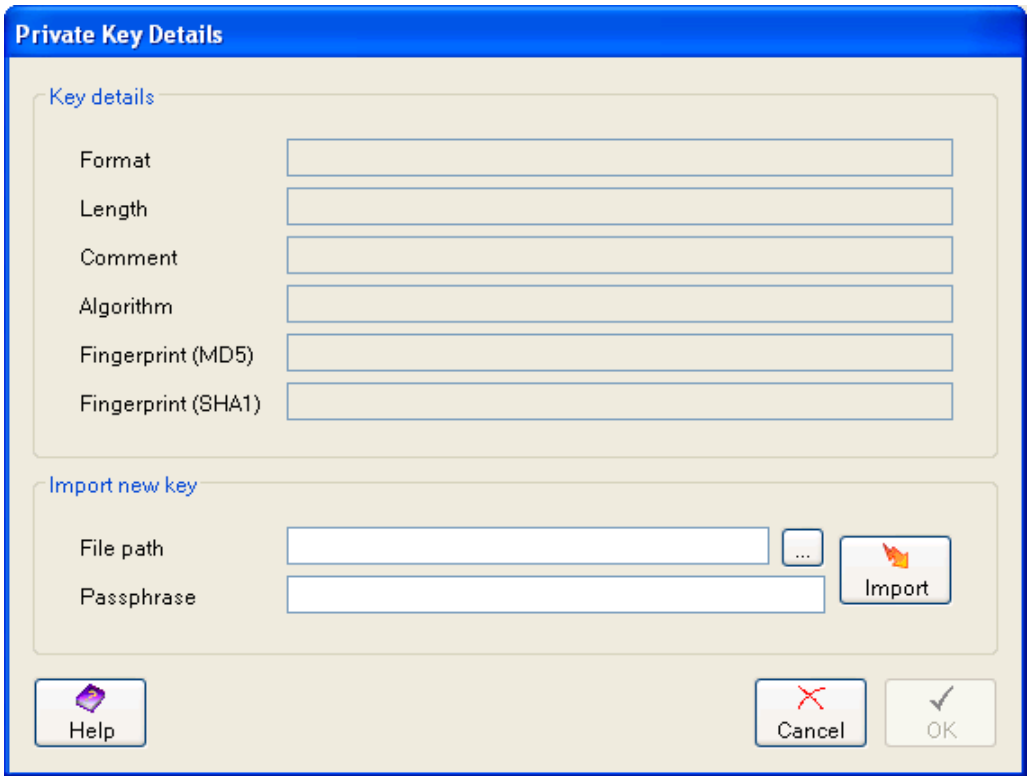
The number of options in this field will depend on whether you have the ability to connect to the Internet from your computer using a modem. If you do not have this ability, there will only be one choice available to you:

- Connect using Local Area Network (LAN).

If you have a modem, and have configured dial-up networking connections (to trading partners or to the Internet) there will be additional entries for each dial-up connection configured.

Adding a Private Key

Private keys used by SSH FTP (SFTP) connections are loaded using the following dialog,



This dialog is split into two sections, Key Details and Import New Key.

Key Details

This section displays information regarding the current private key. These fields are read only and cannot be altered by the user.

Import New Key

This section lets you import a private key from a file on disk. In order to perform the import, you must provide the full path to the location of the private key file on disk and specify the passphrase associated with this private key (if applicable).

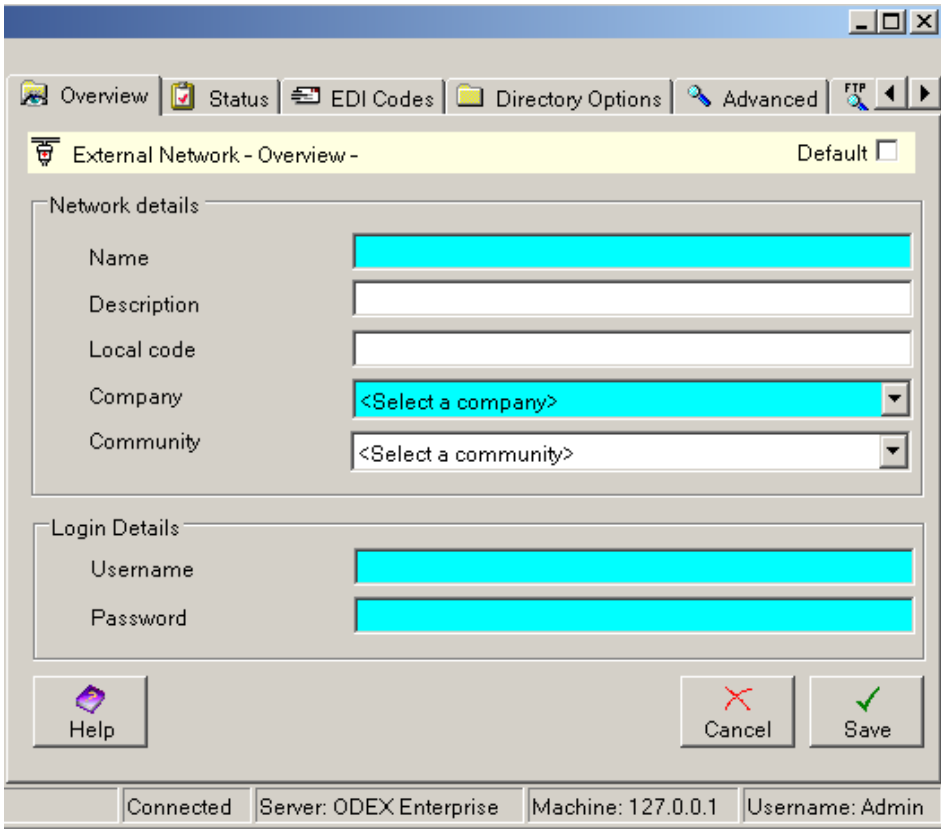
Once these details have been provided, press the Import button to load the details of the private key. If successful, the Key Details section will show information regarding the private key and the OK button will become enabled.

FTP server Network (Trading Partner or Clearing Centre) – Overview

The Overview page requires you to provide mandatory information about the way you are going to communicate with your trading partners or clearing centres.

The only difference between trading partner and clearing centre is that a clearing centre does not have a company selection.

There are only two sections on this page: Network Details and Login Details.



Network details – Name

Type in this field a name for the network. This name will only be used within ODEX, so you can use any name that will help you recognise which network this is.

Network details – Description

You may give a brief description of the network in this field if you wish. You can repeat the name of the network if you like, or include any other information that helps you to recognise it.

Network details – Local code

This field is provided for compatibility with the systems of users who have upgraded from ODEX Professional and who wish to use the Batch Interface. Other users should ignore it.

The local code is simply a unique code designated by you and used to identify the company in a shorthand form, instead of having to remember their EDI code. It is a code internally used by ODEX and will never be seen by your trading partners.

Network details – Company

This field will only be present for Trading Partner Networks, not for Clearing Centre Networks.

Since you are choosing to communicate directly with your trading partner, you must select the appropriate company from the dropdown list in this field.

Network details – Community

This field will only be visible if you are using communities and you are logged on as a user that is a member of multiple communities or a user that is not a member of any communities.

If you are using communities and you are logged on as a user that is a member of one community, the field is hidden because the network will be created and associated with your community automatically.

Select a community if you wish to associate this company with a community. The network and any associated data will then only be visible to users that are a member of the selected community, users that are a member of a group that is a member of the selected community and users that are not a member of any communities, such as the admin user.

Login Details – Username

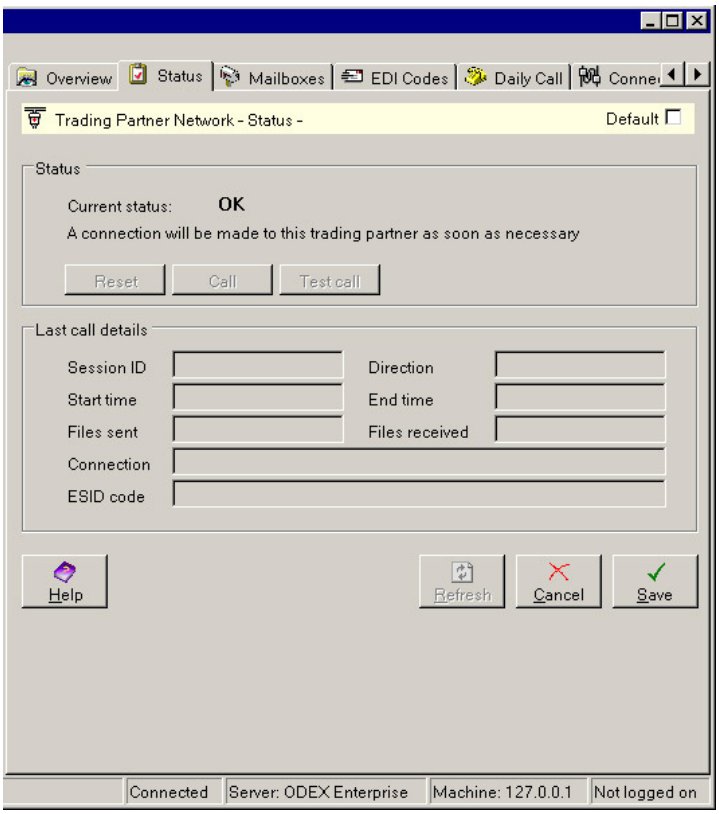
In order for an external trading partner to log into the ODEX FTP server, they require a username and password. This username and password will uniquely identify this network when a user connects to the ODEX FTP server. So the user using this username and the password will have access to all files sent to this network.

Login Details – Password

This is the password for the user to log on to the ODEX FTP server.

Network – Status

The Status page looks like the example below.



If no attempts have yet been made to connect to this network, the Status page will contain no information and most of the buttons will be disabled, as shown in the example above.

Once a connection has been attempted, the fields will be populated and you will be able to use the **Reset**, **Call**, **Test call** and **Refresh** buttons.

Status – Current status

The current status of the network is displayed here. Possible values are:

- OK – the network is OK and will make a call when necessary
- In retry – the network is currently retrying using its primary connection
- In retry with non-primary connection – the network is currently retrying using a non-primary connection
- Failed – the network has failed to connect using any connections

Status – Reset

This button resets the number of attempted calls (retries) to this trading partner or clearing centre to zero. ODEX will not make any further attempts to call a trading partner or clearing centre once the maximum number of retries has been reached. Therefore the **Reset** button allows ODEX to start calling again.

Status – Call

This button initiates a single immediate call to the trading partner or clearing centre, whether the maximum number of retries has been reached or not. It does not reset the number of attempted calls. If the connection is successful, data will be sent and received in the usual way.

Status – Test call

This button initiates a single immediate call to the trading partner or clearing centre, but does not send any data. However, for an OFTP network, your partner may send data back to you.

Last call details – Session ID

This field contains the unique session ID of the last communication session with this trading partner or clearing centre.

Last call details – Direction

This field contains the direction of the last communication session with this trading partner or clearing centre (Incoming or Outgoing).

Last call details – Start time

This field contains the time of the last connection attempt.

Last call details – End time

This field contains either the time the session ended (for overall success) or the time the last connection failed (for overall failure).

Last call details – Files sent

This field contains the number of files that you sent in the given session.

Last call details – Files received

This field contains the number of files that you received in the given session.

Last call details – Connection

This field contains the name of the connection it last tried with.

Last call details – ESID code (OFTP only)

This field will not be present if you are adding or editing an AS2 or FTP network.

This field contains the ESID code of the last connection. This is a 2-digit code that indicates whether the session completed successfully or not. A code of 00 means that it was successful. Any other value indicates an error. Meanings of error codes can be found in an OFTP protocol reference guide.

Last call details – Result (AS2 and FTP client only)

This field will not be present if you are adding or editing an OFTP network.

This field contains a brief description of the result of your last connection to this network.

Refresh

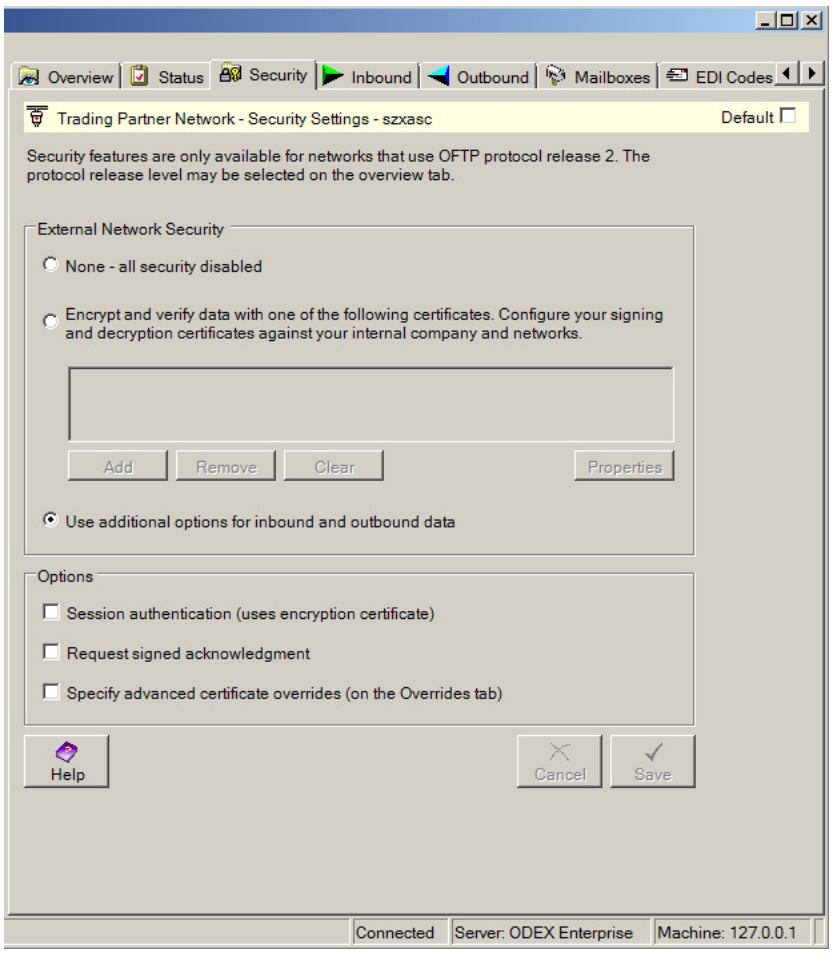
This button refreshes the information in the Last Call Details section.

Network – Security

The Security page is only applicable to OFTP networks that are configured to use OFTP 2. For networks that are configured to use an earlier release level, the security options will be disabled.

You need to enter data on the Security page only if you want to use signing and encryption when exchanging files with this trading partner.

The Security page looks like the example below.



This page is where you specify the public key certificate (if any) that will be used to encrypt data you send to this trading partner and to verify the signature on data you receive from this trading partner.

These settings will be used by all the mailboxes defined against this network. You can, however, choose different settings for any mailbox on the Inbound and Outbound pages of the mailbox.

You are required to configure the details of security to be used. This is not a matter of choice – the configuration must reflect the security arrangement you have agreed with your trading partner. For a fuller explanation of encryption,

decryption, signatures, certificates and public and private keys, please refer to 'Data Security'.

External Network Security

Select "None – all security disabled" if you do not want to send signed and encrypted data to this trading partner and you are not expecting to receive signed and encrypted data in return.

If you do want to sign and encrypt data you send to the trading partner, your trading partner will send you signed and encrypted data, and the trading partner has provided you with a single public certificate, select "Encrypt and verify data with one of the following certificates". Action buttons are enabled for you to choose the certificate(s) to use. See the section entitled 'Dynamic Certificate Selection'.

Note that in this simple case, the specified certificate is used for encrypting data you send to the trading partner and verifying data you receive from the trading partner. You will sign data with the certificate specified against your internal network or mailbox, and decrypt received data with any appropriate internal certificate.

For any scenario that differs from the simple case described above, you will want to select "Use additional options for inbound and outbound data" to open up two additional pages, Inbound and Outbound, where you can indicate the different ways that received and sent data are to be processed.

Options - The Options tick boxes are enabled only if you have selected to use external network security.

The "Session authentication (uses encryption certificate)" tick box should be checked if OFTP session authentication is to be used to confirm the identity of the trading partner. In a standard scenario, this uses your decryption certificates and the trading partner's specified encryption certificate, however this may be overridden.

The "Request signed acknowledgment" tick box should be checked if you would like to receive signed OFTP EERP acknowledgments for files you send to this trading partner. Signing confirms that the file has definitely been received by the intended recipient.

The "Specify advanced certificate overrides" tick box should be checked if you want to override the certificates used for EERP signing (default uses file signing) and session authentication (default uses file encryption). This opens up an additional page, Overrides, where you can specify the certificate overrides.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

If you want to discard all the changes you have made, click the **Cancel** button.

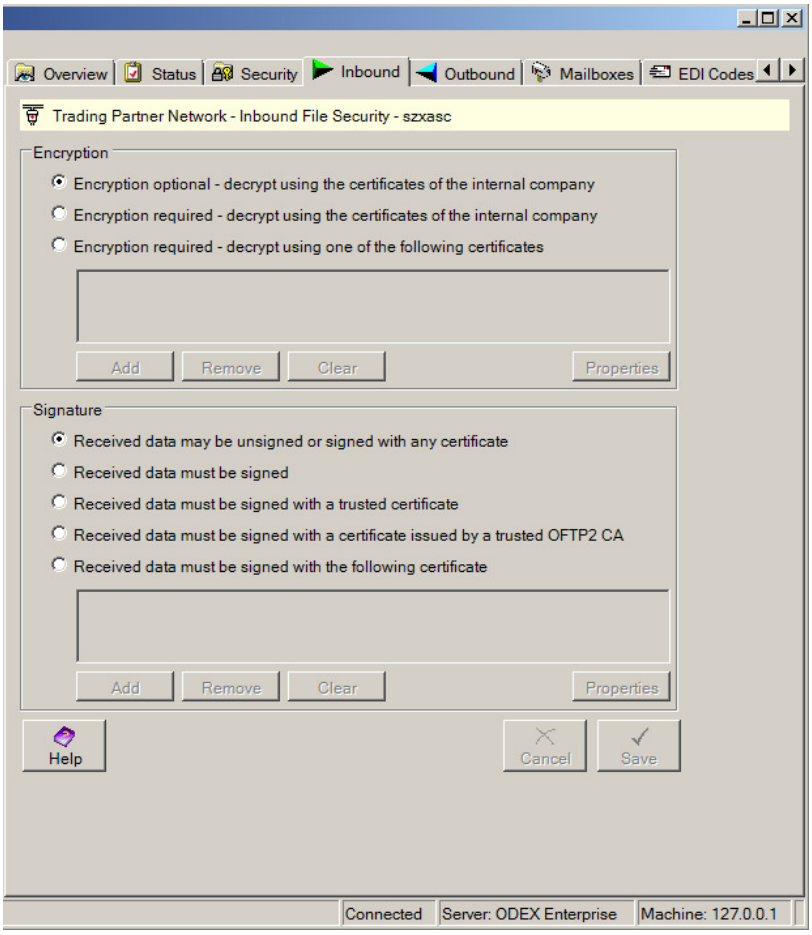
Save

To save any changes you have made in the Security section, click the **Save** button.

Network – Inbound (OFTP)

The OFTP Inbound page is only visible on OFTP networks that are configured to use OFTP 2 with additional options. For networks that are configured to use an earlier release level or simpler security configuration, this page is hidden.

The Inbound page looks like the example below.



The two areas of security are encryption and signatures. You are required to configure the details of security to be used. This is not a matter of choice – the configuration must reflect the security arrangement you have agreed with your trading partner.

Encryption - The Encryption section is where you specify the private key certificate(s) that will be used to decrypt data sent to you by your trading partner. These certificates are considered as belonging to you and thus will be configured against your internal companies.

Select the appropriate radio button. Each button specifies whether encryption is optional or required for this network.

If encryption is required, you can either decrypt your trading partner's files using any of your internal certificates, or you can select specific certificate(s) to use. Action buttons are enabled; see the section entitled 'Dynamic Certificate Selection'.

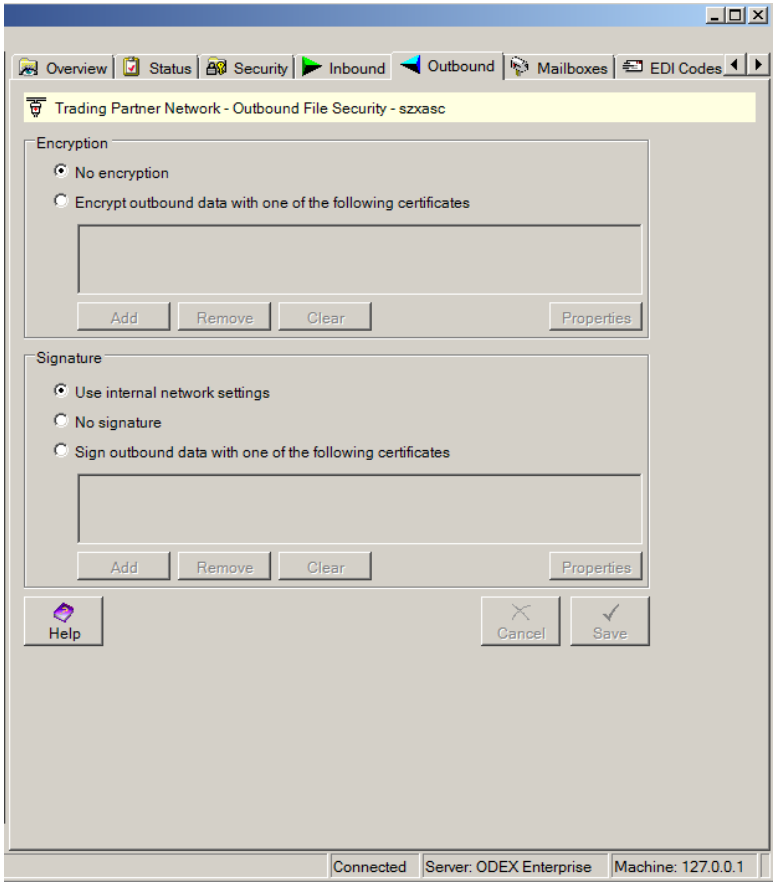
Signature - The Signature section is used to specify whether you require inbound data to be signed, and if so how (possibly including the specification of a trading partner's public key certificate). The certificates used for verification are considered as belonging to and thus provided by the trading partner.

Select the appropriate radio button. The options are all self-explanatory. If you choose a specific certificate, action buttons are enabled, which are explained in the section entitled ‘Dynamic Certificate Selection’.

Network – Outbound (OFTP)

The OFTP Outbound page is only visible on OFTP networks that are configured to use OFTP 2 with additional options. For networks that are configured to use an earlier release level or simpler security configuration, this page is hidden.

The Outbound page looks like the example below.



The two areas of security are encryption and signature. You are required to configure the details of security to be used. This is not a matter of choice – the configuration must reflect the security arrangement you have agreed with your trading partner.

Encryption - The Encryption section is where you specify the public key certificate(s) to use when sending encrypted data to your trading partner. These certificates are considered as belonging to and thus provided by the trading partner.

Select the appropriate radio button. No encryption means that your trading partner does not expect you to encrypt data you send to him.

If you choose to encrypt data, action buttons are enabled, which are explained in the section entitled ‘Dynamic Certificate Selection’.

Signature - The Signature section is where you specify the private key certificate(s) to use when signing data you are sending to your trading partner. These certificates are considered as belonging to your internal companies.

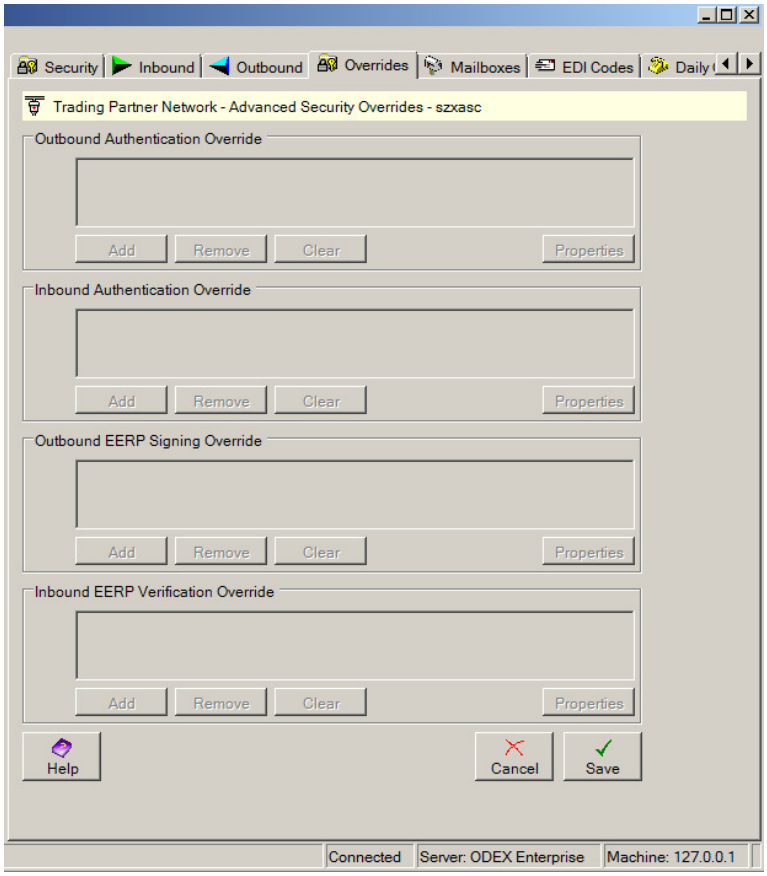
Select the appropriate radio button. No signature means that your trading partner does not expect you to sign your data.

If you choose to sign data, you can either sign using the certificate configured against your internal network, or you can select a different certificate. Action buttons are enabled, which are explained in the section entitled ‘Dynamic Certificate Selection’.

Network – Overrides (OFTP)

The OFTP Overrides page is only visible on OFTP networks that are configured to use OFTP 2 with additional options and advanced overrides. For networks that are configured to use an earlier release level or simpler security configuration, this page is hidden.

The Overrides page looks like the example below.



This page presents a list of certificates for overriding inbound and outbound authentication and EERP signing certificates.

By default, EERP signing will use the configured file signing and verification certificates, whilst session authorisation will use the configured encryption and decryption certificates.

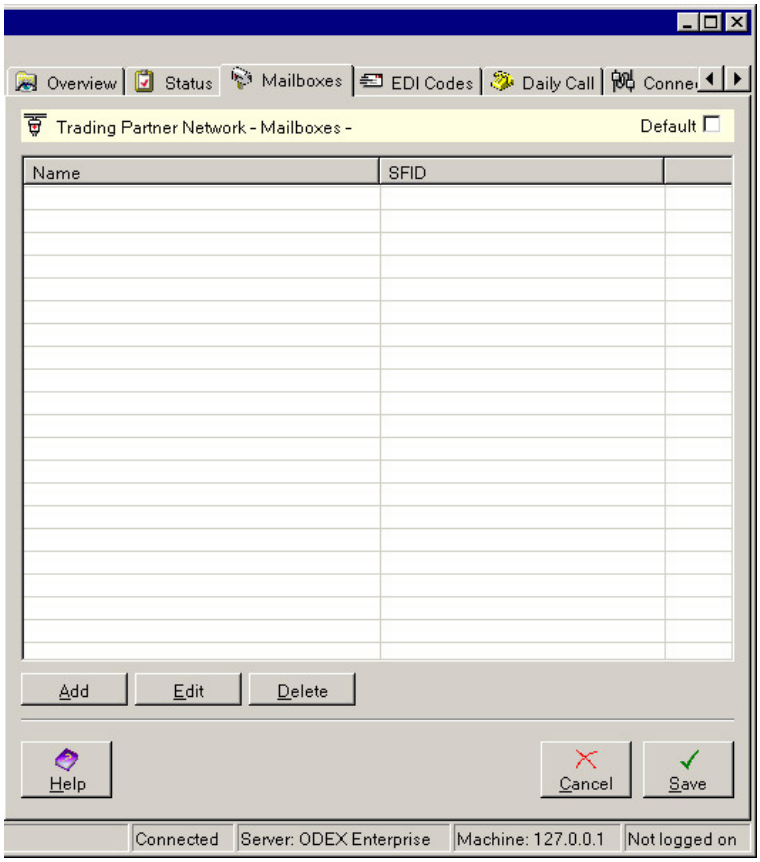
To override any of the 4 cases, use the relevant action buttons as explained in the section entitled ‘Dynamic Certificate Selection’.

Note that you will only be allowed to override those cases for which a specific default certificate has already been defined on the Inbound and Outbound pages.

Network – Mailboxes

The Mailboxes page is only applicable to OFTP and FTP client networks. It will not be present for AS2 networks.

The Mailboxes page looks like the example below.



This page displays a list of existing mailboxes for this network.

Use the **Add**, **Edit** and **Delete** buttons to add new mailboxes, and edit and delete existing mailboxes.

> *For OFTP networks, if your SSID and SFID (mailbox) for this network are both the same, you do not need to add a mailbox for the new network, since it will be created automatically when you click the **Save** button.*

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

If you want to discard all the changes you have made, click the **Cancel** button.

Save

To save any changes you have made in the Mailboxes section, click the **Save** button.

Mailboxes – Add/Edit

Use the **Add** button or **Edit** button to add or edit a mailbox for this network

Mailboxes – Delete

To delete an entry from the list on the Mailboxes page, select the line you want to delete and click the **Delete** button. You will see a message box asking if you are sure you want to delete the selected mailbox. Click **Yes** to delete the mailbox, or **No** to keep the mailbox in the list.

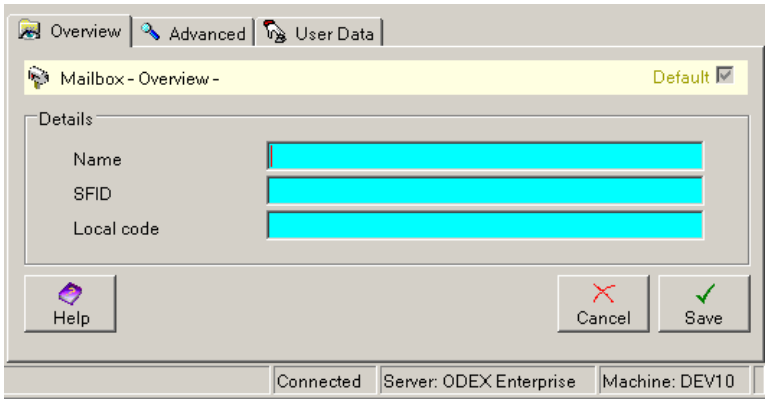
Mailbox pages differ depending on whether they are for an OFTP network or an FTP client network.

OFTP Mailbox

There are five pages associated with an external OFTP mailbox, so let's go through them and find out what information is required. The User Data page is described in the section entitled 'User Data'.

OFTP Mailbox – Overview

The Overview page is where mandatory information has to be provided for each new external OFTP mailbox. The Overview page looks like the example below.



Details – Name

Type in here a name for the mailbox. This is just for your own use within ODEX.

Details – SFID

Type in here the SFID of the mailbox.

Details – Local code

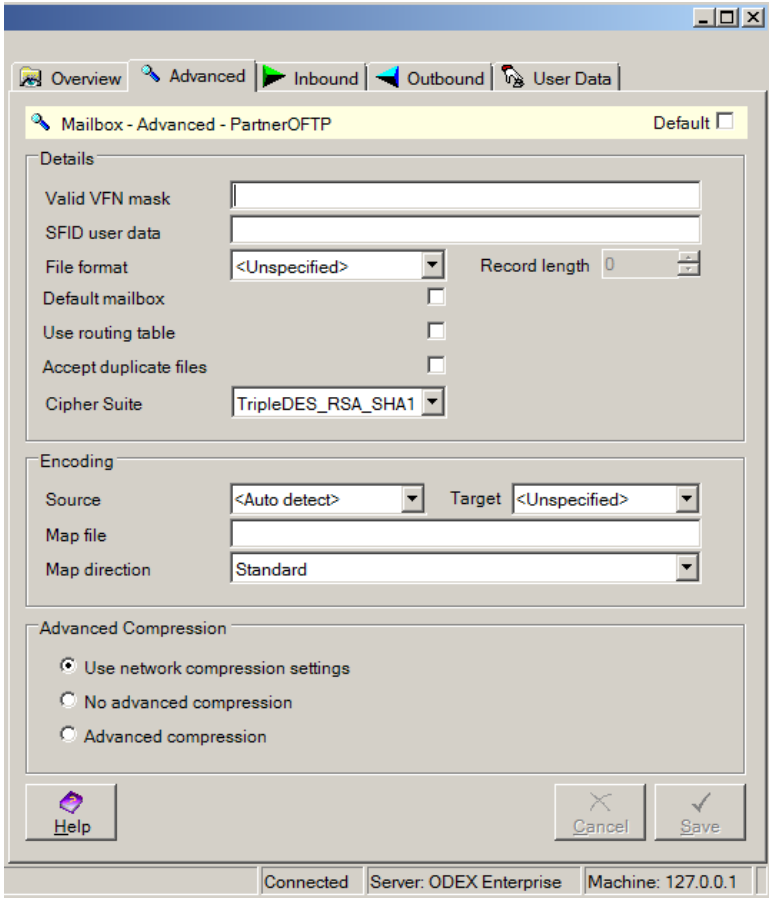
This field is provided for compatibility with the systems of users who have upgraded from ODEX Professional and who wish to use the Batch Interface. Other users should ignore it.

The local code is simply a unique code designated by you and used to identify the company in a shorthand form, instead of having to remember their EDI code. It is a code internally used by ODEX and will never be seen by your trading partners.

If the network specifies "Use additional options for inbound and outbound data" the Inbound and Outbound pages display.

OFTP Mailbox – Advanced

The advanced page contains optional settings that may be changed by advanced users.



Details – Valid VFN Mask

This field allows you to provide a VFN (virtual filename) mask to be matched against files received from this trading partner network. If the VFN of the received file does not match the mask, the file will be rejected.

N.B. Any VFN mask you specify here will override the VFN you specify on the Advanced (OFTP) page for this network.

You may use the asterisk character (*) to signify one or more unspecified characters. You may use the question mark character (?) to signify one unspecified character.

Taking the Ford VFN format as an example, you could use one of the following filename masks to achieve different results:

FORD.S* – accept all Ford files

FORD.SABC12* – accept all Ford messages for the Supplier code ABC12

FORD.S*RE – accept all Ford Release messages for any Supplier code

FORD.S?????ST – accept all Ford DCI messages for any Supplier code (five question marks are more precise than the asterisk but would have the same effect)

Details – SFID user data

Type in here the SFID user data, if applicable. If you are required to provide SFID user data, your trading partner using this mailbox should have informed you.

Details – File format

OFTP files can be sent as fixed record length format, variable record length format, text format or unformatted. When scheduling a file using the schedule

job, the file format may be specified on the schedule job. If the file format is specified on the mailbox to which the file is being scheduled, this file format will override the setting on the schedule file job.

Details – Record length

The record length only needs to be specified when sending a file as fixed format or variable format. For files with variable length records, this is the maximum record length.

Details – Default mailbox

This field allows you to specify that this is the default mailbox for the network. A default mailbox is a mailbox that will be used to receive files when the SFID associated with a received file does not match the SFID of any other mailbox defined on this network.

Details – Accept duplicate files

This allows you to specify that ODEX should accept files sent to this mailbox, regardless of whether another file has been received with the same virtual filename and virtual date/time. When the check box is not checked, ODEX will reject files with a duplicate virtual filename and virtual date/time.

Details – Use routing table

This field allows you to specify that when forwarding files received through this mailbox, the routing table must be used to route the file to its destination.

Details – Cipher Suite

This field allows you to specify the cipher suite to use in OFTP2 communications. Your choice affects the algorithm used for encryption, either TripleDES or AES.

Encoding

The encoding options allow you to specify that any files sent to the mailbox using the schedule file job will automatically have their encoding converted to the target encoding. To have the encoding converted automatically, select a target encoding from the list. You may optionally specify the source encoding, or have the encoding automatically detected.

An alternative method of converting the encoding is to specify a map file instead of a source and target encoding. A map file is a text file containing a mapping between each character in the source encoding and the target encoding. To use a map file, specify the name of the map file on the server machine.

For the encoding to be left unaltered, select ‘unspecified’ for the target encoding and leave the map file field blank.

Advanced Compression

OFTP advanced compression attempts to reduce the amount of data transmitted, potentially reducing call times and costs. “Use network compression settings” means use the value specified on the external network Advanced(OFTP) page field “Use advanced compression”. Check the appropriate tick box.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

If you want to discard all the changes you have made, click the **Cancel** button.

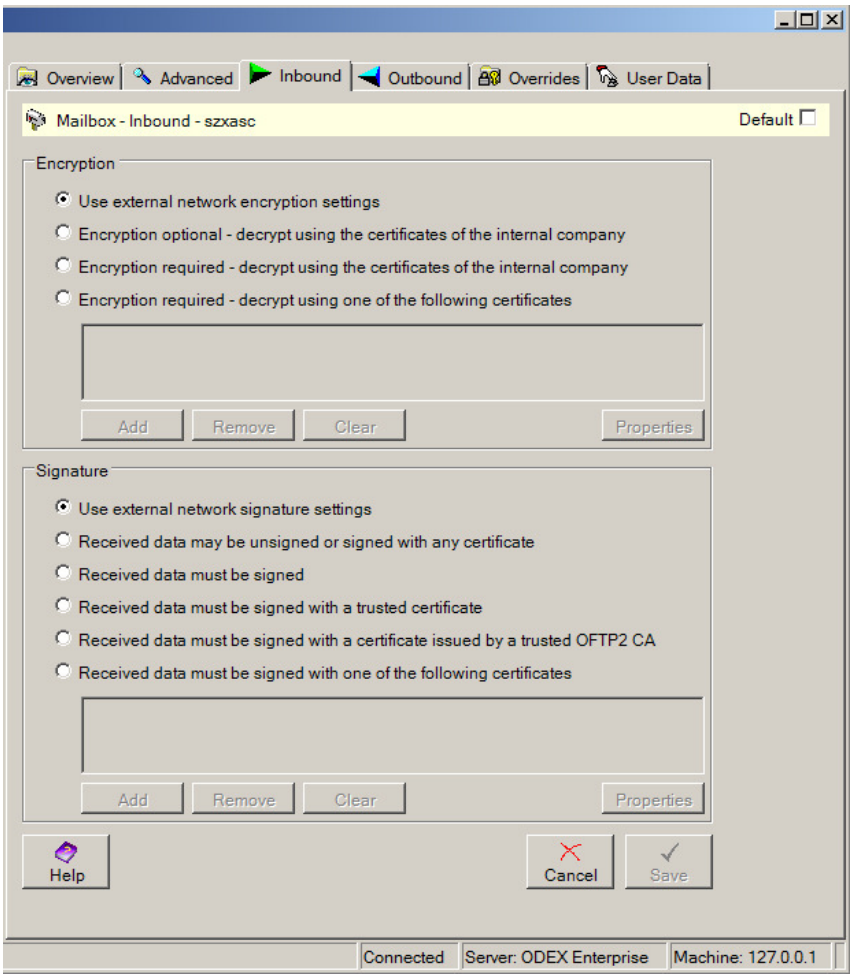
Save

To save details of the new mailbox, click the **Save** button.

OFTP Mailbox – Inbound

The Inbound page allows you to configure the Security Settings to be used for inbound data from this trading partner mailbox. These values override the settings at the network level.

The Inbound page looks like the example below.



The two areas of security are encryption and signatures. You are required to configure the details of security to be used. This is not a matter of choice – the configuration must reflect the security arrangement you have agreed with your trading partner.

Encryption

The Encryption section is where you specify the private key certificate(s) that will be used to decrypt data sent to you by your trading partner. These certificates are considered as belonging to you and thus will be configured against your internal companies.

Select the appropriate radio button. Each button specifies whether encryption is optional or required for this network.

“Use external network encryption settings” means the settings specified on the external network for inbound data decryption should be used.

If encryption is required, you can either decrypt your trading partner's files using any of your internal certificates, or you can select specific certificate(s) to use. Action buttons are enabled; see the section entitled 'Dynamic Certificate Selection'.

Signature

The Signature section is used to specify whether you require inbound data to be signed, and if so how (possibly including the specification of a trading partner's public key certificate). The certificates used for verification are considered as belonging to and thus provided by the trading partner.

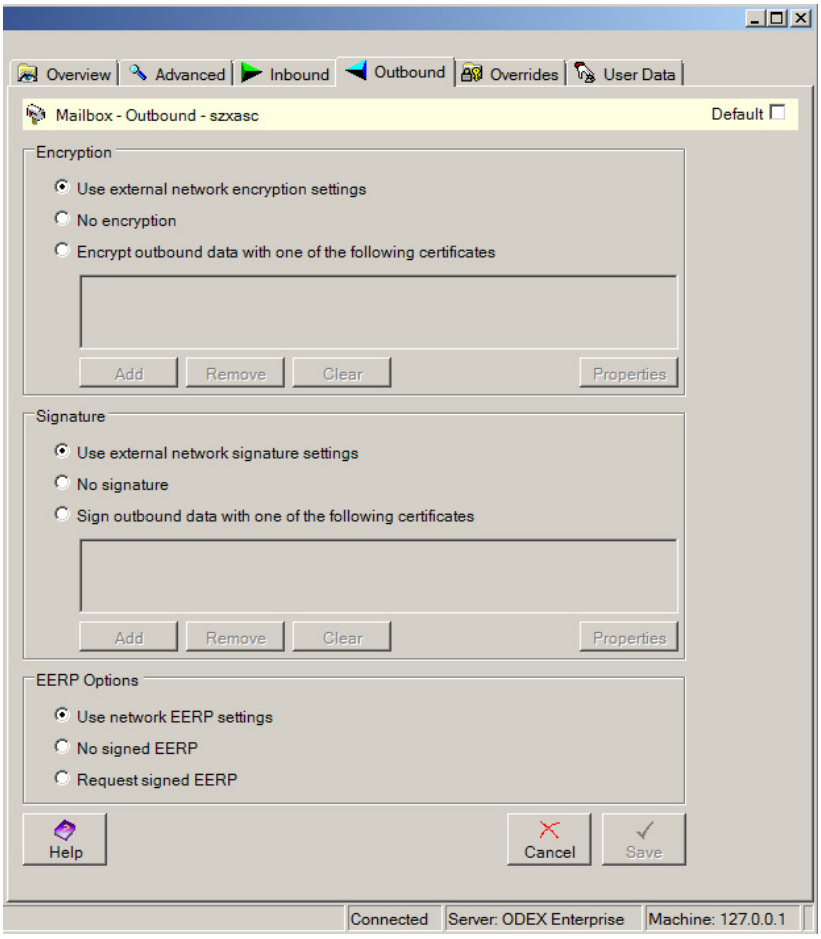
Select the appropriate radio button. The options are all self-explanatory. If you choose a specific certificate, action buttons are enabled, which are explained in the section entitled 'Dynamic Certificate Selection'.

"Use external network signature settings" means the settings specified on the external network for inbound data verification should be used.

OFTP Mailbox – Outbound

The Outbound page allows you to configure the security settings to be used for outbound data to your trading partner or clearing centre. These values override the settings at the network level.

The Outbound page looks like the example below.



The three sections on this page are encryption, signature and EERP options. You are required to configure the details of security to be used. This is not a matter of choice – the configuration must reflect the security arrangement you have agreed with your trading partner.

Encryption

The Encryption section is where you specify the public key certificate(s) to use when sending encrypted data to your trading partner. These certificates are considered as belonging to and thus provided by the trading partner.

Select the appropriate radio button. No encryption means that your trading partner does not expect you to encrypt data you send to him.

“Use external network encryption settings” means the settings specified on the external network for encryption should be used.

If you choose to encrypt data, action buttons are enabled, which are explained in the section entitled ‘Dynamic Certificate Selection’.

Signature

The Signature section is where you specify the private key certificate(s) to use when signing data you are sending to your trading partner. These certificates are considered as belonging to your internal companies.

Select the appropriate radio button. No signature means that your trading partner does not expect you to sign your data.

“Use external network signature settings” means the settings specified on the external network for signing should be used.

If you choose to sign data, you can either sign using the certificate configured against your internal network, or you can select a different certificate. Action buttons are enabled, which are explained in the section entitled ‘Dynamic Certificate Selection’.

EERP Options

The mailbox settings override the network settings.

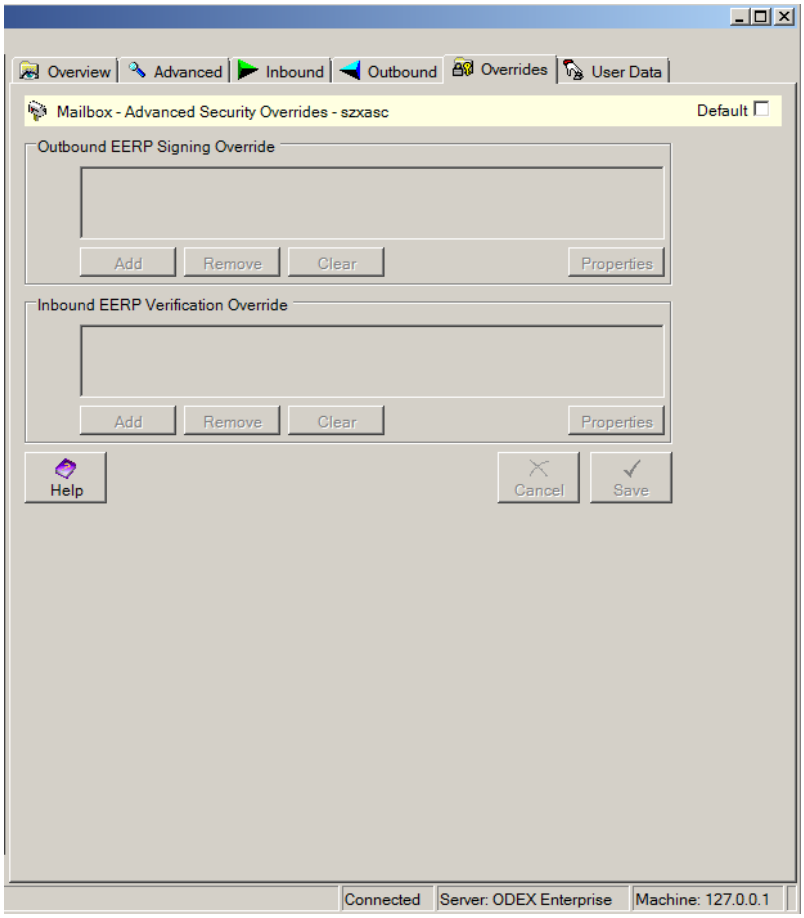
The “Request signed EERP” tick box should be checked if you would like to receive signed OFTP EERP acknowledgments for files you send to this trading partner. Signing confirms that the file has definitely been received by the intended recipient.

“Use network EERP settings” means the setting specified on the network “Request signed acknowledgment” should be used.

OFTP Mailbox – Overrides

The OFTP Overrides page is only visible on mailboxes of OFTP networks that are configured to use OFTP 2 with additional options. For networks that are configured to use an earlier release level or simpler security configuration, this page is hidden.

The Overrides page looks like the example below.



This page presents a list of certificates for overriding inbound and outbound EERP signing certificates.

By default, EERP signing will use the configured file signing and verification certificates. To override these, use the relevant action buttons as explained in the section entitled 'Dynamic Certificate Selection'.

Note that you will only be allowed to override those cases for which a specific default certificate has already been defined on the Inbound and Outbound pages.

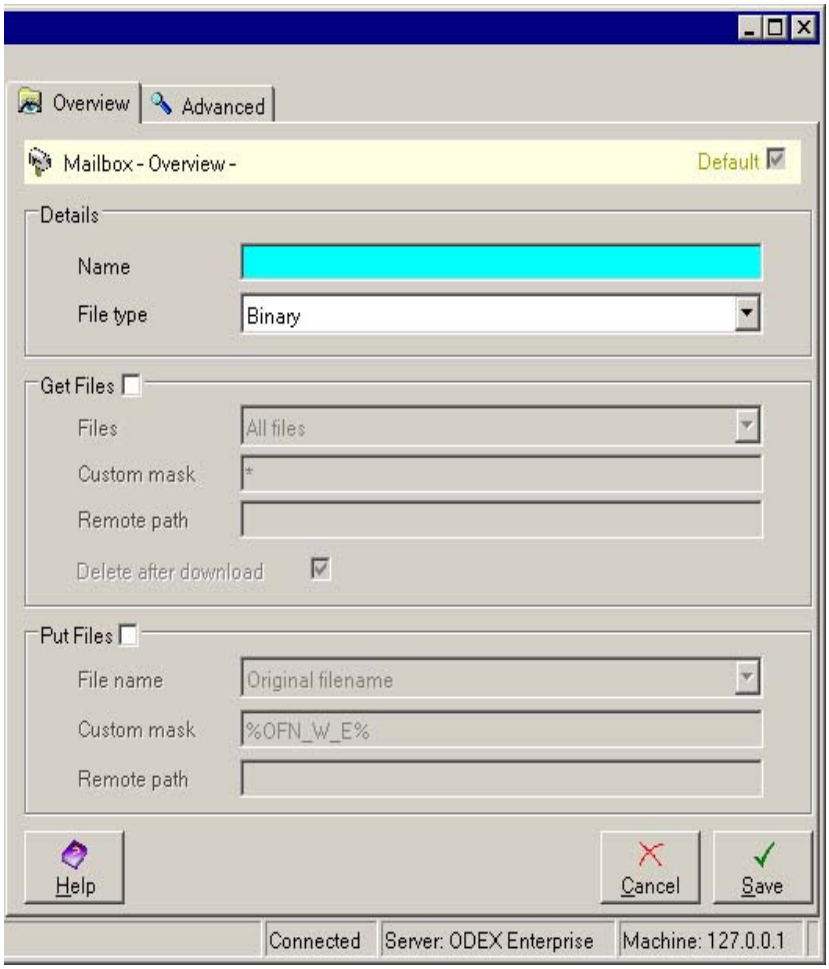
FTP client Mailbox

There are three pages associated with an external FTP client mailbox, so let's go through them and find out what information is required. The User Data page is described in the section entitled 'User Data'.

FTP client Mailbox – Overview

The Overview page is where mandatory information has to be provided for each new external FTP client mailbox. The Overview page looks like the example below.

There are three sections on this page – Details, Get Files and Put Files



Details – Name

Type in here a name for the mailbox. This is just for your own use within ODEX.

Details – File type

Use the dropdown list to select the encoding (ASCII/EBCDIC/Binary) of the files that you exchange with your trading partner. PCs and Unix machines use ASCII for plain text files while AS/400s and IBM mainframes use EBCDIC.

Changing the file type effects the format that the server expects files in and gives files to the client in. In Binary mode there is no conversion and files will be received exactly the same as they are on the FTP server. In ASCII mode the FTP server will convert all files to ASCII as they are sent to us, but will also expect files sent to it to be sent in ASCII.

If you retrieve files then these will be in the format specified here, ODEX FTP client will not perform any conversion.

The format that the FTP server stores a file in is up to the FTP server implementation. For instance you could set the type to ASCII and send a file in ASCII to an AS/400 machine and it could convert it back to EBCDIC before storing it, since this is the default text format on that machine. Specifying a type to send the file as implies it is a text file and allows whichever FTP server receives it to convert the file into the native text format.

So select “ASCII” if you exchange plain text files and want them to be inter-converted. If your files are not plain text (e.g. engineering drawings) or you specifically don’t want them converted, select “Binary” and FTP will exchange them unaltered.

Get Files

Check this tick box if you want to retrieve files from this trading partner. Once checked the other fields in this section become enabled.

Get Files – Files

Use the dropdown list to choose which files you will retrieve from your trading partner.

Get Files – Custom mask

Use this field to specify the name(s) of the file(s) you want to retrieve.

You can use the '*' and '?' characters to specify the mask. '?' Means a single character of any type, where as '*' means any number of characters (0,1 or more) of any type or order.

For example, "m?atp*s" matches "meatpies" and "maatps" but not "matpies".

Get Files – Remote path

Enter the location on you trading partner's machine where the files you wish to retrieve are to be found.

Get Files – Delete after download

If you check this tick box, when you have successfully retrieved files, FTP will delete them from your trading partner's disk. If you don't check this box, retrieved files will remain on your trading partner's disk until he does something with them and you could receive the same files again in later communication sessions. FTP only deletes files that have been received successfully.

Put Files

Check this tick box if you want to send files to this trading partner. Once checked the other fields in this section become enabled.

Put Files – File name

Use the dropdown list to choose which files you will send to your trading partner.

Put Files – Custom mask

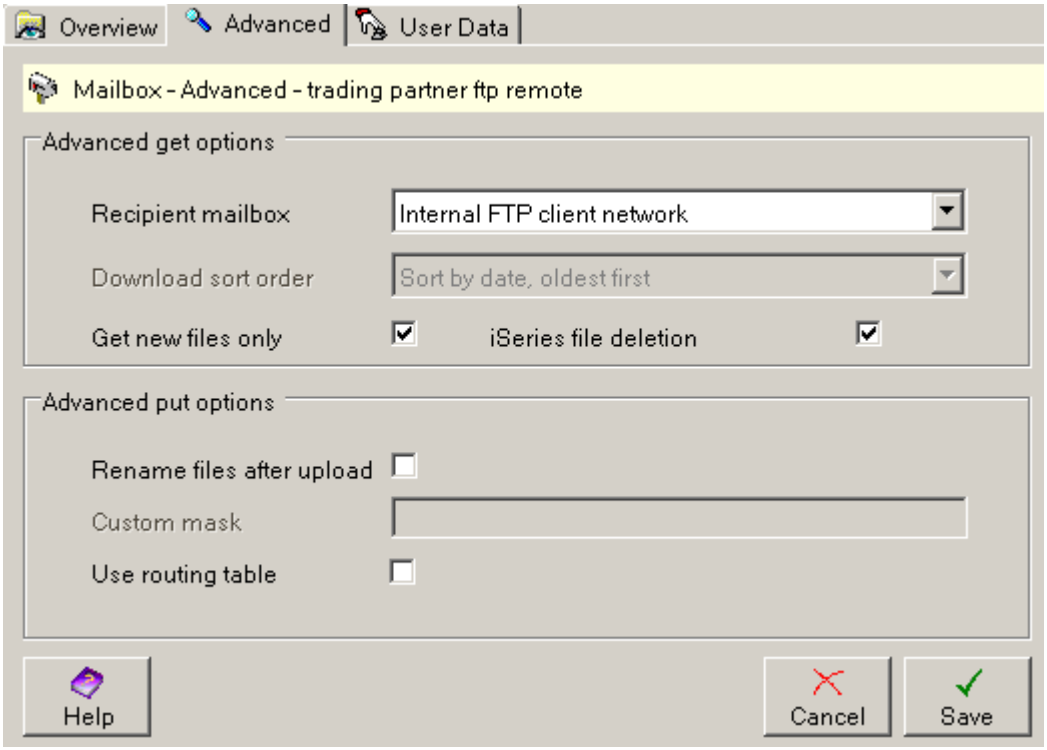
Use this field to change the name(s) of the file(s) you send.

Put Files – Remote path

Enter the location on you trading partner's machine where the files you send should be saved.

FTP client Mailbox – Advanced

The Advanced page is where you can specify extra options to control the exchange of files. The Advanced page looks like the example below.



There are two sections on this page – Advanced get options and Advanced put options.

Advanced get options – Recipient mailbox

Use the dropdown list to choose the internal mailbox into which received files will be written.

Advanced get options – Download sort order

Use the dropdown list to choose the order in which retrieved files will be read from the trading partner.

Advanced get options – iSeries file deletion

This option is enabled only when the 'Delete after download' check box option under the 'Get Files' section is enabled. This option needs to be used only if the FTP server is running on an AS/400 machine and we need both the File and its corresponding Members to be deleted after we GET file from a library.

Advanced get options – Get new files only

We recommend using this option only if it is impossible to delete the files after they have been retrieved as this ensures that a file is always retrieved and never retrieved twice as well as letting the owner of the ftp server aware which files have been retrieved.

This option gets only new files from the directory. It does this by analysing the directory listings and extracting out file date times and only downloading files with a date-time after the last retrieved file. If a file has the same file-date time then it is downloaded in filename ascending order.

Since most ftp servers do not give the second the file was uploaded, if two files are uploaded in the same minute and Odex calls into the ftp server whilst uploading the first file and the second file is alphabetically before the first one then the file may be missed and not retrieved. If this rare situation occurs, a warning will be given in the comms monitor.

Advanced put options – Rename files after upload

Check this tick box if, after they have been sent successfully from you to your trading partner, you want files on your trading partner's disk to be renamed.

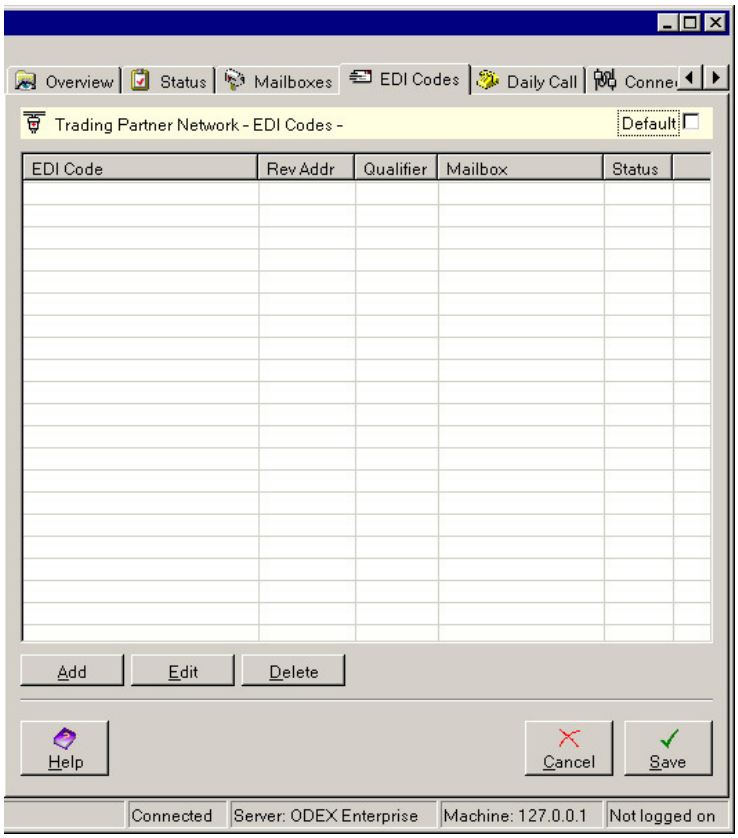
Advanced put options – Custom mask

Use this field to specify the new name(s) of the file(s) you have sent and are to be renamed on your trading partner's disk.

Network – EDI Codes

The EDI Codes page looks like the example below, though for AS2 and FTP server networks the Mailbox column will not be present.

This page will not be present for Clearing Centre networks.



This page shows all the EDI codes currently defined for the currently selected network.

If you are adding a new OFTP network, and your SSID, SFID (Mailbox) and EDI code for this network are all the same, you do not need to add a Mailbox or an EDI code, since they will be created automatically when you click the **Save** button to save the Network details.

However, if you do need to add a mailbox and EDI code for this network, you must add the mailbox and save the Network details before you will be able to add the associated EDI code.

Mailboxes are not applicable to AS2 and FTP server networks. An EDI code will not be created automatically for an AS2, FTP client or FTP server network.

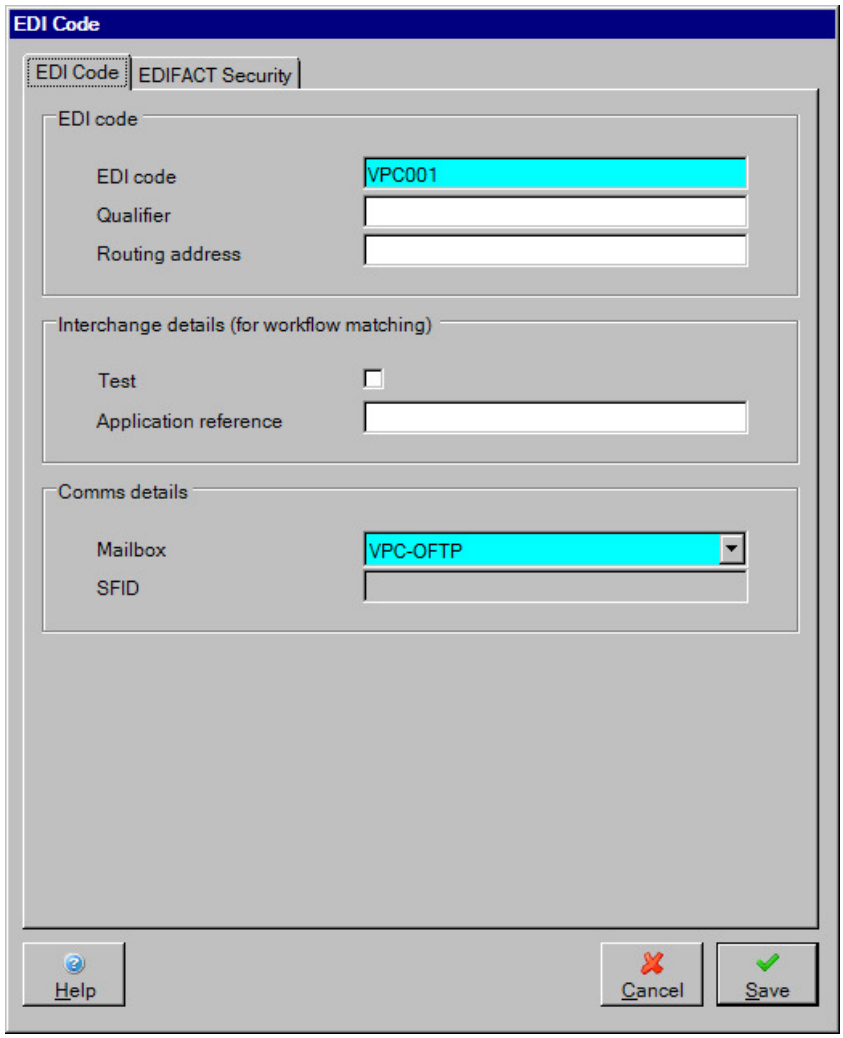
EDI codes – Add, Edit and Delete

Use the **Add** button to add a new EDI code for this network.

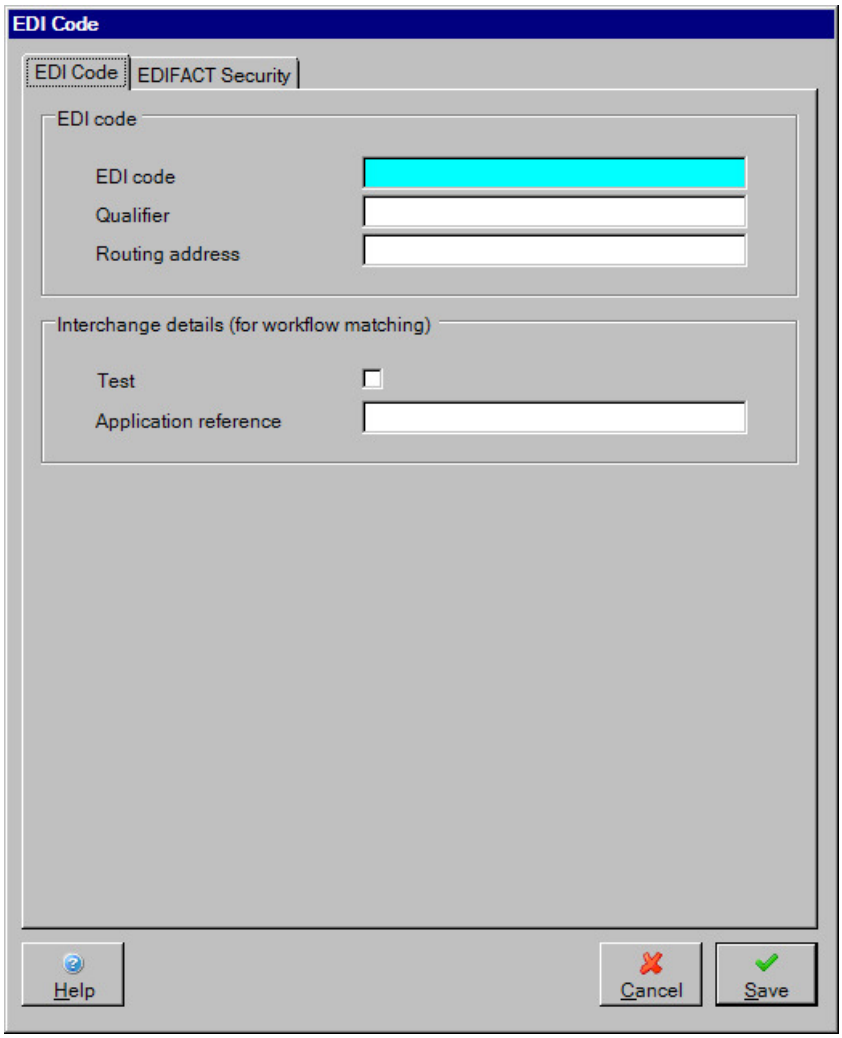
Use the **Edit** button to edit the details of an existing EDI code for this network. The dialog you see will be the same as for adding a new EDI code, but the details will be filled in ready for you to edit.

Use the **Delete** button to edit the details of an existing EDI code for this network.

Clicking the **Add** or **Edit** button will bring up the following dialog for an OFTP network:



or the following dialog for an AS2, FTP server network:



In both cases there is an additional tab used for specifying EDIFACT security information. Details can be found in the section ”EDIFACT Security Settings”.

For an OFTP or FTP client network, this dialog is divided into three sections: EDI code, Interchange details and Comms details.

For an AS2 or FTP server network, this dialog only displays the EDI code and interchange details.

EDI Code – EDI code

Type in this field the EDI code to be used with this network.

EDI Code – Qualifier

You only need to provide a value in this field if your trading partners require it.

EDI Code – Reverse routing address

You only need to provide a value in this field if your trading partners require it.

Interchange details – Test

Select this tickbox if you want to treat ‘Test’ EDI files from this trading partner to be treated differently from ‘Live’ files.

N.B. A ‘Test’ EDI file has a special flag set in the EDI message to indicate its Test status. A ‘Live’ EDI message simply does not have the flag set. For example, in an EDIFACT message, a ‘1’ in element 0035 of the UNB segment indicates a Test message. If this element is blank, the message is Live.

Interchange details – Application reference

You only need to provide a value in this field if you want to treat messages from this trading partner differently according to the application reference they contain.

The application reference is held in element 0026 of the UNB segment.

Comms details – Mailbox (OFTP and FTP client only)

Select the appropriate mailbox for this network from the dropdown list. If the mailbox you require is not in the list, you must first add it on the Mailboxes page and save it.

Comms details – SFID (OFTP and FTP client only)

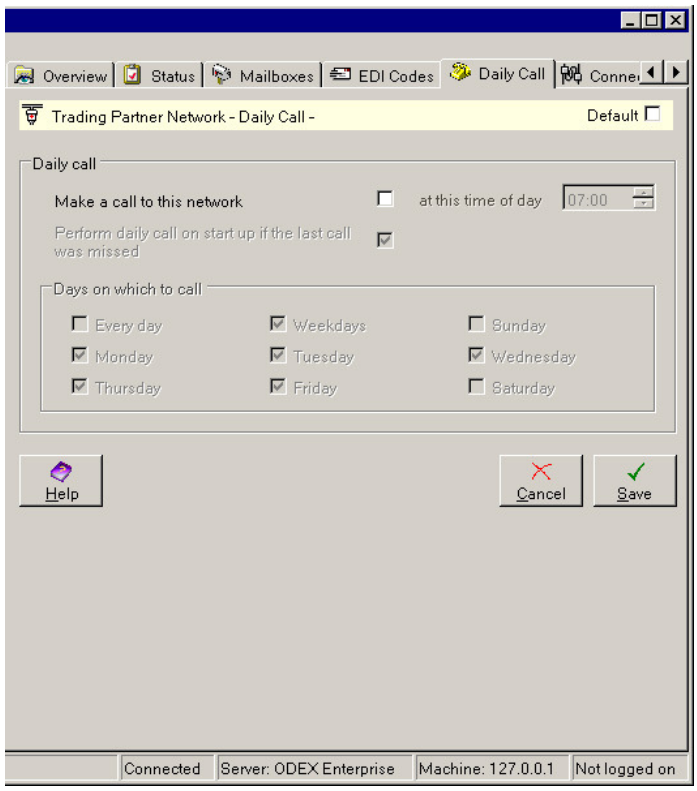
This field is not editable.

Once you have selected a mailbox in the field above, the associated SFID will appear in this field.

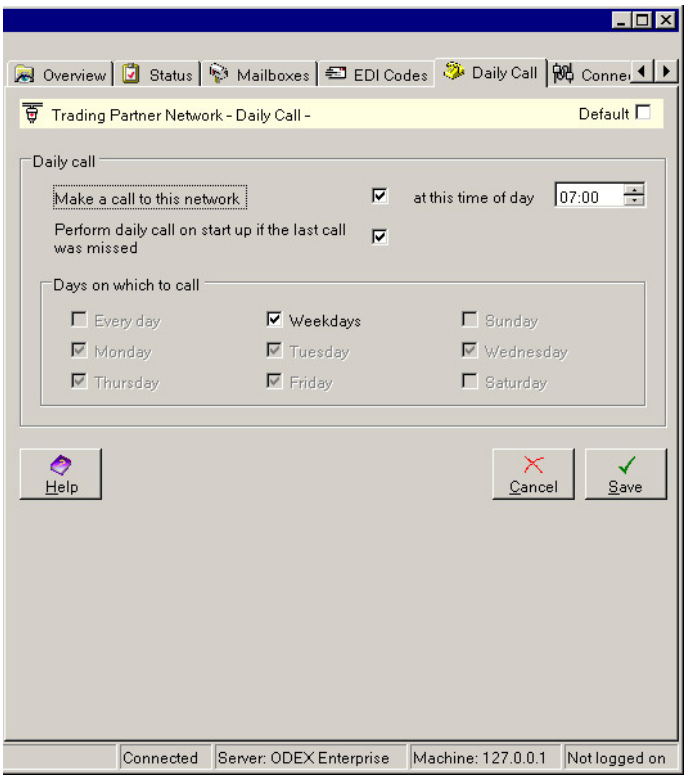
Network – Daily Call

Please remember that Daily Call details set up for one network have no effect on the other networks. If you want to automate daily calls for all your networks you must provide these details separately for each network.

By default, the Daily Call page looks like the example below. The Daily Call functionality is not available until you check the "Make a call to this network" tickbox.



By default, the Daily Call functionality is de-activated for all networks. To set your required daily call details, place a tick in the "Make a call to this network" checkbox. All fields on the Daily Call page will then become enabled, as shown below:



As you can see, this page is mostly made up of tickboxes.

Make a call to this network

Tick this checkbox to activate the daily call functionality.

Deselect this checkbox to de-activate the daily call functionality.

at this time of day

Use the up and down arrows at the side of this field to specify the time of day at which the automated call should be made. This field uses a 24-hour clock system e.g. 5pm will be shown as 17:00:00.

Perform daily call on start up if the last call was missed

Sometimes a call might be missed if the server is not running at the time the call should be made. A tick in this box means that, if a call has been missed, a call will be made to the network as soon as the server is started .

Days on which to call

The default for this section is "Weekdays", which means an automated call will be made on Monday, Tuesday, Wednesday, Thursday and Friday.

If you want to change this selection, first uncheck the "Weekdays" tickbox. This will make all the tickboxes available to you. Then use the tickboxes to select which days of the week you want ODEX to make an automated call. We have also provided an "Everyday" tickbox, which will automatically select each day's tickbox for you.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

If you want to discard the changes you have made on this page, click the **Cancel** button.

Save

To save the changes you have made on this page, click the **Save** button.

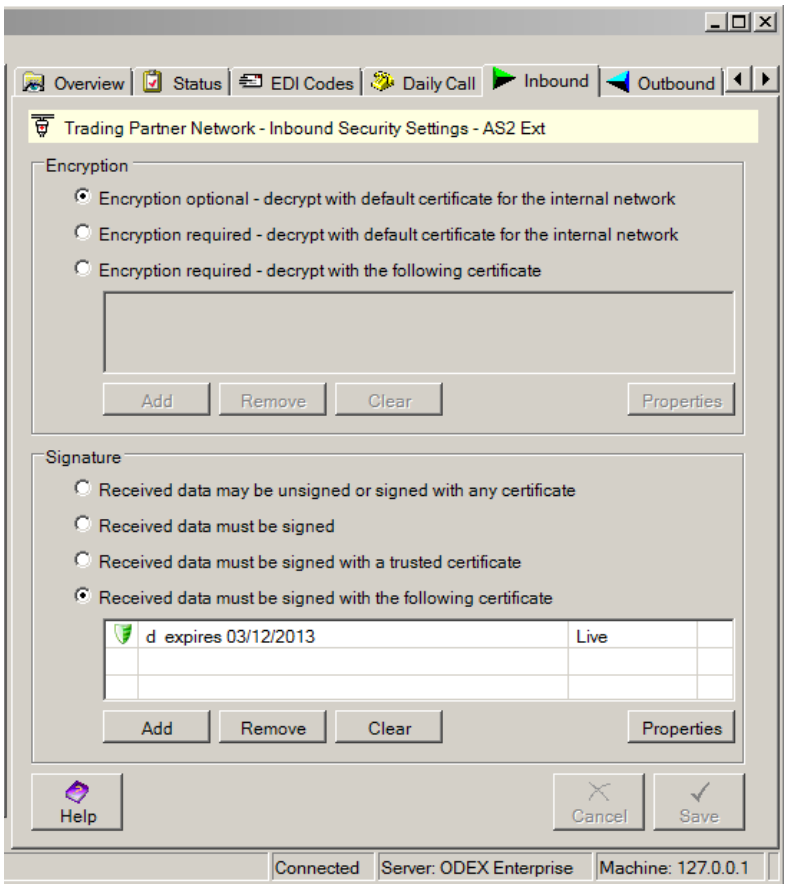
Network – Inbound (AS2)

This section describes the AS2 Inbound page. It allows you to configure the Security Settings to be used for inbound data from your trading partner or clearing centre.

You will already have configured the Security Settings for your internal network. The decryption certificate defined there may be used here too, by selecting the appropriate option.

The two areas of security are decryption and signatures. You are required to configure the details of security to be used. This is not a matter of choice – the configuration must reflect the security arrangement you have agreed with your trading partner.

The Inbound page looks like the example below.



There are two sections on this page – Encryption and Signature.

Encryption

The Encryption section is where you specify the private key certificate (if any) that will be used to decrypt data sent to you by your trading partners.

Select the appropriate radio button. Each button specifies whether encryption is optional or required for this network.

If encryption is required, you can either decrypt your trading partner's files using the certificates selected in your internal network section, or you can specify them here. Action buttons are enabled for you to choose the certificate(s). See the section entitled 'Dynamic Certificate Selection'.

Signature

The Signature section is used to specify whether you require inbound data to be signed, and if so how (possibly including the specification of a trading partner's public key certificate).

Select the appropriate radio button.

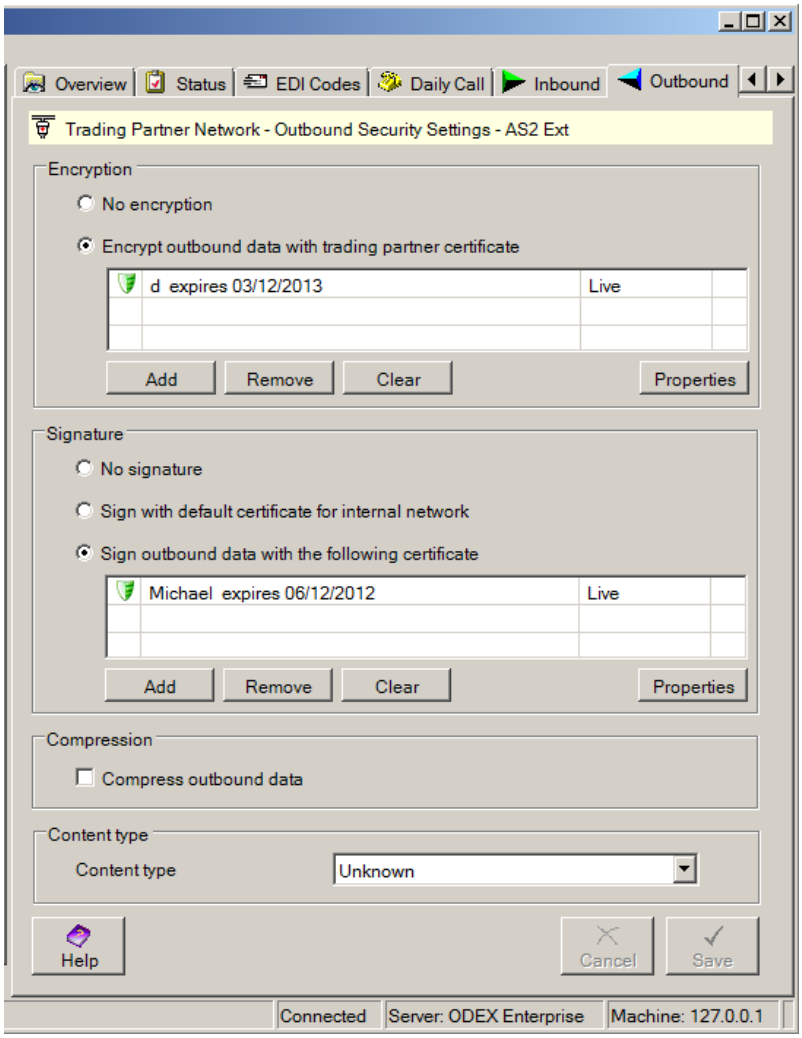
The options are all self-explanatory.

Network – Outbound (AS2)

This section describes the AS2 Outbound page. It allows you to configure the security settings, compression requirements and content type to be used for outbound data to your trading partner or clearing centre.

The four sections on this page are decryption, signatures, compression and content type. You are required to configure the details of security to be used. This is not a matter of choice – the configuration must reflect the security arrangement you have agreed with your trading partner.

The Outbound page looks like the example below.



There are three sections on this page – Encryption, Signature and Compression.

Encryption

The Encryption section is where you specify the public key certificate to use when sending encrypted data to your trading partner.

Select the appropriate radio button.

No encryption means that your trading partner does not expect you to encrypt data you send to him.

If he does expect you to use encryption, you must select “Encrypt outbound data with one of the following certificates” to specify the certificate(s) to use for encrypting outbound data. Action buttons are enabled for you to choose the certificate(s). See the section entitled ‘Dynamic Certificate Selection’.

Signature

The Signature section is where you specify the private key certificate to use when signing data sent by you to your trading partner.

Select the appropriate radio button.

No signature means that your trading partner does not expect you to sign your data.

If he is expecting you to use a signature, you can either sign using the certificate(s) selected in your internal network section, or you can specify the certificate(s) to use. Action buttons are enabled for you to choose the certificate(s). See the section entitled ‘Dynamic Certificate Selection’.

Compression

Select the 'Compress outbound data' tickbox if you want to compress the data that you send, and your trading partner has indicated that compressed data is acceptable.

Content Type

The content type indicates to your trading partner the format of the data that you are sending. When sending a file using AS2, the content type of the file is sent with the file in the AS2 message. You may change the content type used for outbound messages, should your trading partner require this.

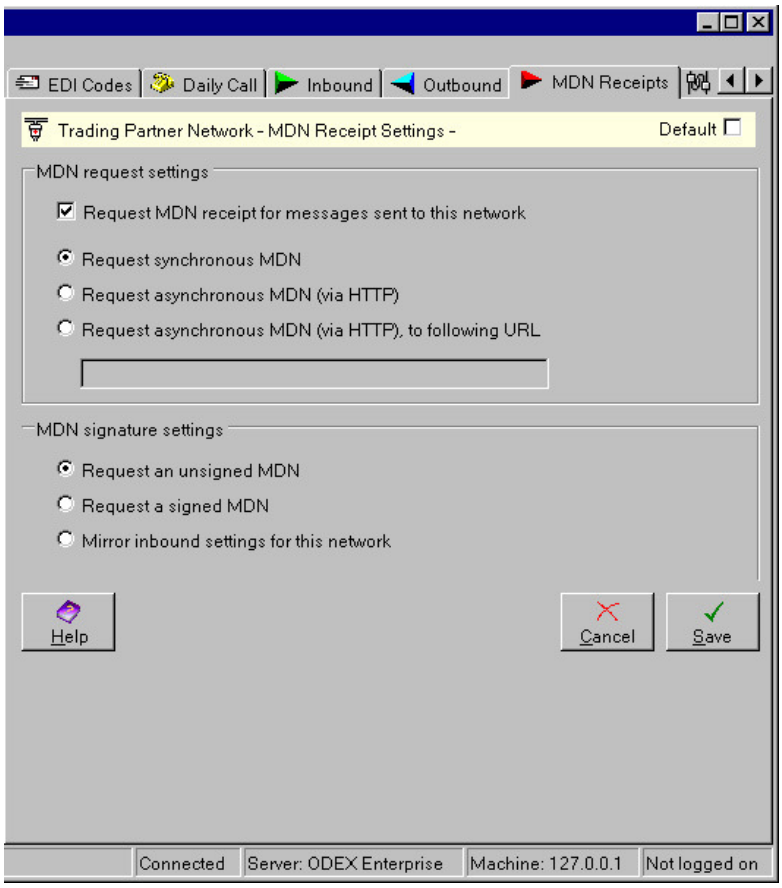
Network – MDN Receipts

The MDN Receipts page is only applicable to AS2 networks. It allows you to configure the settings to be used for MDN receipts from your trading partner or clearing centre.

MDN stands for Message Disposition Notifications. They are an acknowledgement that your partner has received the data you sent and that the encryption and signatures were OK.

The settings you choose are a matter of personal preference.

The MDN Receipts page looks like the example below.



There are two sections on this page – MDN request settings and MDN signature settings.

MDN request settings

The Request MDN receipt tickbox is selected by default. The default MDN settings are:

- Request synchronous MDN
- Request an unsigned MDN

If you uncheck the tickbox, the AS2 messages you send will not include requests for MDNs. When the tickbox is unchecked, the rest of the page will be disabled.

You may accept the default settings or choose the way MDNs are sent to you. The choices are as follows:

- Request synchronous MDN – this option means that the MDN will be sent to you in the same AS2 comms session in which you send the data
- Request asynchronous MDN (via HTTP) – this option means that the MDN will be sent to you in a different AS2 comms session from the one in which you sent the data. The MDN will be sent back to the same URL that sent the original file.
- Request asynchronous MDN (via HTTP) to following URL – this option means that the MDN will be sent to you in a different AS2 comms session from the one in which you sent the data. If you select this option, the field below it will become enabled, allowing you to type in the URL to which you want the MDN to be sent.

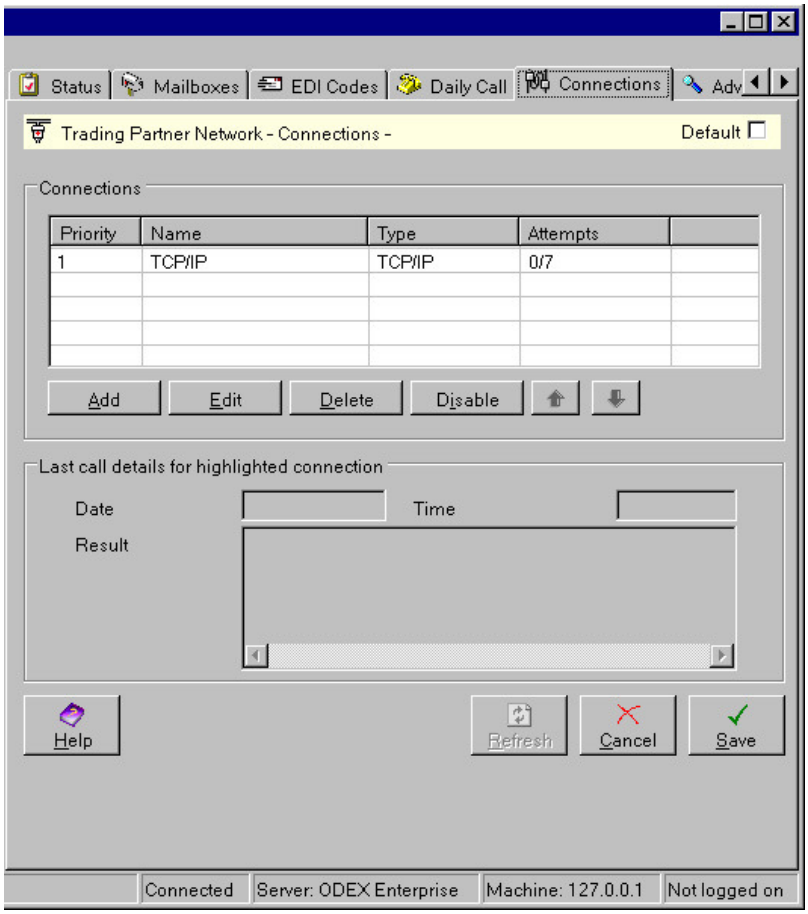
MDN signature settings

You have a choice of three self-explanatory settings in this section:

- Request an unsigned MDN
- Request a signed MDN
- Mirror inbound settings for this network

Network – Connections

The Connections page looks like the example below.

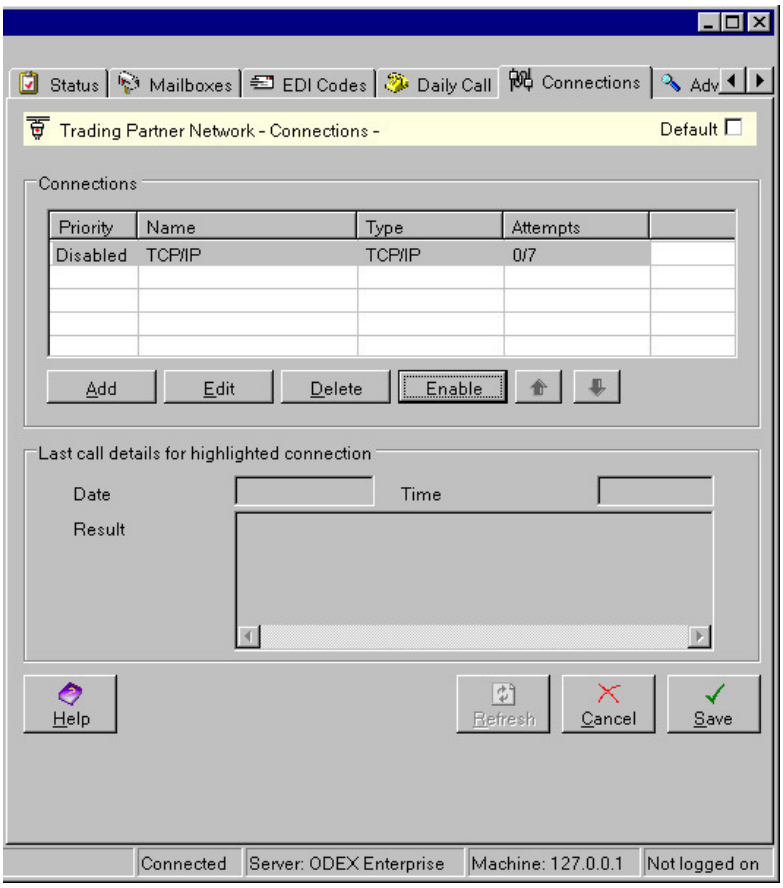


This page shows all the connections that can be used with this network, together with their type and priority and an indication of how many attempts have been made to connect. The first entry in the list shows the details of this network, which is the main connection.

You may change the priority of any entry in the list (provided there is more than one entry in the list) by highlighting an entry and clicking on the up and down arrows on this screen. This will increase and decrease, respectively, the value shown in the Priority column for the selected entry.

The effect of the Priority field is as follows. Let's say you have five TCP/IP connections for different customers, with priorities 1, 2, 3, 4 and 5. ODEX will first try to connect to the network with priority 1. If that fails, it will try priority 2, and so on until each connection has been attempted. Any files for failed connections will be queued up until next time ODEX connects to that network.

The **Disable** button can be used to disable a selected entry in the list. If you disable an entry, the value in the Priority column will change to "Disabled" and the **Disable** button will become the **Enable** button, as shown below.



If you highlight an entry in the list, details of its last call will be shown in the section at the bottom of the page. If no details are shown, this indicates that the selected connection has not yet been used. The last call details are as follows:

Last call details – Date

This is the date on which the last attempt was made to connect using the highlighted connection.

Last call details – Time

This is the time at which the last call was made to connect using the highlighted connection.

Last call details – Result

This field shows the result of the last attempt to connect using the highlighted connection.

"Normal session termination" means that the last attempt was successful.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

If you want to discard all the changes you have made in the Connections section, click the **Cancel** button.

Save

To save all the changes you have made in the Connections section, click the **Save** button.

Adding a new Network Connection

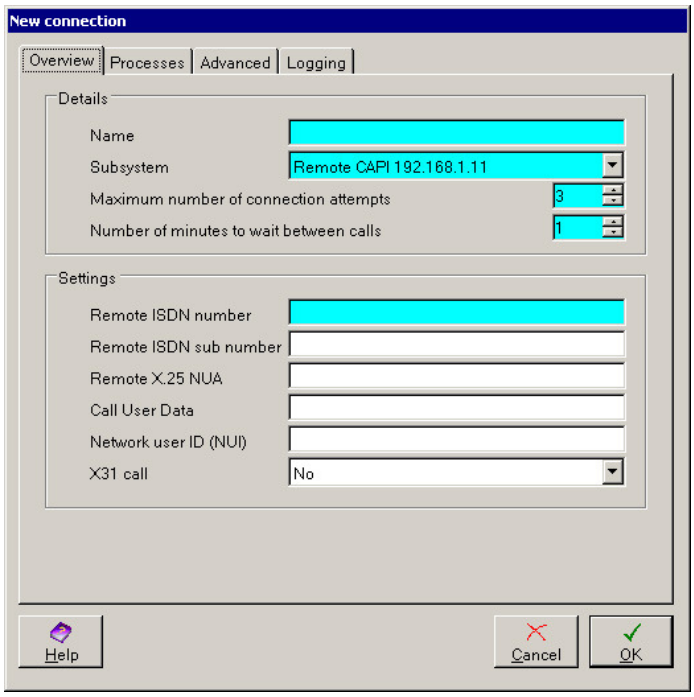
Local or Remote CAPI Connections – Add, Edit and Delete

Use the **Add** button to add a new connection for this network.

Use the **Edit** button to edit the details of an existing connection for this network. The dialog you see will be the same as for adding a new connection, but the details will be filled in ready for you to edit.

Use the **Delete** button to edit the details of an existing connection for this network.

Clicking the **Add** or **Edit** button will bring up the following dialog:



New/Edit Local or Remote CAPI connection – Overview

The Overview page contains the following fields.

Details – Name

Type in here a name for the connection. This name is just for your own use within ODEX.

Details – Subsystem

Select the CAPI subsystem using the dropdown arrow to the right of this field.

Details – Maximum number of connection attempts

Use the up and down arrows at the side of this field to select the maximum number of attempts that should be made to connect using this connection before ODEX stops trying.

The default value is 3, the maximum value is 100.

Details – Number of minutes to wait between calls

Use the up and down arrows at the side of this field to select the number of minutes that ODEX should wait between call attempts.

The default value is 1, the maximum value is 1000.

Settings – Remote ISDN number

Type in this field the ISDN number of the trading partner network or clearing centre network when using this connection.

Settings – Remote ISDN sub number

Type in this field the ISDN sub-address number of the trading partner network or clearing centre network when using this connection.

Settings – Remote X.25 NUA

Type in this field the X.25 NUA of the trading partner network or clearing centre network when using this connection.

Settings – Call User Data

The Call User Data field is used for whatever purpose is agreed by the two parties exchanging calls. It may, for example, be used by the receiver for call routing, sending the incoming data to an OFTP service rather than to a remote terminal logon service.

To allow any values to be input into this area, the codes may be input as ASCII characters or coded as hexadecimal numbers. Each hexadecimal number must be preceded by a single ~ (tilde) character. For example, to code the character A followed by an ENQ (hex 15) and carriage return (hex 0D) and line feed (hex 0A) characters, the following string should be input A~15~0D~0A.

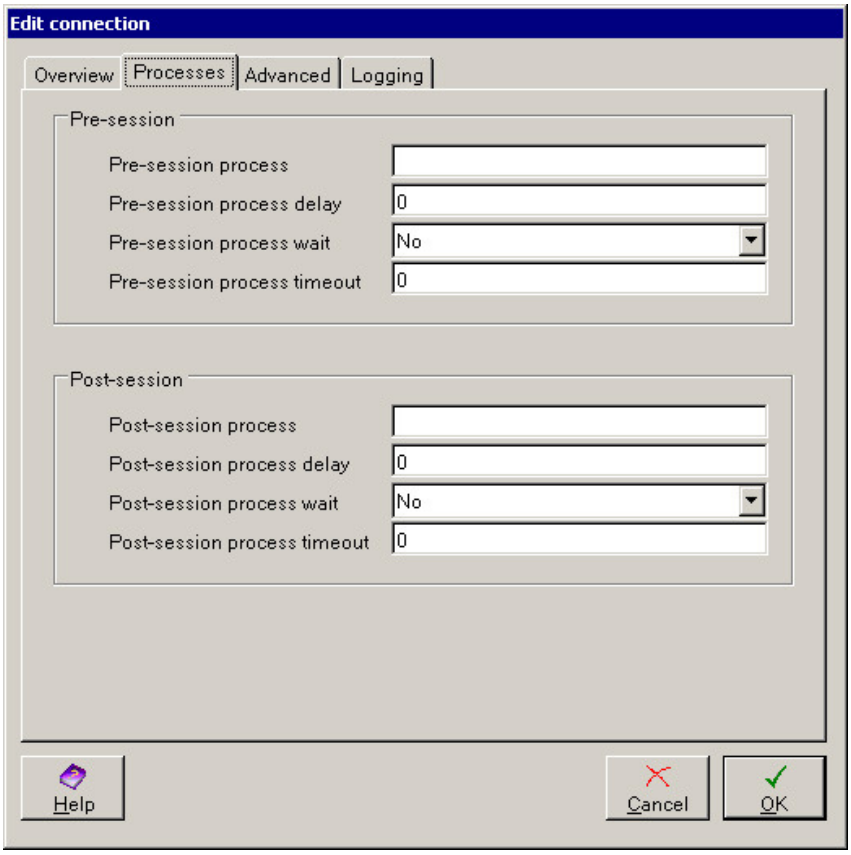
Settings – Network user ID (NUI)

Type in this field the NUI of the trading partner network or clearing centre network when using this connection.

Settings – X.31 call

If you wish to make an X.31 call using this connection, select Yes from the dropdown list.

New/Edit connection – Processes



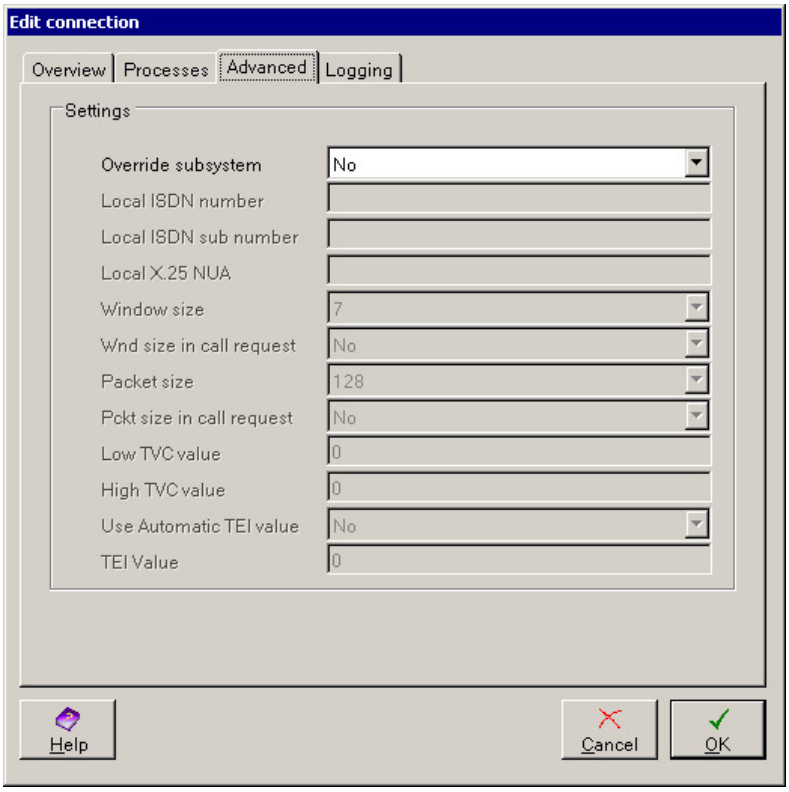
This dialog is divided into two sections – Pre-session and Post-session.

These fields allow you to specify batch files to be run before and/or after a communications session, together with delay, wait and timeout details.

In most cases, you will not need to use the fields on this page. If you do need to use them, the values you provide will be specific to your own system and so there is little to be gained by discussing them here.

New/Edit connection – Advanced

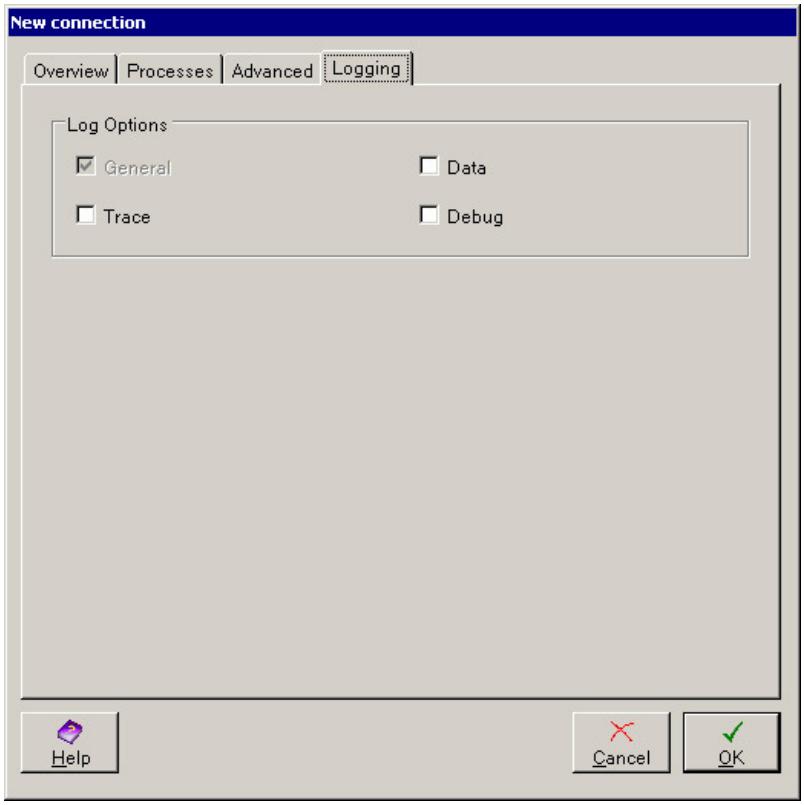
The dialog below will be seen if you have selected a Local or Remote CAPI subsystem.



The first field allows you to override the existing settings for this subsystem (which are found in the Subsystems node of the Comms Administrator). If you select Yes, all the remaining fields on the page will become enabled.

These fields are described in the section entitled "CAPI2 subsystem Advanced".

New/Edit connection – Logging



The four possible types are: General, Data, Trace and Debug.

- Data indicates high-level logging, displaying the data contents of the received/sent protocol and files being exchanged.
- Trace messages provide information about what is happening during communications sessions.
- Debug messages are another type of trace message, giving an indication of what is happening during communications sessions.
- General indicates any other log information that is not covered by the other three categories. Such information is not necessarily related to communications. This option is always selected and cannot be deselected.

Any log options that are selected but disabled indicate that these logging levels have been selected at a higher level within ODEX.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

If you want to discard the changes you have made on these four pages, click the **Cancel** button.

OK

To save the changes you have made on these four pages, click the **OK** button.

TCP/IP Connections – Add, Edit and Delete

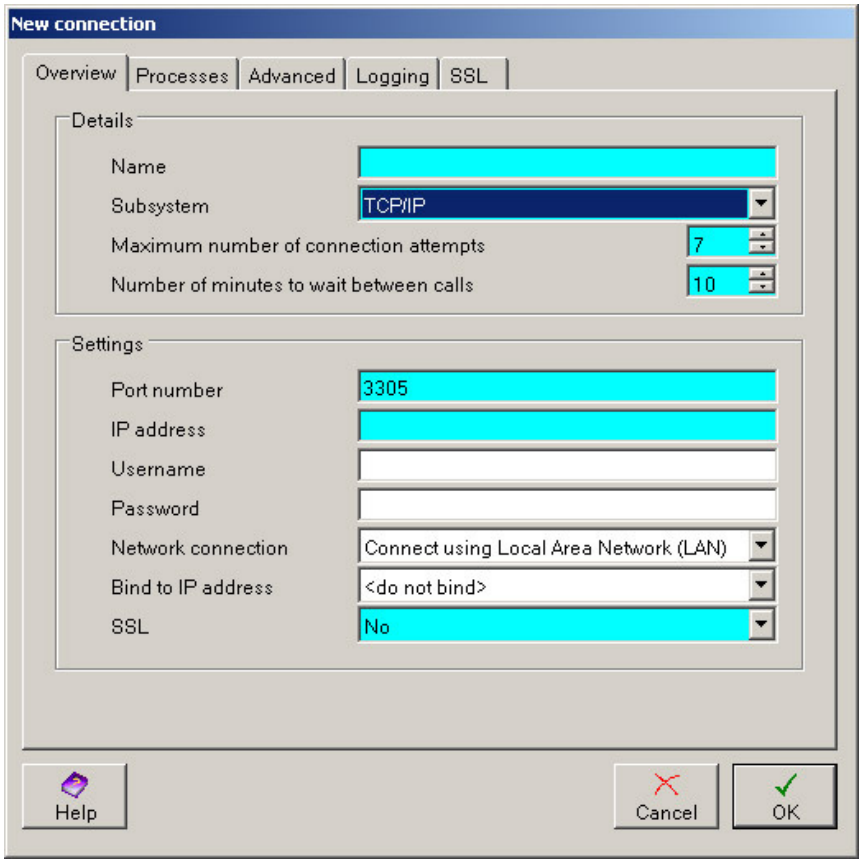
Use the **Add** button to add a new connection for this network.

Use the **Edit** button to edit the details of an existing connection for this network. The dialog you see will be the same as for adding a new connection, but the details will be filled in ready for you to edit.

Use the **Delete** button to edit the details of an existing connection for this network.

New/Edit TCP/IP connection – Overview

Clicking the **Add** or **Edit** button will bring up the following dialog:



The Overview page contains the following fields.

Details – Name

Type in here a name for the connection. This name is just for your own use within ODEX.

Details – Subsystem

Select the TCP/IP subsystem using the dropdown arrow to the right of this field.

Details – Maximum number of connection attempts

Use the up and down arrows at the side of this field to select the maximum number of attempts that should be made to connect using this connection before ODEX stops trying.

The default value is 7, the maximum value is 100.

Details – Number of minutes to wait between calls

Use the up and down arrows at the side of this field to select the number of minutes that ODEX should wait between call attempts.

The default value is 10, the maximum value is 1000.

Settings – Port number

Type in this field the port number of the trading partner network or clearing centre network to be used with this connection.

Settings – IP address

Type in this field the IP address of the trading partner network or clearing centre network to be used with this connection.

Settings – User name

Type in this field the user name, if applicable, of the trading partner network or clearing centre network for use with this connection.

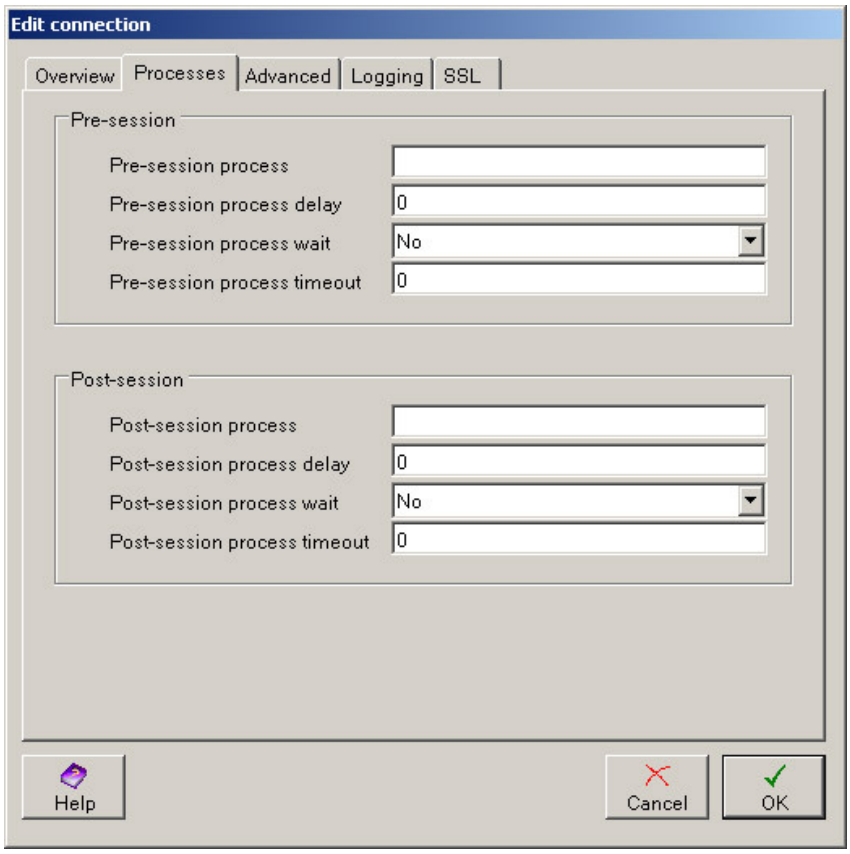
Settings – Password

Type in this field the password, if applicable, of the trading partner network or clearing centre network for use with this connection.

Settings – Network connection

Use the dropdown arrow to select the network connection to be used for this connection.

New/Edit connection – Processes



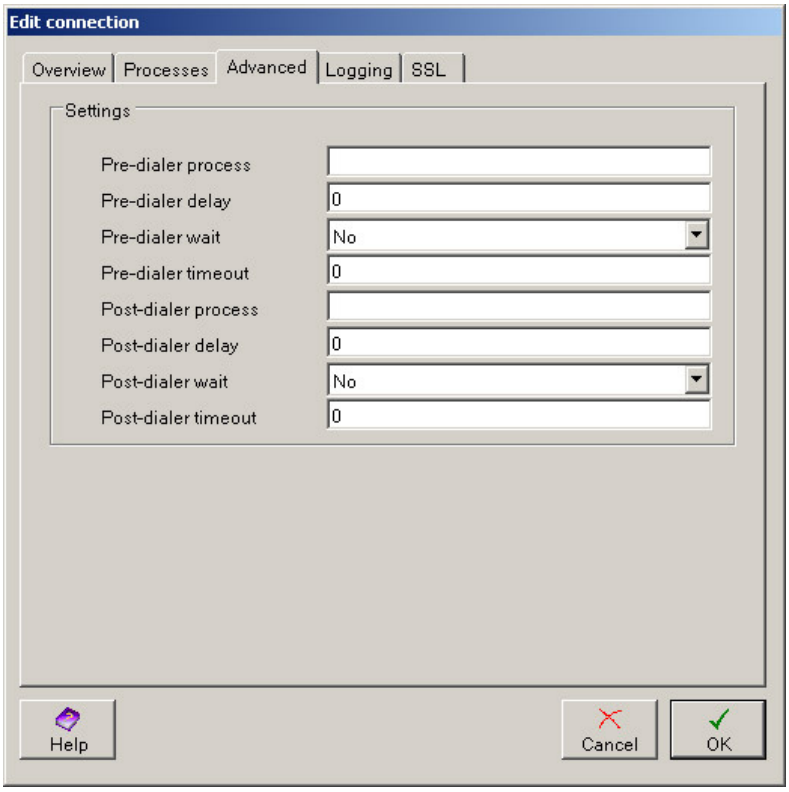
This dialog is divided into two sections – Pre-session and Post-session.

These fields allow you to specify batch files to be run before and/or after a communications session, together with delay, wait and timeout details.

In most cases, you will not need to use the fields on this page. If you do need to use them, the values you provide will be specific to your own system and so there is little to be gained by discussing them here.

New/Edit connection – Advanced

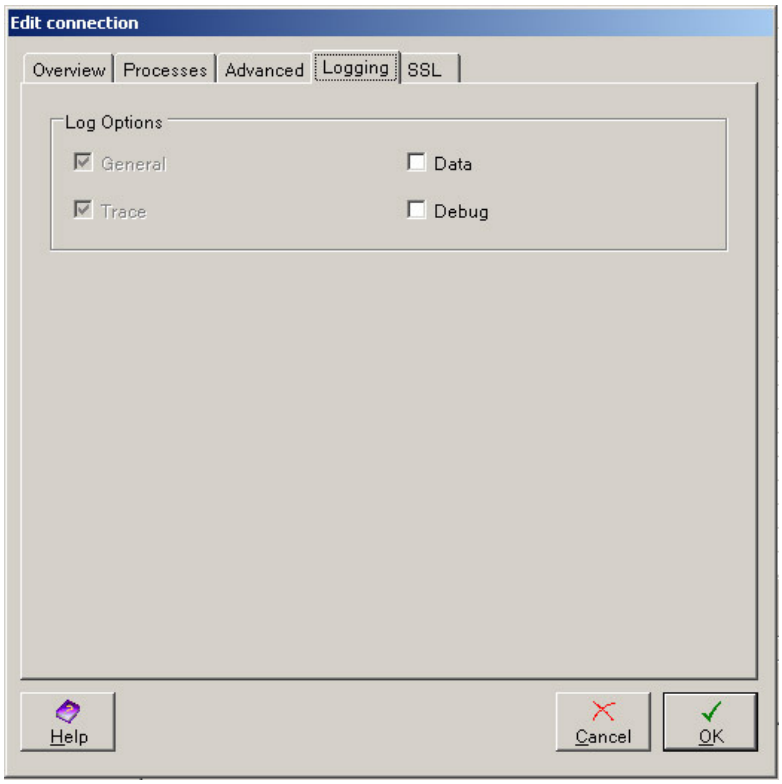
The dialog below will be seen if you have selected a TCP/IP subsystem.



These fields allow you to specify batch files to be run before and/or after a communications session, together with delay, wait and timeout details.

In most cases, you will not need to use the fields on this page. If you do need to use them, the values you provide will be specific to your own system and so there is little to be gained by discussing them here.

New/Edit connection – Logging

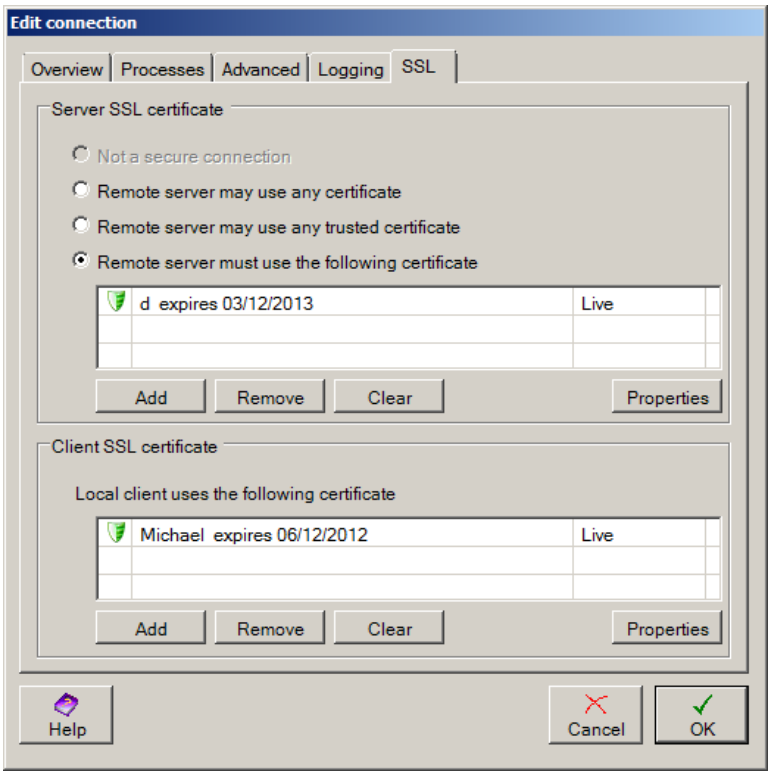


The four possible types are: General, Data, Trace and Debug.

- Data indicates high-level logging, displaying the data contents of the received/sent protocol and files being exchanged.
- Trace messages provide information about what is happening during communications sessions.
- Debug messages are another type of trace message, giving an indication of what is happening during communications sessions.
- General indicates any other log information that is not covered by the other three categories. Such information is not necessarily related to communications. This option is always selected and cannot be deselected.

Any log options that are selected but disabled indicate that these logging levels have been selected at a higher level within ODEX.

New/Edit connection – SSL



Use this dialog to implement SSL security for the TCP/IP connection. By default, “Not a secure connection” is selected. In order to enable SSL, you must set SSL to ‘Yes’ from the Overview page. This will allow you to specify the type of SSL security to use for this connection.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

If you want to discard the changes you have made on these four pages, click the **Cancel** button.

OK

To save the changes you have made on these four pages, click the **OK** button.

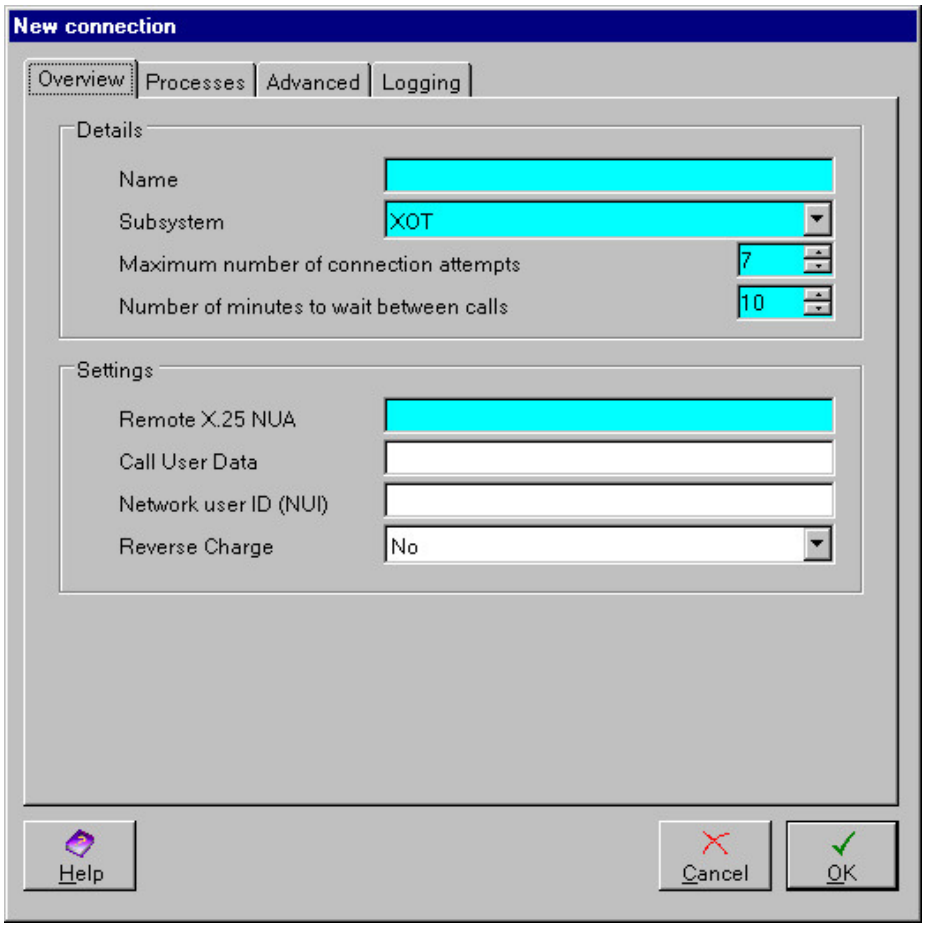
XOT Connections – Add, Edit and Delete

Use the **Add** button to add a new connection for this network.

Use the **Edit** button to edit the details of an existing connection for this network. The dialog you see will be the same as for adding a new connection, but the details will be filled in ready for you to edit.

Use the **Delete** button to edit the details of an existing connection for this network.

Clicking the **Add** or **Edit** button will bring up the following dialog:



New/Edit XOT connection – Overview

These settings, and the settings on the Connections Advanced page, are all used in the X.25 Call Request Packet. Only the Remote X.25 NUA is mandatory for the Call Request Packet.

Details – Name

Type in here a name for the connection. This name is just for your own use within ODEX.

Details – Subsystem

Select the XOT subsystem using the dropdown arrow to the right of this field.

Details – Maximum number of connection attempts

Use the up and down arrows at the side of this field to select the maximum number of attempts that should be made to connect using this connection before ODEX stops trying.

The default value is 7, the maximum value is 100.

Details – Number of minutes to wait between calls

Use the up and down arrows at the side of this field to select the number of minutes that ODEX should wait between call attempts.

The default value is 10, the maximum value is 1000.

Settings – Remote X.25 NUA

Type in this field the X.25 Network User Address of your trading partner's or clearing centre's system.

Settings – Call User Data

The Call User Data field is used for whatever purpose is agreed by the two parties exchanging calls. It may, for example, be used by the receiver for call routing, sending the incoming data to an OFTP service rather than to a remote terminal logon service.

To allow any values to be input into this area, the codes may be input as ASCII characters or coded as hexadecimal numbers. Each hexadecimal number must be preceded by a single ~ (tilde) character. For example, to code the character A followed by an ENQ (hex 15) and carriage return (hex 0D) and line feed (hex 0A) characters, the following string should be input A~15~0D~0A.

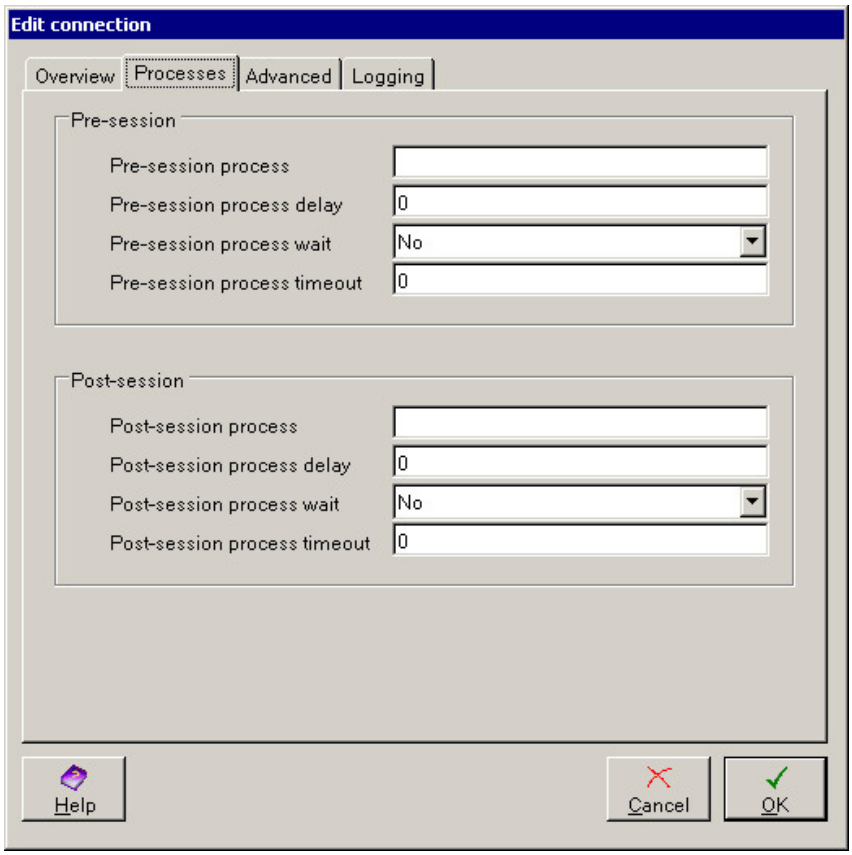
Settings – Network User ID (NUI)

If X.32 is being used, there will be some necessary security negotiation between ODEX and the X.25 system being contacted. In this case the NUI will be needed to identify this user on the network.

Settings – Reverse charge

If this field is set to Yes, then reverse charging will be requested from the X.25 system. This means that the receiver of the call will pay the X.25 charges. Many users will not accept reverse charges on their X.25 lines so this facility should be used with caution and only when agreed by prior arrangement with the remote site.

New/Edit connection – Processes



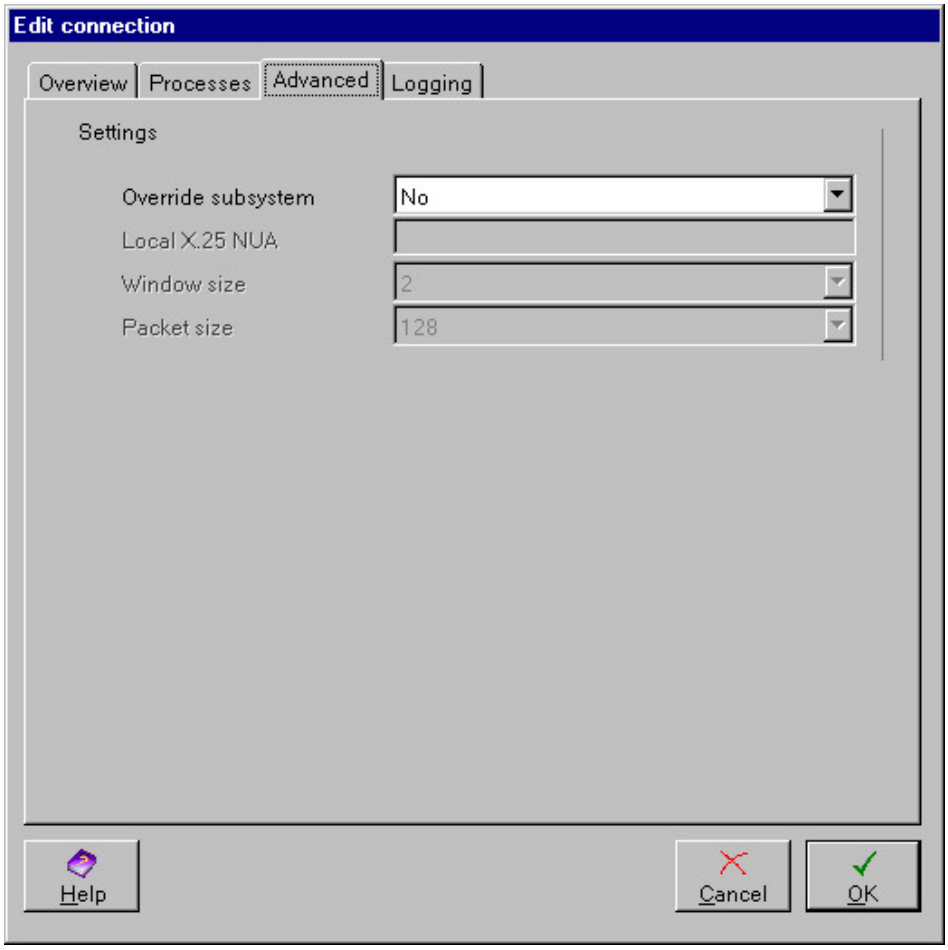
This dialog is divided into two sections – Pre-session and Post-session.

These fields allow you to specify batch files to be run before and/or after a communications session, together with delay, wait and timeout details.

In most cases, you will not need to use the fields on this page. If you do need to use them, the values you provide will be specific to your own system and so there is little to be gained by discussing them here.

New/Edit connection – Advanced

The dialog below will be seen if you have selected an XOT subsystem.



Settings – Override subsystem

This field allows you to override the existing settings for this subsystem (which are found in the Subsystems node of the Comms Administrator). If you select 'Yes' in this field, all the remaining fields on the page will become enabled.

The following settings, and the settings on the Connections Overview page, are all used in the X.25 Call Request Packet.

Settings – Local X.25 NUA

Type in here, if required, the X.25 Network User Address of your own system.

Settings – Window size

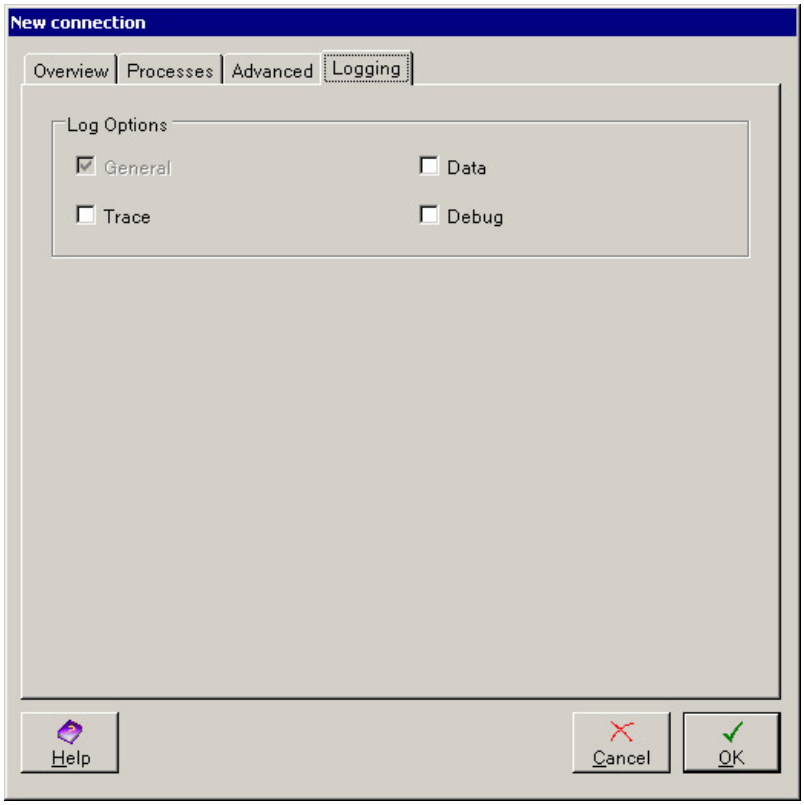
Window size refers to the X.25 window size (in Level 3 of the OSI 7-layer model). Window size is the number of X.25 packets that the transmitting system will send before stopping to wait for a response from the remote. The normal OFTP packet window size for native X.25 is 2.

Select the required (or preferred) window size using the drop-down arrow.

Settings – Packet size

Packet size refers to the X.25 packet size (in Level 3 of the OSI 7-layer model). This parameter is the X.25 packet size, which should normally be 128 as laid down in the OFTP specifications. Other values may be requested but this is not recommended. Select the required (or preferred) Packet size using the drop-down arrow.

New/Edit connection – Logging



The four possible types are: General, Data, Trace and Debug.

- Data indicates high-level logging, displaying the data contents of the received/sent protocol and files being exchanged.
- Trace messages provide information about what is happening during communications sessions.
- Debug messages are another type of trace message, giving an indication of what is happening during communications sessions.
- General indicates any other log information that is not covered by the other three categories. Such information is not necessarily related to communications. This option is always selected and cannot be deselected.

Any log options that are selected but disabled indicate that these logging levels have been selected at a higher level within ODEX.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

If you want to discard the changes you have made on these four pages, click the **Cancel** button.

OK

To save the changes you have made on these four pages, click the **OK** button.

AS2 Connections – Add, Edit and Delete

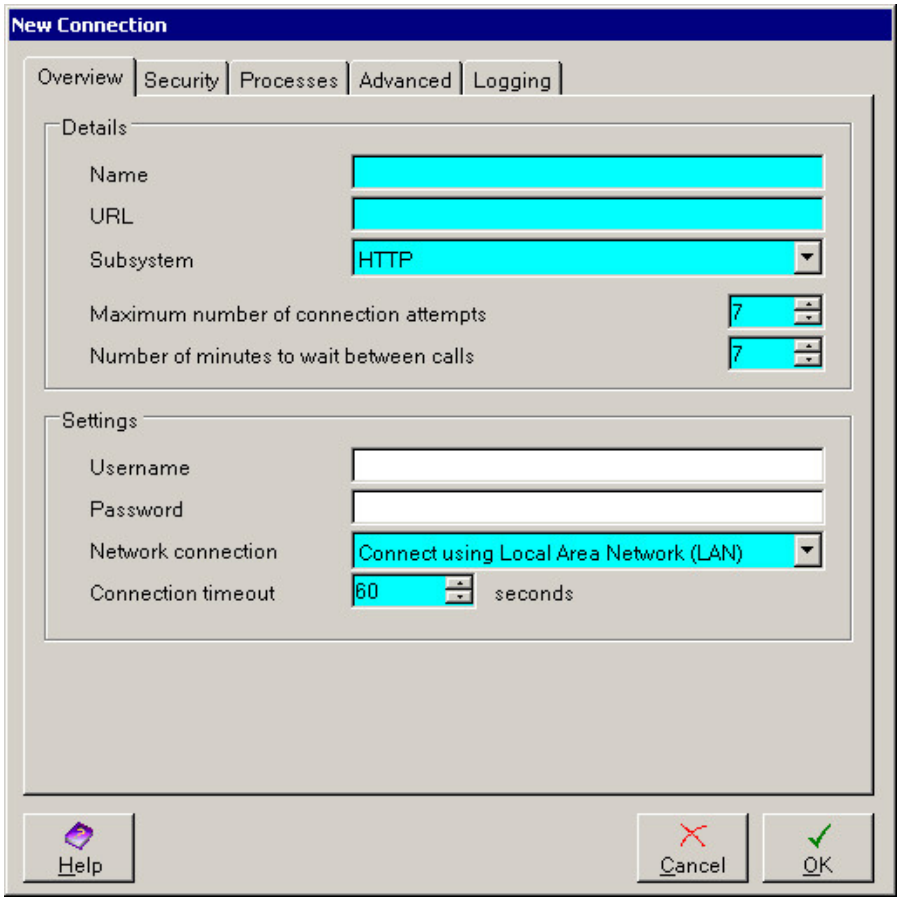
You may add extra connections to be used with this AS2 network, which will generally be used if the main connection is unavailable for any reason.

Use the **Add** button to add a new connection for this network.

Use the **Edit** button to edit the details of an existing connection for this network. The dialog you see will be the same as for adding a new connection, but the details will be filled in ready for you to edit.

Use the **Delete** button to edit the details of an existing connection for this network.

Clicking the **Add** or **Edit** button will bring up the following dialog:



The details on this page relate to the remote server.

New/Edit AS2 connection – Overview

The Overview page contains the following fields.

Details – Name

Type in here a name for the connection. This name is just for your own use within ODEX.

Details – URL

Type in here the URL for the connection. This should be in the format

http://0.0.0.0:0/

or

https://0.0.0.0:0/ (for a secure connection using SSL)

The three parts of the URL are:

- the URL 'scheme' (http or https)
- the IP address (://0.0.0.0)
- the port (:0/)

it is also possible to follow the port with extra path info (e.g. http://0.0.0.0:00/abc/def)

Details – Subsystem

Select the required subsystem using the dropdown arrow to the right of this field. Only HTTP subsystems will be shown in the list.

Details – Maximum number of connection attempts

Use the up and down arrows at the side of this field to select the maximum number of attempts that should be made to connect using this connection before ODEX stops trying.

The default value is 7, the maximum value is 100.

Details – Number of minutes to wait between calls

Use the up and down arrows at the side of this field to select the number of minutes that ODEX should wait between call attempts.

The default value is 7, the maximum value is 1000.

Settings – Username

If the remote server requires a username, type it in this field. This will be used to verify who you are.

Settings – Password

If the remote server requires a password, type it in this field. This will be used to verify who you are.

Settings – Network connection

Select the appropriate option using the dropdown list in this field.

The number of options in this field will depend on whether you have the ability to connect to the Internet from your computer using a modem. If you do not have this ability, there will only be one choice available to you:

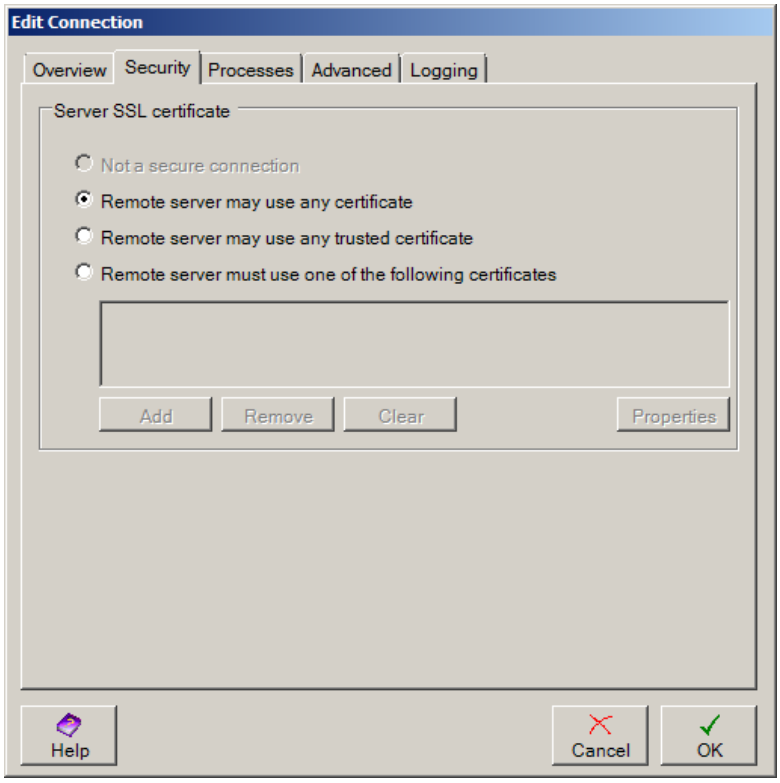
- Connect using Local Area Network (LAN).

If you have a modem, and have configured dial-up networking connections (to trading partners or to the Internet) there will be additional entries for each dial-up connection configured.

Settings – Connection timeout

This field allows you to select the number of seconds you want ODEX to wait before closing the connection when no comms activity is occurring i.e. nothing is happening on this connection.

New/Edit AS2 connection – Security



The Security page is only active if you have specified a URL which uses SSL on the Overview page (i.e. an https URL).

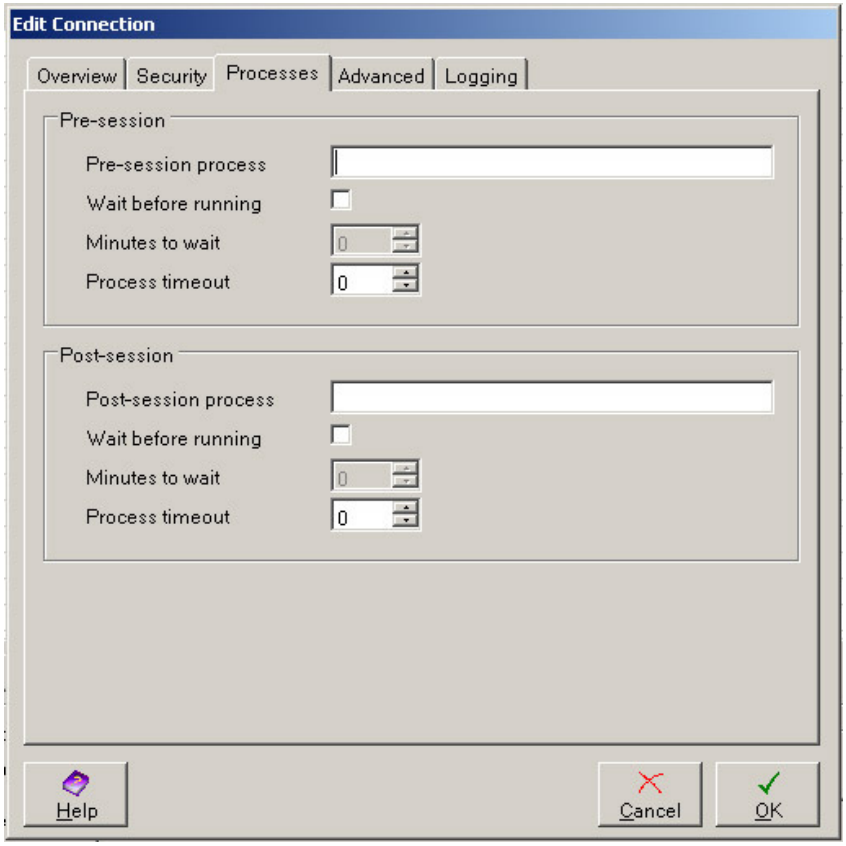
If you have specified an http URL, the 'Not a secure connection' option will be selected automatically and the remaining options will be disabled.

If the page is active you may choose from the following options:

- Remote server may use any certificate
- Remote server may use any trusted certificate
- Remote server must use the following certificate

If you choose the last option, action buttons are enabled for you to choose the certificate(s). See the section entitled ‘Dynamic Certificate Selection’.

New/Edit connection – Processes



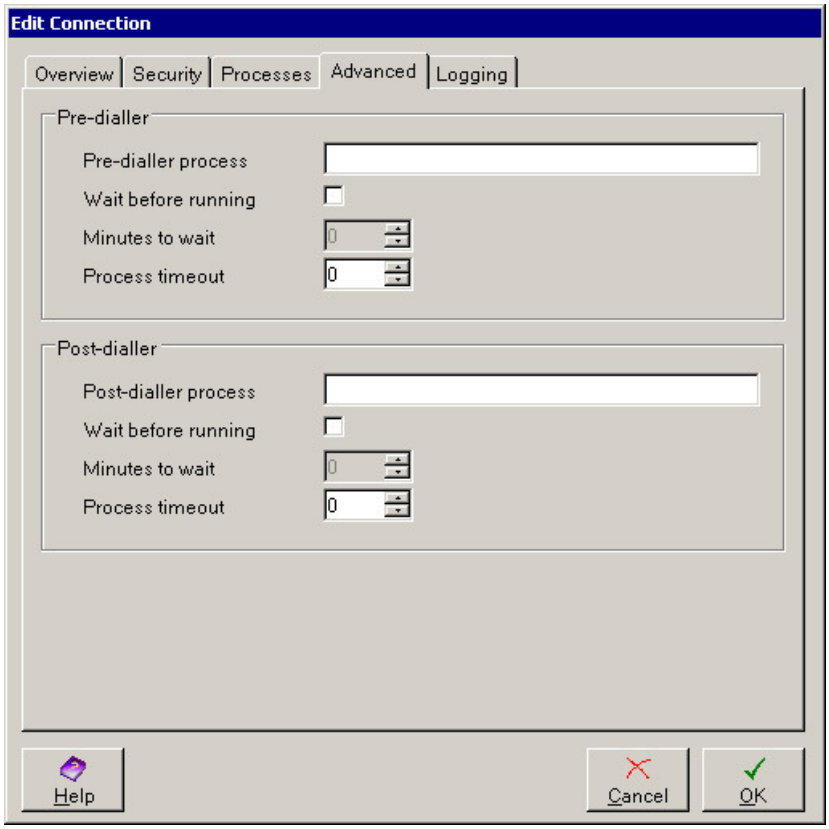
This dialog is divided into two sections – Pre-session and Post-session.

These fields allow you to specify batch files to be run before and/or after a communications session, together with delay, wait and timeout details.

In most cases, you will not need to use the fields on this page. If you do need to use them, the values you provide will be specific to your own system and so there is little to be gained by discussing them here.

New/Edit connection – Advanced

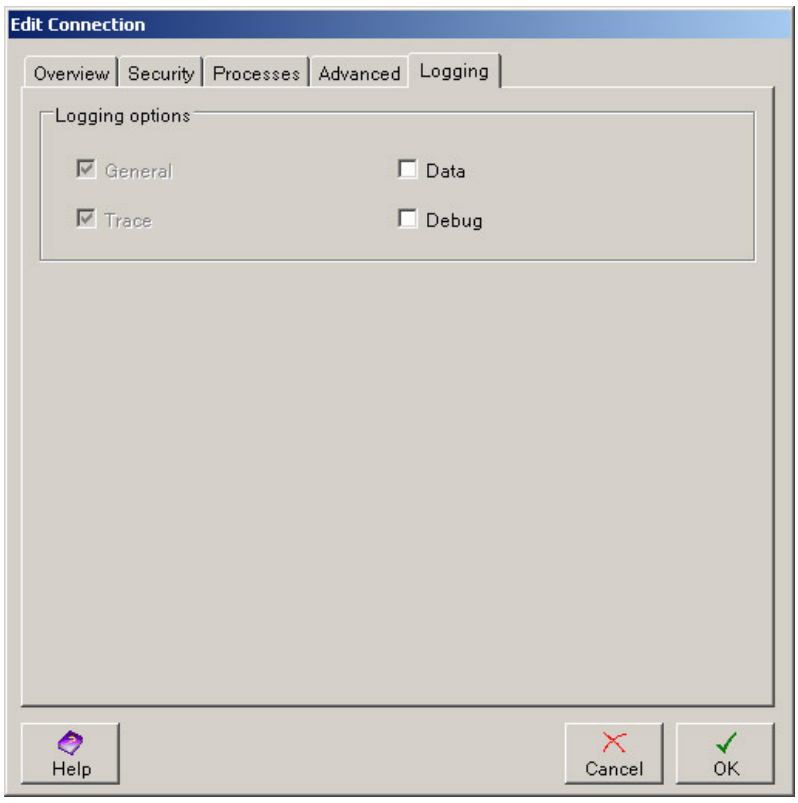
The dialog below will be seen if you have selected an AS2 subsystem.



These fields allow you to specify batch files to be run before and/or after a communications session, together with delay, wait and timeout details.

In most cases, you will not need to use the fields on this page. If you do need to use them, the values you provide will be specific to your own system and so there is little to be gained by discussing them here.

New/Edit connection – Logging



The four possible types are: General, Data, Trace and Debug.

- Data indicates high-level logging, displaying the data contents of the received/sent protocol and files being exchanged.
- Trace messages provide information about what is happening during communications sessions.
- Debug messages are another type of trace message, giving an indication of what is happening during communications sessions.
- General indicates any other log information that is not covered by the other three categories. Such information is not necessarily related to communications. This option is always selected and cannot be deselected.

Any log options that are selected but disabled indicate that these logging levels have been selected at a higher level within ODEX.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

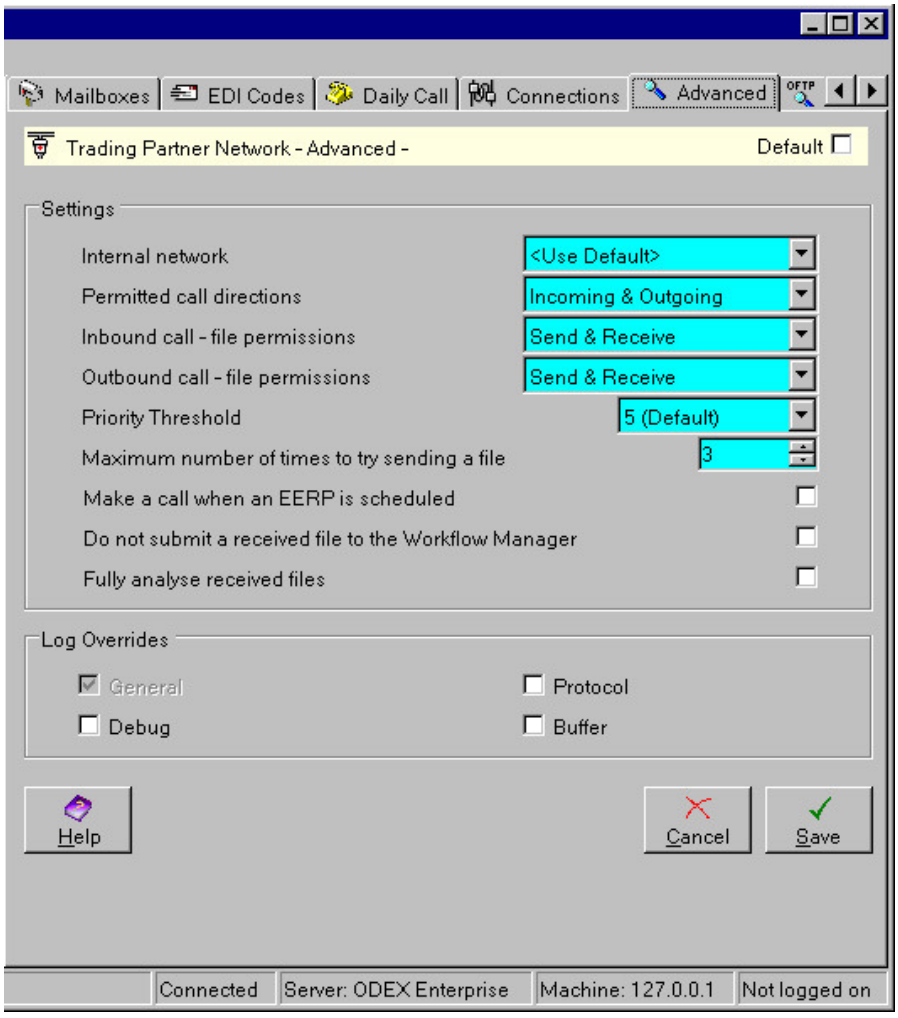
If you want to discard the changes you have made on these four pages, click the **Cancel** button.

OK

To save the changes you have made on these four pages, click the **OK** button.

OFTP Network – Advanced

The Advanced page looks like the example below.



There are two sections on this page – Settings and Log Overrides.

Settings

The Settings section allows you to select the values and settings of certain elements used during OFTP communications.

Settings – Internal network

Allows you to choose which internal network node (SSID) you want this network to communicate with.

This field will initially show the **<Use default>** option. If you do not want to use the default internal network, use the dropdown arrow to select the required internal network.

Settings – Permitted call directions

Specifies the direction of calls to be permitted with this network. Calls may be none, incoming only, outgoing only or both incoming and outgoing.

If you select "Incoming", this will disable the "Outbound call – file permissions" field below.

If you select "Outgoing", this will disable the "Inbound call – file permissions" field below.

Call direction of “none” means no calls can be made or received, though files may be received or sent through another network. Selecting this disables both file permissions.

Settings – Inbound call – file permissions

Specifies whether files may be received and/or sent during inbound calls. Files may be received only, sent only, or both received and sent.

This field is disabled if you have selected "Outgoing" in the "Permitted call directions" field.

Settings – Outbound call – file permissions

Specifies whether files may be received and/or sent during outbound calls. Files may be received only, sent only, or both received and sent.

This field is disabled if you have selected "Incoming" in the "Permitted call directions" field.

Settings – Priority threshold

Allows you to choose the priority of files to be sent to this network. Priority 5 (the default) is neither high (choose 1) nor low (choose 10).

Settings – Maximum number of times to try sending a file

Allows you to choose the maximum number of times you want ODEX to try and send a file to this network if it does not succeed first time. The default value is 3.

Settings – Make a call when an EERP is scheduled

Select this tickbox if you want ODEX to make a call to this network when an EERP is scheduled to be sent. This applies only to manually scheduled EERPs.

Settings – Do not submit a received file to the Workflow Manager

If you want to use ODEX purely as a communications application (i.e. you do not want ODEX to perform any processing on your files) you should tick this checkbox. This will ensure that any received files associated with this network will not be submitted to the Workflow Manager.

Settings – Fully analyse received files

If you want to use the RCVODETT command in the batch interface, you will need to select this option.

Log Overrides

The Log Overrides section allows you to select OFTP log settings which will work in conjunction with the usual log settings. The General option is always selected and cannot be deselected.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

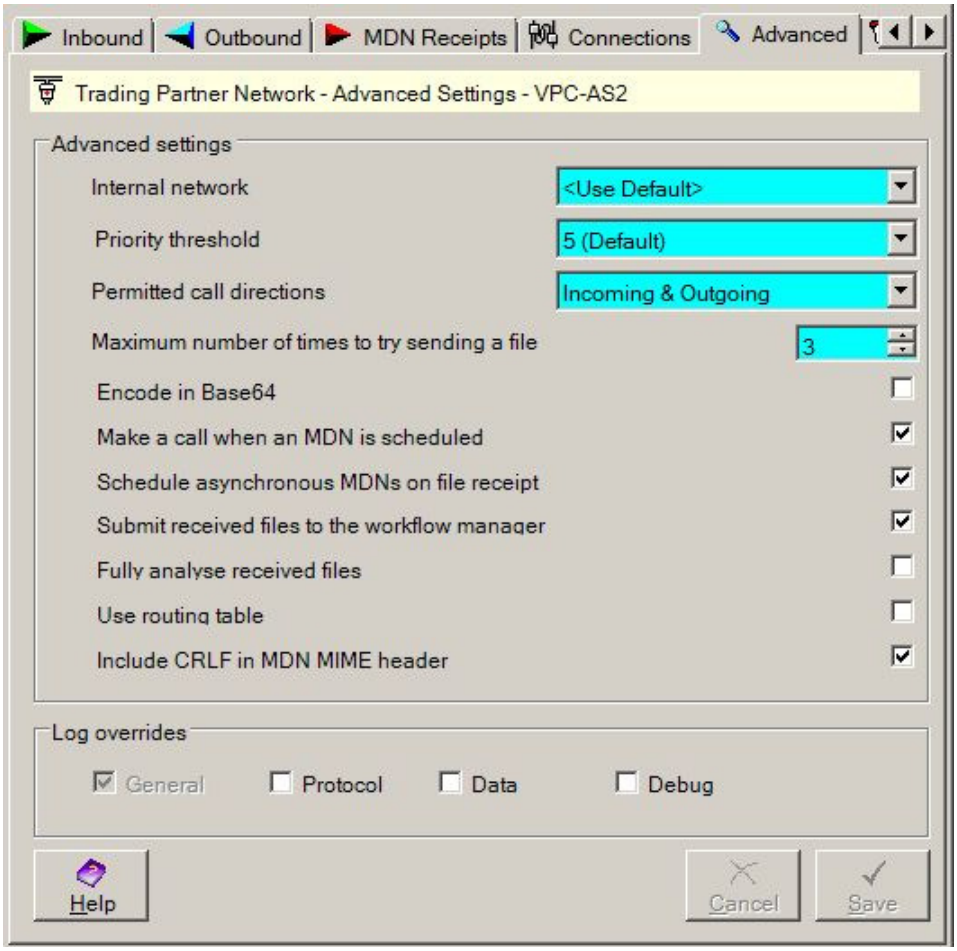
If you want to discard the changes you have made on this page, click the **Cancel** button.

Save

To save the changes you have made on this page, click the **Save** button.

AS2 Network – Advanced

The Advanced page looks like the example below.



There are two sections on this page – Advanced settings and Log overrides.

Advanced settings

The Settings section allows you to select the values and settings of certain elements used during AS2 communications.

Settings – Internal network

Allows you to choose which internal AS2 network you want this network to communicate with.

This field will initially show the **<Use default>** option. If you do not want to use the default internal network, use the dropdown arrow to select the required internal network.

Settings – Priority threshold

Allows you to choose the priority of files to be sent to this network. Priority 5 (the default) is neither high (choose 1) nor low (choose 10).

Settings – Permitted call directions

Specifies the direction of calls to be permitted with this network. Calls may be incoming only, outgoing only, both incoming and outgoing or none.

Settings – Maximum file retry attempts

Allows you to choose the maximum number of times you want ODEX to try and send a file to this network if it does not succeed first time. The default value is 2.

Settings – Schedule asynchronous MDNs on file receipt

If the trading partner requests an asynchronous MDN when sending files, when this option is selected, the MDN will be sent immediately after receiving a file.

When this option is disabled, the MDN can be sent at a later time, for example as part of a workflow.

Settings – Make a call when an MDN is scheduled

Select this tickbox if you want ODEX to make a call to this network when an MDN is scheduled to be sent. MDN scheduling occurs automatically but will not be sent automatically unless you select this tickbox.

Settings – Submit received files to the workflow manager

If you want to use ODEX purely as a communications application (i.e. you do not want ODEX to perform any processing on your files) you should deselect this checkbox. This will ensure that any received files associated with this network will not be submitted to the workflow manager.

Settings – Fully analyse received files

If you want to use the RCVODETT command in the batch interface, you will need to select this option.

Settings – Use routing table

This option specifies that all files received through this network must be forwarded to other trading partners, using the routing table to establish the destination.

Settings – Include CRLF in MDN MIME header

This option is used to control the format of the MDN when it is signed to ensure compatibility with different remote systems. The option is selected by default and should remain selected in most cases. However, if your trading partner rejects signed MDNs that you send, then deselect this option.

Log Overrides

The Log Overrides section allows you to select OFTP log settings which will work in conjunction with the usual log settings. The General option is always selected and cannot be deselected.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

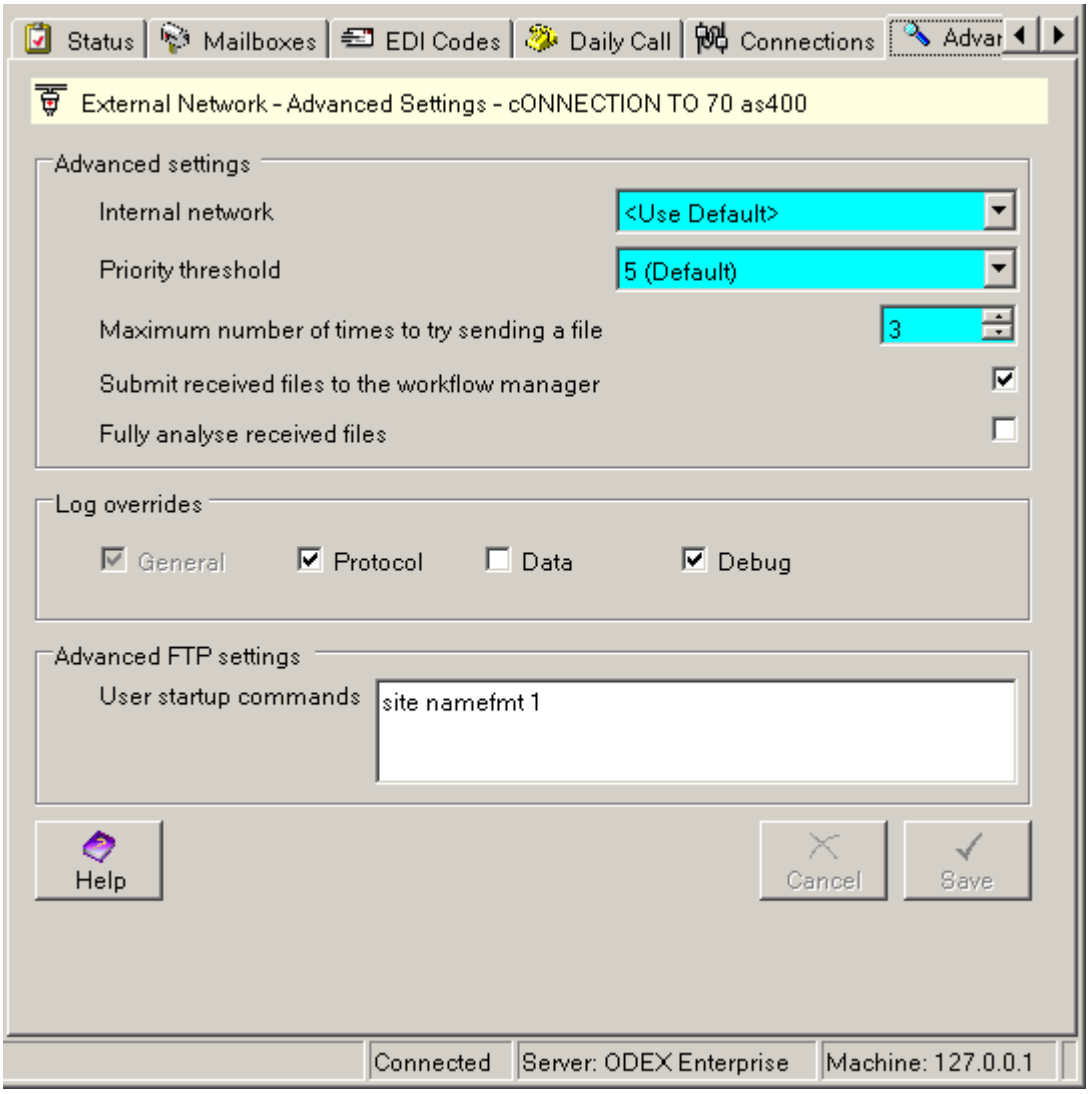
If you want to discard the changes you have made on this page, click the **Cancel** button.

Save

To save the changes you have made on this page, click the **Save** button.

FTP Client Network – Advanced

The FTP Client Advanced page looks like the example below,



There are two sections on this page – Advanced settings and Log Overrides.

Advanced Settings

The Settings section allows you to select the values and settings of certain elements used during FTP communications.

Advanced settings – Internal network

Allows you to choose which internal network node you want this network to communicate with.

This field will initially show the **<Use default>** option. If you do not want to use the default internal network, use the dropdown arrow to select the required internal network.

Advanced settings – Priority threshold

Allows you to choose the priority of files to be sent to this network. Priority 5 (the default) is neither high (choose 1) nor low (choose 10).

Advanced settings – Maximum number of times to try sending a file

Allows you to choose the maximum number of times you want ODEX to try and send a file to this network if it does not succeed first time. The default value is 3.

Advanced settings – Submit received files to the Workflow Manager

If you want to use ODEX purely as a communications application (i.e. you do not want ODEX to perform any processing on your files) you should deselect this checkbox. This will ensure that any received files associated with this network will not be submitted to the Workflow Manager.

Advanced settings – Fully analyse received files

If you want to use the RCVODETT command in the batch interface, you will need to select this option.

Log overrides

The Log Overrides section allows you to select OFTP log settings which will work in conjunction with the usual log settings. The General option is always selected and cannot be deselected.

Advanced FTP settings – User startup commands

These are FTP commands that are sent to the server at the beginning of an FTP session. They can be used to navigate to a different home directory, change settings that effect behaviour or anything required by a non standard FTP server.

For AS/400 this can be set to “site namefmt 1” as in the example in order to change the naming format used for files and directories.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

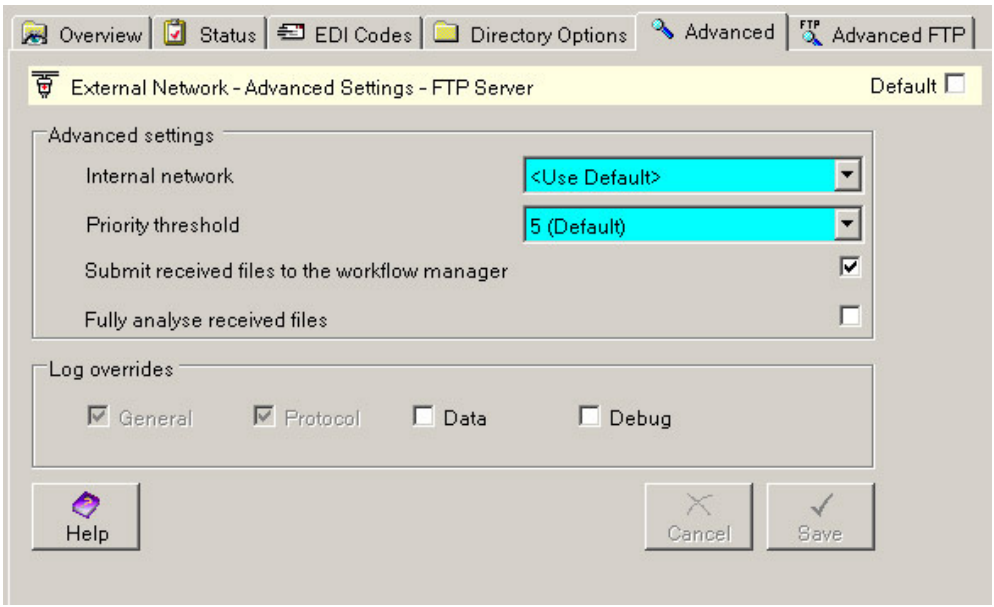
If you want to discard the changes you have made on this page, click the **Cancel** button.

Save

To save the changes you have made on this page, click the **Save** button.

FTP Server Network – Advanced

The FTP Server Advanced page looks like the example below,



There are two sections on this page – Advanced settings and Log Overrides.

Advanced Settings

The Settings section allows you to select the values and settings of certain elements used during FTP communications.

Advanced settings – Internal network

Allows you to choose which internal network node you want this network to communicate with.

This field will initially show the **<Use default>** option. If you do not want to use the default internal network, use the dropdown arrow to select the required internal network.

Advanced settings – Priority threshold

Allows you to choose the priority of files to be sent to this network. Priority 5 (the default) is neither high (choose 1) nor low (choose 10).

Advanced settings – Submit received files to the Workflow Manager

If you want to use ODEX purely as a communications application (i.e. you do not want ODEX to perform any processing on your files) you should deselect this checkbox. This will ensure that any received files associated with this network will not be submitted to the Workflow Manager.

Advanced settings – Fully analyse received files

If you want to use the RCVODETT command in the batch interface, you will need to select this option.

Log overrides

The Log Overrides section allows you to select OFTP log settings which will work in conjunction with the usual log settings. The General option is always selected and cannot be deselected.

Help

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

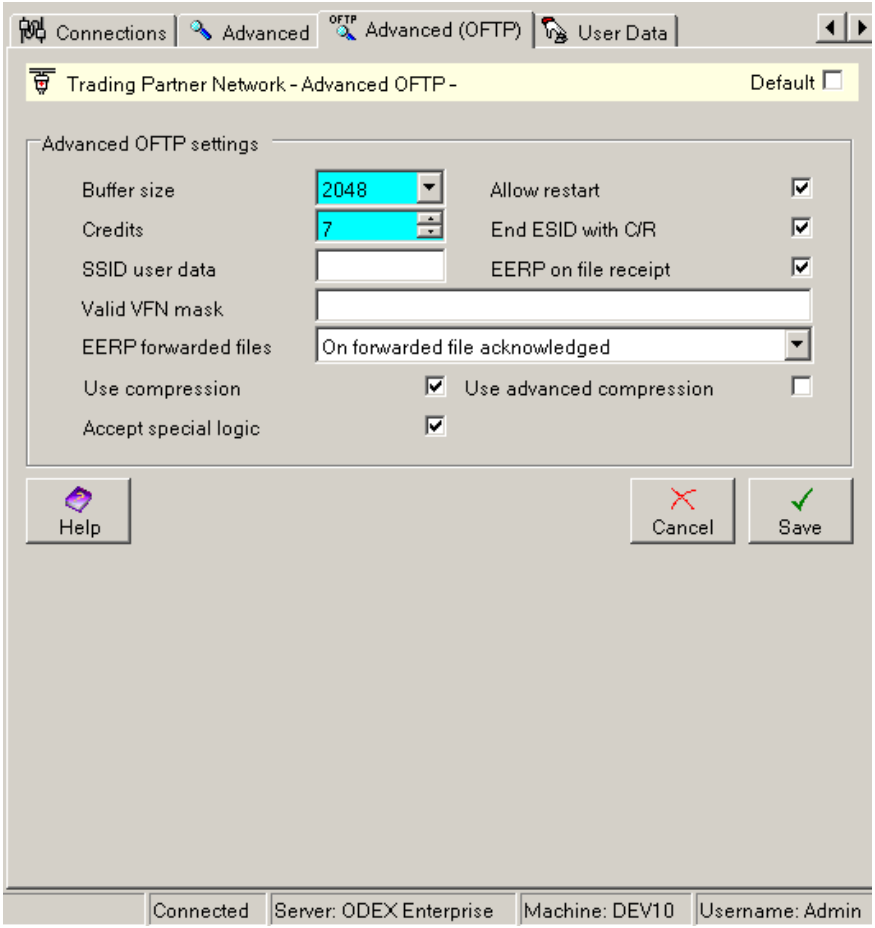
If you want to discard the changes you have made on this page, click the **Cancel** button.

Save

To save the changes you have made on this page, click the **Save** button.

Network – Advanced (OFTP)

The Advanced (OFTP) page is only applicable to OFTP networks and is described below.



There is one section on this page – Advanced OFTP Settings.

Advanced OFTP settings

The Advanced OFTP settings section allows you to select the values and settings of certain elements used during OFTP communications.

These values and settings are to be agreed mutually between your company and this trading partner or clearing centre.

Advanced OFTP settings – Buffer size

This is the size of the exchange buffers used to communicate with this network. When ODEX transmits a file it does so in a number of exchange buffers, passing each buffer full to the communications medium or receiving buffers from the exchange medium. The communications medium (X.25 or Async) must then send that buffer. The larger the exchange buffer the better as the throughput will be greatly increased.

Advanced OFTP settings – Allow restart

If this tickbox is checked (the default value) then restart is supported by ODEX. If the box is not checked, then restart will not be supported and any attempt to restart part way through a file will be rejected by ODEX. In the latter case, if a file is part way through transmission and an interruption occurs on the line, re-connection to the trading partner will mean that the file is restarted again from the beginning.

Advanced OFTP settings – Credits

The credit value controls the flow of information between the partners and is closely associated with the exchange buffer size. When a file is being sent, ODEX will send a buffer of information across the communications medium. It

will then assemble another exchange buffer for sending. If it has not yet sent the number of buffers set in the Credits field, then it will keep sending data buffers until it has. Once it has sent this number of exchange buffers, it will wait for a Credit (an OFTP CDT command) to come from the remote end, stating that all the exchange buffers have been received. When it gets this credit, ODEX will then send another set of exchange buffers. The credit limit is acting as the "window size" of a data flow control mechanism.

Most users should set the Credit limit to a value of 7 for maximum throughput.

Advanced OFTP settings – End ESID with CR

Most trading partners expect the OFTP ESID command to end with a carriage return character. Therefore the default setting for this field is to check the tick box. However, Daimler Chrysler will reject an ESID which ends with a carriage-return character so the tick box should be unchecked if this network is for DC.

Advanced OFTP settings – SSID user data

This field allows you to provide any SSID user data requested by your trading partner.

Advanced OFTP settings – EERP on file receipt

This tickbox should be selected if you wish to send an EERP to your trading partner immediately on successful receipt of a file. This means that EERPs for received files will be sent in the same session as the files are received.

Advanced OFTP settings – Valid VFN mask

This field allows you to provide a VFN (virtual filename) mask to be matched against files received from this trading partner network. If the VFN of the received file does not match the mask, the file will be rejected.

N.B. Any VFN mask you specify in the Mailbox section for this network will override the VFN on this page.

You may use the asterisk character (*) to signify one or more unspecified characters. You may use the question mark character (?) to signify one unspecified character.

Taking the Ford VFN format as an example, you could use one of the following filename masks to achieve different results:

FORD.S* – accept all Ford files

FORD.SABC12* – accept all Ford messages for the Supplier code ABC12

FORD.S*RE – accept all Ford Release messages for any Supplier code

FORD.S?????ST – accept all Ford DCI messages for any Supplier code (five question marks are more precise than the asterisk but would have the same effect)

Advanced OFTP settings – EERP forwarded files

The values in the EERP forwarded files field only apply to files that are being forwarded, as in a clearing centre environment. If files are not being forwarded, only the EERP on file receipt option applies. The options in the list are as follows :

On forwarded file acknowledged - when forwarding a file, schedule an EERP to the originating trading partner when the forwarded file is acknowledged.

On forwarded file sent - when forwarding a file, schedule an EERP to the originating trading partner as soon as the forward file is sent.

Never - don't send an EERP for forward files. This allows the EERP to be generated manually or by using the acknowledge job.

Advanced OFTP settings – Use compression

This tickbox should be selected if you wish to use compression on your data transfers. Compression is a method of making a large file smaller when transmitting it, by taking similar characters and encoding the transmission so that each character only occurs once but is preceded by a repetition number.

For example if you were sending a file containing the data “0100000000101”, what would be sent would be 01 then a single character stating that the following character will occur 8 times, then the 0 multiple occurrence character, then the number 101. In this example 13 characters are compressed into 7.

Files with a large quantity of repetition (space characters for example) are the best candidates for compression. If in doubt, it is recommended that compression is selected.

Advanced OFTP settings – Use advanced compression

This option is only available for networks that are configured to use OFTP revision 2. Revision 2 of the OFTP specification introduced a more efficient compression method. Check this tick box if the trading partner uses at least Revision 2 of the protocol.

If you need more information about the fields on this page and how to fill them in, click on the **Help** button.

Cancel

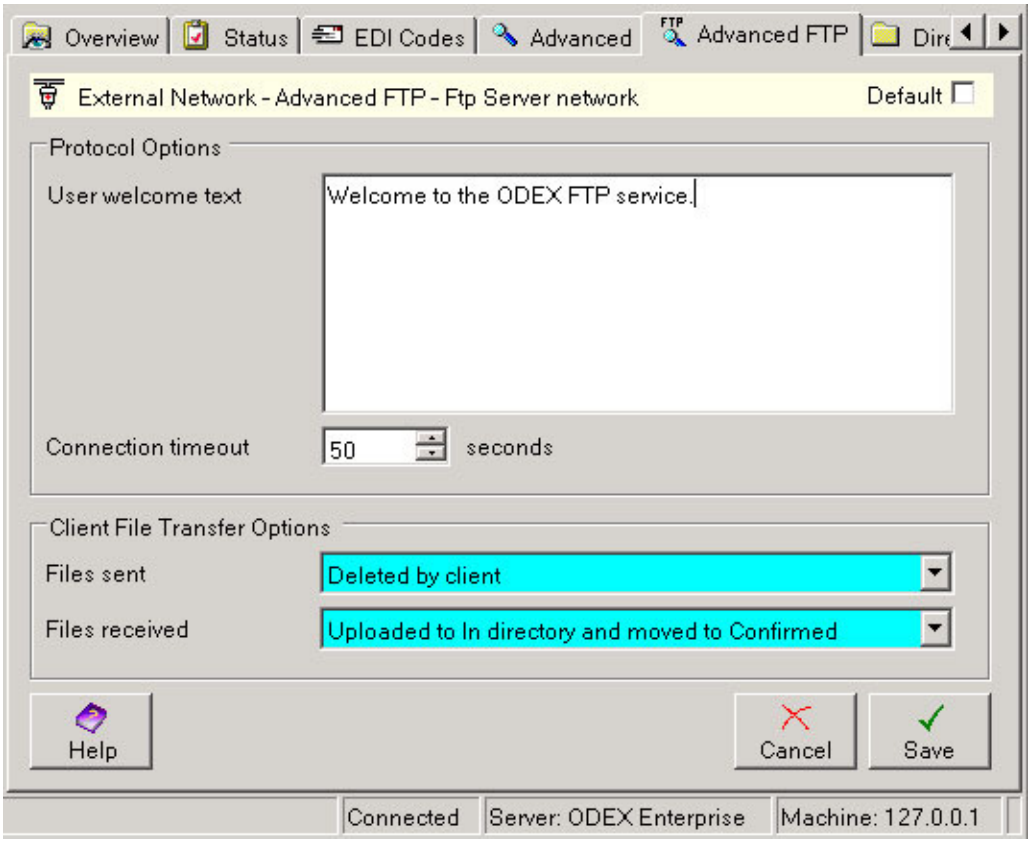
If you want to discard the changes you have made on this page, click the **Cancel** button.

Save

To save the changes you have made on this page, click the **Save** button.

Network – Advanced FTP

The Advanced page looks like the example below, and is present for an FTP server network in order to allow specification of advanced FTP server options.



The page is divided into two sections, Protocol Options and Client File Transfer Options.

Protocol Options

This defines protocol specific options for the user defined by this network.

Protocol Options – User welcome text

There is an opportunity to send text back to a client at two points. The first is when a client connects and this is specified in the FTP server subsystem, the other is when the user has successfully logged in. The message here will be sent to the user once their username and password have been verified. Please note that if you are connecting to the ODEX FTP server using an automated client, such as ODEX then this message may not be explicitly shown to the user.

New lines can be used to add emphasis.

Protocol Options – Connection timeout

This is the amount of time in seconds before the connection times out. If the client does not communicate with the server for this amount of time then the connection will be automatically and immediately severed. If the client using this network (e.g. the trading partner or a client on your LAN) has an automated FTP client then this timeout value can be very low as an automated client will not wait before sending the next command. If however the user is connecting by hand then there may be longer pauses between communications and you may wish to raise the timeout level.

Client File Transfer Options

These are modes of working and define the way in which the server will react to files stored and retrieved on the server. It is important that the trading partner or other user is aware of the way in which you wish them to work and that it corresponds to these settings.

Client File Transfer Options – Files sent

This option defines the way in which ODEX handles files sent to this FTP server network, for an external FTP client to pick up. There are two options.

- 'Deleted by client' – This is the default option and specifies that the client must delete a file once it has received it successfully in order to indicate to ODEX that it has been received and we no longer need to make this file available any longer.
- 'Deleted by ODEX' – This means that once the FTP server thinks the client has successfully received a file, it will remove that file from the "Out" directory and mark the file as sent and acknowledged within ODEX.

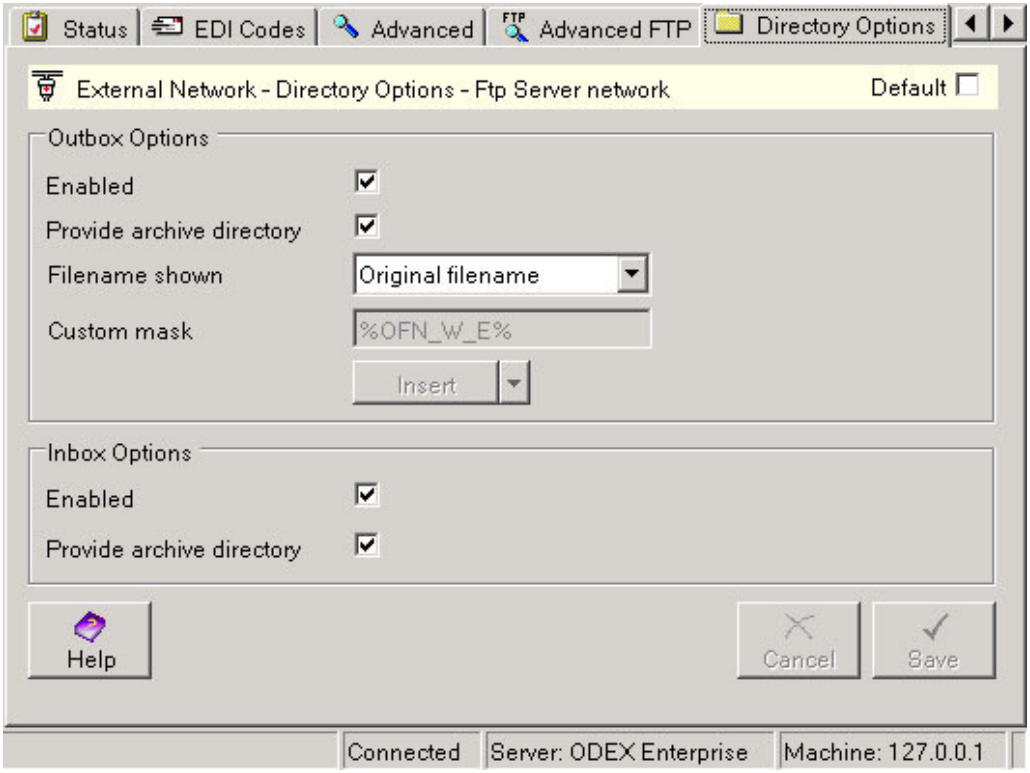
Client File Transfer Options – Files received

This option defines the way ODEX handles files that have been received from the external FTP client, files coming in to ODEX through this network. Again, there are two options.

- 'Uploaded to In and moved to Confirmed' – This option means that ODEX will not receive a file from the client until it has been moved from the In directory where it was uploaded to, to the Confirmed directory. This means that a file can be uploaded repeatedly until the client is sure it has been correctly received and then move it in order to signal ODEX to pick it up. Files can be moved by using the FTP rename command and specifying a different path, e.g. "rename /In/NewFile /Confirmed/ConfEDI0102". Files not confirmed by moving will be disregarded and deleted at the end of a session.
- 'Uploaded to In directory' – This option means that ODEX will receive and process a file as soon as it is moved into the "In" directory as long as it thinks it has been received correctly. However be aware that a unexpected network disconnect during file transfer could leave ODEX FTP server thinking a file has been received correctly and processing it even though it would have only been partly received.

Network – Directory Options

Directory options appear for an FTP server network and the page looks like the example below.



The page is made up of two sets of options, Outbox Options and Inbox Options.

Outbox Options

These are options that affect the Outbox, which means they affect the way files are sent to this network from ODEX.

Outbox Options – Enabled

This switches on the “Out” directory. Inside are all files sent to this network. If this is disabled then the directory will not be visible or traversable to an FTP client which means the client will not be able to pick up any files sent to it from ODEX.

Outbox Options – Provide archive directory

The archive directory, called “OutArchive” will contain all files that have previously been sent to this network that have not been deleted (either automatically or by hand in the ODEX Workstation. Disabling the option will make the directory invisible and no previously sent files will be available to any FTP client logging on.

Outbox Options – Filename shown

This option relates to the filename that is shown to the client for files that have been scheduled to this network. The original filename will be the original name of the file if it was picked up from disk, or the VFN if it came from an OFTP network. If this option is system filename then a unique name will be shown for every file. Custom mask allows you to enter yourself where the filename comes from.

Outbox Options – Custom mask

This option is enabled if the filename shown is set to “Custom mask” and allows the use of placeholders from the button below to construct any filename. Care should be taken, as it could be confusing to a trading partner if all the files have the same name and ODEX will not schedule a file if the filename is empty. For example, a file from an AS2 network will not have an original filename, so

specifying Original Filename would cause empty filenames. More information on placeholders and there meanings is given in the section on placeholders.

Inbox Options

The Inbox defines the way in which files are received from the external network to ODEX.

Inbox Options – Enabled

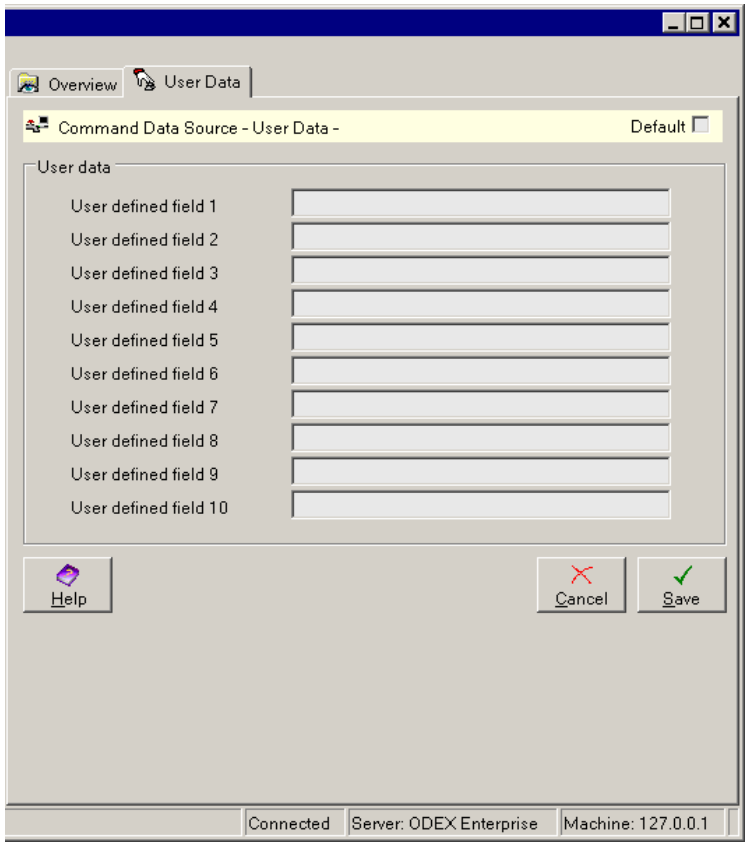
Switching on this option provides the client with an 'In' directory (and possibly a 'Confirmed' directory – see the Advanced FTP section) which allows the client to upload files. Disabling the Inbox means that this network user will not be able to transfer files to ODEX.

Inbox Options – Provide archive directory

The archive directory for the Inbox provides the client with an 'InArchive' directory which contains every file that the external network client has sent to ODEX that has not been deleted (either automatically or by hand in ODEX Workstation).

Network – User Data

The User Data page allows you to provide a number of fields that can be used throughout Odex. For example, you can set up a User Data field against each Network to specify a different email subject for each Network. Then, if a workflow is set up to send you an email whenever a file is received from this network, you can use a placeholder to specify that the network User Data should be used for the email subject. Using this technique you can tailor your emails to be Network specific, without having a number of channels/workflows defined.



Simply edit the fields you wish to use and they can then be accessed using placeholders in jobs and actions (see the Placeholders section for more details).

ENGDAT Relationships

The ENGDAT relationships section of the ODEX Administrator is where you define the settings that will be used when exchanging ENGDAT folders with your trading partners. The settings include originator and destination details, validation profile, contacts and default field values.

Before you begin to add details to this section, you should ensure that you have configured the company, contact and communication details for your company and your trading partners. Please refer to the following sections for information on how to configure your company details:

Adding/Editing Internal Companies

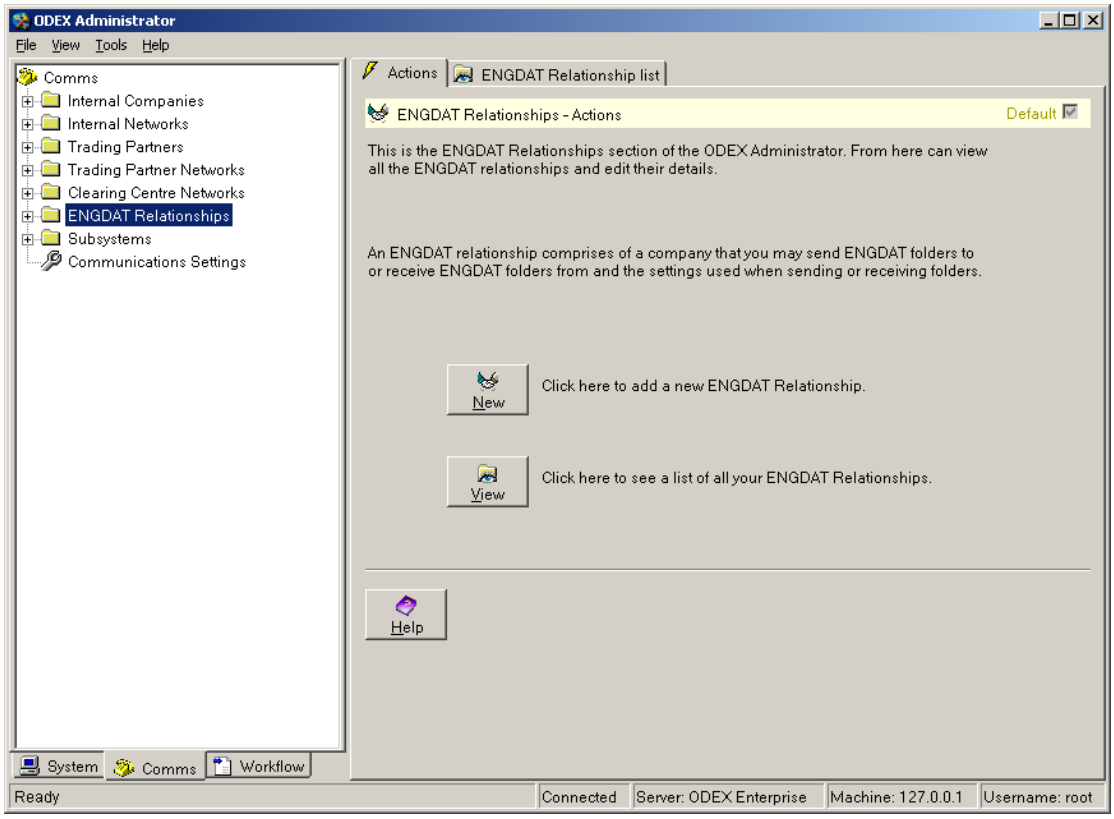
Adding/Editing an Internal OFTP Network

For details of how to set up your trading partner's details, please refer to the following sections:

Adding/Editing Trading partners

Adding/Editing Networks

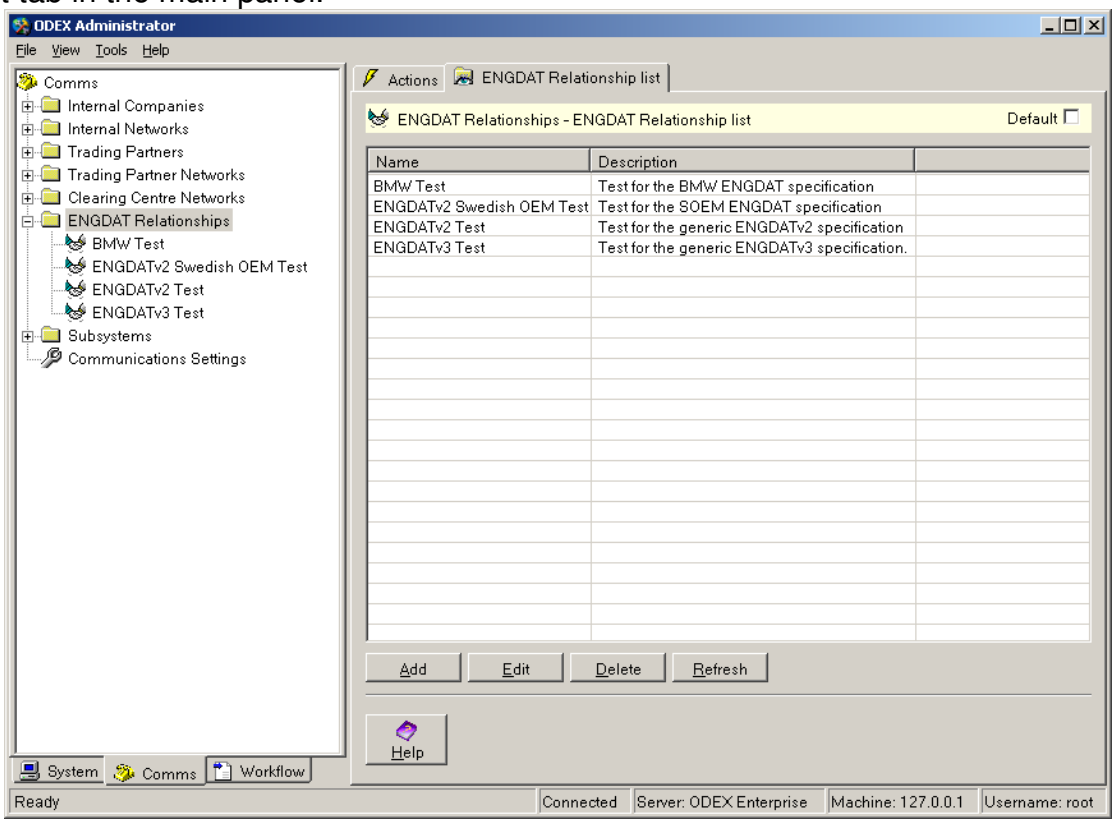
Click on the name ENGDAT Relationships in the Navigation Panel to see the default page for the ENGDAT Relationships section. By default this is the Actions page, as shown below.



From this section you can add, view and edit your ENGDAT Relationships. As with other sections, there are two tabs on the Information Panel: Actions and ENGDAT Relationship List. In the Actions tab there are two buttons: **New** allows you to add a new relationship, and **View** allows you to see a list of existing relationships, from where you can add, view, edit and delete them.

Viewing your ENGDAT relationships

The page shown below can be reached by either clicking the **View** button on the ENGDAT Relationships – Actions page or clicking on the ENGDAT Relationship List tab in the main panel.



As you can see, the Information Panel now shows a table with a summary of the ENGDAT Relationships you have stored. This table details the names and descriptions of each, so that they can easily be distinguished.

The following actions can be taken from this page:

Add

Clicking the **Add** button will add a new blank ENGDAT Relationship and send you to the set of pages for that new relationship, described under ENGDAT Relationship – Overview.

Edit

Clicking the **Edit** button allows you to edit the details of an existing ENGDAT Relationship, by sending you to the same set of pages for the selected relationship under ENGDAT Relationship – Overview. Equivalently, you can press Enter with the chosen relationship selected, or double click on the chosen relationship, to invoke the same action.

Delete

Clicking the **Delete** button will permanently remove the selected ENGDAT Relationship from the list. Equivalently, you can press the Delete key to invoke the same action. If you choose to do so, a confirmation dialogue will come up as a safeguard against accidental deletion. Click **Yes** to proceed with the deletion, or **No** to cancel.

Help

Clicking the **Help** button or pressing the F1 key will bring up this page.

Adding/Editing ENGDAT Relationships

In order to add a new ENGDAT relationship, you can click the **New** button on the ENGDAT Relationships – Actions page or the **Add** button on the ENGDAT Relationship list page of the same section.

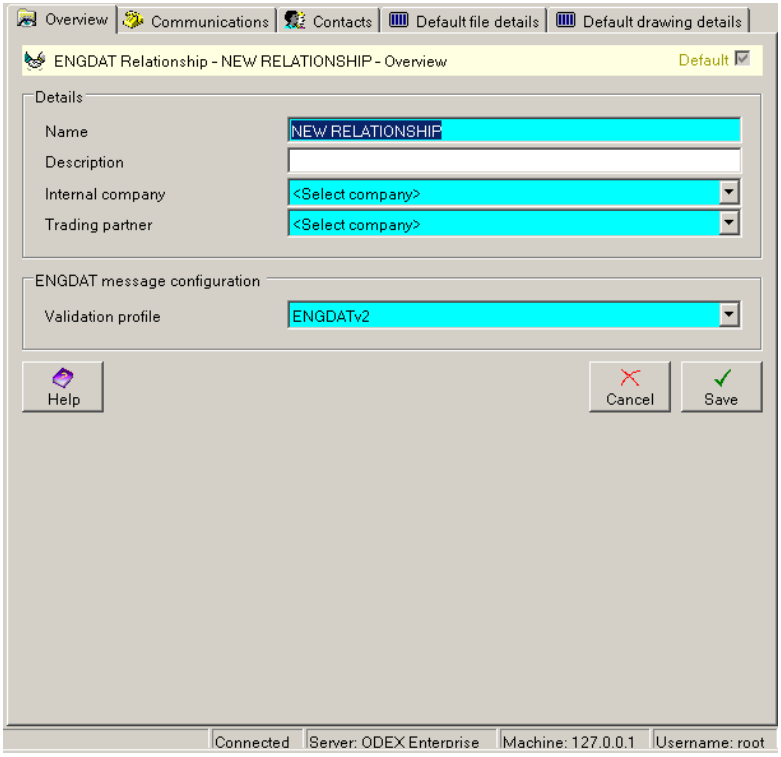
If you want to edit an existing ENGDAT relationship, select the desired relationship from the ENGDAT Relationship list page, then either click the **Edit** button or press the **Enter** key. Alternatively, you can simply double click the desired relationship on that list.

Either action results in the same set of pages being displayed. If you choose to create a new relationship, all the fields in each page will be either blank or filled with default values. If you chose to edit an existing relationship, the fields will be filled with the information on that selected relationship. There are three basic tabs, as well as multiple possible additional tabs depending on the validation profile chosen.

Please note that each **Save** and **Cancel** button in this section works universally for the whole relationship – so you need not click **Save** until you have entered the desired data in each tab, and clicking **Cancel** will discard all unsaved data in every tab.

ENGDAT Relationship – Overview

The Overview page contains mandatory information regarding the relationship itself, including how the relationship will be identified in the ENGDAT Relationship List. When creating a new relationship, you must fill in the mandatory fields on this page before you fill in the details on any of the other pages. Below is an example of what this page will look like.



Details – Name

This is the name by which the relationship will be identified.

Details – Description

This is an optional description of the relationship, allowing it to be easily identified in the future.

Details – Internal company

This dropdown box allows you to choose the internal company to be the originator of the ENGDAT messages

Details – Trading partner

This dropdown box allows you to choose the trading partner to be the recipient of the ENGDAT messages.

ENGDAT message configuration – Validation profile

This dropdown box allows you to choose the validation profile containing the settings for ENGDAT messages. A validation profile determines which ENGDAT message version will be used, the maximum and minimum permitted field lengths in the message and determines which fields are required in the message.

Note that changing the validation profile changes which tabs are available. This is discussed further in the 'default details' section. When you change the validation profile, this will also change the exchange reference pattern (on the communications tab) to the default for the validation profile.

Help

This page, containing details on each field, can be reached by clicking the **Help** button.

Cancel

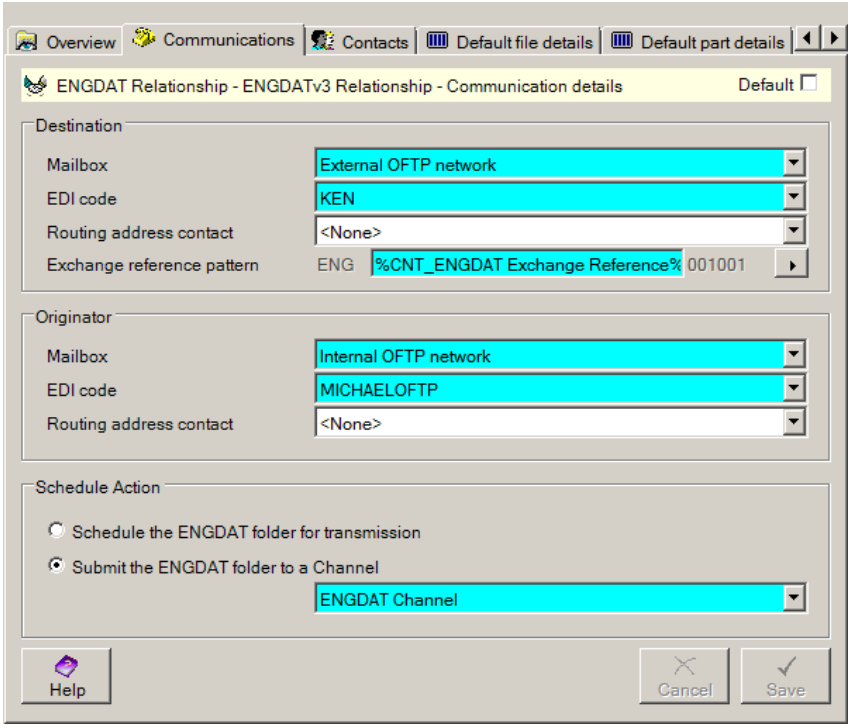
Clicking the **Cancel** button with unsaved changes will bring up a confirmation dialogue. Clicking **Yes** will discard all unsaved changes, and clicking **No** will abort the operation.

Save

To save all unsaved changes that you have made in this section, click the **Save** button.

ENGDAT Relationship – Communications

The Communications page contains further details of the destination and originator of the message relevant to communications. Below is an example of what this page will look like.



The information available here is dependent on what was chosen as the Internal Company and Trading Partner in the Overview tab, therefore values for those fields must be selected before this tab can be accessed.

Destination – Mailbox

This field allows you to choose from a list of mailboxes for the chosen recipient company. Outbound ENGDAT folders will be sent to this mailbox.

Destination – EDI Code

This field allows you to choose from a list of EDI codes for the chosen recipient company. Where an ENGDAT EDI message is to be sent, this EDI code will be set as the destination EDI code in the message, unless a value is selected for the routing address contact (see below).

Destination – Routing address contact

Contacts in ODEX have a routing code property. If required, the routing code stored against a contact may be used as the destination EDI code in outbound ENGDAT EDI messages sent to the trading partner. If you select a contact in this field, the contact's routing code will override the selected destination EDI code.

Destination – Exchange reference pattern

This field allows you to specify what will make up the exchange reference generated for each folder. Note that the exchange reference of an ENGDAT folder is the portion of the virtual filename between the first 3 VFN characters (ENG) and the final 6 digits of the VFN (the number of files in the folder and the sequence number of the file). It is not necessary to add the ENG characters or the final 6 digits of the VFN.

If you click the button marked with the arrow, you can choose from a list of placeholders regarding possible data fields that can go into the exchange reference when it is generated. When a folder is saved for the first time, these placeholders will be automatically replaced by the pertinent data.

Trading partners require that the exchange reference be unique. In most cases, it will be sufficient to use a numerical counter, though it is also possible to include other values, such as the current date and time. An exchange reference pattern will automatically be entered in this field for you, depending on which validation profile you choose.

Originator – Mailbox

This field allows you to choose from a list of mailboxes for the chosen originating company. This is the mailbox from which outbound ENGDAT folders will be sent.

Originator – EDI Code

This field allows you to choose from a list of EDI codes for the chosen originating company. This EDI code will be set as the origin EDI code for outbound ENGDAT EDI messages, unless a routing address contact is selected (see below).

Originator – Routing address contact

Contacts in ODEX have a routing code property. If required, the routing code stored against a contact may be used as the originator EDI code in outbound ENGDAT EDI messages sent to the trading partner.

Schedule Action – Schedule ENGDAT folder for transmission

If this is selected then the folder will be immediately scheduled to the trading partner specified in the relationship.

Schedule Action – Submit ENGDAT folder to a Channel

If submit is selected then each file in the folder is placed on the workflow specified by the channel. In order to be scheduled for transmission the 'Schedule ENGDAT file' job must be on this workflow. For more information see Using the Gedas Com-Secure Application with ODEX.

Help

This page, containing details on each field, can be reached by clicking the **Help** button.

Cancel

Clicking the **Cancel** button with unsaved changes will bring up a confirmation dialogue. Clicking **Yes** will discard all unsaved changes, and clicking **No** will abort the operation.

Save

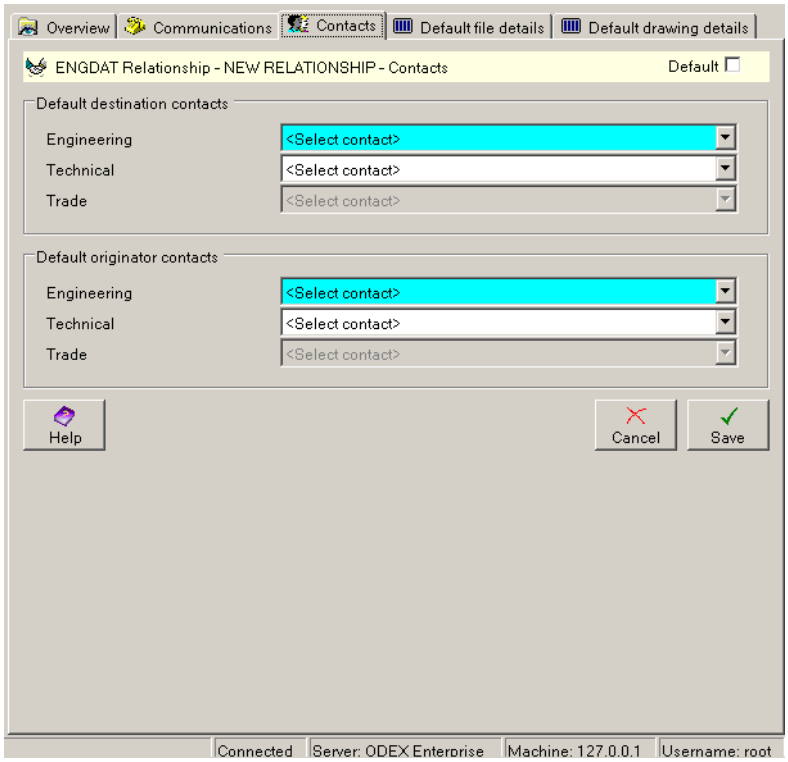
To save all unsaved changes that you have made in this section, click the **Save** button.

ENGDAT Relationship – Contacts

In ENGDAT messages, origin and destination contact details must be given. The Contacts page allows you to choose which contacts will be selected by default when you create an ENGDAT folder using this ENGDAT relationship.

In ENGDAT versions 1 and 2, details of an origin and destination engineering contact must be given. Some trading partners may also require you to provide details of technical or trade contacts. Trade contact details are only available when exchanging ENGDAT version 3 messages with a trading partner.

Below is an example of what the page will look like. Note that the Trade contact fields are disabled because of the current ENGDATv2 validation profile being used.



Default destination contacts – Engineering

This dropdown box allows you to choose from all the contacts in the selected trading partner company. The selected contact will be the contact that is selected as the destination engineering contact when you create a new ENGDAT folder using this relationship.

Default destination contacts – Technical

This dropdown box allows you to choose from all the contacts in the selected trading partner company. The selected contact will be the contact that is selected as the destination technical contact when you create a new ENGDAT folder using this relationship.

This field may be unavailable if your trading partner does not require technical contact details to be provided.

Default destination contacts – Trade

This dropdown box allows you to choose from all the contacts in the selected trading partner company. The selected contact will be the contact that is

selected as the destination trade contact when you create a new ENGDAT folder using this relationship.

Note that you will only be able to select a trade contact if the relationship is configured to use ENGDAT version 3 messages.

Default originator contacts – Engineering

This dropdown box allows you to choose from all the contacts in the selected originator company. The selected contact will be the contact that is selected as the origin engineering contact when you create a new ENGDAT folder using this relationship.

Default originator contacts – Technical

This dropdown box allows you to choose from all the contacts in the selected origin company. The selected contact will be the contact that is selected as the origin technical contact when you create a new ENGDAT folder using this relationship.

This field may be unavailable if your trading partner does not require technical contact details to be provided.

Default originator contacts – Trade

This dropdown box allows you to choose from all the contacts in the selected origin company. The selected contact will be the contact that is selected by default as the origin trade contact when you create a new ENGDAT folder using this relationship.

Note that you will only be able to select a trade contact if the relationship is configured to use ENGDAT version 3 messages.

Help

This page, containing details on each field, can be reached by clicking the **Help** button.

Cancel

Clicking the **Cancel** button with unsaved changes will bring up a confirmation dialogue. Clicking **Yes** will discard all unsaved changes, and clicking **No** will abort the operation.

Save

To save all unsaved changes that you have made in this section, click the **Save** button.

ENGDAT Relationship – Default Details

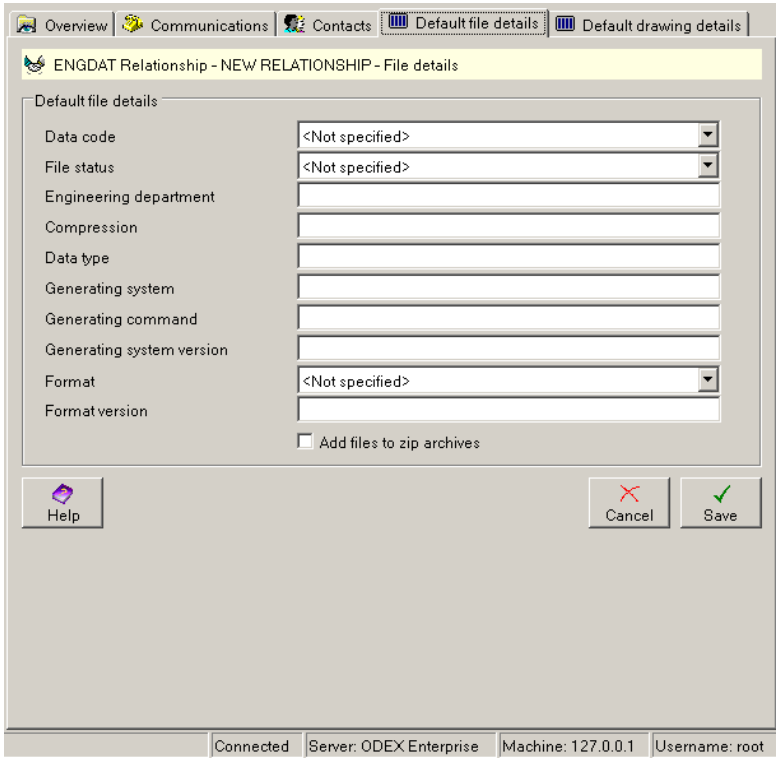
When a file is added to an ENGDAT folder, fields are provided allowing characteristics of the file to be specified, such as details of the file format and the system that generated the file etc. These field values are then included in the ENGDAT message.

The pages described in this section allow default values for these fields to be specified. When a new file is added to a folder, the available fields will then initially be populated with any values specified on these pages. This allows a 'template' for new files to be created and eliminates the need to enter the same information repeatedly for different files.

The available fields depend on the validation profile selected on the overview. If you chose a validation profile that uses ENGDAT version 1 or version 2, the

‘Default file details’ and ‘Default drawing details’ tabs will be available. For ENGDAT version 3 relationships, ‘Default file details’, ‘Default part details’ and ‘Default contained file details’ will be available.

Below is an example of one of these defaults tabs.



Default details

Any values you enter here will be used as the default value when adding a new file to an ENGDAT folder. For example, if you select a data code of ‘ASCII, 7 bit’, every time you add a new file to an ENGDAT folder that was created using this relationship, ‘ASCII, 7 bit’ will be selected by default in the data code field.

You may also select ‘Add files to zip archives’. When this option is selected, every file that you add to a new folder will automatically be compressed to a zip archive before it is sent. You may still override this setting for individual files as you add the files to an ENGDAT folder.

Please consult the help pages on the ENGDAT Workstation for details on each field.

Help

This page, containing details on each field, can be reached by clicking the **Help** button.

Cancel

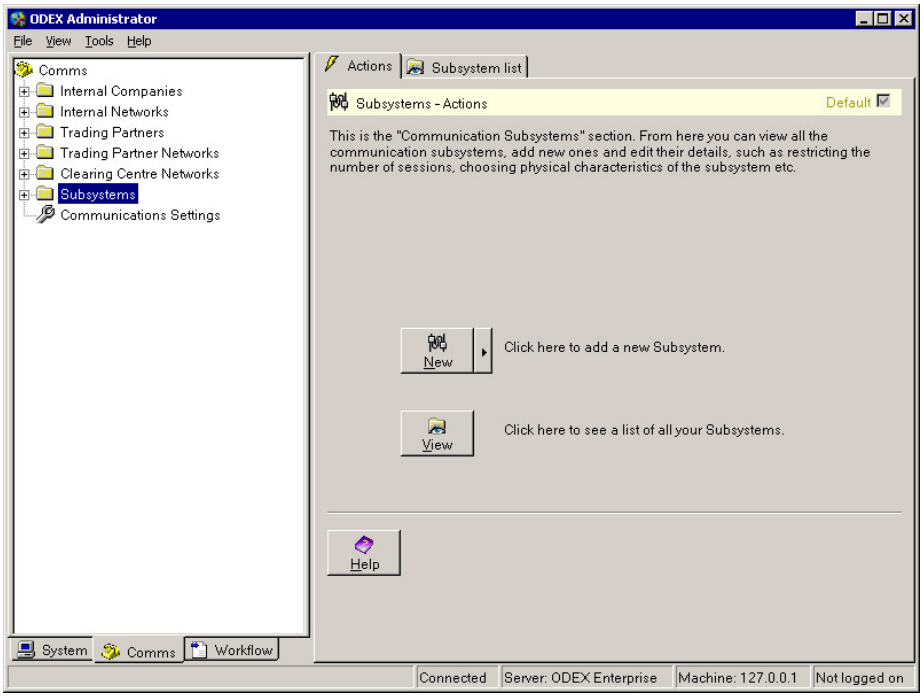
Clicking the **Cancel** button with unsaved changes will bring up a confirmation dialogue. Clicking **Yes** will discard all unsaved changes, and clicking **No** will abort the operation.

Save

To save all unsaved changes that you have made in this section, click the **Save** button.

Subsystems

Click on the name Subsystems in the Navigation Panel to see the default page for the Subsystems section, as shown below. This is the Subsystems – Actions page.



There are 5 different types of subsystem you can currently use within ODEX. These are:

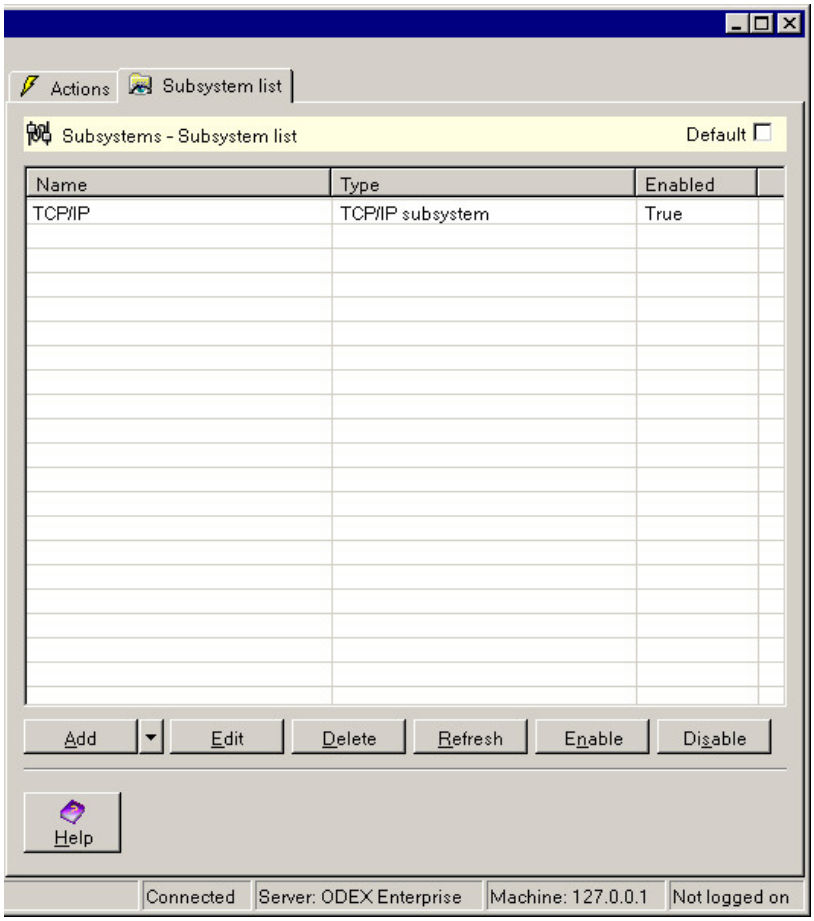
- Local CAPI2 card subsystem (OFTP only)
- Remote CAPI2 server subsystem (OFTP only)
- TCP/IP subsystem (OFTP only)
- HTTP subsystem (AS2 only)
- XOT subsystem (OFTP only)

A TCP/IP subsystem has already been profiled for you.

Select the type you want to add from the arrow alongside the **New** button.

Viewing all your subsystems

To view any of your existing subsystems, click the **View** button. This will bring up the Subsystem list page, shown below, from which you can add new subsystems, edit, delete, enable and disable existing subsystems.



This page lists all the subsystems you currently have defined in your system. The Enabled column shows whether the subsystem is currently enabled or not.

Adding/Editing a CAPI2 subsystem

Both the Local and Remote CAPI2 subsystems have five pages: Overview, Listeners, Advanced, Controllers and Device Details.

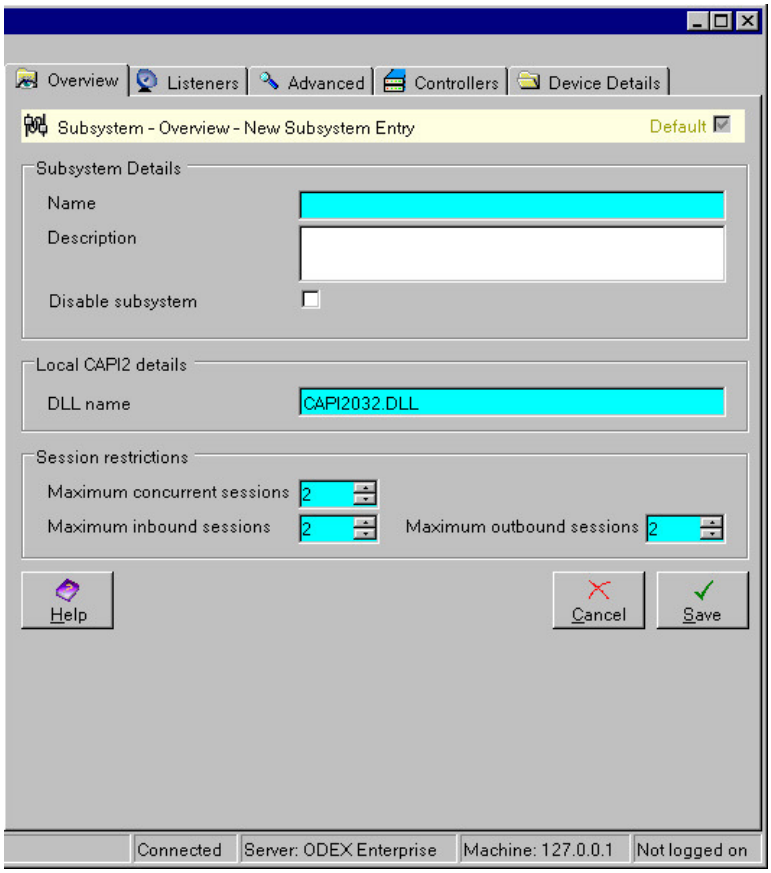
The Remote CAPI2 subsystem only differs from the Local CAPI2 subsystem in one section on the Overview page. Therefore we have described both these subsystems in one section, where the difference on the Overview page is indicated.

Each page is described below.

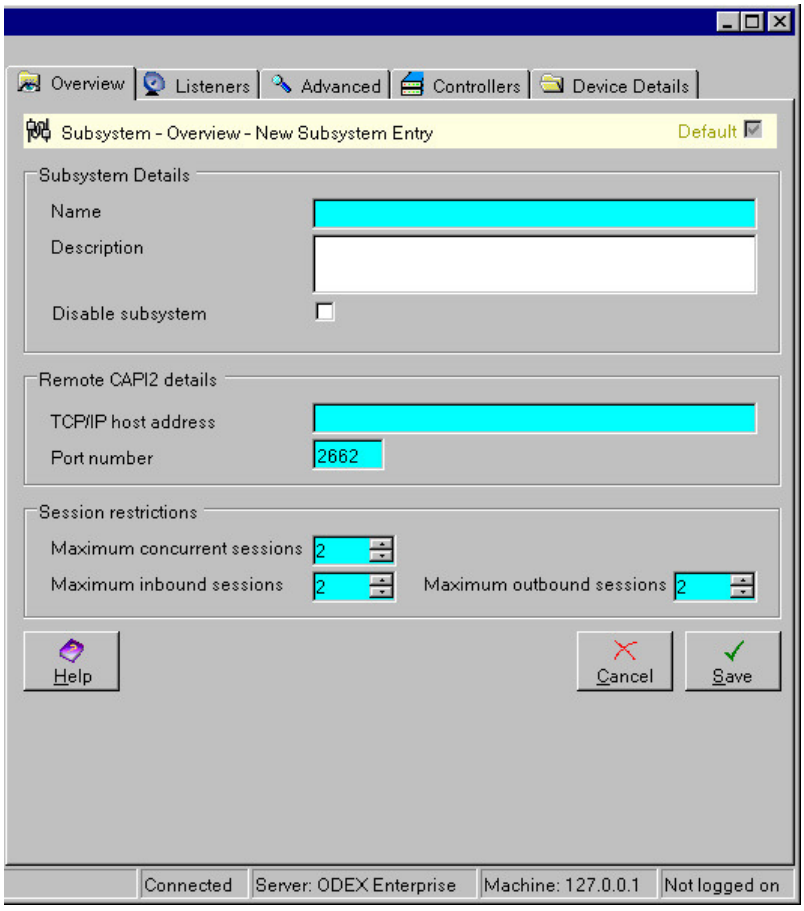
CAPI2 subsystem Overview

The fields on this page are described below. The two pages displayed below show the Overview page for a Local CAPI2 card subsystem and a Remote CAPI2 server subsystem respectively.

Local CAPI2 card subsystem Overview page



Remote CAPI2 server subsystem Overview page



Subsystem Details – Name

This is the name for the Subsystem. This name must be unique among your other Subsystems, but it can be whatever you want it to be. The name is a unique identifier, enabling you to recognise it easily when you want to use this Subsystem.

Subsystem Details – Description

You may provide a description of the Subsystem in this field if you wish. The description is intended to help you remember what the Subsystem is for.

Subsystem Details – Disable subsystem

Select this tickbox if you wish to temporarily disable the subsystem.

Local CAPI2 details – DLL name

This field is only applicable to a Local CAPI2 subsystem.

This is a DLL, local to the ODEX Server, which communicates with a CAPI device such as a local ISDN card.

If the DLL is in one of the default system folders, you can simply type in the DLL name. Otherwise you must provide the full file path.

This field will already be filled in with the most common CAPI2 DLL name. You may change it if necessary.

Remote CAPI2 details – TCP/IP host address

This field is only applicable to a Remote CAPI2 subsystem.

Type in this field the address of the TCP/IP host.

Remote CAPI2 details – Port number

This field is only applicable to a Remote CAPI2 subsystem.

This field will already be filled in with the most commonly used port number. You may change it if necessary.

Session Restrictions – Maximum concurrent sessions

The default value for this field is 2. This means that a maximum of 2 communications sessions using this subsystem may be active at any one time.

You may change this value to suit your system capabilities.

Session Restrictions – Maximum inbound sessions

The default value for this field is 2. This means that a maximum of 2 inbound communications sessions using this subsystem may be active at any one time.

You may change this value to suit your system capabilities.

Session Restrictions – Maximum outbound sessions

The default value for this field is 2. This means that a maximum of 2 outbound communications sessions using this subsystem may be active at any one time.

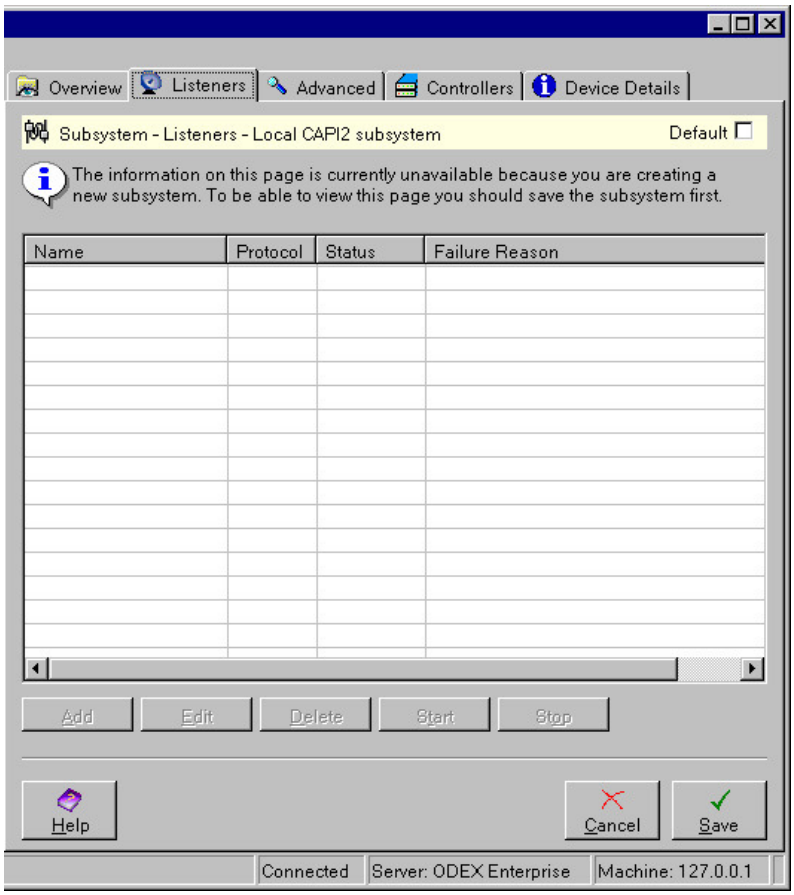
You may change this value to suit your system capabilities.

CAPI2 subsystem Listeners

If you are adding a new subsystem, the buttons on this page will not be available until you have completed the new subsystem and saved the details.

Once you have saved the subsystem details you will be able to add new listeners, and edit, delete, start and stop existing listeners.

At least one listener needs to be defined if you are going to receive incoming calls.



This page displays a list of all the listeners that are currently defined for this subsystem, showing their name, the protocol they use, their status and a reason for failure, if applicable.

The **Edit**, **Start** and **Stop** buttons will only be available if you select a single entry in the list. The **Delete** button will only be available if you select one or more entries in the list.

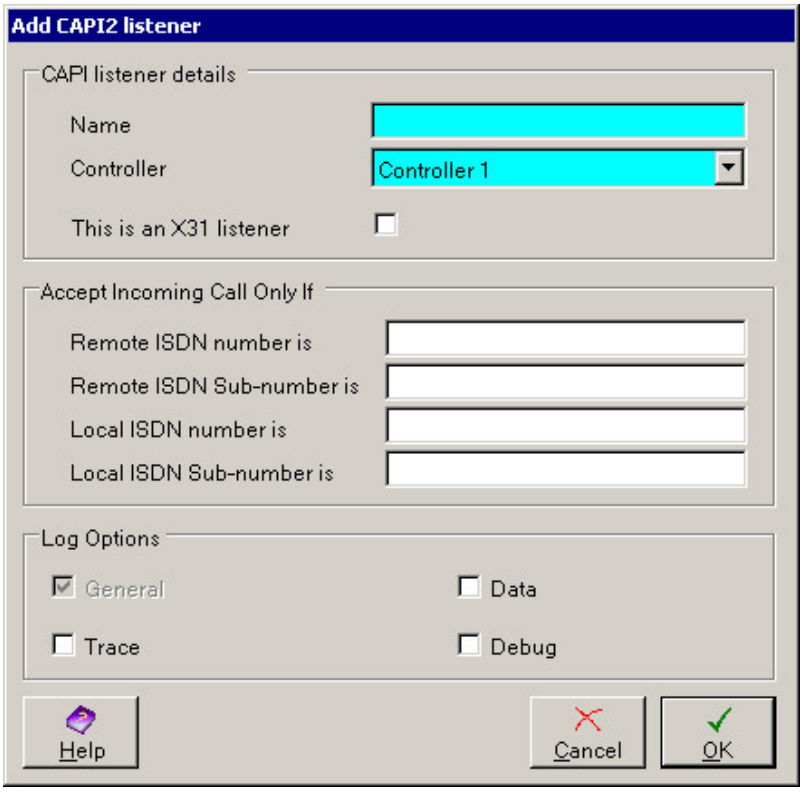
The **Stop** button is only available if the status of the selected listener is “Listening”. The **Start** button is only available if the status of the selected listener is “Stopped”.

To delete, start or stop a listener, select a listener in the list and click the **Delete**, **Start** or **Stop** button respectively.

To add a new listener, click the **Add** button

Add/Edit CAPI2 Listener

The Add/Edit CAPI2 Listener dialog is shown below.



CAPI listener details – Name

This is your name for the Listener. This name must be unique among your other Listeners, but it can be whatever you want it to be. The name is a unique identifier, enabling you to recognise it easily when you want to use this Listener.

CAPI listener details – Controller

Use the dropdown arrow to select the appropriate controller for this listener. The contents of the list will depend on the CAPI device you have installed.

CAPI listener details – This is an X31 listener

Select this tickbox if this listener is an X31 listener. If you select this tickbox, the "Accept Incoming Call Only If" section will be disabled.

Accept Incoming Call Only If

This section allows you to specify which ISDN number this listener will accept calls from and which ISDN number this listener will accept calls to.

If you want to accept all incoming ISDN calls, wherever they are from and to, you may leave this section blank.

If you want to accept calls from (or to) some numbers but not from (or to) others, you will have to set up a separate listener for each number that you will accept.

Log Options

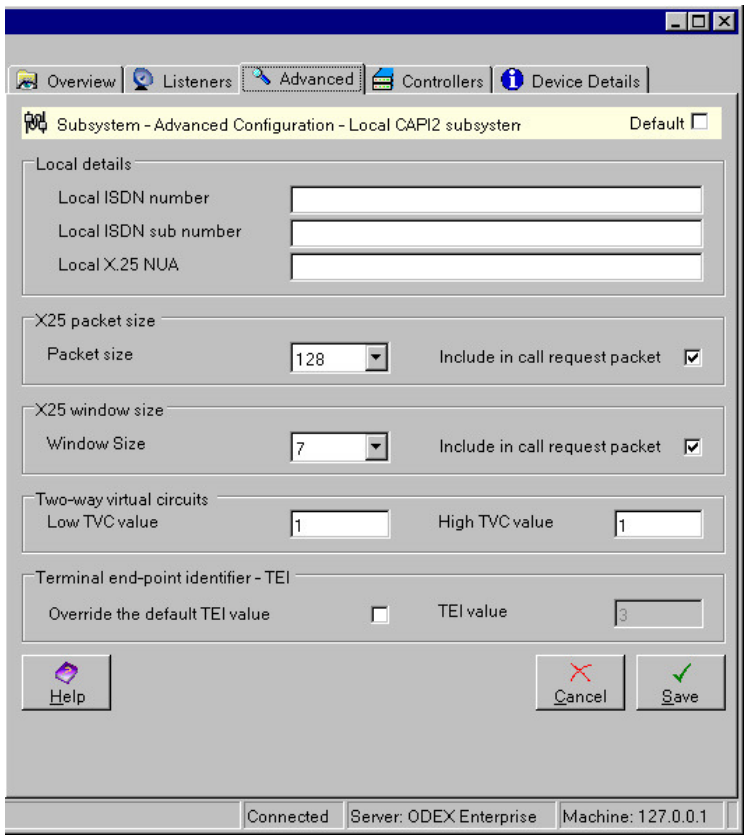
You may choose any or all of the log options, but please bear in mind that you will probably only need them for support purposes. Options that have been selected at a higher level (e.g. system log level) are shown selected and disabled – so if 'Debug', for example, is selected at the system level it will not be alterable here.

CAPI2 subsystem Advanced

The fields on this page are described below.

Please note that all these fields are optional and, whether they are filled in or not, can be overridden for individual trading partners by adding new Connections details in the Trading Partner Networks section (Advanced page).

However, it is suggested that you provide, as a minimum and for convenience, your local ISDN number.



Local Details – Local ISDN Number

Insert the number of your local ISDN line to be used in communications with your trading partners.

Local Details – Local ISDN Sub Number

This field is only relevant to people using multiple devices on a local ISDN line. If applicable, type in the sub-address for this ISDN number.

Local Details – Local X.25 NUA

Type in this field the NUA to be called once the ISDN connection has been established and the X.25 layer is ready.

X25 Packet Size – Packet Size

The X.25 packet size should normally be 128, as laid down in the OFTP specifications. Other values may be requested but this is not recommended.

X25 Packet Size – Include in call request packet

This tickbox allows you to include the X.25 packet size in the call request packet. This is the default setting. However, you may have some trading partners who will reject call requests containing the X.25 packet size, so this tickbox should be deselected for them.

Ideally you should select the tickbox here, and override the settings for individual partners where necessary in the Trading Partner Networks or Clearing Centre Networks section (Connections – Advanced page).

X25 Window Size – Window Size

This is the number of X.25 packets that the transmitting system will send before stopping to wait for a response from the remote. OFTP standards state that this value must be set to 7.

X25 Window Size – Include in call request packet

This tickbox allows you to include the X.25 window size in the call request packet. This is the default setting. However, you may have some trading partners who will reject call requests containing the X.25 window size, so this tickbox should be deselected for them.

Ideally you should select the tickbox here, and override the settings for individual partners where necessary in the Trading Partner Networks or Clearing Centre Networks section (Connections – Advanced page).

Two-way Virtual Circuits – Low TVC Value

Two-way virtual circuits means that the sessions are not open all the time but may be switched on and off to different users like dialling a phone number.

The Low TVC value should be the minimum number of TVCs in your system.

Two-way Virtual Circuits – High TVC Value

Two-way virtual circuits means that the sessions are not open all the time but may be switched on and off to different users like dialling a phone number.

The High TVC value should be the maximum number of TVCs in your system.

TEI – Override the default TEI value

TEI stands for Terminal Endpoint Identifier.

If this tickbox is not selected, this specifies that the subsystem should use the default TEI value. If this box is selected, then the value for the TEI must be specified in the next edit field.

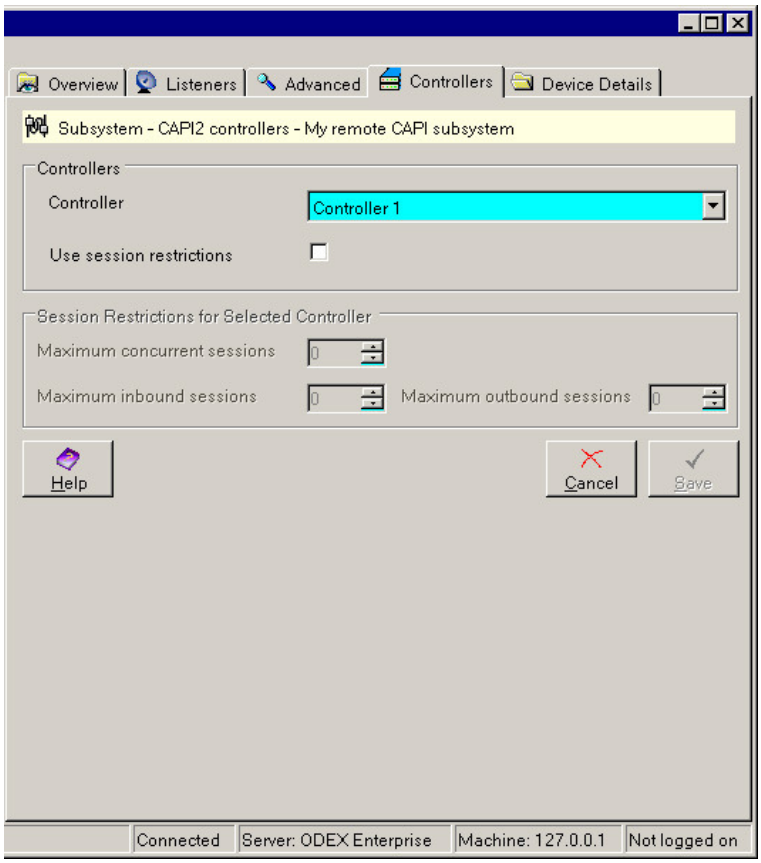
TEI – TEI value

This field will not be enabled unless you have selected the "Override the default TEI value" tickbox. You should type in here the value you want to use for the TEI.

CAPI2 subsystem Controllers

If you are adding a new subsystem, the fields on this page will not be available until you have completed the new subsystem and saved the details.

The fields on this page are described below.



Controllers – Controller

Select the appropriate Controller from the dropdown list at the side of the Controller field. The contents of the list will depend on the CAPI device you have installed.

Controllers – Use session restrictions

If you select the 'Use session restrictions' tickbox, the fields below will become enabled.

Restrictions for Selected Controller – Maximum concurrent sessions

This field is used to specify the maximum number of communications sessions using this subsystem that may be active at any one time.

You may edit this value to suit your system capabilities.

Restrictions for Selected Controller – Maximum inbound sessions

This field is used to specify the maximum number of inbound sessions using this subsystem that may be active at any one time.

You may edit this value to suit your system capabilities.

Restrictions for Selected Controller – Maximum outbound sessions

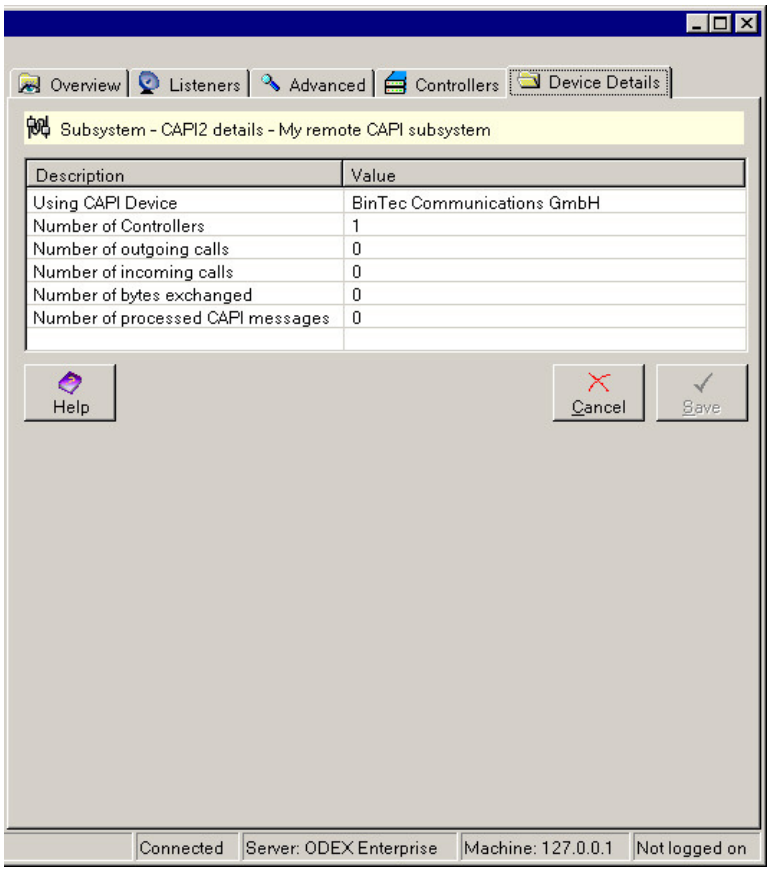
This field is used to specify the maximum number of outbound sessions using this subsystem that may be active at any one time.

You may edit this value to suit your system capabilities.

CAPI2 subsystem Device Details

If you are adding a new subsystem, the fields on this page will not be available until you have completed the new subsystem and saved the details.

This page simply contains details of the CAPI device and its usage so far.

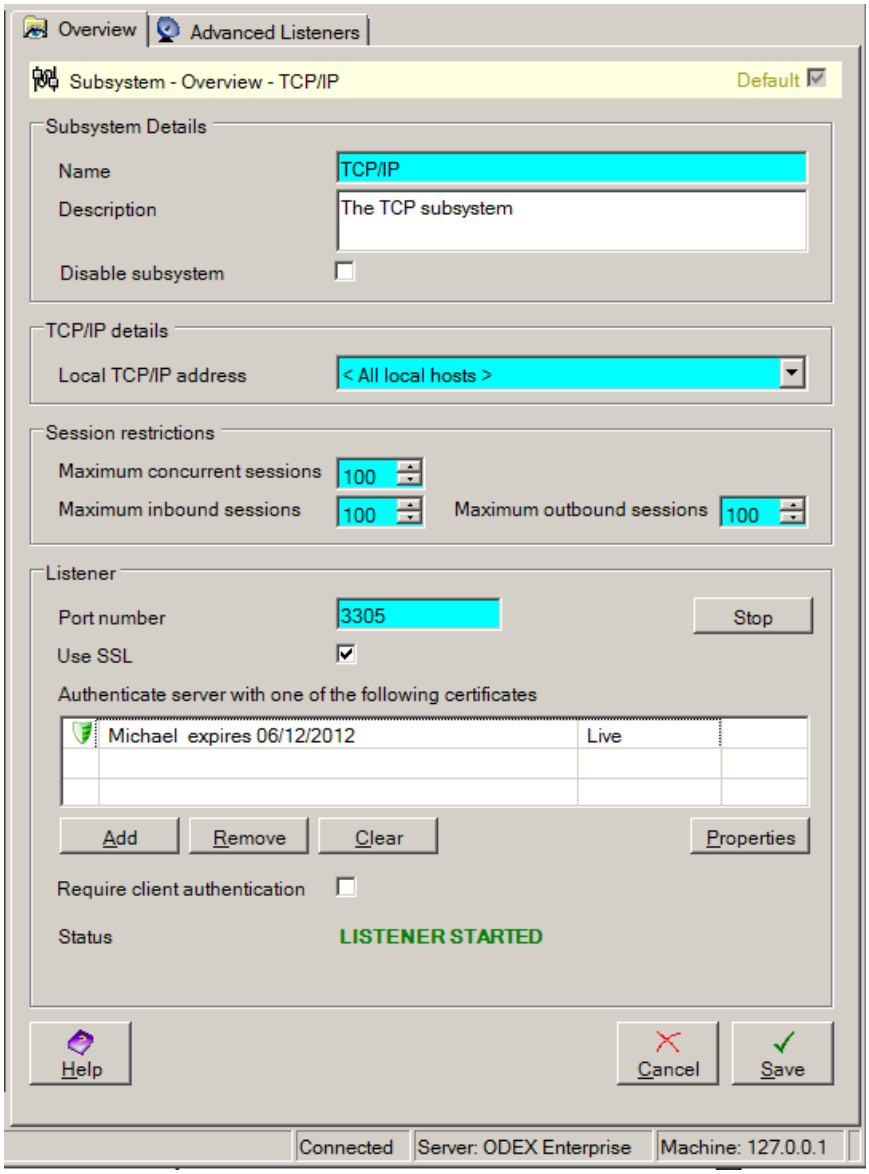


Adding/Editing a TCP/IP subsystem

The TCP/IP subsystem has two pages: Overview and Listeners.

TCP/IP subsystem Overview

The Overview page is described below.



The fields on this page are described below.

Subsystem Details – Name

Type in here a name for the Subsystem. This name must be unique among your other Subsystems, but it can be whatever you want it to be. The name is a unique identifier, enabling you to recognise it easily when you want to use this Subsystem.

Subsystem Details – Description

You may provide a description of the Subsystem in this field if you wish. The description is intended to help you remember what the Subsystem is for.

Subsystem Details – Disable subsystem

Select this tickbox if you wish to temporarily disable the subsystem.

TCP/IP details – Local TCP/IP address

Type in this field the address of the local TCP/IP network.

Session Restrictions – Maximum concurrent sessions

The default value for this field is 100. This means that a maximum of 100 communications sessions using this subsystem may be active at any one time.

You may change this value to suit your system capabilities.

Session Restrictions – Maximum inbound sessions

The default value for this field is 100. This means that a maximum of 100 inbound communications sessions using this subsystem may be active at any one time.

You may change this value to suit your system capabilities.

Session Restrictions – Maximum outbound sessions

The default value for this field is 100. This means that a maximum of 100 outbound communications sessions using this subsystem may be active at any one time.

You may change this value to suit your system capabilities.

Listener – Port Number

This is the port that ODEX listens for incoming TCP/IP connections. By default, the port is set to 3305, but can be changed to suit your system requirements.

Listener – Use SSL

Check this box if you wish to use SSL security.

Listener – Server certificate - This is the certificate for the SSL security to be used. Action buttons are enabled for you to choose the certificate(s). See the section entitled 'Dynamic Certificate Selection'.

Listener – Require client authentication - Check this box to force SSL clients to use a trusted certificate to authenticate themselves.

Listener – Status

This shows the current status of the listener.

Listener – Start / Stop button

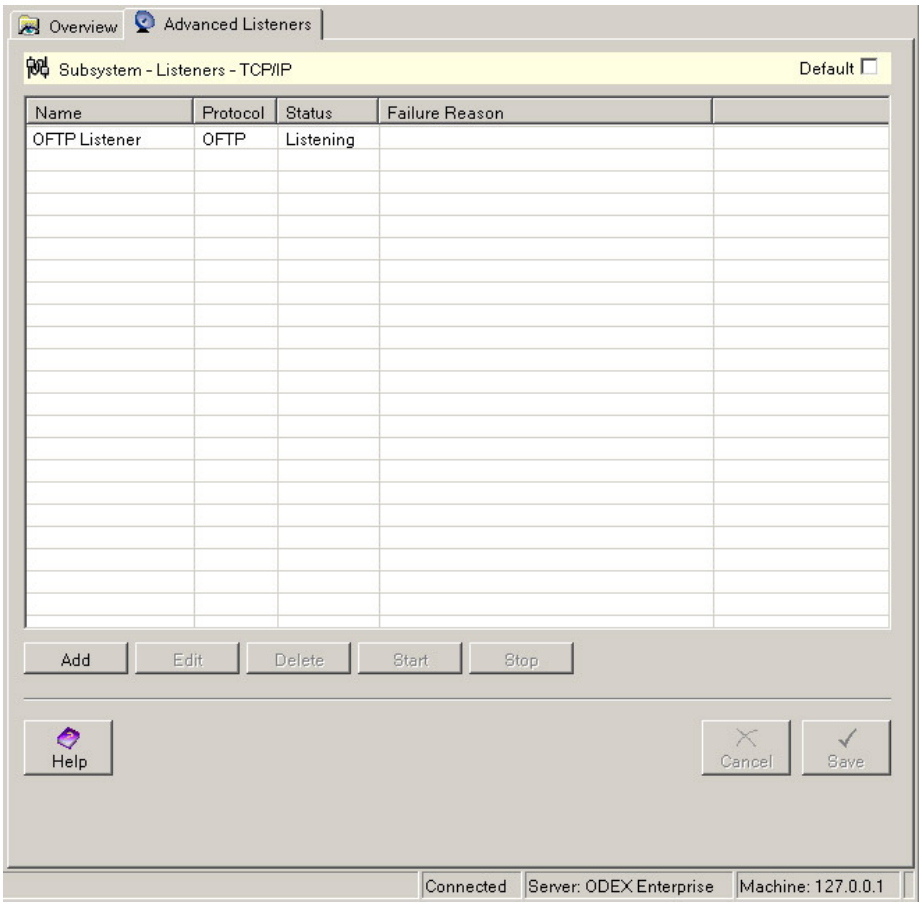
The listener can be switched on or off by simply clicking this button.

TCP/IP subsystem Listeners

If you are adding a new subsystem, the buttons on this page will not be available until you have completed the new subsystem and saved the details.

Once you have saved the subsystem details you will be able to add new listeners, and edit, delete, start and stop existing listeners.

The columns and buttons on this page are described below.



This page displays a list of all the listeners that are currently defined for this subsystem, showing their name, the protocol they use, their status and a reason for failure, if applicable.

The **Edit**, **Start** and **Stop** buttons will only be available if you select a single entry in the list. The **Delete** button will only be available if you select one or more entries in the list.

The **Stop** button is only available if the status of the selected listener is “Listening”. The **Start** button is only available if the status of the selected listener is “Stopped”.

To add a new listener, click on the **Add** button.

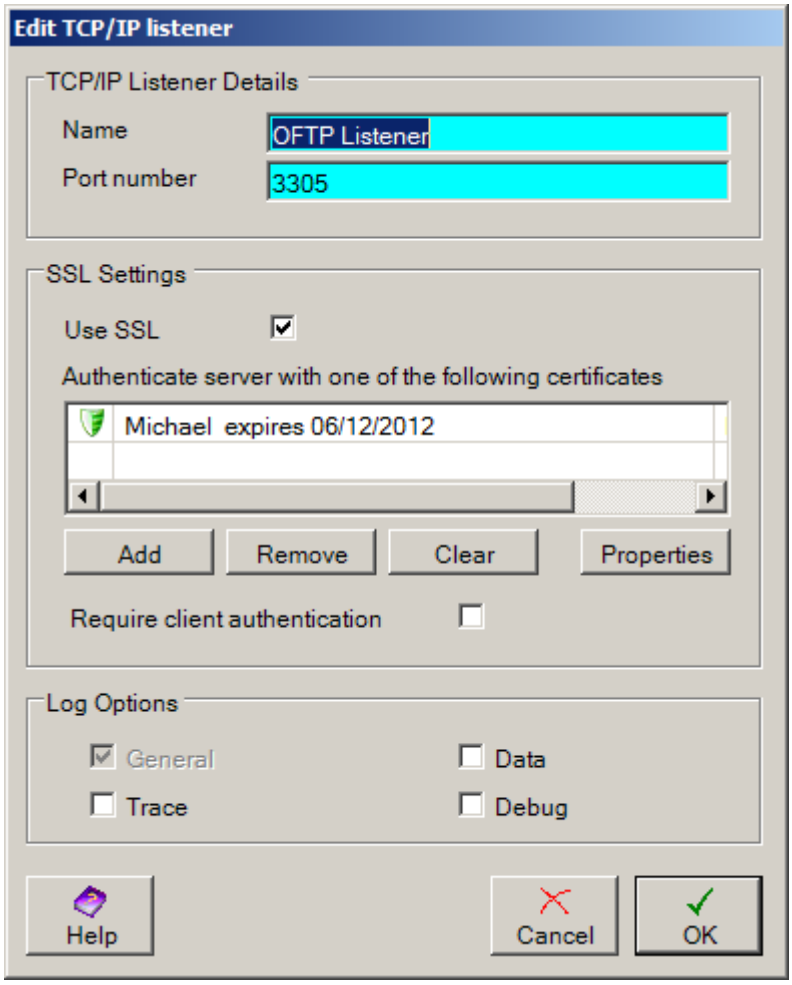
To delete, start or stop a listener, select a listener and click the **Delete**, **Start** or **Stop** button respectively.

After any changes, you must save the details from the Listeners page before you can use the **Start** and **Stop** buttons for any other listeners.

Add/Edit TCP/IP Listener

The Add/Edit TCP/IP Listener dialog is shown below.

After adding a new listener, you must save the details from the Listeners page before you can start it.



Name

This is the name of the TCP/IP listener. This name must be unique among your other listeners, but it can be whatever you want it to be. The name is a unique identifier, enabling you to recognise it easily when you want to use this Listener.

Port number

The port number should be the port on which ODEX will listen for incoming communications.

SSL Settings

To use SSL security, check the Use SSL box. Action buttons are enabled for you to choose the certificate(s). See the section entitled 'Dynamic Certificate Selection'. By default SSL is not used.

Log Options

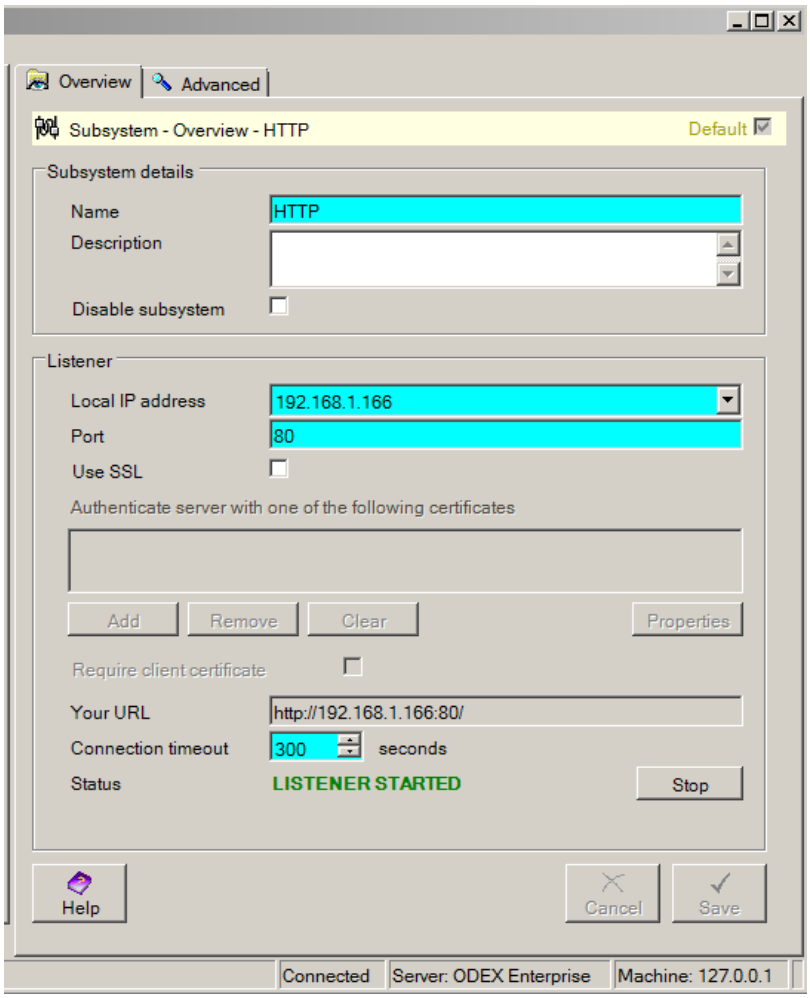
You may choose any or all of the log options, but please bear in mind that you will probably only need them for support purposes. Options that have been selected at a higher level (e.g. system log level) are shown selected and disabled – so if 'Debug', for example, is selected at the system level it will not be alterable here.

Adding/Editing an HTTP subsystem

The HTTP subsystem has two pages: Overview and Advanced.

HTTP subsystem Overview

The Overview page is described below.



The fields on this page are divided into two sections – Subsystem details and Listener. The fields and buttons are described below.

Subsystem Details – Name

Type in here a name for the Subsystem. This name must be unique among your other Subsystems, but it can be whatever you want it to be. The name is a unique identifier, enabling you to recognise it easily when you want to use this Subsystem.

Subsystem Details – Description

You may provide a description of the Subsystem in this field if you wish. The description is intended to help you remember what the Subsystem is for.

Subsystem Details – Disable subsystem

Select this tickbox if you wish to temporarily disable the subsystem.

Listener – Local IP address

This field will be filled in automatically by ODEX with the local IP address of your computer. If your computer has more than one IP address, select one of them.

Listener – Port

Type in this field the port number on which ODEX will listen for incoming communications of type HTTP or HTTPS.

Listener – Use SSL

To use SSL for this subsystem, select this tickbox. Action buttons are enabled for you to choose the certificate(s). See the section entitled ‘Dynamic Certificate Selection’.

Listener – Server certificate

The button for this field will only be active if you have selected the 'Use SSL' tickbox. Use the arrow and the Select option to choose a certificate for the server.

Listener – Your URL

This field will be filled in automatically by ODEX with the local IP address and port you have selected above. The contents of this field can then be copied for sending to your trading partner, as he will need this information for setting up his own system for communication with you.

Listener – Connection timeout

This field allows you to select the number of seconds you want ODEX to wait before closing the connection when no comms activity is occurring i.e. nothing is happening on this connection.

Listener – Status

If you have stopped this subsystem, the status will be displayed in red as 'Listener Stopped'.

If the subsystem has not been stopped, the status will be displayed in green as 'Listener Started'.

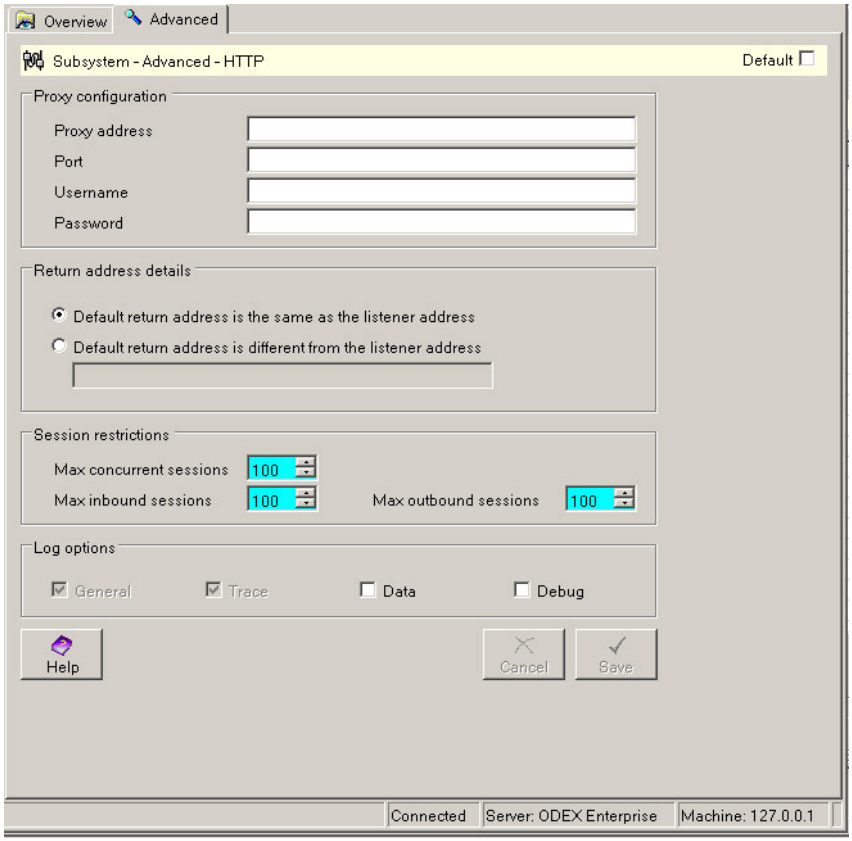
Listener – Stop/Start button

Use this button to start or stop the AS2 listener. The status will change as you do so.

The **Edit**, **Start** and **Stop** buttons will only be available if you select a single entry in the list. The **Delete** button will only be available if you select one or more entries in the list.

HTTP subsystem Advanced

The fields on this page are divided into three sections – Proxy configuration, Session restrictions and Log options.



The proxy configuration is only required if your Internet system can only be accessed via a proxy server.

Proxy configuration – Proxy address

Type in the address of the proxy server.

Proxy configuration – Port

Type in the port number of the proxy server.

Proxy configuration – Username

If your proxy server requires a username, type it in this field.

Proxy configuration – Password

If your proxy server requires a password, type it in this field.

Return Address Details

When connecting via a proxy using your external IP address, your trading partner may not be aware of your internal IP address. This means that your default return address should be that of the external proxy, rather than the internal IP address of your machine. To overcome this issue, you can specify a specific Default Return Address by ticking the radio button and entering your external IP address, which is known by your trading partners.

Session Restrictions – Max concurrent sessions

The default value for this field is 100. This means that a maximum of 100 communications sessions using this subsystem may be active at any one time.

You may change this value to suit your system capabilities.

Session Restrictions – Max inbound sessions

The default value for this field is 100. This means that a maximum of 100 inbound communications sessions using this subsystem may be active at any one time.

You may change this value to suit your system capabilities.

Session Restrictions – Max outbound sessions

The default value for this field is 100. This means that a maximum of 100 outbound communications sessions using this subsystem may be active at any one time.

You may change this value to suit your system capabilities.

Log Options

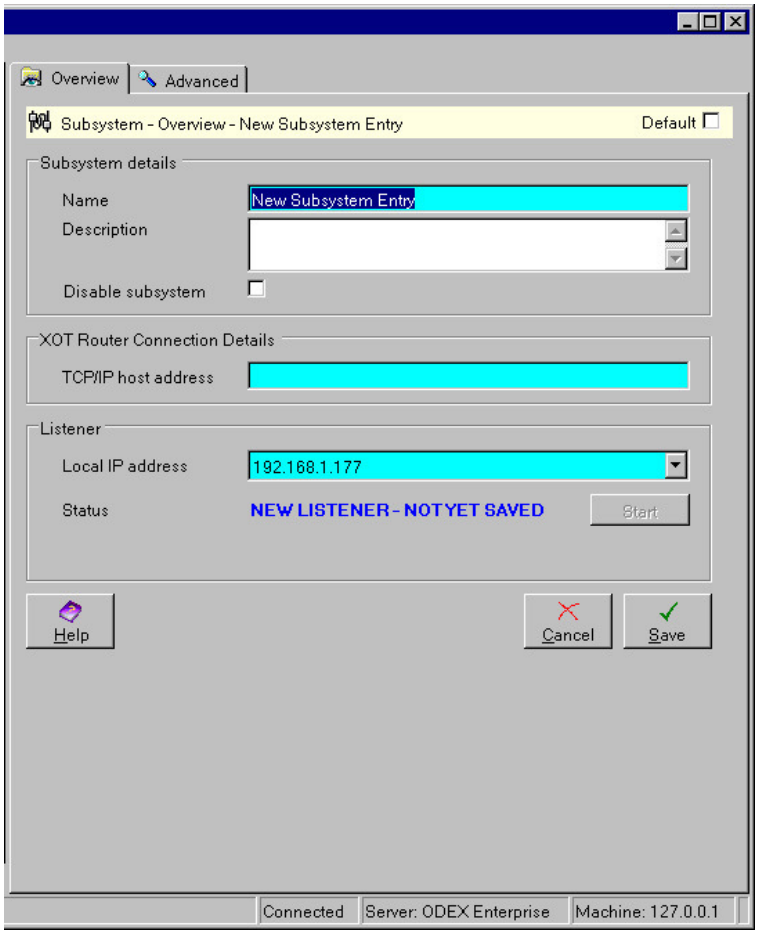
You may choose any or all of the log options, but please bear in mind that you will probably only need them for support purposes. Options that have been selected at a higher level (e.g. system log level) are shown selected and disabled – so if 'Debug', for example, is selected at the system level it will not be alterable here.

Adding/Editing an XOT subsystem

The XOT subsystem has two pages: Overview and Advanced.

XOT subsystem Overview

The Overview page is described below.



The fields on this page are divided into three sections – Subsystem details, XOT router connection details and Listener. The fields and buttons are described below.

Subsystem Details – Name

Type in here a name for the Subsystem. This name must be unique among your other Subsystems, but it can be whatever you want it to be. The name is a unique identifier, enabling you to recognise it easily when you want to use this Subsystem.

Subsystem Details – Description

You may provide a description of the Subsystem in this field if you wish. The description is intended to help you remember what the Subsystem is for.

Subsystem Details – Disable subsystem

Select this tickbox if you wish to temporarily disable the subsystem.

XOT router connection details – TCP/IP host address

Type in here the TCP/IP address of the router that will be used to make the X.25 call.

Listener – Local IP address

This is the IP address that must be configured in the router for X.25 calls that should be passed to ODEX.

This field will be filled in automatically by ODEX with the local IP address of your computer. If your computer has more than one IP address, select one of them from the dropdown list.

Listener – Status

If you have stopped this subsystem, the status will be displayed in red as 'Listener Stopped'.

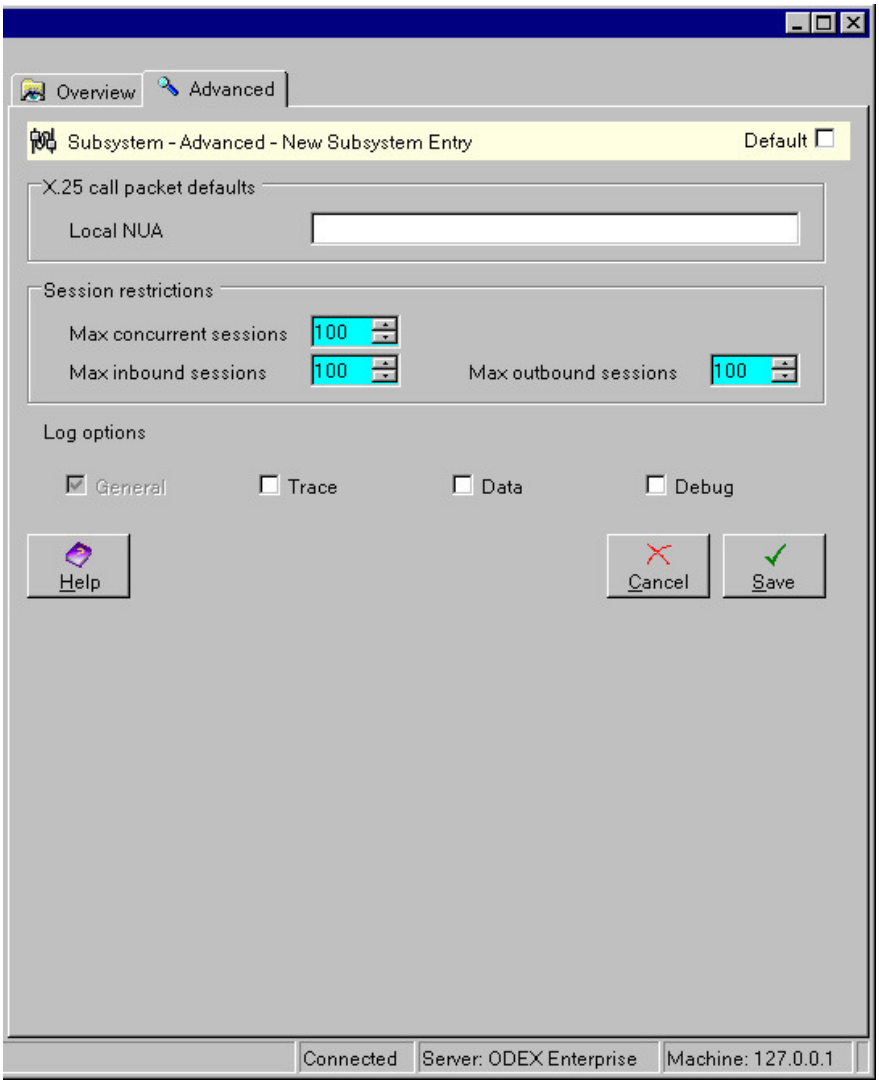
If the subsystem has not been stopped, the status will be displayed in green as 'Listener Started'.

Listener – Stop/Start button

Use this button to start or stop the XOT listener. The status will change as you do so.

XOT subsystem Advanced

The fields on this page are divided into three sections – X.25 call packet defaults, Session restrictions and Log options.



X.25 call packet defaults – Local NUA

Type in the X.25 Network User address (NUA) of the local machine.

This is usually not required and will be provided by the X.25 network.

N.B. The XOT subsystem will default to a Window size of 2 and a Packet size of 128, but these values can be overridden on the Advanced page tab of the Network Connection dialog.

Session Restrictions – Max concurrent sessions

The default value for this field is 100. This means that a maximum of 100 communications sessions using this subsystem may be active at any one time.

You may change this value to suit your system capabilities.

Session Restrictions – Max inbound sessions

The default value for this field is 100. This means that a maximum of 100 inbound communications sessions using this subsystem may be active at any one time.

You may change this value to suit your system capabilities.

Session Restrictions – Max outbound sessions

The default value for this field is 100. This means that a maximum of 100 outbound communications sessions using this subsystem may be active at any one time.

You may change this value to suit your system capabilities.

Log Options

You may choose any or all of the log options, but please bear in mind that you will probably only need them for support purposes. Options that have been selected at a higher level (e.g. system log level) are shown selected and disabled – so if 'Debug', for example, is selected at the system level it will not be alterable here.

XOT Logging

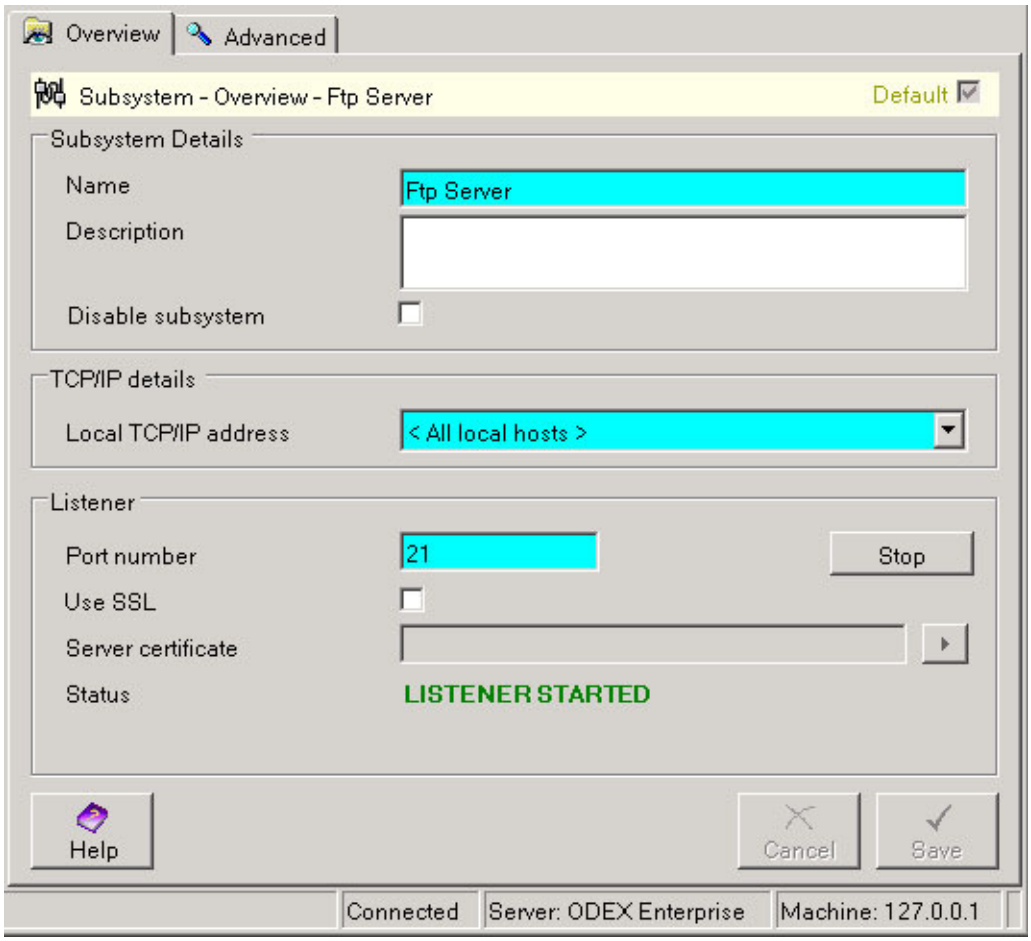
In order to view all of the X.25 packets that are being transmitted and received by ODEX, you should select the 'Buffer' option against the XOT protocol on the Communications Settings node (accessed from the Comms tab in the Administrator). To view the actual hex contents of the XOT buffers, select 'Buffer' against the TCP protocol there too.

Adding/Editing an FTP server subsystem

An FTP server subsystem is a representation of an FTP server, whilst the trading partner networks and clearing centre networks are users on the FTP server. An FTP server subsystem must be created in order to use the ODEX FTP server functionality.

FTP server subsystem Overview

The overview page for an FTP server subsystem looks like the example given below.



The page is allows a user to set all the mandatory information about the FTP server. It is divided into three sections.

Subsystem Details

This section defines ODEX specific information about the subsystem.

Subsystem Details – Name

This is the name as the subsystem is referred to within ODEX.

Subsystem Details – Description

This is the description that could be helpful in letting an ODEX user identify this subsystem. It is not used or transmitted to any other party's.

Subsystem Details – Disable subsystem

Disabling the subsystem will stop the listener which means ODEX will not accept any incoming FTP server sessions, so the ODEX FTP server will be disabled.

TCP/IP details – Local TCP/IP address

This allows a user to select the local IP address that the server is bound too. If a computer has two network cards, one for a LAN and one for the Internet then this would allow binding to one or the other IP addresses or to all local hosts.

Listener

This defines information about the TCP/IP listener that is waiting for a connection to the ODEX FTP server.

Listener – Port Number

This is the port number that the FTP server listens on. The port number for the FTP control connection is defined as 21, which is the default value, although any open port number could be used.

Listener – Use SSL

ODEX supports the use of SSL on all TCP/IP connections, however it is not recommended that it is setup for the FTP server.

Listener – Server Certificate

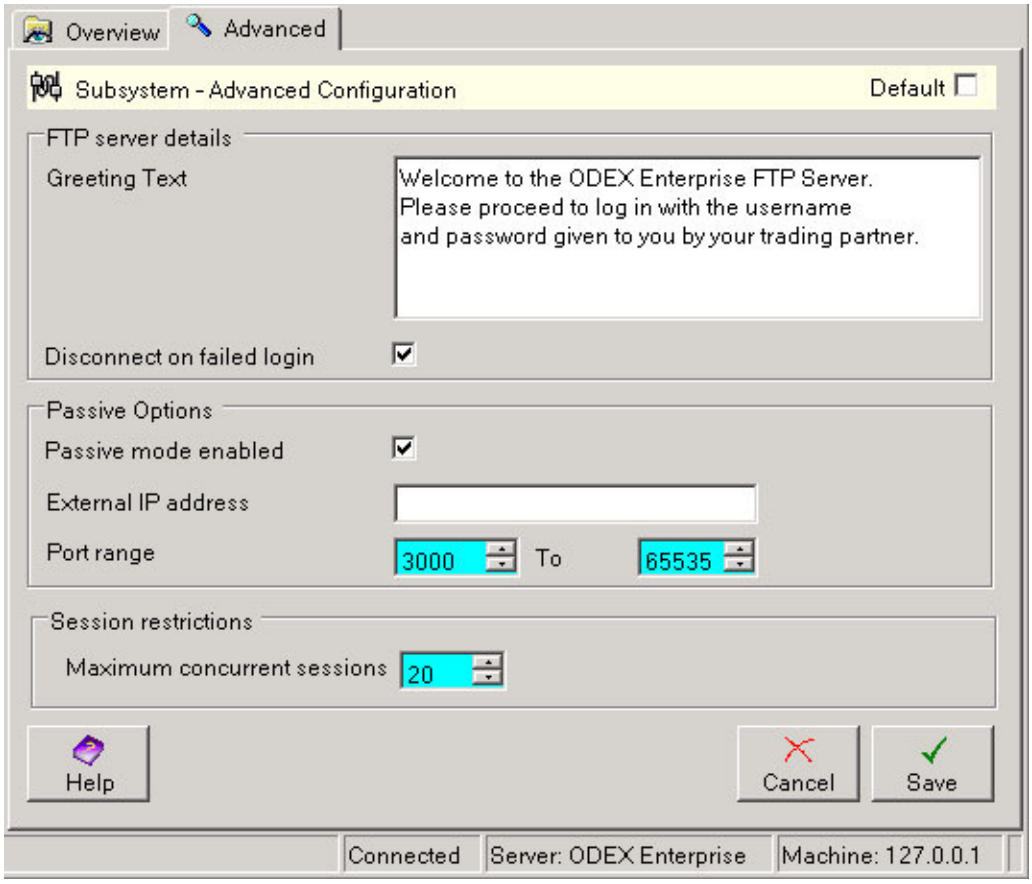
This is the certificate used to encrypt the TCP/IP connection if SSL is selected.

Listener – Status

This is the status of the current TCP/IP listener, e.g. whether we are listening for incoming FTP connections or if there has been some problem in setting up the listener (for example the port could already be in use).

FTP server subsystem Advanced

The advanced page allows the specification of advanced FTP server details. The page will look like the example given below.



This is divided into three sections, which will be explained below.

FTP server details

These are general options affecting the FTP server before a user logs on.

FTP server details – Greeting text

This is the text that is displayed to a user when they first connect to the FTP service. This text can be seen by anyone who is on the network the FTP server is listening on. If the FTP server is listening on an IP address connected to the Internet then anyone connected to the Internet could connect to the ODEX FTP server and get this message. They would be unable to progress further however unless they had a correct username and password.

FTP server details – Disconnect on failed login

The standard behaviour for FTP is to stay connected when a user fails to log on. This enables a connected client to continue trying different usernames and passwords. This option immediately disconnects a user if they fail to log on correctly.

Passive options

As explained in the introduction to FTP, FTP is capable of a passive mode where the server specifies which port on its IP address the client should connect to for data. Passive mode enables the FTP client to not have any ports open and is quite common. These options allow you to tailor the ODEX FTP server to your security solution.

Passive options – Passive mode enabled

If passive mode is enabled then clients trying to initiate passive mode will be told it is not supported.

Passive options – External IP address

This is the IP address you want sent to the client for them to connect to the ODEX FTP server with. This should be filled in only if your external IP address differs from the address available on the server machine that the FTP server is bound too. In most situations it should not be necessary to fill in this option.

Passive options – Port range

The port range specifies the ports on the server machine that are open and available for the FTP server to use for data connections. If every network is connected at the same time then the server will require a different port for each session. You will never require more ports than the number of allowed concurrent sessions.

Session restrictions – Maximum concurrent sessions

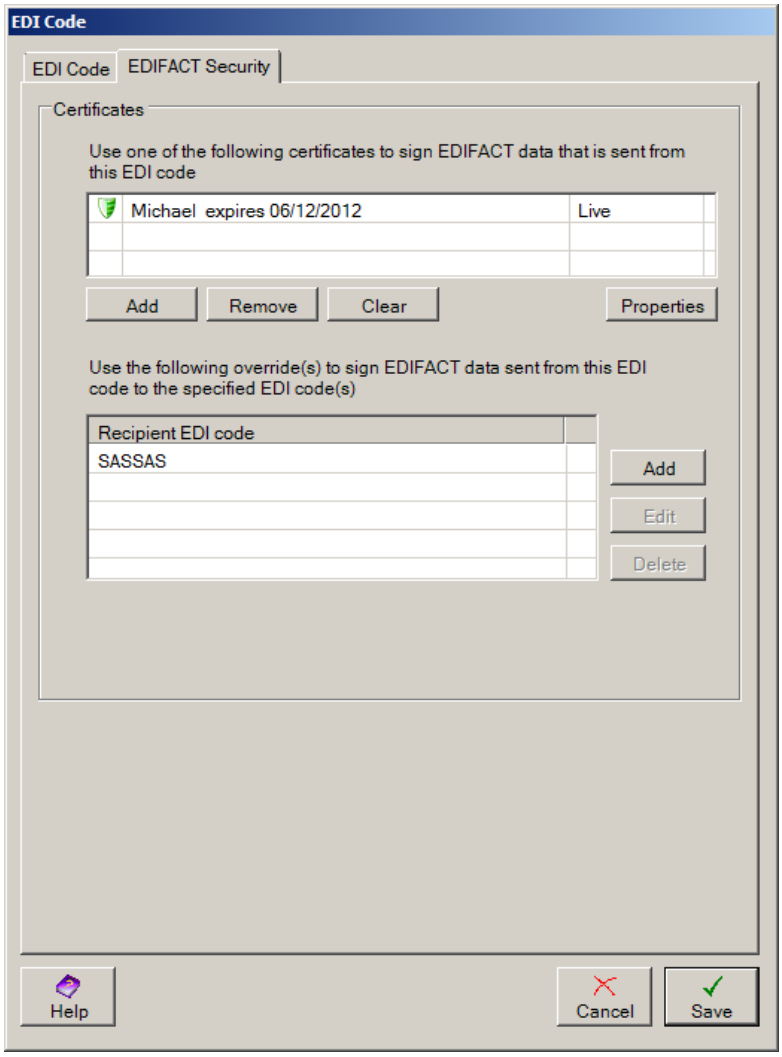
This value is the number of concurrent sessions allowed to be running on the ODEX FTP server. Once this number is met, new connections with the ODEX FTP server will be denied until a session ends. The number this is set to should be considered with the available port range if passive mode is enabled.

EDIFACT Security Settings

The options to be used in the three EDIFACT security workflow jobs (Sign EDI, Verify Signed EDI, Process AUTACK) can be overridden for a single EDI code using the EDI code dialog. The following sections describe how this works.

Internal EDI Code - Certificates

In the case of internal EDI codes the following dialog tab is displayed.

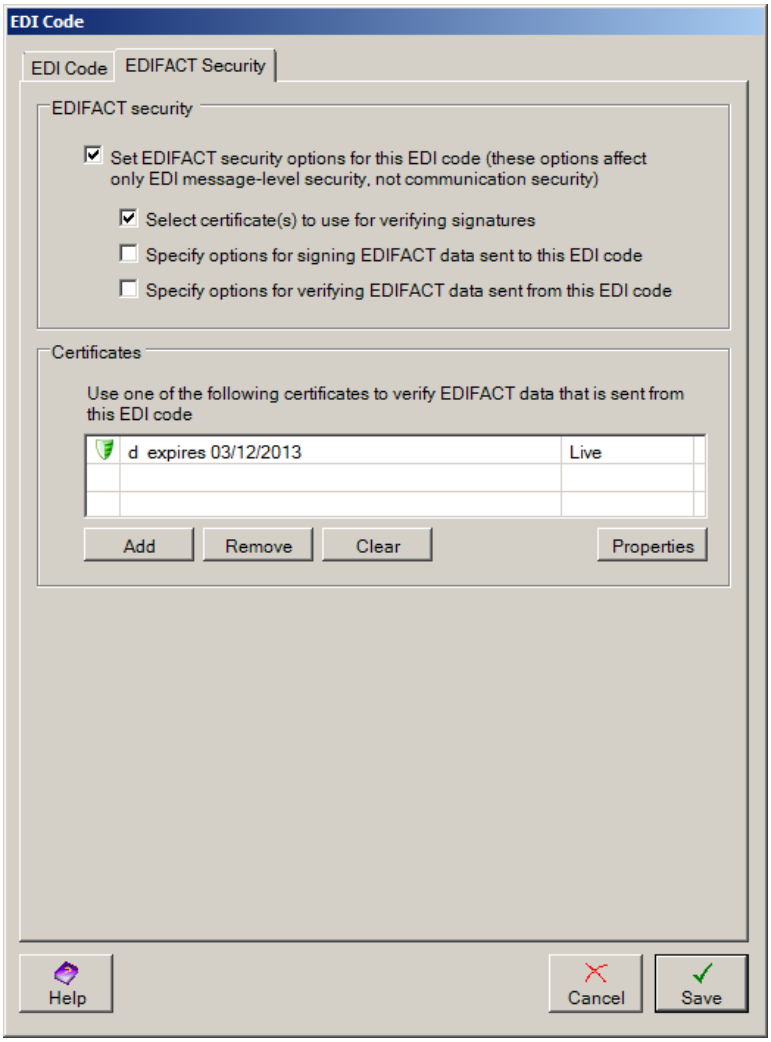


The **Certificates** section contains the following options:

- Select the certificate to use for signing EDI data sent **from** the EDI code. This selection overrides the signing certificate specified on the Sign EDI workflow job.
- **Add** further overrides to specify the certificate to use for a given recipient EDI code. **Edit** or **Delete** a selected override by recipient.

External EDI Code – Security Options and Certificates

In the case of external EDI codes the following dialog tab is used to specify EDIFACT security overrides and certificates:



The check boxes in the **EDIFACT security** section are used to indicate which set of options you want to override. The choices are:

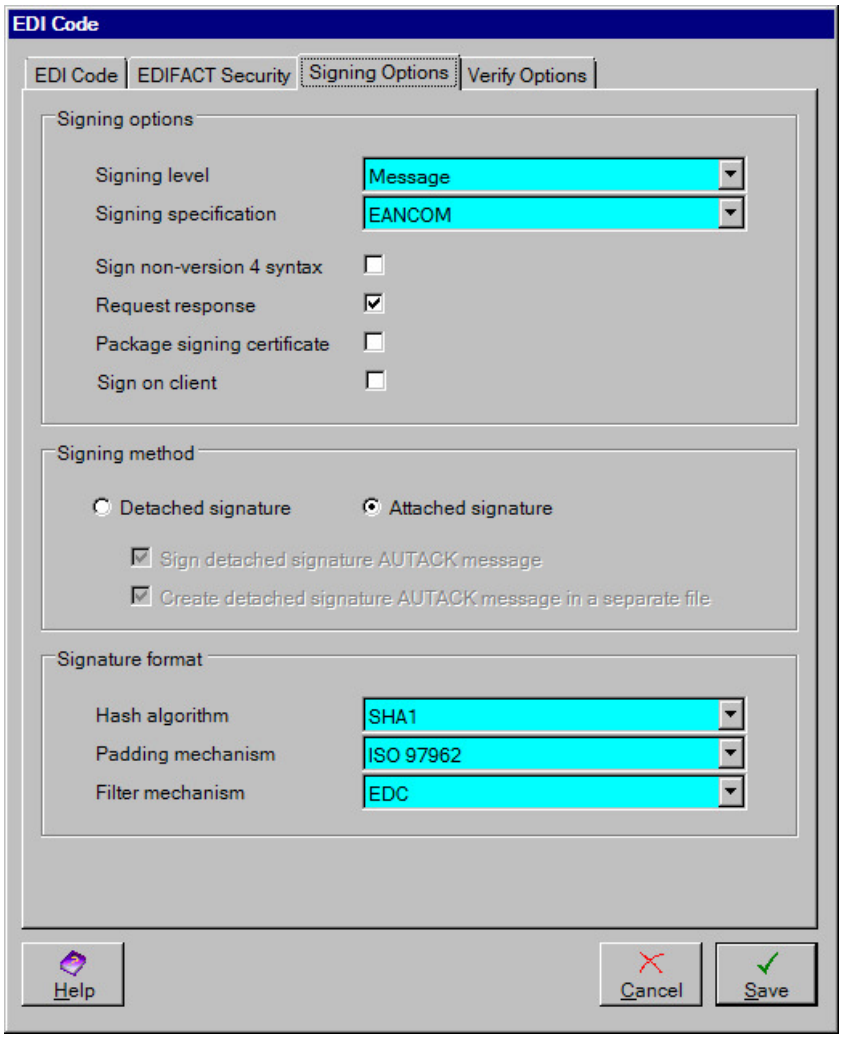
- Override the certificate(s) used for verifying signatures sent **from** the EDI code. When you check this box the **Certificates** section will be enabled.
- Override the options for signing EDI data sent **to** the EDI code. When you check this box the **Signing Options** tab will be displayed.
- Override the options for verifying EDI data sent **from** the EDI code. When you check this box the **Verify Options** tab will be displayed.

The **Certificates** section contains the following option:

- Select the certificate to use for verifying EDI data sent **from** the EDI code. This selection overrides the verification certificate specified on the Verify Signed EDI workflow job.

Signing Options

The following dialog tab is used to specify override options by EDI code for signing EDIFACT data:

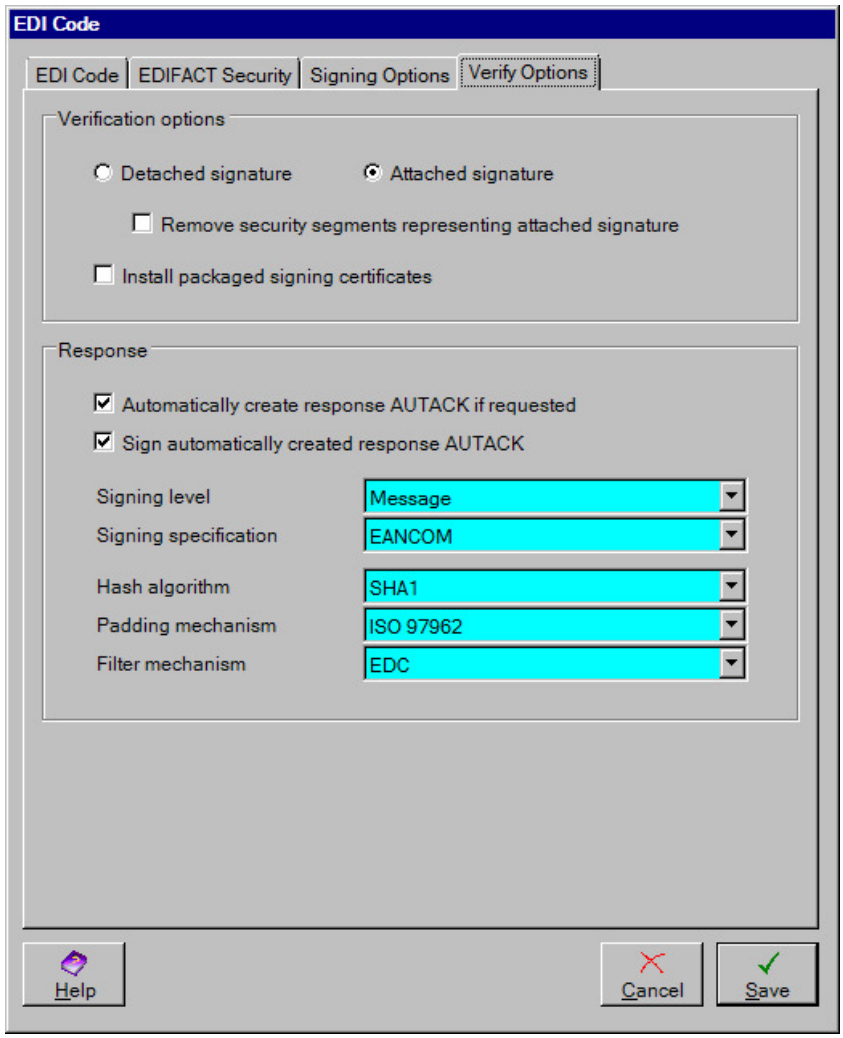


The following options are supported:

- Signing level – whether to sign the message or interchange.
- Signing specification – select the signing standard to use.
- Sign non-version 4 – allows EDIFACT version 3 and below to be signed.
- Request response – request that a response AUTACK is sent.
- Package signing certificate – include the certificate used for signing in an EDIFACT package following the signed data.
- Sign on client – that data is to be held on the workflow pending signing on the ODEX Workstation client.
- Signing method – select attached or detached signature.
- Sign detached signature AUTACK – when sending a detached signature sign the AUTACK message.
- Create detached signature AUTACK in separate file.
- Hash algorithm – select the algorithm to use for hashing the EDI data.
- Padding mechanism – select the padding mechanism to use when creating the signature.
- Filter mechanism – select the filter function to use for rendering the signature to an EDI message.

Verify Options

The following dialog tab is used to specify override options by EDI code for verifying signed EDIFACT data:



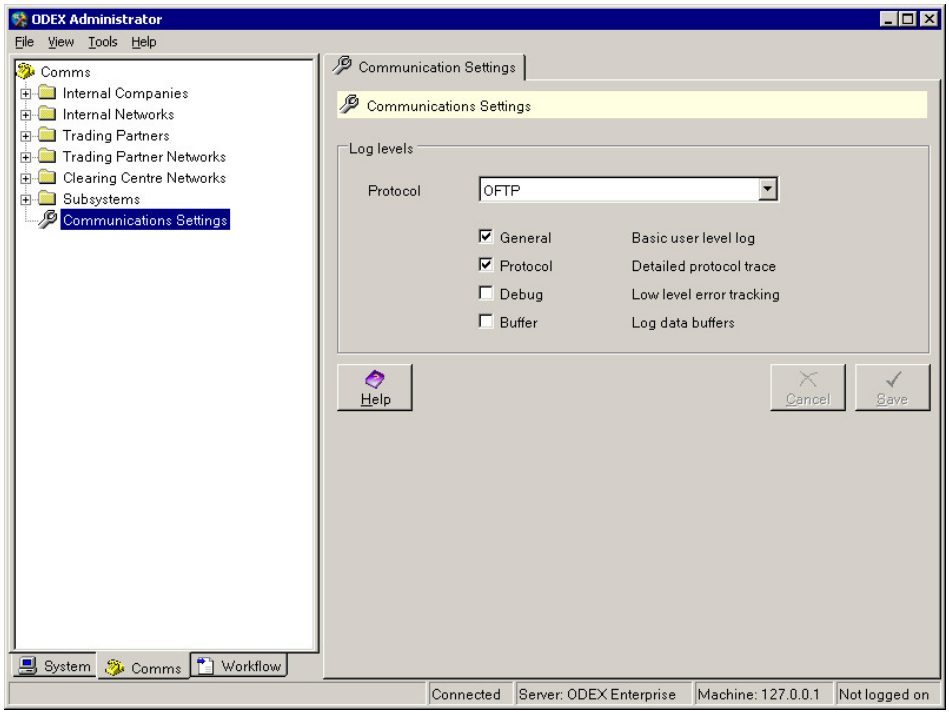
The following options are supported:

- Signing method – select attached or detached signature.
- Remove security segments – where the signature is attached you can choose to have ODEX remove the security service segments during verification.
- Install certificates – specify whether ODEX should install certificates received in EDIFACT packages on the server machine.
- Create AUTACK – specify whether to create a response AUTACK when requested by the sender. When a response is created it is places in a child workflow file. You will need to handle the child file by adding a child file return code action to the Verify Signed EDI or Process AUTACK job to move the file to a channel which will schedule it appropriately.
- Sign response AUTACK – whether to sign the automatically created response AUTACK.
- Signing level – when signing the AUTACK, whether to sign the message or interchange.

- Signing specification – select the signing standard to use when signing the AUTACK.
- Hash algorithm – select the algorithm to use for hashing the EDI data.
- Padding mechanism – select the padding mechanism to use when creating the signature.
- Filter mechanism – select the filter function to use for rendering the signature to an EDI message.

Communication Settings

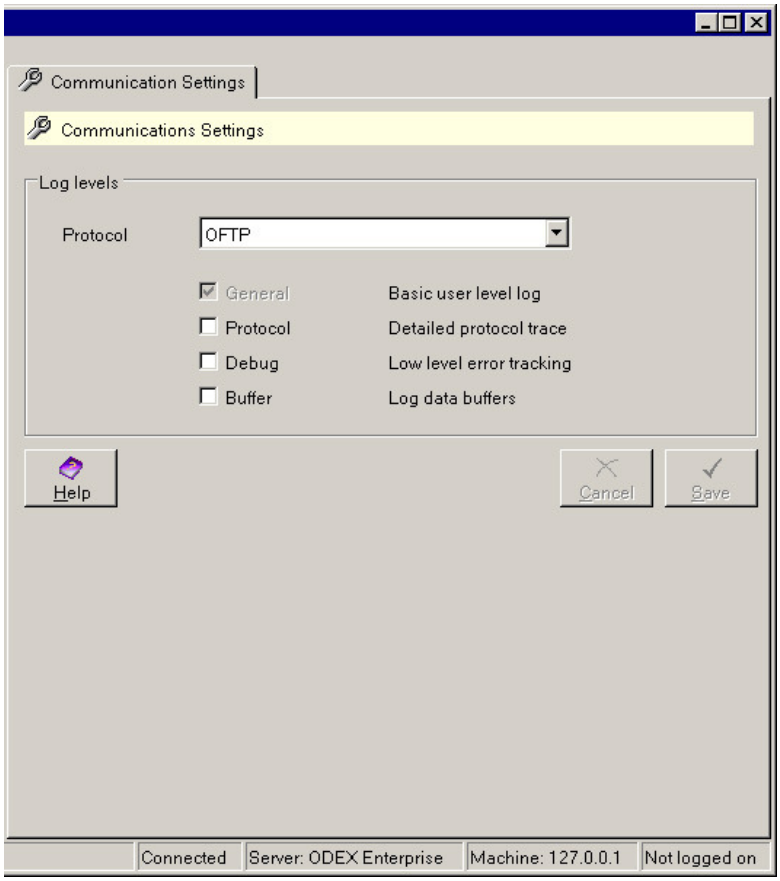
Click on the name Communication Settings in the Navigation Panel to see the Communication Settings page, as shown below.



On this page you can set the logging options for the protocols you use to communicate with your trading partners or clearing centres.

Communication Settings

To view the logging options for each different protocol, click on the Communications Settings node. This will bring up the Communications Settings page, shown below:



On this page you can select various log options for the protocols you will be using. The General option will always be selected and cannot be deselected.

The currently available protocols are AS2, CAPI2, FTP client, FTP server, HTTP, OFTP, TCP and XOT. The default settings are to have General logging for all protocols. This will help to keep your log to a manageable size.

Select one of the protocols from the dropdown list so that you can set its log levels.

Select one or more of the log overrides for the protocols you are using, according to how much information you want to see in the log. You will generally only need to increase logging levels for support purposes.

General will provide basic information about the communications session.

Protocol will show all the protocol activity (e.g. for OFTP this will be the SSRM, SSID, SFPA, DATA, EERP etc)

Debug should only be selected if requested by the Data Interchange Plc support team.

Buffer will show the full contents of each file sent and received during the session.

XOT Logging

In order to view all of the X.25 packets that are being transmitted and received by ODEX, you should select the 'Buffer' option against the XOT protocol. To view the actual hex contents of the XOT buffers, select 'Buffer' against the TCP protocol too.

Workflow Manager

Introduction

The Workflow Manager (WFM) is the engine that drives file processing within ODEX Enterprise. It is here that you provide the configuration for the way that any file within the ODEX system is to be processed.

When a file is given to the system via any entry point (picked up from a monitored directory, manually entered, or imported via a communications protocol) the Workflow Manager will start to process the file.

The first decision by the WFM will be to decide whether or not to analyse the file and split it into individual interchanges or messages. This will be decided according to the system configuration that you have provided.

Once the WFM knows enough information about the file (having either analysed it, or realised it can make a decision without analysis) the file will be processed according to the configuration. At this point the file may go through various processes, including:

- Mapping (using XLATE)
- Saving the analysis (for later statistical analysis)
- Validation (of the EDI data, such as syntax, interchange control reference, digital signatures)
- Output (write to directory or schedule to a network/mailbox)
- Notifications (e-mail)
- An external application

At all points through this processing, files can be tracked, using the ODEX Workstation application, to view the current state of the system.

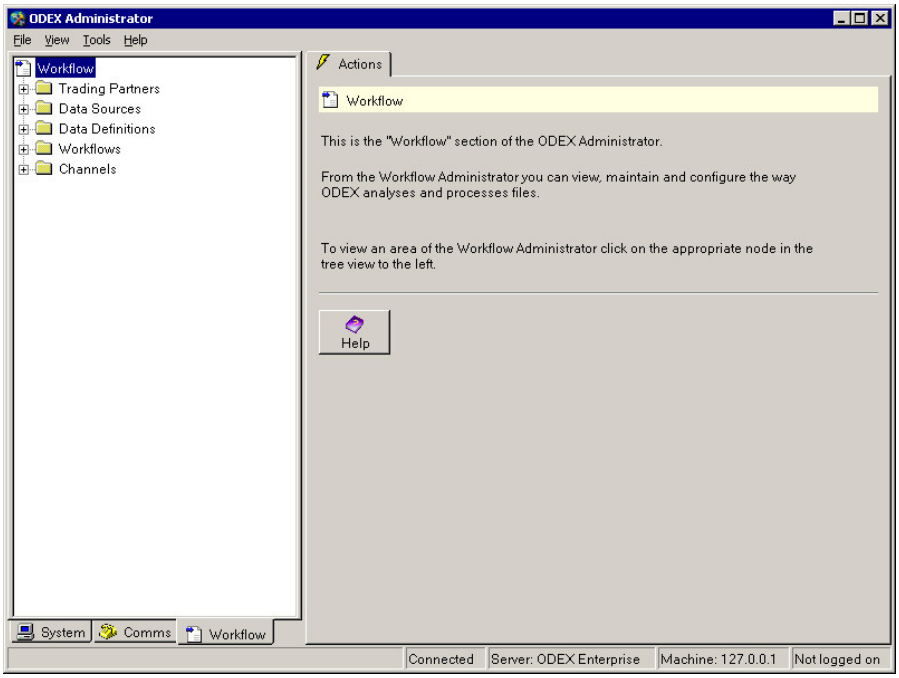
At any point, you will be able to find out:

- How many files are in the system
- Where each file is (In a process? On a processes queue?)
- What jobs have already been carried out on each file

How to use the Workflow Manager

You are strongly advised to read about Workflows in the section entitled "ODEX Concepts" before using the Workflow Manager, in order to understand all the concepts and terms that will be used here.

Click on the Workflow page tab in the Navigation Panel to see the default page for the Workflow Manager section, as shown below. This is the Workflow – Actions page.



From the Workflow Administrator you can view, maintain and configure the way ODEX analyses and processes files.

To view an area of the Workflow Administrator, click on the appropriate node in the tree view to the left.

Trading Partners

This section of the Workflow Administrator enables you to add further trading partners to ODEX, in order to include them in your Workflows and Channels.

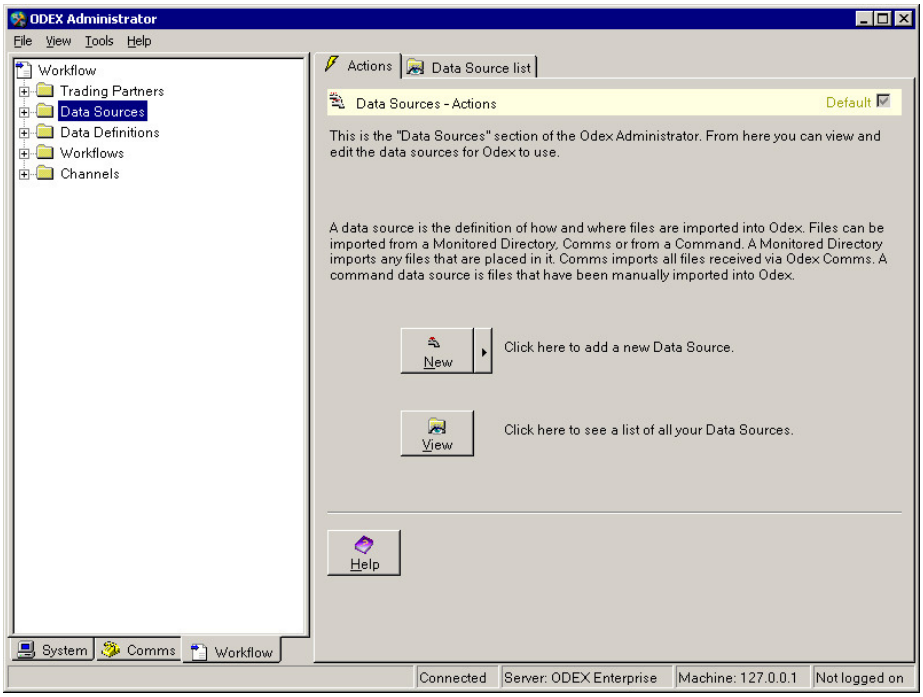
The Trading Partners section of the Workflow Administrator is exactly the same as the Trading Partners section of the Comms Administrator. Any trading partners you have already added will be viewable from here. Likewise, any trading partners you add or edit here will be viewable from the Comms Administrator.

For full details of how to add or edit trading partner details, please refer to the section entitled "Adding/Editing Trading partners".

Data Sources

This section of the Workflow Administrator enables you to define the different data sources you will be using to import files into ODEX.

When you click on the Data Sources node in the tree view, you will see the following screen.



This is the Data Sources – Actions screen. From here you can add new data sources or view and edit existing data sources.

To add a new data source

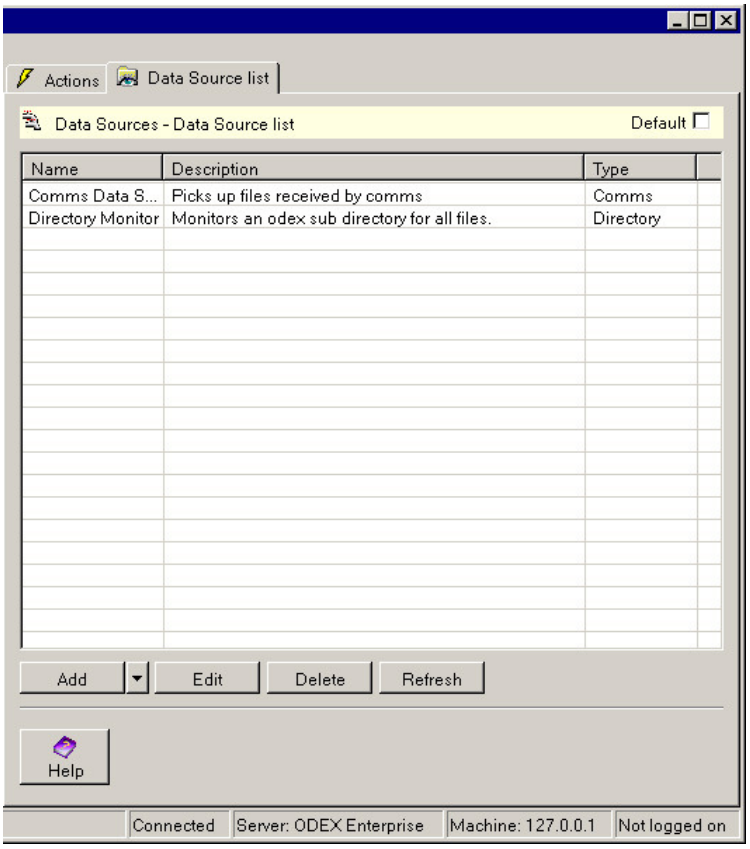
Click the **New** button to add a new data source, or open the Data Source list page and click the **Add** button on that page. You will be offered the choice of Command, Comms and Directory data sources.

To edit an existing data source

Double-click on an existing data source in the tree view, or open the Data Source list page, select an entry and click the **Edit** button.

Viewing all your data sources

If you wish to see a list of all the data sources currently in the ODEX database, you can either click the **View** button on the Data Sources – Actions page or click the Data Source list tab. Both have the same result, as in the example below.



The Information Panel now shows the Data Source list page. This is divided into two columns, showing the Data Source Name and its Description.

The actions that can be taken from this page are as follows:

Add

New data sources may be added to the list by using the **Add** button. If this button is clicked you will see another three options, allowing you to select the particular type of data source you want to add. The three options are:

Command data source – described in the section “Add/Edit Command data source”.

Comms data source – described in the section "Add/Edit Comms data source".

Directory data source – described in the section "Add/Edit Directory data source".

Edit

You may edit the details of existing data sources by using the **Edit** button. Highlight the entry you want to edit and click this button to bring up the appropriate set of pages.

Delete

If you wish to delete a data source from the list, highlight the line that you wish to delete, then click on the **Delete** button. ODEX will bring up a dialog box, asking if you are sure you want to delete the selected items. This is to safeguard against accidentally deleting the wrong item. Click **Yes** to delete or **No** to keep the item in the list.

Refresh

Click this button to refresh the details on this page, for example if you have just made some changes which have not yet appeared on this page.

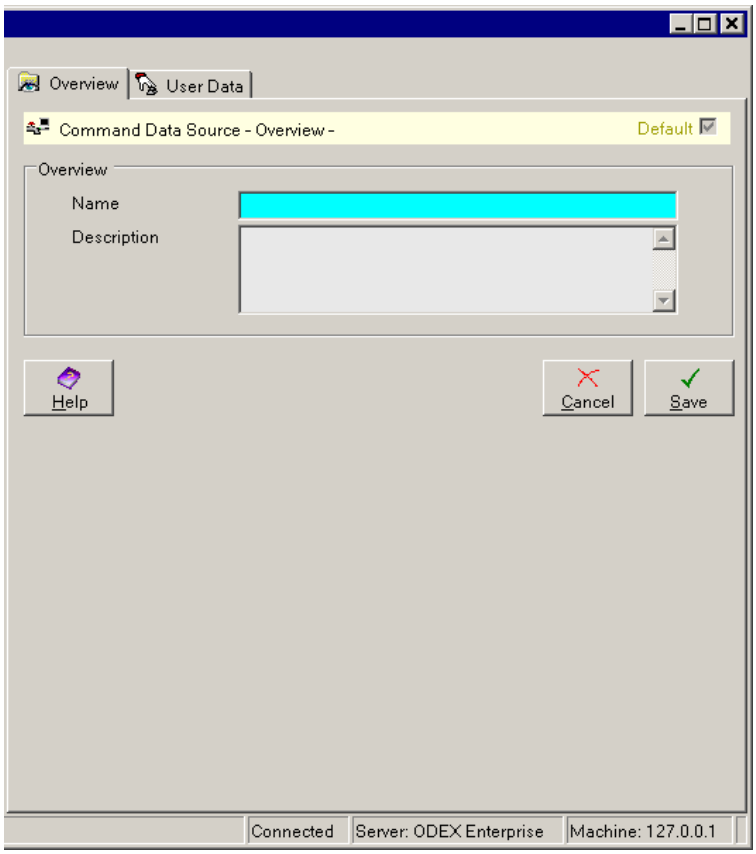
Help

If you need more information about the fields and buttons on this page, click on the **Help** button.

Add/Edit Command data source

Data Source – Overview

The Command Data Source – Overview page is shown below.



Overview – Name

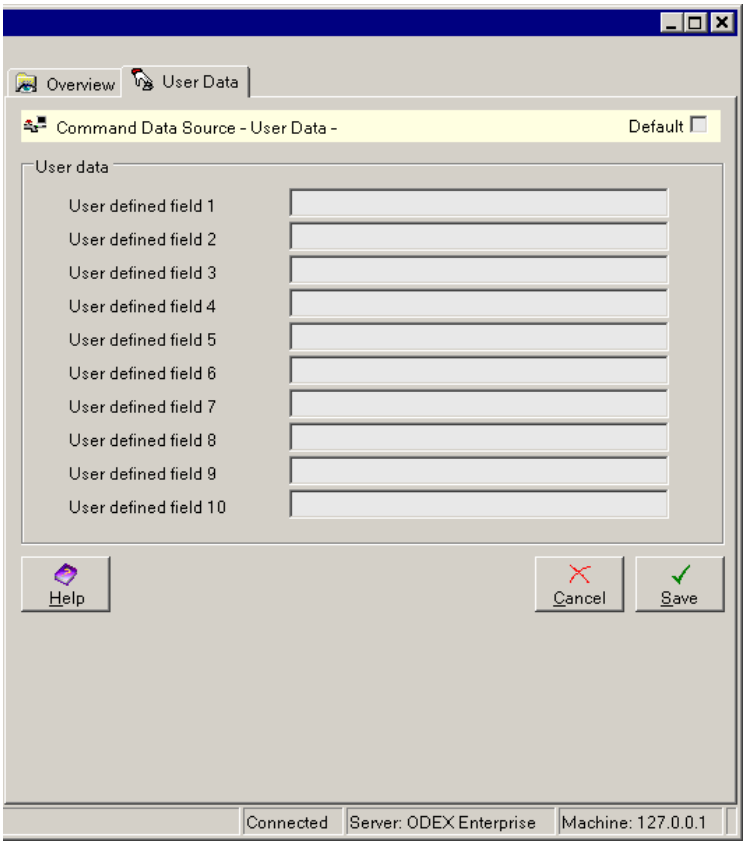
This field requires a name for the Command Data Source. This name must be unique among your other Command Data Sources, but it can be whatever you want it to be. The name is a unique identifier, enabling you to recognise it easily when you want to use this Data Source.

Overview – Description

You may provide a description of the Data Source in this field if you wish. The description is intended to help you remember what the Data Source is for.

Data Source – User Data

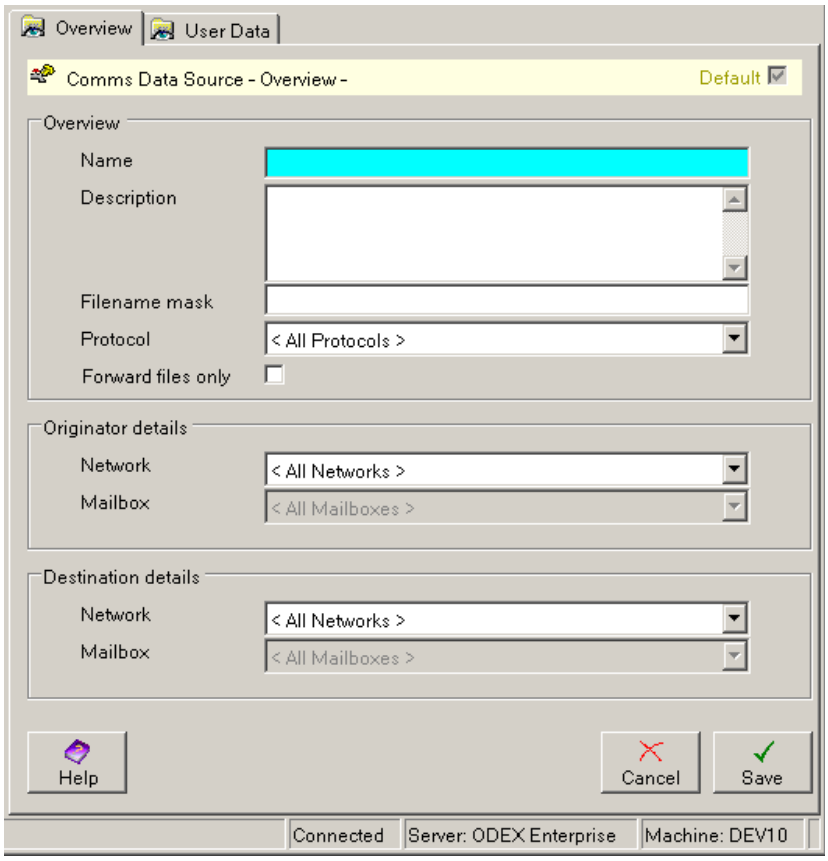
The User Data page allows you to provide a number of fields that can be used throughout Odex. For example, you can set up a User Data field against each Data Source to specify a different email subject for each Source. Then, if a workflow is set up to send you an email whenever a file is received, you can use a placeholder to specify the data sources User Data should be used for the email subject. Using this technique you can tailor your emails to be Data Source specific, without having a number of channels/workflows defined.



Simply edit the fields you wish to use and they can then be accessed using placeholders in jobs and actions (see the Placeholders section for more details).

Add/Edit Comms data source

The Comms Data Source – Overview page is shown below.



Overview – Name

This field requires a name for the Comms Data Source. This name must be unique among your other Comms Data Sources, but it can be whatever you want it to be. The name is a unique identifier, enabling you to recognise it easily when you want to use this Data Source.

Overview – Description

You may provide a description of the Data Source in this field if you wish. The description is intended to help you remember what the Data Source is for.

Overview – Filename mask

This field is not applicable to AS2 files.

This field allows you to specify a filename mask for files that are to be filtered by this data source. Since all OFTP comms files will have a virtual filename when they arrive in ODEX, any filename mask you give here should correspond to the virtual filename format used by the Originator whose details you will provide below.

You may use the asterisk character (*) to signify one or more unspecified characters. You may use the question mark character (?) to signify one unspecified character.

Taking the Ford VFN format as an example, you could use one of the following filename masks to achieve different results:

FORD.S* – filter all Ford files

FORD.SABC12* – filter all Ford messages for the Supplier code ABC12

FORD.S*RE – filter all Ford Release messages for any Supplier code

FORD.S?????ST – filter all Ford DCI messages for any Supplier code (five question marks are more precise than the asterisk but would have the same effect)

Overview – Protocol

Use this field to filter by communications protocol. You may either select a specific protocol for this data source, or allow files arriving via all protocols to be handled.

The protocol you choose will determine the behaviour of the fields below.

If you select “AS2” in this field, the ‘Filename mask’ field above will be disabled.

Overview – Forward files only

This option is for use in a clearing centre environment. It specifies that only files received that are to be forwarded on to another destination will be matched to this data source. This applies to files received where the destination mailbox is defined on an external network.

Originator details – Network

Use this field to filter by Originator Network. You can choose <All Networks> or select a specific network using the dropdown list.

If you have selected <All protocols> above, this field will allow you to choose any of your networks.

If you have selected a specific protocol above, this field will only allow you to choose a network associated with that protocol.

Originator details – Mailbox

This field will only be enabled if you have chosen a specific OFTP network in the field above. Use this field to filter by Originator Mailbox. You can choose <All Mailboxes> or select a specific mailbox using the dropdown list.

Destination details – Network

Use this field to filter by Destination Network. You can choose <All Networks> or select a specific network using the dropdown list.

If you have selected <All protocols> above, this field will allow you to choose any of your networks.

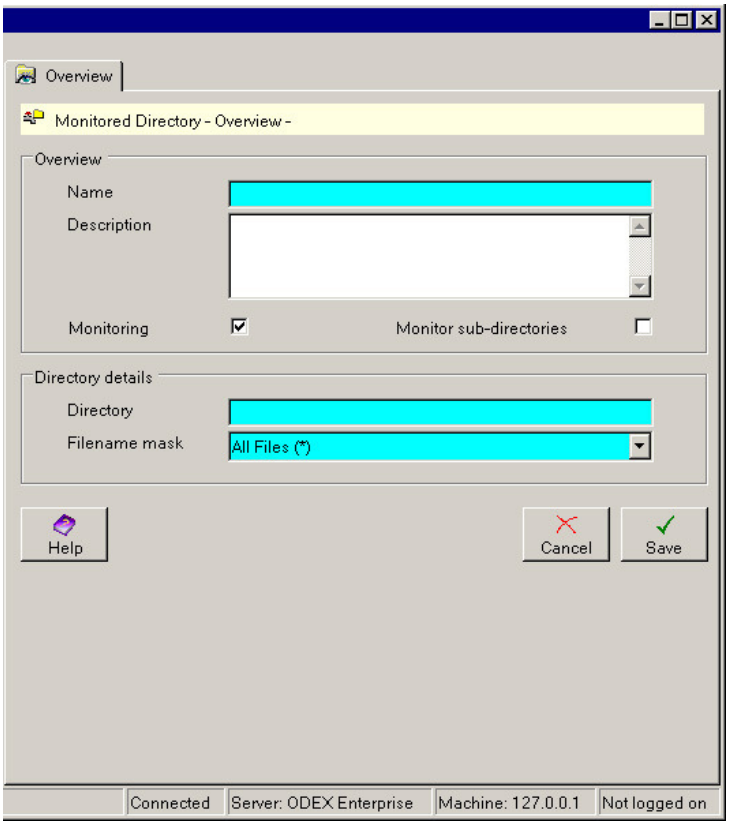
If you have selected a specific protocol above, this field will only allow you to choose a network associated with that protocol.

Destination details – Mailbox

This field will only be enabled if you have chosen a specific OFTP network in the field above. Use this field to filter by Destination Mailbox. You can choose <All Mailboxes> or select a specific mailbox using the dropdown list.

Add/Edit Directory data source

The Monitored Directory – Overview page is shown below.



Overview – Name

This field requires a name for the Monitored Directory Data Source. This name must be unique among your other Monitored Directory Data Sources, but it can be whatever you want it to be. The name is a unique identifier, enabling you to recognise it easily when you want to use this Data Source.

Overview – Description

You may provide a description of the Data Source in this field if you wish. The description is intended to help you remember what the Data Source is for.

Monitoring tickbox

This tickbox is selected by default. Deselect it if you want to turn off monitoring of the directory temporarily or if you prefer to poll the directory data source using the ODEX Event Actions facility.

ODEX relies on Windows notifications to tell it when a file has been copied to a directory. If the directory is an NFS share (on a non-Windows system), or a Novell share, these notifications are not generated and ODEX does not know about new files. The only exception to this is that, when first started, ODEX checks all of the monitored directories, as there may have been notifications which occurred whilst ODEX was not running.

If you are using an NFS share or a Novell share, you should deselect the "Monitoring" flag, then configure ODEX to look in the directory periodically, as follows:

From the System tab of the ODEX Administrator, select Event Actions and create a new entry which has the action "Poll Monitored Directory". You can use an existing schedule (e.g. Hourly), or create a new schedule to run this action.

Monitor sub-directories tickbox

This tickbox is deselected by default. Select this tickbox if you want to monitor all sub-directories below the directory specified in the field below.

Directory details – Directory

Type in this field the name of the directory to be monitored. Please be aware that files will be removed from the monitored directory for processing by ODEX.

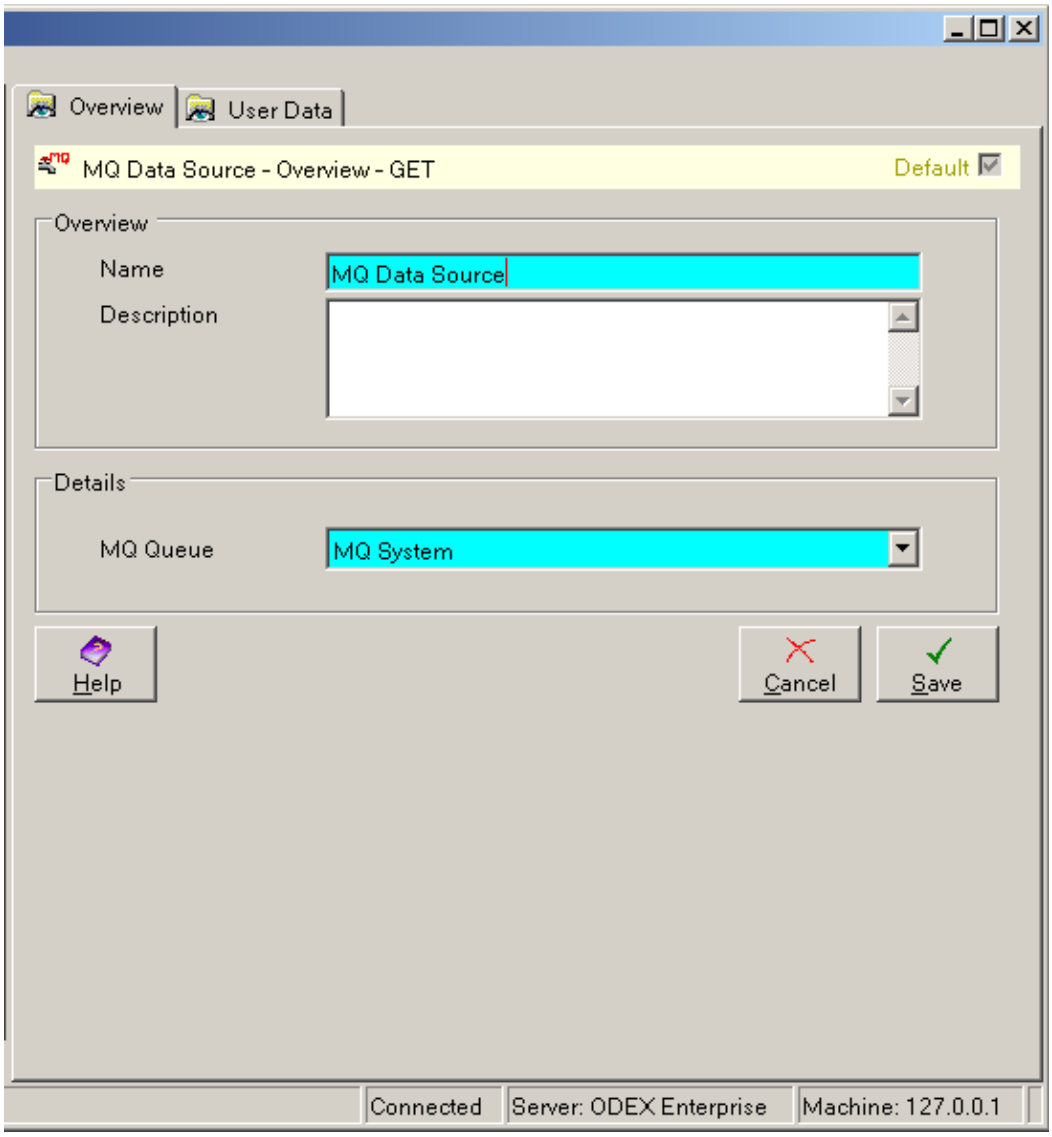
Directory details – Filename mask

Use the dropdown list to select the type of files you want to be taken from this directory. Available options are *.edi files, *.hse files, *.xml files or all files (*).

Add/Edit MQ data source

For detailed instructions on the usage of MQ data sources please see the WebSphereMQ section in ODEX concepts.

MQ Data Source – Overview page is shown below.



Overview – Name

This field requires a name for the MQ Data Source. This name must be unique among your other MQ Data Sources, but it can be whatever you want it to be. The name is a unique identifier, enabling you to recognise it easily when you want to use this Data Source.

Overview – Description

You may provide a description of the Data Source in this field if you wish. The description is intended to help you remember what the Data Source is for.

Overview – MQ Queue

This required field is the MQ queue which you wish to poll for data. You will need to set up an event action that links to this MQ Data Source.

Data Definitions

The Data Definitions section allows you to define the different types of data that you will be processing, the trading partners the data will come from, and the type of data encoding used, in order to ensure that each file is processed by the appropriate workflow channel(s).

There are five types of data definition, which form a kind of hierarchy.

At the lowest level is the non-EDI Data Definition. This only requires you to specify what type of encoding is used for the non-EDI files.

At the same level is the invalid EDI Data Definition. This only requires you to provide a name for the data definition. This type of data definition represents EDI files that cannot be analysed due to errors in the file.

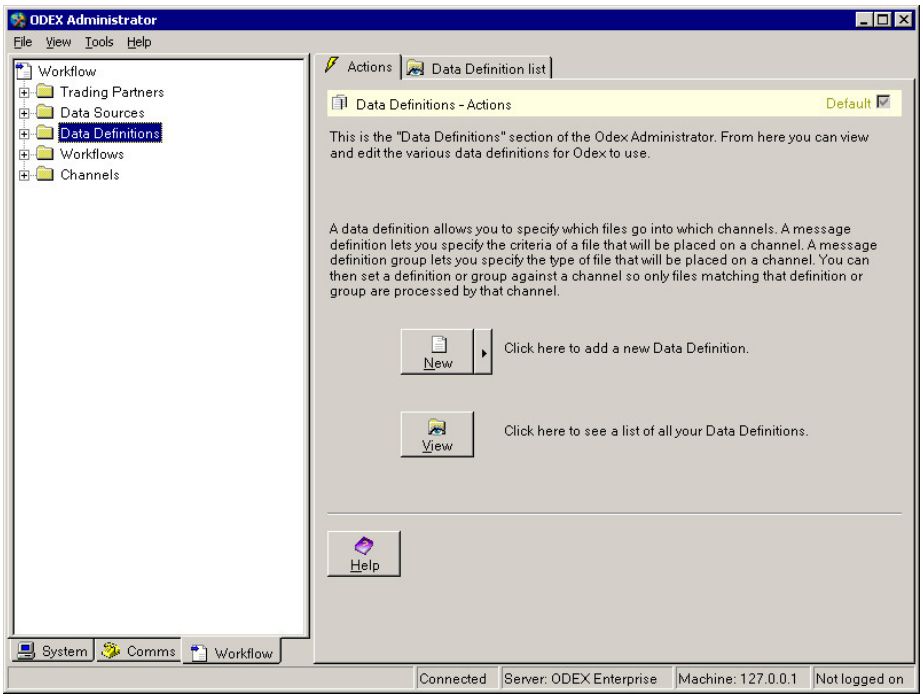
This level also contains the EDI Message Definition. This requires you to provide a name and message definition details, such as the syntax of the EDI message e.g. name = DELFOR, syntax = EDIFACT. This would create a data definition for all EDIFACT DELFOR messages.

At the level above this is the EDI Message Group Definition. This allows you, if you wish, to group together two or more of the EDI Message Definitions you have defined.

At the top of the hierarchy is the EDI Data Definition. This allows you to be as specific as possible about the data that is to be processed by the same workflow channels.

Using combinations of the four definitions described above, you can create an extremely flexible system of data channelling.

When you click on the Data Definitions node in the tree view, you will see the following screen.



This is the Data Definitions – Actions screen. From here you can add new data definitions or view and edit existing data definitions.

To add a new data definition

Click the **New** button to add a new data definition, or open the Data Definition list page and click the **Add** button on that page. You will be offered the choice of EDI Data Definition, Invalid EDI Data Definition, non-EDI Data Definition, EDI Message and EDI Message Group. Select the appropriate option to see the set of pages described in the following sections:

Add/Edit Non-EDI Data Definition

Add/Edit Invalid EDI Data Definition

Add/Edit EDI Message

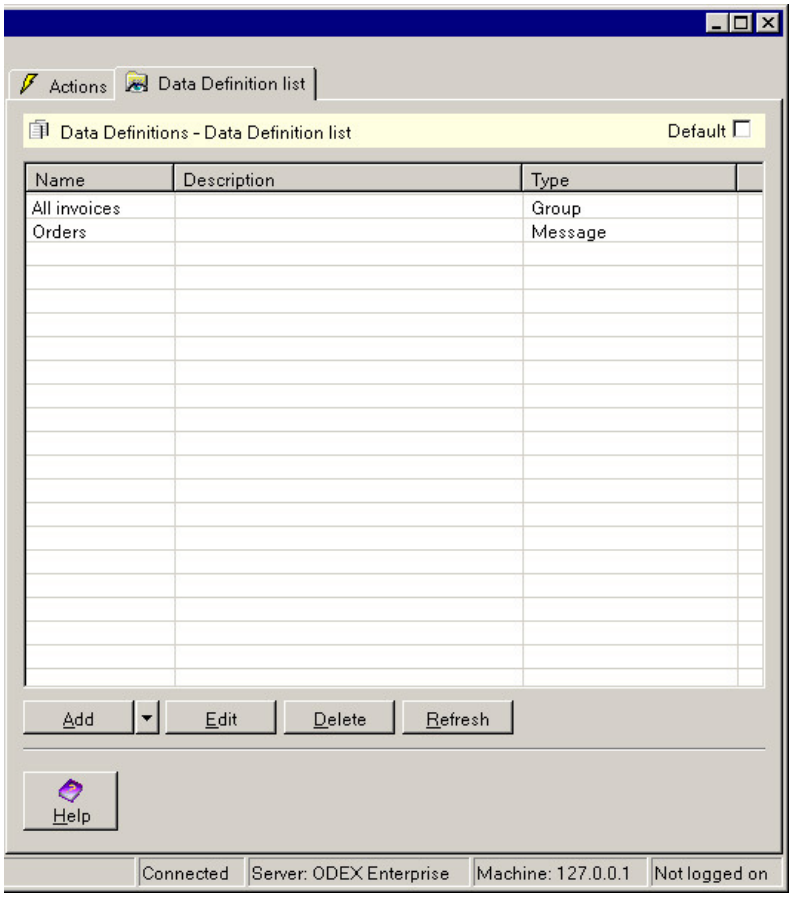
Add/Edit EDI Message Group

To edit an existing data definition

Double-click on an existing data definition in the tree view, or open the Data Definition list page, select an entry and click the **Edit** button.

Viewing all your data definitions

If you wish to see a list of all the data definitions currently in the ODEX database, you can either click the **View** button on the Data Definitions – Actions page or click the Data Definition list tab. Both have the same result, as in the example below.



The Information Panel now shows the Data Definition list page. This is divided into three columns, showing the Data Definition Name, its Description and its Type.

The actions that can be taken from this page are as follows:

Add

New data definitions may be added to the list by using the **Add** button. If this button is clicked you will see another four options, allowing you to select the particular type of data definition you want to add. The four options are:

EDI Data Definition – described in the section "Add/Edit EDI Data Definition"

Invalid EDI Data Definition – described in the section Add/Edit Invalid EDI Data Definition

Non-EDI Data Definition – described in the section "Add/Edit Non-EDI Data Definition"

EDI Message – described in the section "Add/Edit EDI Message"

EDI Message Group – described in the section "Add/Edit EDI Message Group"

Edit

You may edit the details of existing data definitions by using the **Edit** button. Highlight the entry you want to edit and click this button to bring up the appropriate set of pages.

Delete

If you wish to delete a data definition from the list, highlight the line that you wish to delete, then click on the **Delete** button. ODEX will bring up a dialog box, asking if you are sure you want to delete the selected items. This is to safeguard against accidentally deleting the wrong item. Click **Yes** to delete or **No** to keep the item in the list.

Refresh

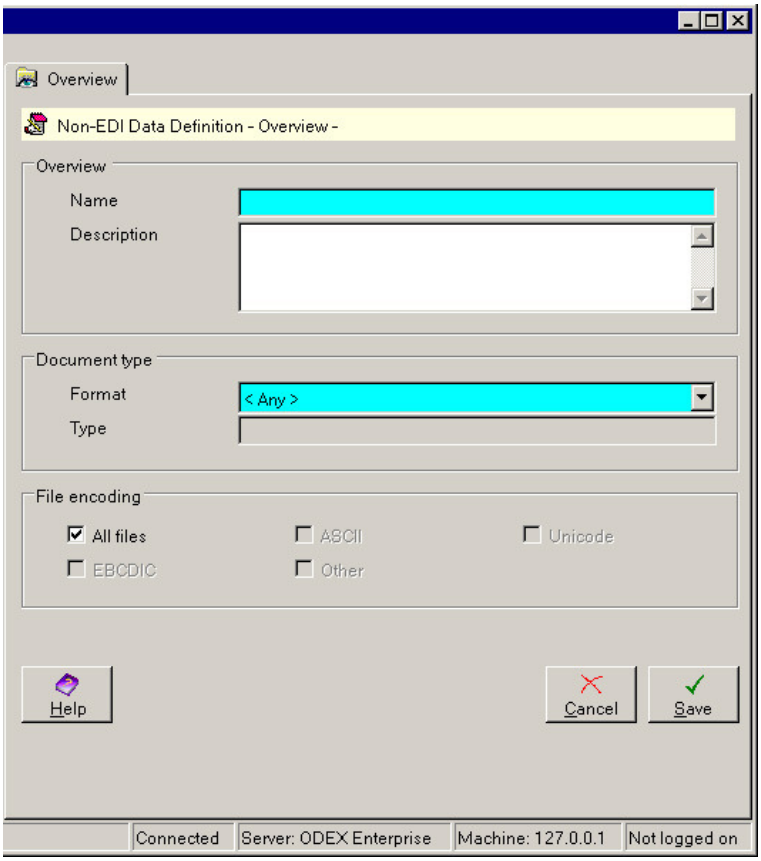
Click this button to refresh the details on this page, for example if you have just made some changes which have not yet appeared on this page.

Help

If you need more information about the fields and buttons on this page, click on the **Help** button.

Add/Edit Non-EDI Data Definition

The non-EDI Data Definition – Overview page is shown below.



Overview – Name

This field requires a name for the Non-EDI Data Definition. This name must be unique among your other Non-EDI Data Definitions, but it can be whatever you want it to be. The name is a unique identifier, enabling you to recognise it easily when you want to use this Non-EDI Data Definition.

Overview – Description

You may provide a description of the Non-EDI Data Definition in this field if you wish. The description is intended to help you remember what the Data Definition is for.

Document type – Format

Use the dropdown list to choose the format of non-EDI data to be handled by this Data Definition. Current choices are Any, SAP IDoc and Unrecognised.

<Any> handles any type of non-EDI data.

"SAP IDoc" handles only SAP IDoc files.

"Unrecognised" handles all non-EDI files that are not included in the other categories.

If you select SAP IDoc, the Type field below will become enabled.

Document type – Type

This field will only be enabled if you have selected "SAP IDoc" in the Format field above.

You may provide a specific type of IDoc in this field e.g. DELINS. Alternatively, leave the field blank to handle all IDoc types.

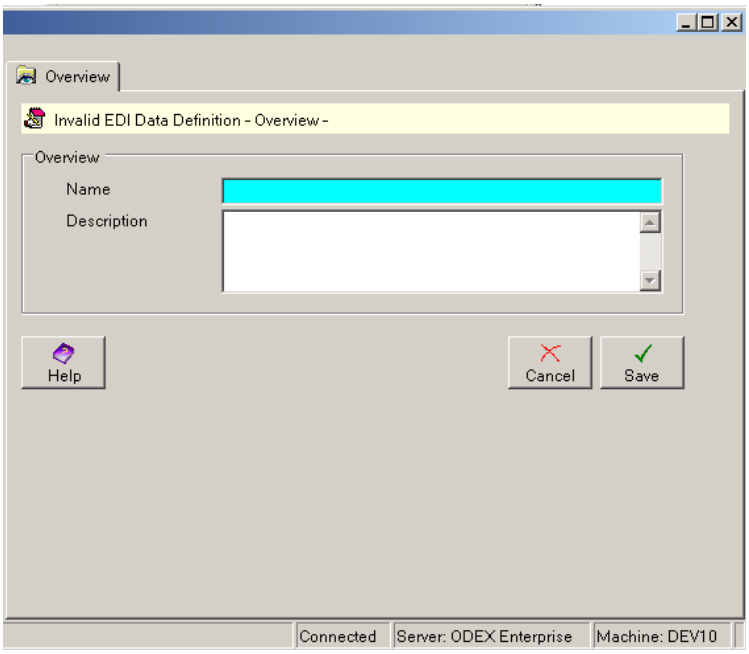
File encoding

This field will only be enabled if you have selected "Any" in the Format field above.

By default, the 'All files' tickbox is selected. If you wish, you can restrict the Data Definition by selecting one of the other types of encoding. First de-select the 'All files' tickbox to enable the other tickboxes. Then select one or more of the other types of encoding.

Add/Edit Invalid EDI Data Definition

The Invalid EDI Data Definition – Overview page is shown below. This allows you to create a Data Definition that will match files that are EDI files, where the files cannot be analysed due to errors in the files.



Overview – Name

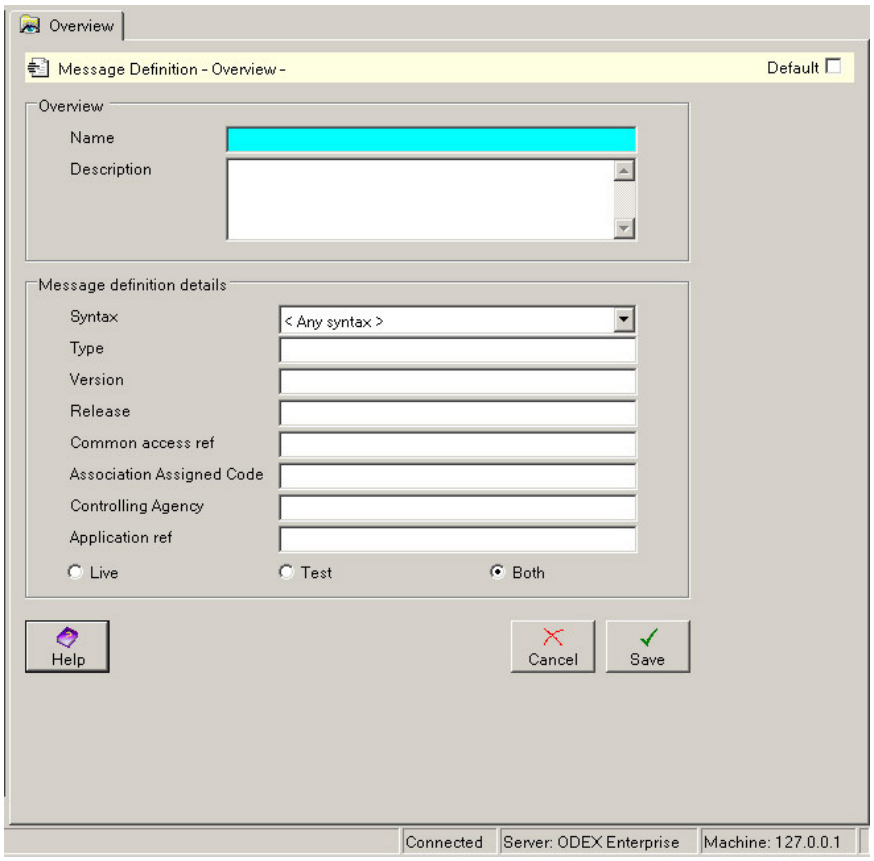
This field requires a name for the Data Definition. This name must be unique among your other EDI Data Definitions, but it can be whatever you want it to be. The name is a unique identifier, enabling you to recognise it easily when you want to use this Non-EDI Data Definition.

Overview – Description

You may provide a description of the Invalid EDI Data Definition in this field if you wish. The description is intended to help you remember what the Data Definition is for.

Add/Edit EDI Message

The Message Definition – Overview page is shown below.



Overview – Name

This field requires a name for the Message Definition. This name must be unique among your other Message Definitions, but it can be whatever you want it to be. The name is a unique identifier, enabling you to recognise it easily when you want to use this Message Definition.

Overview – Description

You may provide a description of the Message Definition in this field if you wish. The description is intended to help you remember what the Message Definition is for.

Message definition details – Syntax

Use this field to select the syntax of messages to which you want to restrict this Message Definition. If all your received messages use the same syntax, you may leave this field set to <Any syntax>.

Message definition details – Type

Use this field to specify the type of messages to be handled by this Message Definition. Leave the field empty if you want this Message Definition to handle all types of messages.

The name you type in here must correspond to the message type as defined by the standards body responsible for the message.

For an EDIFACT message, the type can be found in the second element of the UNH service segment. In the example below, the Type would be DELFOR:

UNH+123456+**DELFOR**:D:96A:UN:A09041+Ref+1'

For a VDA message, type in the 4-digit name of the message e.g. 4905 for a Release message, 4915 for a Call-Off message.

Message definition details – Version

This field is only applicable to EDIFACT and EDIFACT V4 messages.

Use this field to specify the version of messages to be handled by this Message Definition. Leave the field empty if you want this Message Definition to handle all message versions.

The version you type in here must correspond to the message version as given in the UNH segment of the incoming message.

For example, for the following UNH segment, the Version would be D (highlighted)

UNH+123456+DELFOR:**D**:96A:UN:A09041+Ref+1'

Message definition details – Release

This field is only applicable to EDIFACT and EDIFACT V4 messages.

Use this field to specify the release code of messages to be handled by this Message Definition. Leave the field empty if you want this Message Definition to handle all message release codes.

The release code you type in here must correspond to the release code as given in the UNH segment of the incoming message.

For example, for the following UNH segment, the Release would be 96A (highlighted)

UNH+123456+DELFOR:D:**96A**:UN:A09041+Ref+1'

Message definition details – Common access ref

This field is only applicable to EDIFACT and EDIFACT V4 messages.

Use this field to specify the common access reference code of messages to be handled by this Message Definition. Leave the field empty if you want this Message Definition to handle all common access reference codes.

The common access reference code you type in here must correspond to the common access reference code as given in the UNH segment of the incoming message.

For example, for the following UNH segment, the Common access reference code would be A09041 (highlighted)

UNH+123456+DELFOR:D:96A:UN:A09041+**Ref**+1'

Message definition details – Association Assigned Code

This field is only applicable to EDIFACT and EDIFACT V4 messages.

Use this field to specify the association assigned code of messages to be handled by this Message Definition. Leave the field empty if you want this Message Definition to handle all association assigned codes.

The association assigned code you type in here must correspond to the association assigned code as given in the UNH segment of the incoming message.

For example, for the following UNH segment, the association assigned code would be (highlighted)

UNH+123456+DELFOR:D:96A:UN:**A09041**+Ref+1'

Message definition details – Controlling Agency

This field is only applicable to EDIFACT and EDIFACT V4 messages.

Use this field to specify the controlling agency of messages to be handled by this Message Definition. Leave the field empty if you want this Message Definition to handle all controlling agencies.

The controlling agency you type in here must correspond to the controlling agency as given in the UNH segment of the incoming message.

For example, for the following UNH segment, the controlling agency code would be (highlighted)

UNH+123456+DELFOR:D:96A:**UN**:A09041+Ref+1'

Message definition details – Application ref

This field is only applicable to EDIFACT and EDIFACT V4 messages.

Use this field to specify the application reference of messages to be handled by this Message Definition. Leave the field empty if you want this Message Definition to handle all application references.

The application reference you type in here must correspond to the application reference as given in the UNB segment of the incoming message.

Message definition details – Live, Test, Both

This field is only applicable to EDIFACT and EDIFACT V4 messages.

Use this field to specify the test indicator of messages to be handled by this Message Definition. The test indicator can be set to Live, Test or Both.

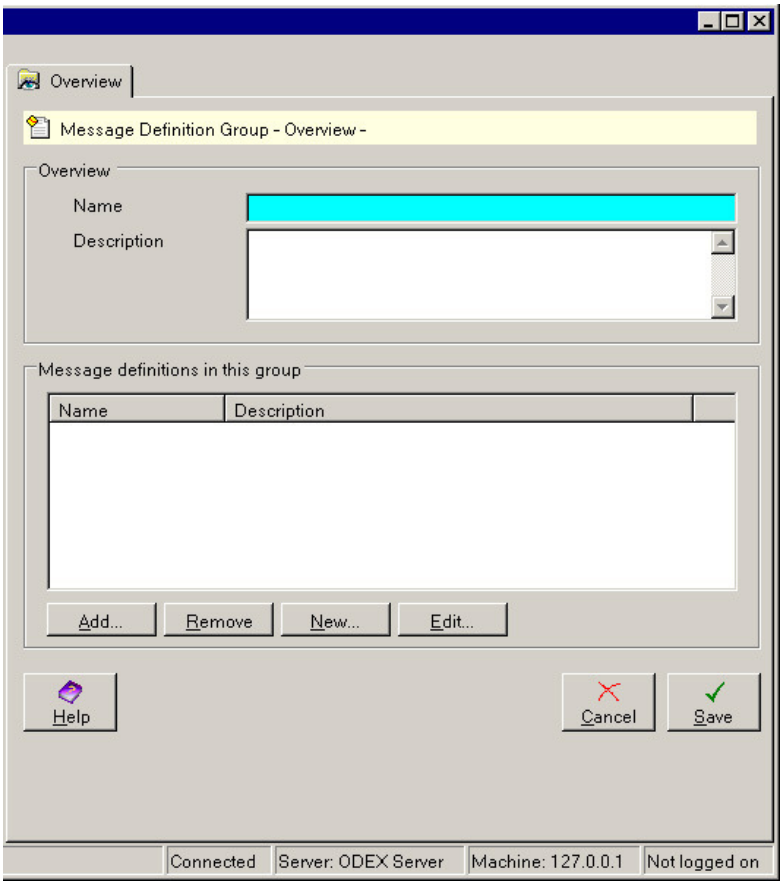
The test indicator defined here must correspond to the test indicator as given in the UNB segment of the incoming message.

Add/Edit EDI Message Group

The Message Definition Group – Overview page is shown below.

This page can be used to:

- Create a message group in which you can include new or existing message definitions
- Add to an existing group any message definitions that you have already defined
- Create new message definitions which will automatically be added to this group. Adding a new message definition here is just the same as adding it by using the **New** button on the Data Definitions Actions page or by using the **Add** button on the Data Definition list page.



Overview – Name

This field requires a name for the Message Definition Group. This name must be unique among your other Message Definition Groups, but it can be whatever you want it to be. The name is a unique identifier, enabling you to recognise it easily when you want to use this Message Definition Group.

Overview – Description

You may provide a description of the Message Definition Group in this field if you wish. The description is intended to help you remember what the Message Group is for.

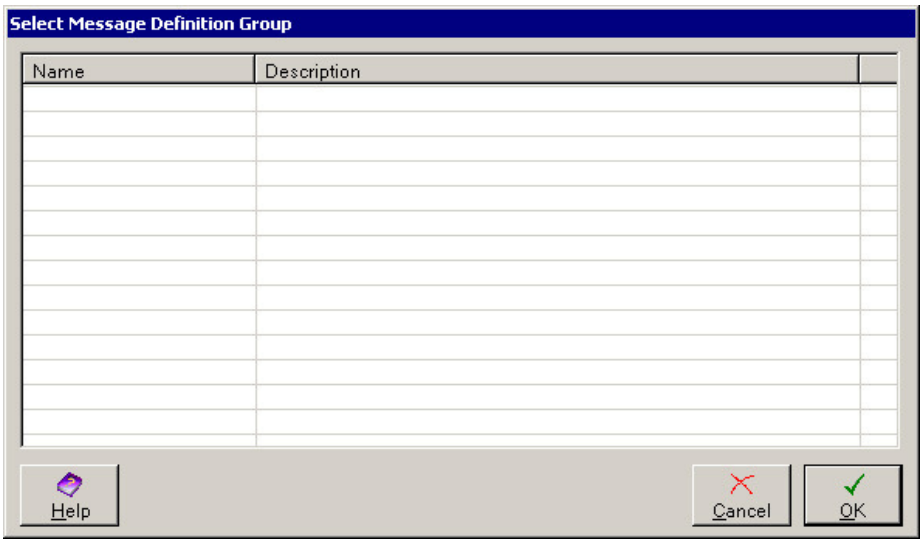
Message definitions in this group

This section shows a list of the message definitions that already belong to this group. An empty list means that the group contains no message definitions yet. This section has four buttons:

- **Add** – use this button to add existing message definitions to the group
- **Remove** – use this button to remove message definitions from the group
- **New** – use this button to create a new message definition that will be added automatically to the group
- **Edit** – use this button to edit an existing message definition that belongs to this group

Add message definition

If you click the **Add** button, you will see the dialog below.



This dialog will contain a list of all the message definitions you have already defined. Select one or more of them and click **OK** to add them to this group.

Remove message definition

To remove message definitions from the group, select one or more message definitions from the list and click the **Remove** button.

Create a new message definition

To create a new message definition to be added automatically to this group, click the **New** button. This will bring up the Add New Message Definition dialog, which requires the same information as the Message Definition Overview page, described in the section entitled Add/Edit EDI Message.

Edit a message definition

To edit a message definition that already belongs to this group, click the **Edit** button. This will bring up the Edit Message Definition dialog, which requires the same information as the Message Definition Overview page, described in the section entitled Add/Edit EDI Message.

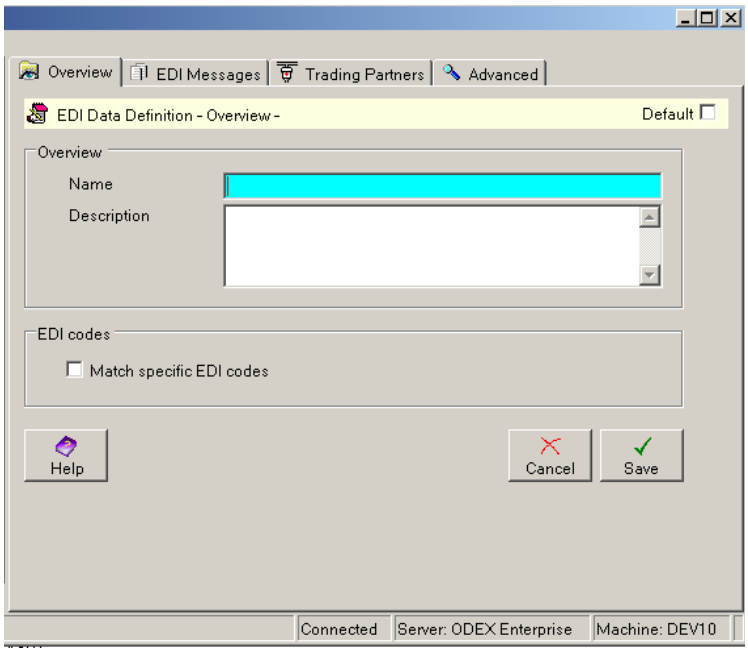
Add/Edit EDI Data Definition

The EDI Data Definition section allows you great flexibility in the way you categorise the data that is to be channelled.

The EDI Data Definition section consists of four or five pages, depending on how you configure you Data Definition: Overview, EDI Messages, Trading Partners, EDI codes and Advanced. The EDI Messages, Trading Partners, EDI codes and Advanced pages allow you to select the appropriate entries for channelling your data.

They are each described below.

EDI Data Definition – Overview



Overview – Name

This field requires a name for the EDI Data Definition. This name must be unique among your other EDI Data Definitions, but it can be whatever you want it to be. The name is a unique identifier, enabling you to recognise it easily when you want to use this EDI Data Definition.

Overview – Description

You may provide a description of the EDI Data Definition in this field if you wish. The description is intended to help you remember what the EDI Data Definition is for.

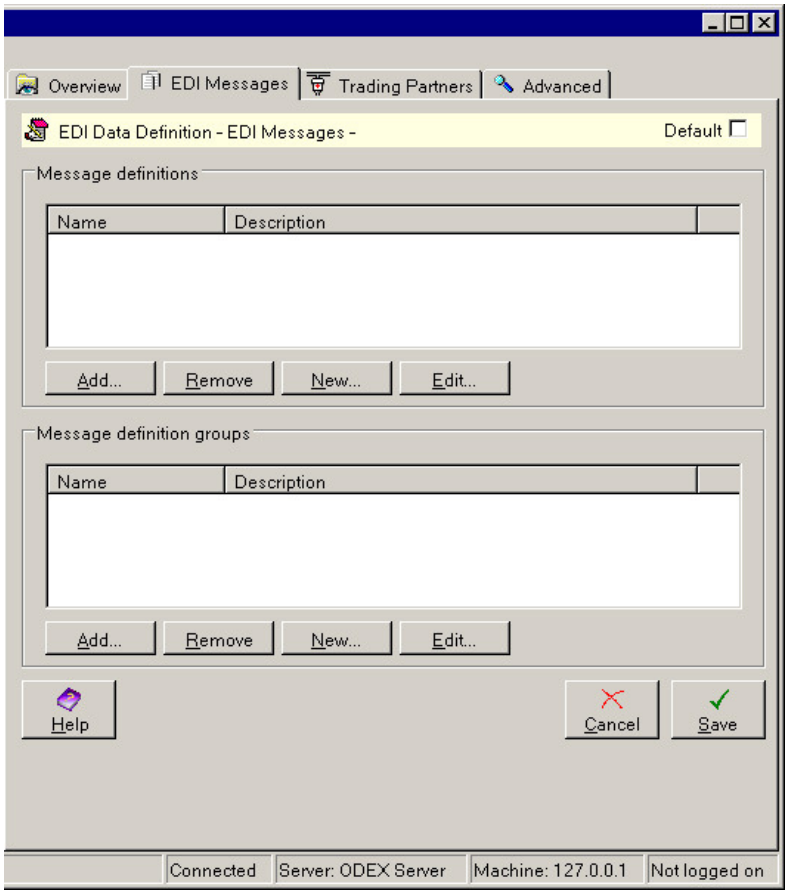
EDI codes – Match specific EDI codes

When this option is not selected, four tabs will be displayed as above. If you select this option, an additional 'EDI Codes' tab will be added to the view.

When this option is not selected, you can only add trading partners and EDI codes to the Data Definition using the Trading Partners tab. For more details, see the section entitled "Trading Partners"

If you select 'Match specific EDI codes', the Trading Partners tab will be changed to allow you to add origin and destination Trading Partners. For more details, see the section entitled "Trading Partners". An additional tab will be added to allow you to add origin and destination EDI Codes. For more information see the section entitled "EDI Codes".

EDI Data Definition – EDI Messages

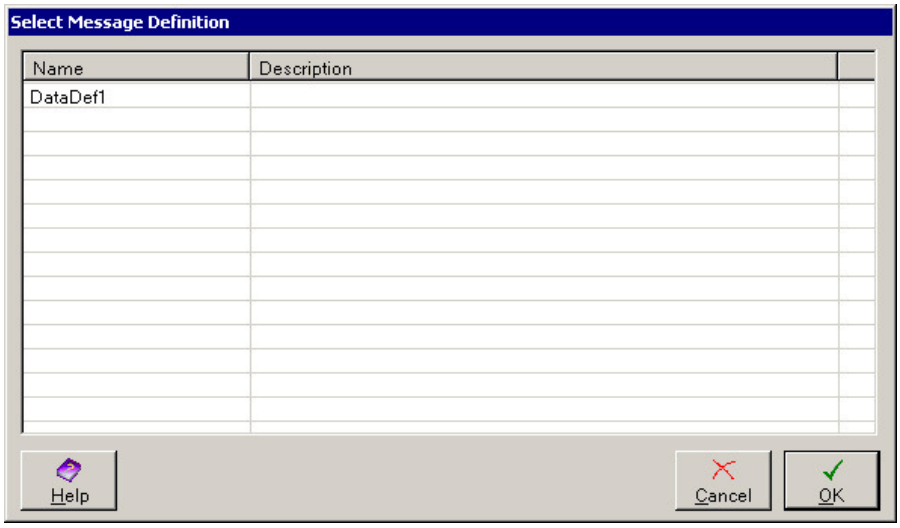


This page is divided into two sections: Message definitions and Message definition groups.

Each section contains an **Add** button, a **Remove** button, a **New** button and an **Edit** button.

Add message definition

If you click the **Add** button, you will see the dialog below.



This dialog will contain a list of all the message definitions you have already defined. Select one or more of them and click **OK** to add them to this group.

Remove message definition

To remove message definitions from the group, select one or more message definitions from the list and click the **Remove** button.

Create a new message definition

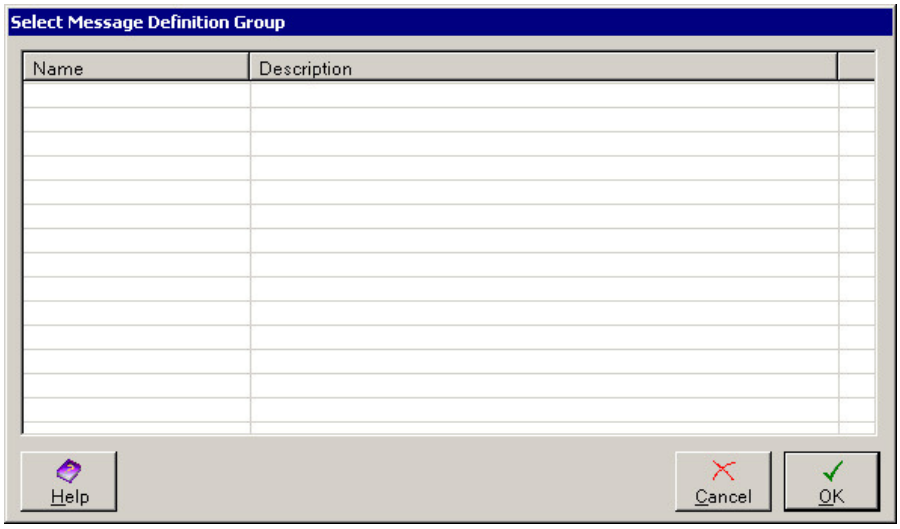
To create a new message definition to be added automatically to this group, click the **New** button. This will bring up the Add New Message Definition dialog, which requires the same information as the Message Definition Overview page, described in the section entitled Add/Edit EDI Message.

Edit a message definition

To edit a message definition that already belongs to this group, click the **Edit** button. This will bring up the Edit Message Definition dialog, which requires the same information as the Message Definition Overview page, described in the section entitled Add/Edit EDI Message.

Add message definition group

If you click the **Add** button, you will see the dialog below.



This dialog will contain a list of all the message definition groups you have already defined. Select one or more of them and click **OK** to add them to this EDI Data Definition.

Remove message definition group

To remove message definition groups from the EDI Data Definition, select one or more message definition groups from the list and click the **Remove** button.

Create a new message definition group

To create a new message definition group to be added automatically to this EDI Data Definition, click the **New** button. This will bring up the Add New Message Definition Group dialog, which requires the same information as the Message Definition Group Overview page, described in the section entitled Add/Edit EDI Message Group.

Edit a message definition group

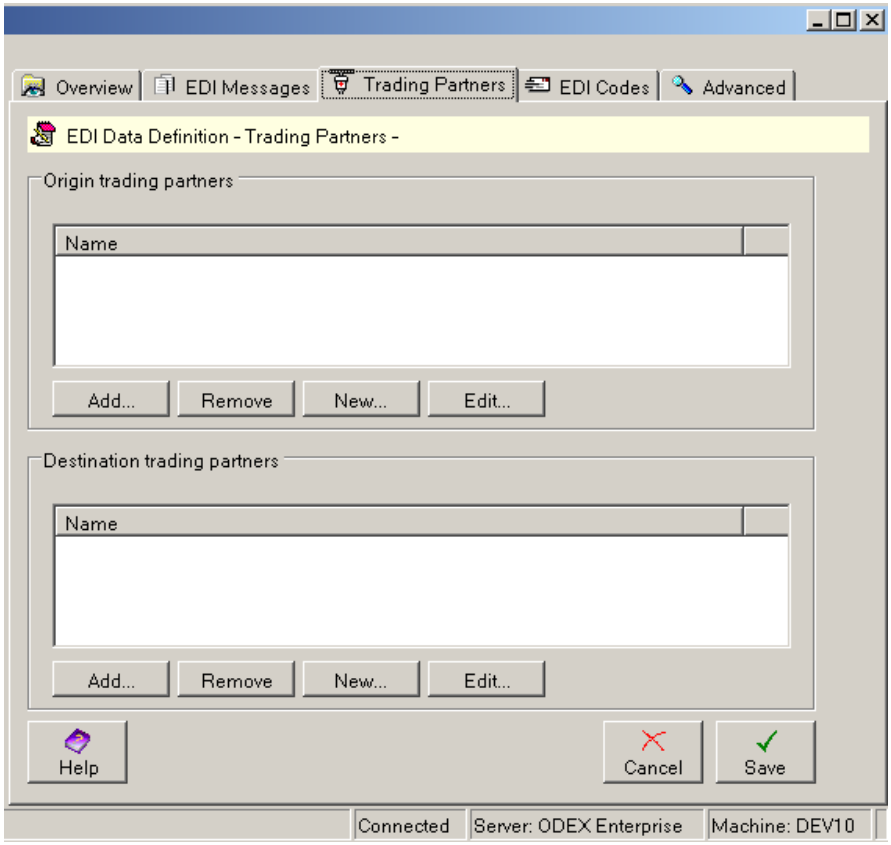
To edit a message definition group that already belongs to this EDI Data Definition, click the **Edit** button. This will bring up the Edit Message Definition Group dialog, which requires the same information as the Message Definition

Group Overview page, described in the section entitled Add/Edit EDI Message Group.

Of course, if you edit a message definition group, you will also be able to edit the message definition(s) which make up that group.

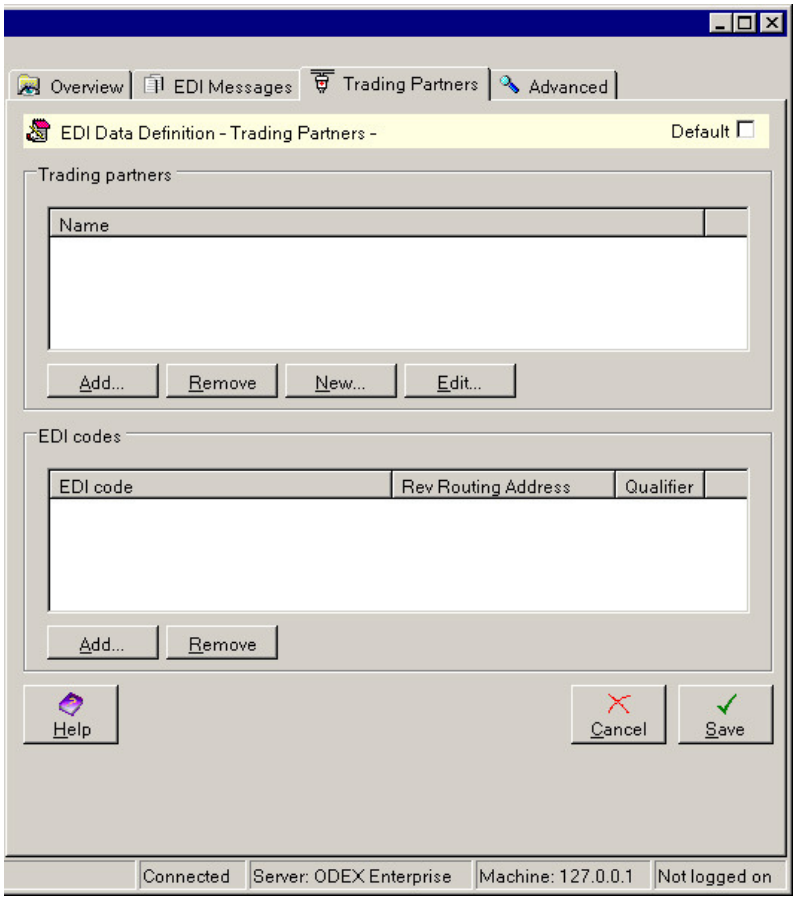
Trading Partners

This page is divided into two sections. If you are configuring the Data Definition to match specific EDI codes, the two sections are Origin Trading Partners and Destination Trading Partners, as shown below. To add specific EDI codes to the Data Definition, you must use the EDI codes tab.



When the Data Definition is set up in this way, the Data Definition matches any files where the origin EDI code matches an EDI code of one of the origin Trading Partners and the destination EDI code matches an EDI code of one of the destination Trading Partners.

Alternatively, if the Data Definition is set up such that it will not match specific EDI codes, the page will be divided into two sections – one for trading partners and one for EDI codes, as shown below.

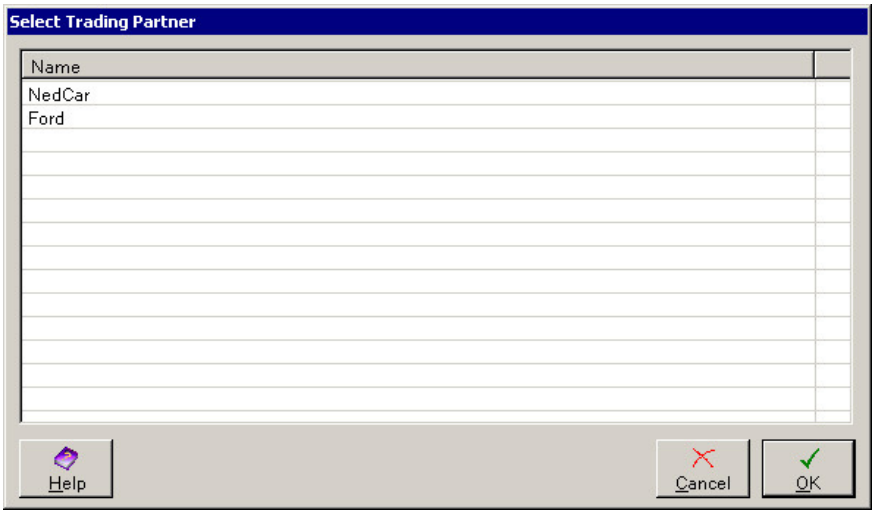


When the Data Definition is set up in this way, any inbound files with an origin EDI code matching one of the EDI codes in the list or an EDI code of one of the trading partners in the list will be matched to the Data Definition. Any outbound files with a destination EDI code matching one of the EDI codes in the list or an EDI code of one of the trading partner's in the list will be matched to the Data Definition.

Both Trading Partner sections and EDI code sections contain an **Add** button and a **Remove** button. Trading partner sections also contain a **New** button and an **Edit** button.

Add trading partner

If you click the **Add** button, you will see the dialog below.



This dialog will contain a list of all the trading partners you have already defined. If you are adding an originating trading partner, this list will also include the

internal companies that you have defined. Select one or more of them and click **OK** to add them to this EDI Data Definition.

Remove trading partner

To remove trading partners from the data definition, select one or more trading partners from the list and click the **Remove** button.

Create a new trading partner

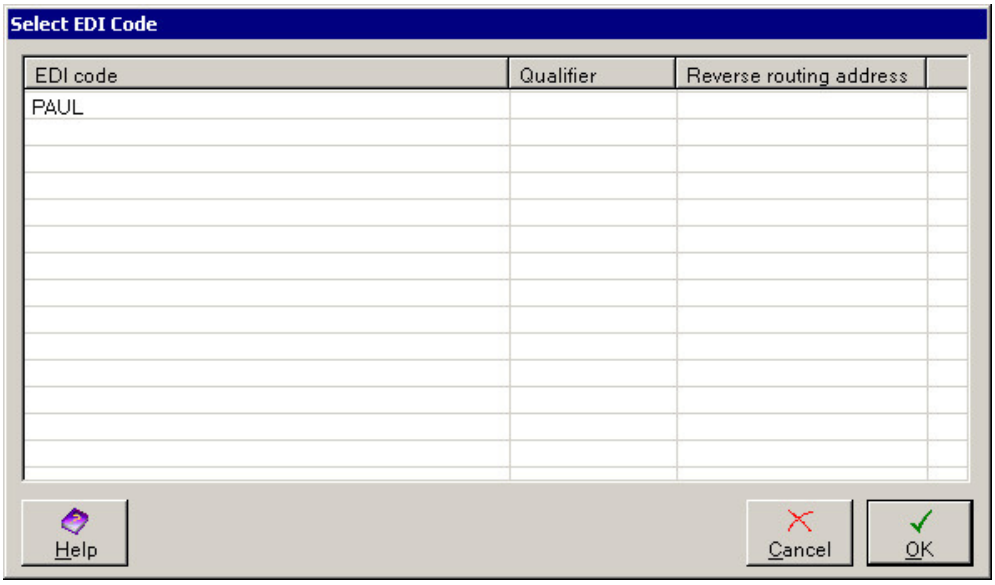
To create a new trading partner to be added automatically to this data definition, click the **New** button. This will bring up the Add New Trading Partner dialog, which requires the same information as the Trading Partner Overview page, described in the section entitled "Trading Partner – Overview".

Edit a trading partner

To edit a trading partner that already belongs to this data definition, click the **Edit** button. This will bring up the Edit Trading Partner dialog, which requires the same information as the Trading Partner Overview page, described in the section entitled "Trading Partner – Overview".

Add EDI code

If you click the **Add** button, you will see the dialog below.



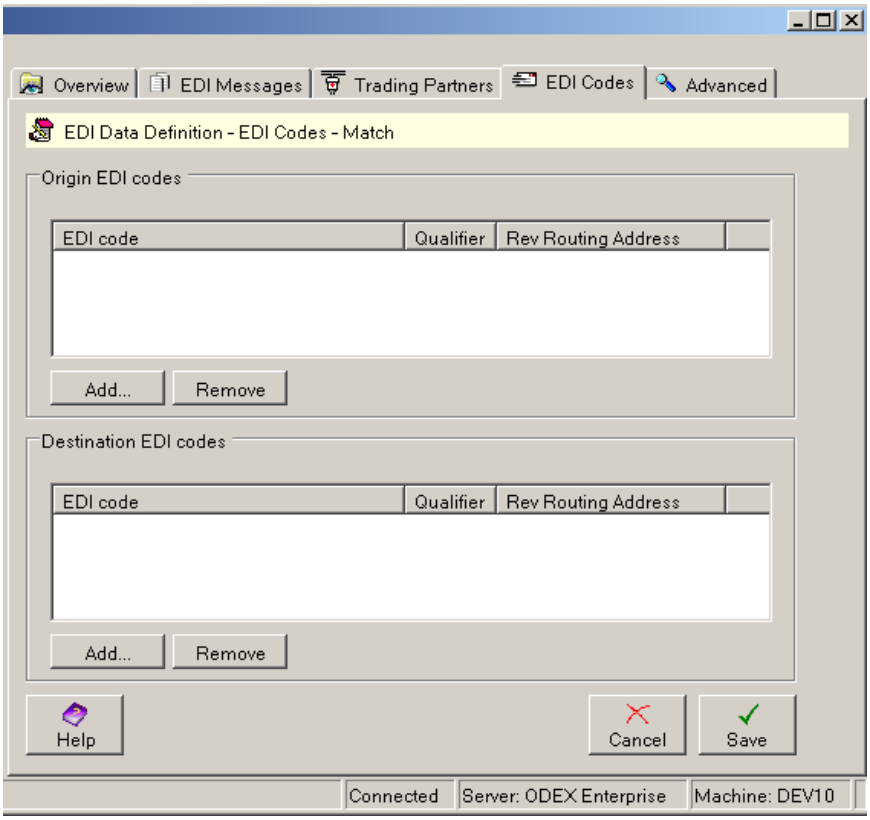
This dialog will contain a list of all the EDI codes you have already defined. Select one or more of them and click **OK** to add them to this EDI Data Definition.

Remove EDI code

To remove EDI codes from the data definition, select one or more EDI codes from the list and click the **Remove** button.

EDI Codes

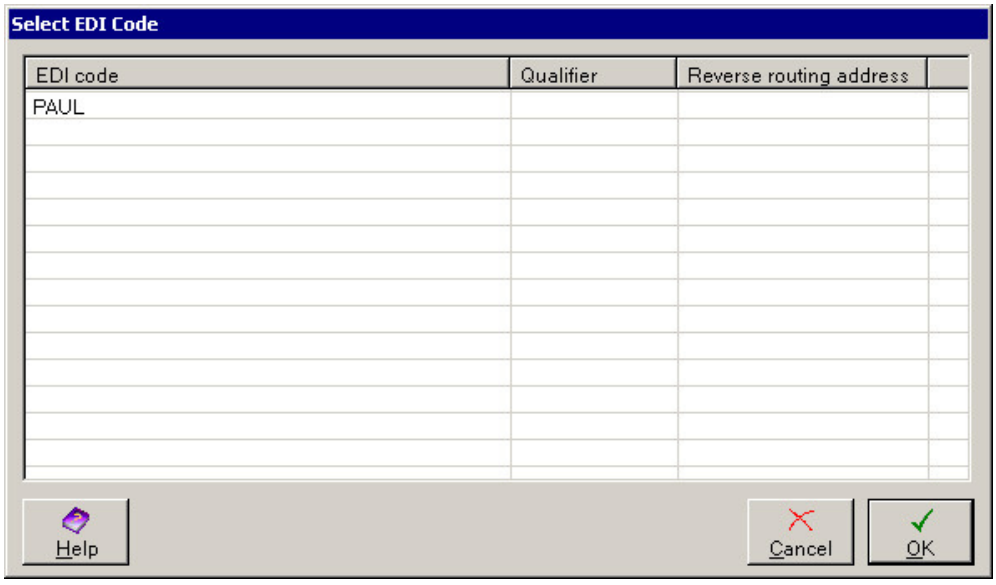
This page is only available if you are configuring a Data Definition to match to specific EDI codes. It is divided into two sections – Origin EDI Codes and Destination EDI codes.



Each EDI code section contains two buttons – **Add** and **Remove**.

Add An EDI code

If you click the **Add** button, you will see the dialog below.

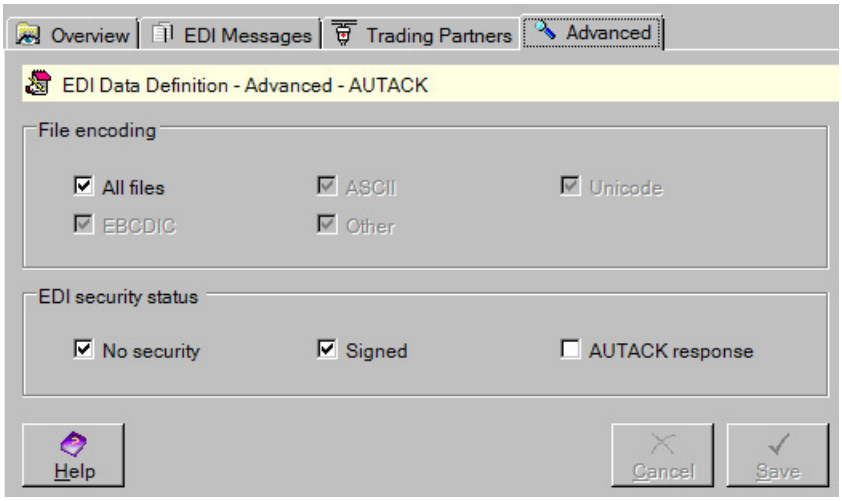


This dialog will contain a list of all the EDI codes you have already defined. Select one or more of them and click **OK** to add them to this EDI Data Definition.

Remove An EDI code

To remove EDI codes from the data definition, select one or more EDI codes from the list and click the **Remove** button.

Advanced



This page contains a list of file encoding types. The default type is 'All files'. If you want to select a different encoding type, first deselect the 'All files' option, then select one or more of the other types.

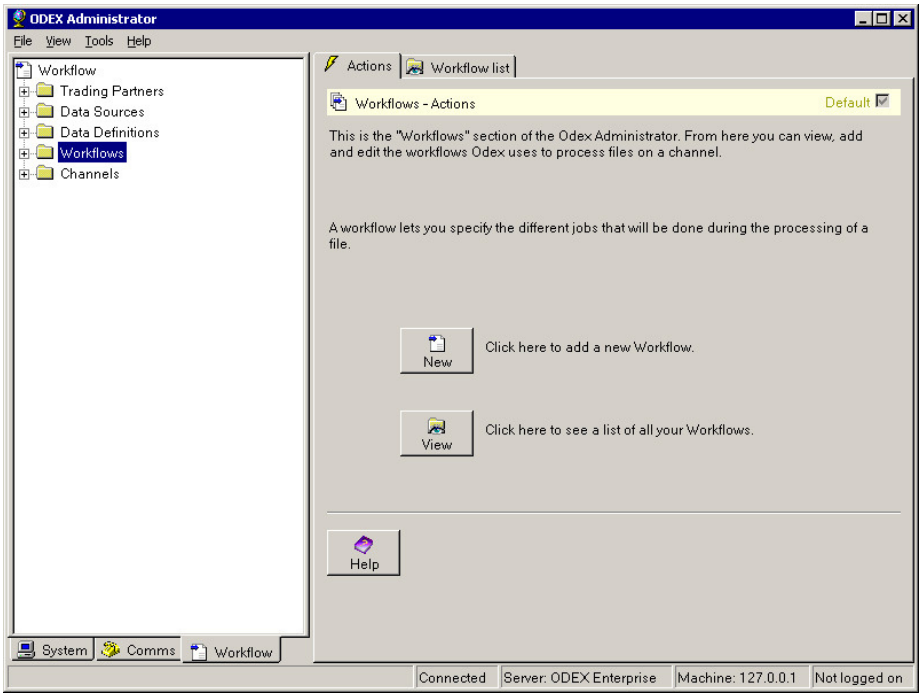
The page also allows you to filter by the security status of the incoming message. The relevant security statuses are:

- No security – no EDIFACT security segments in the received data.
- Signed – the received data contains one or more digital signatures in EDIFACT security segments.
- AUTACK response – the received data is an AUTACK response message.

Workflows

This section of the Administrator allows you to view and edit existing workflows, and to create new workflows. These workflows are what ODEX uses to process files within a channel. Each workflow allows you to specify the different jobs that will be done during the processing of a file.

When you click on the Workflows node in the tree view, you will see the following screen.



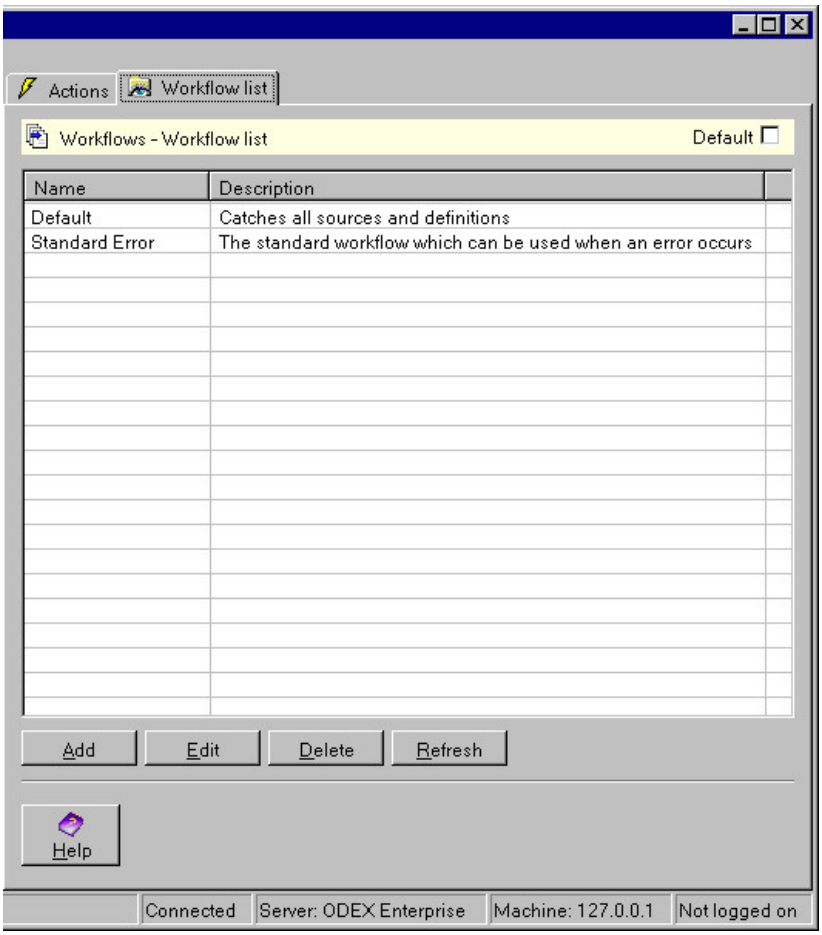
This is the Workflows – Actions screen. From here you can add new workflows or view and edit existing workflows.

To add a new workflow

Click the **New** button to add a new workflow, or open the Workflow list page and click the **Add** button on that page.

Viewing all your workflows

If you wish to see a list of all the workflows currently in the ODEX database, you can either click the **View** button on the Workflows – Actions page or click the Workflow list tab. Both have the same result, as in the example below.



The Information Panel now shows the Workflow list page. This is divided into two columns, showing the Workflow Name and its Description.

The actions that can be taken from this page are as follows:

Add

New workflows may be added to the list by using the **Add** button.

Edit

You may edit the details of existing workflows by using the **Edit** button. Highlight the entry you want to edit and click this button to bring up the appropriate set of pages.

Delete

If you wish to delete a workflow from the list, highlight the line that you wish to delete, then click on the **Delete** button. ODEX will bring up a dialog box, asking if you are sure you want to delete the selected items. This is to safeguard against accidentally deleting the wrong item. Click **Yes** to delete or **No** to keep the item in the list.

Refresh

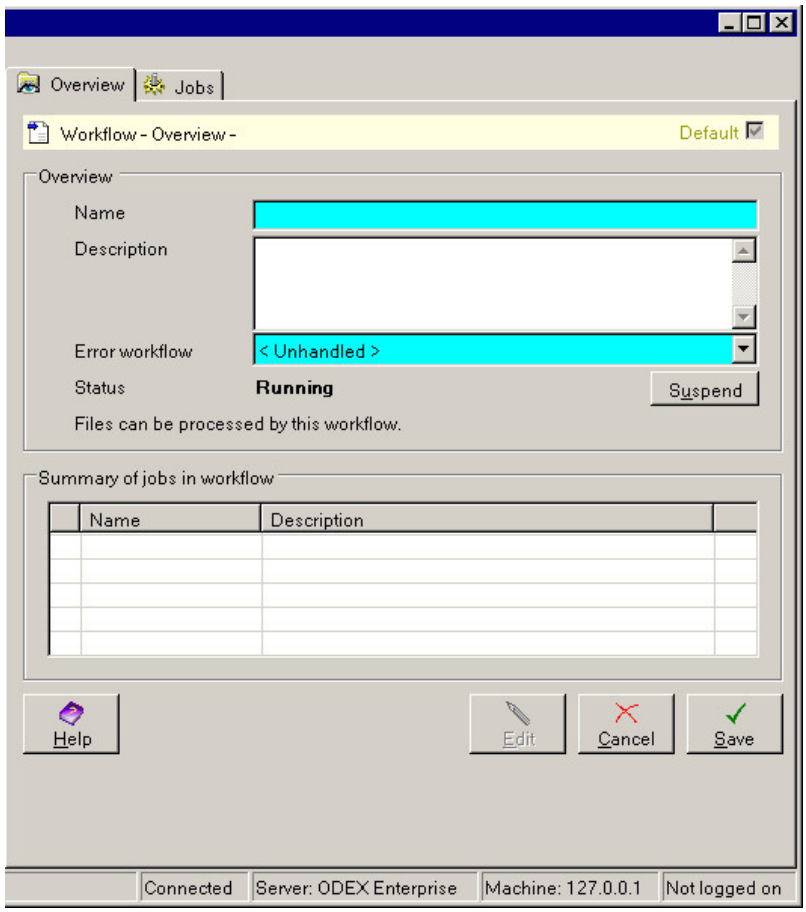
Click this button to refresh the details on this page, for example if you have just made some changes which have not yet appeared on this page.

Help

If you need more information about the fields and buttons on this page, click on the **Help** button.

Workflow – Overview

The Workflow – Overview page is shown below. This page is divided into two sections: Overview and Summary of jobs in workflow.



Edit button

The **Edit** button on the Overview and Jobs pages (alongside the **Cancel** and **Save** buttons) will only be enabled for Workflows that have previously been saved.

If the **Edit** button is enabled, all other fields and buttons on these two pages (apart from the **Suspend** button) are disabled. Once you click the **Edit** button you can edit any of the fields and use any of the buttons on these two pages.

As you will appreciate, it would be dangerous to edit workflows that might be in the middle of processing your files. The **Edit** button provides a safe way of editing workflows without causing any disruption to current processing.

As soon as you click the **Edit** button, ODEX blocks access to the workflow for any further files. It will finish processing any files that are already being handled by this workflow, and will not allow you to save any changes that you have made until all these files have been processed. If you do attempt to save the changes before this, you will see a message telling you how many files remain to be processed before you can save your changes.

Overview – Name

This field requires a name for the workflow. You may give it any name you choose, but it should be unique within the workflow section.

Overview – Description

This field allows you to provide a description of the workflow. This may be useful if you want to give more information than can be provided in the Name alone.

Overview – Error workflow

This field contains a list of all the error workflows currently defined in your ODEX system. You should choose whichever is most appropriate for this workflow. If you have not yet defined any error workflows yourself, the default option of <Unhandled> will be selected for you.

<Unhandled> means that the file will be marked as having an unhandled error (i.e. an error for which no specific action has been defined).

Overview – Status

Alongside this caption is the current status of the workflow. Normally it will be "Running". If you have suspended the workflow, using the **Suspend** button, it will be "Suspended".

Below this caption is a description of the workflow status.

Overview – Suspend/Resume

This toggle button allows you to suspend or resume the workflow. The effect of this button is immediate and does not require you to click the **Save** button to become effective.

Summary of jobs in workflow

This section shows a list of all the jobs currently defined in this workflow. The Name and Description are provided by ODEX.

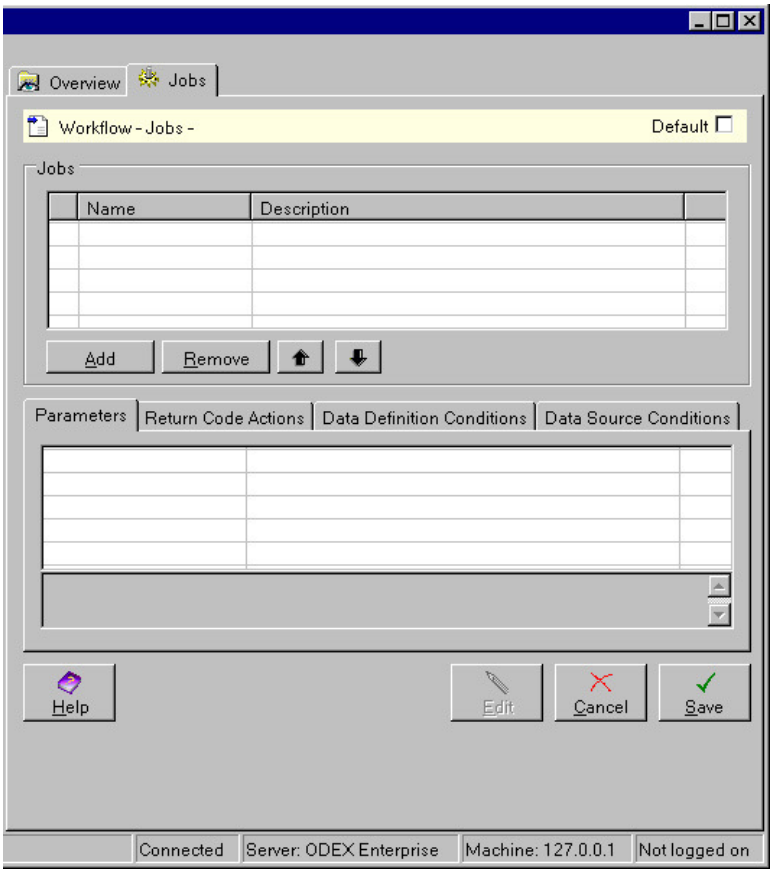
To add jobs to or remove jobs from the workflow, use the Jobs page tab.

Workflow – Jobs

The Workflow – Jobs page is shown below. This page allows you to specify the actions to be performed on all files that are processed by this workflow. The current list of available jobs comprises:

- Acknowledge – Schedules an acknowledgement (EERP) for transmission
- Analyse – Performs analysis of files to determine content
- Call Network – Calls a trading partner or clearing centre network
- Construct – Constructs an EDI file from an in-house file
- Convert File Encoding – Converts the encoding of a file between code pages and allows for conversion from one file format to another.
- Copy – Copies or appends a workflow file
- Copy (with Xml) – Copies a workflow file along with a Data Interchange standard XML file (this job can be used for exporting files to restricted versions of DARWIN3)
- E-mail – Sends an e-mail to a specified address. Please note that you must provide details of your e-mail server and default sender address before you can successfully use this job. For details, please refer to the section entitled "E-mail page".
- Extract Data – Extracts data from a file given a start and end byte position.
- Insert Data – Inserts data into a file from another file, at a given byte position
- Map – Maps a file from one format to another using the Xe mapping engine
- Print Report– Sends a report file generated by the Xe mapper to a printer.

- Process AUTACK - Processes received AUTACK messages (responses and detached signatures).
- Process Functional Acknowledgement – Processes received EDI functional acknowledgements and updates waiting workflow files
- Reformat – Reformat an EDI file
- Run Application – Runs a specified external application
- SAP (Associate) – Associates the file with the SAP monitor. This causes status records to be exported to SAP as the file is constructed and transmitted.
- SAP (Export) – Queues an IDoc file to be exported to SAP
- Schedule – Schedules a file for transmission
- Sign EDI - Applies digital signatures to EDI interchanges and messages.
- Split – Splits files into separate interchanges
- Translate – Translates an EDI message into an in-house file format
- Update ENGDAT Folder – Processes inbound ENGDAT files and adds the files to ENGDAT folders.
- Verify Signed EDI - Verifies digital signatures on EDI interchanges and messages
- Wait for Acknowledgement – Pauses execution until the file has been acknowledged
- Wait for Transmission – Waits for a communications event on a file
- Windows Application Log – Writes a message to the Windows application log
- Write To File – Writes details of an event to a file
- Write to MQ Message Queue – Writes data to a IBM WebSphere message queue.

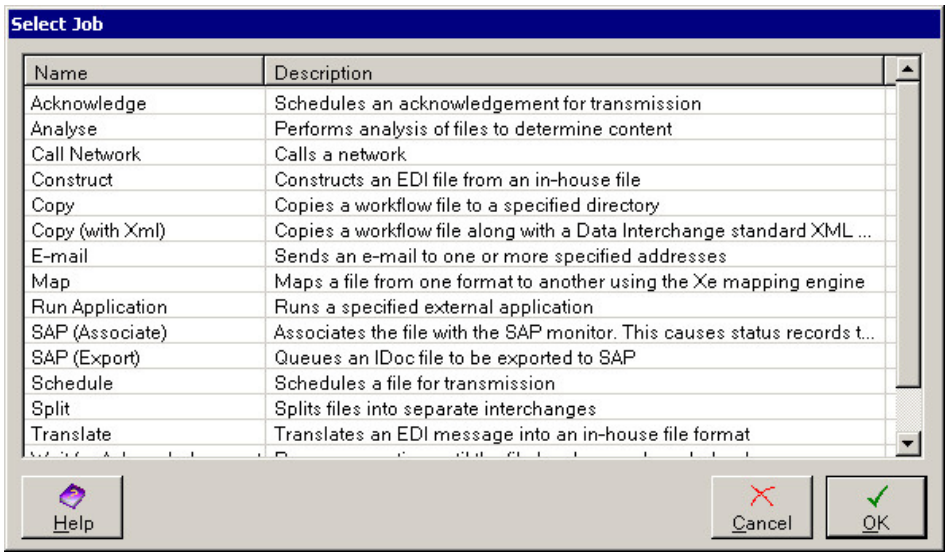


This page is divided into two sections: Jobs and Parameters/Return Code Actions/Conditions.

Jobs – Add

To add one or more jobs to this workflow, click the **Add** button. This will bring up the Select Job dialog, shown below.

For full details of each job and its parameters, please refer to the section entitled "Workflow – Jobs".



Highlight the job(s) you want to add and click the **OK** button. (To select more than one job at once, hold down the **Ctrl** key while selecting each job with your left mouse button).

You will then be returned to the Workflow – Jobs page, where you will now see that the Jobs section has been populated with the jobs you just selected.

The jobs will initially be listed in alphabetical order, and will be performed in this order unless you change it. To alter the order in which the jobs are performed, simply highlight one of the jobs and press the up or down arrow button to move that job up or down in the list.

Jobs – Remove

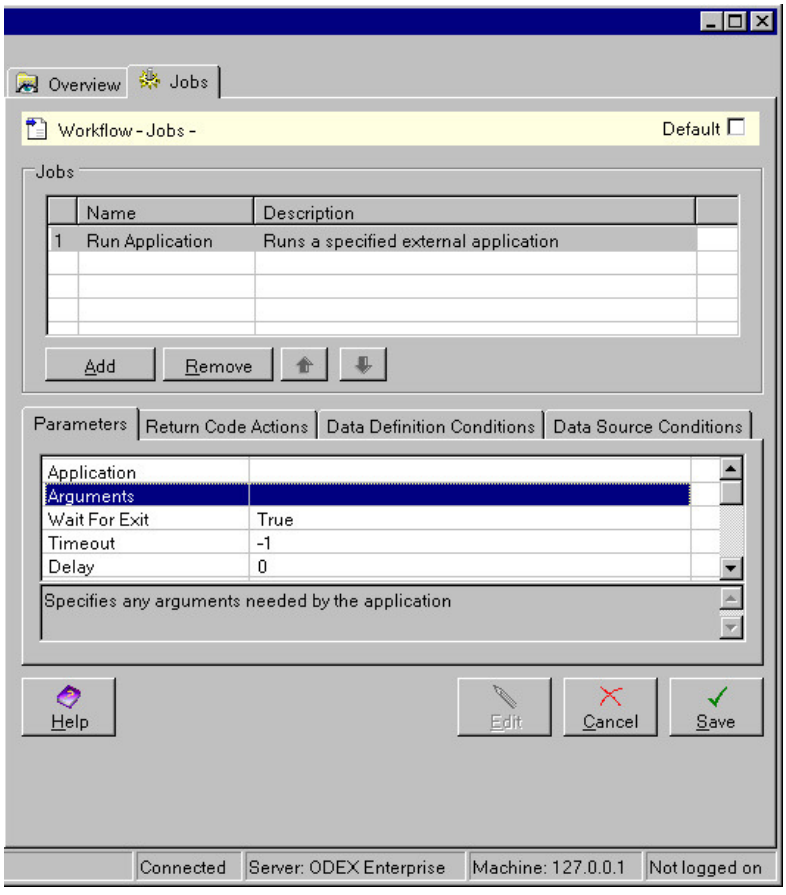
If you want to remove any jobs from the list, highlight the job to be deleted and click the **Remove** button. You will be prompted to confirm the deletion.

Jobs – Parameters

Once you have added one or more jobs to the workflow, you can highlight any individual job in the top section in order to see, displayed in the lower section of the page, the parameters, return code actions and conditions appropriate to the selected job.

Parameters and return code actions are initially all set to default values. You should change them if necessary.

Conditions will initially be blank and must be set up by you if required.



Highlight each parameter to see a description of that parameter's purpose in the grey box below it. An example is shown above, where the Arguments parameter of the Run Application job is highlighted.

Some parameters will be shown with a default value, such as ‘True’. Others will have a blank value, which, in many cases, may be left blank. When you try to save the Workflow details, ODEX will inform you if there are any parameters you need to provide.

For full details of each job and its parameters, please refer to the section entitled “Workflow – Jobs”.

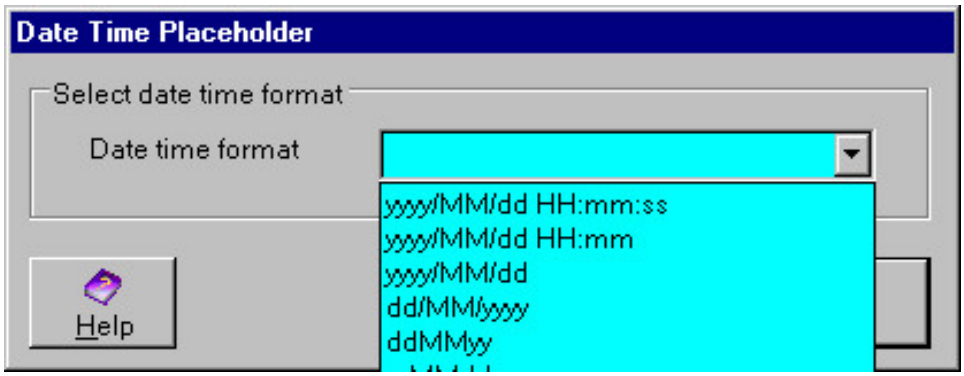
To edit the value of any parameter, double click on the parameter you want to edit. For a parameter whose value is ‘True’ or ‘False’, double-clicking will toggle between the two values. For all other parameters, double-clicking will bring up the appropriate Edit Parameter dialog.

For further details of how to edit a parameter in order to provide or change its value, please refer to the section entitled "Editing Parameters".

Jobs – Placeholders

Some Job parameters, such as E-mail Body and any parameter that creates a new file, allow you to use placeholders. A full list of placeholders and their meaning is included in the section entitled “Placeholders”.

If you select a date/time placeholder associated with a comms file or workflow file, you will be required to choose the format in which you want the date and time to be displayed, using the dialog below.

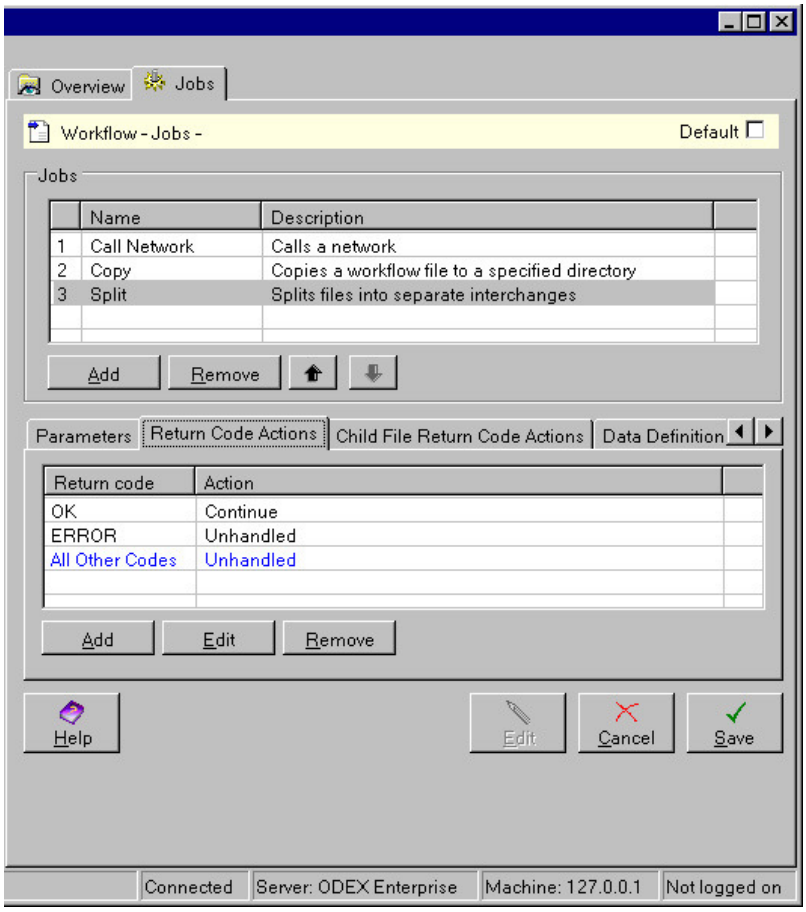


You can either select one of the formats from the dropdown list or type in a format of your own choosing.

ODEX will interpret MM as the month and mm as minutes. You must include separators if you want them. For full details of date/time placeholders, please refer to the section entitled “Date/Time Placeholders”.

Jobs – Return Code Actions

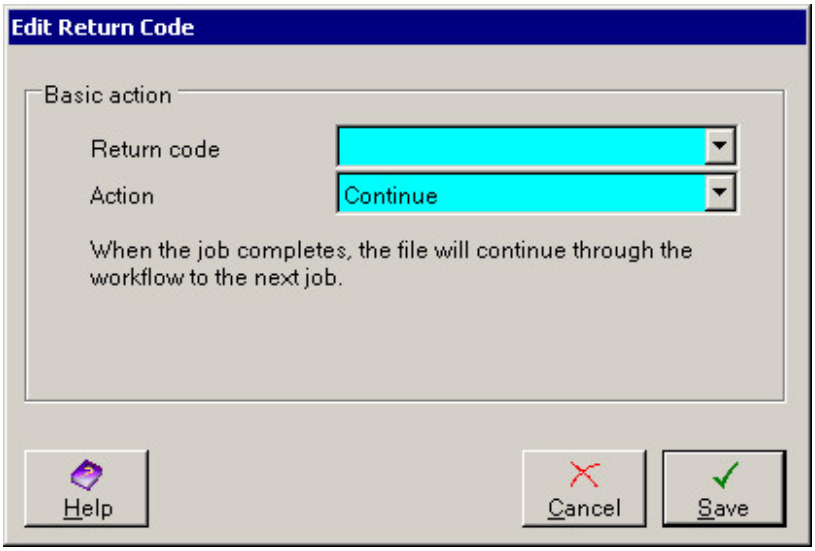
Click on the Return Code Actions page tab to see the Return Code Actions for a selected Job.



To start with, the Return Code Actions for all Jobs will be set to their default values:

- OK = Continue
- ERROR = Unhandled
- All other codes = Unhandled (this entry will be coloured blue, to indicate that it must always be present, but you may edit it to change the action).

For most Jobs, there are no more return codes available to be added. However, for some Jobs you will be able to add further return codes. Clicking the **Add** button while one of these jobs is selected will bring up the following dialog.



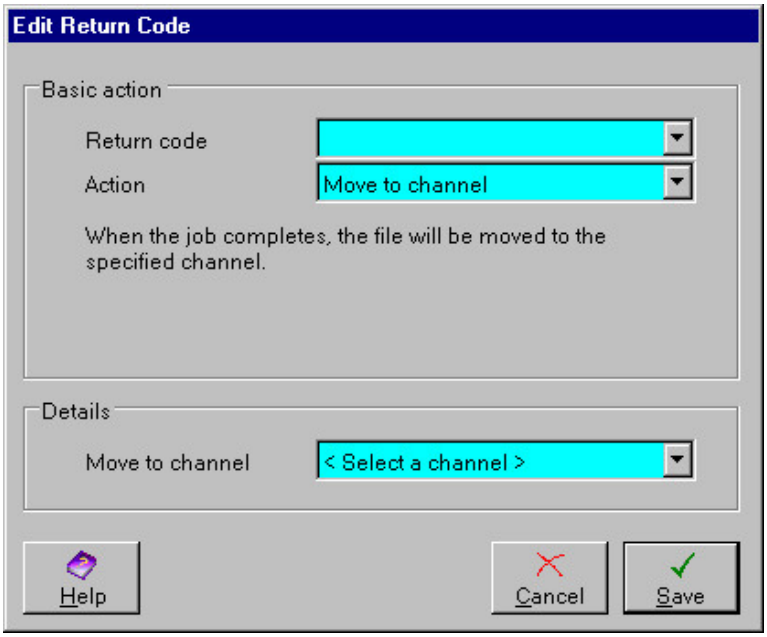
Use the dropdown arrows to select an appropriate Return Code and an appropriate Action. It may also be possible in some cases to type in a Return Code that does not appear in the list.

As you select an Action, a description of that Action will appear below the field.

Depending on the Action you choose, the dialog may change, as illustrated in the examples below.

Move to channel

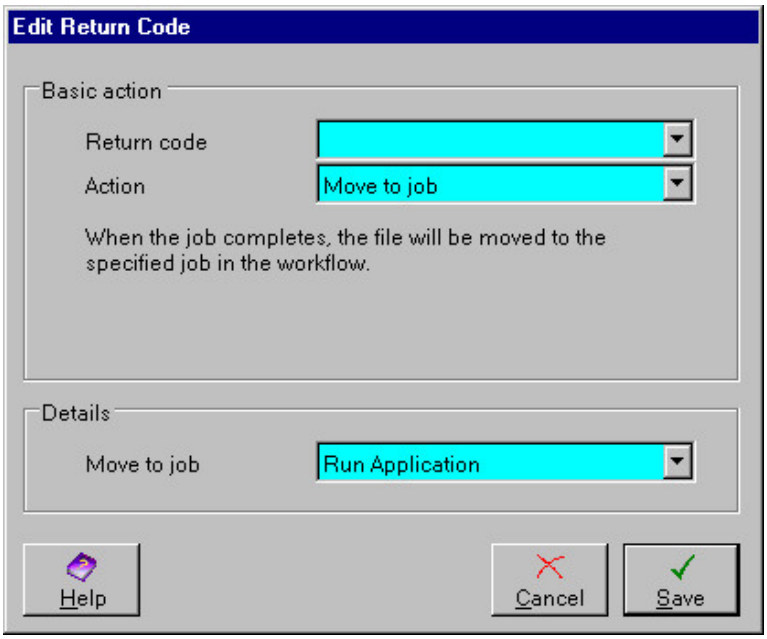
If the selected Action is 'Move to channel', the dialog will change to resemble the one shown below.



In the Details section at the bottom of the dialog you must select the channel for the file to be moved to if the return code matches the one selected at the top of the dialog.

Move to job

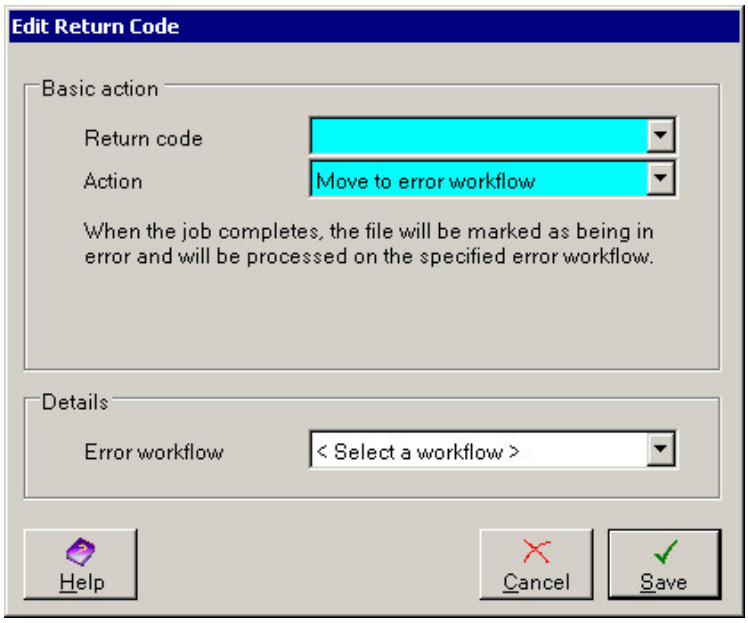
If the selected Action is 'Move to job', the dialog will change to resemble the one shown below.



In the Details section at the bottom of the dialog you must select the job for the file to be moved to if the return code matches the one selected at the top of the dialog.

Move to error workflow

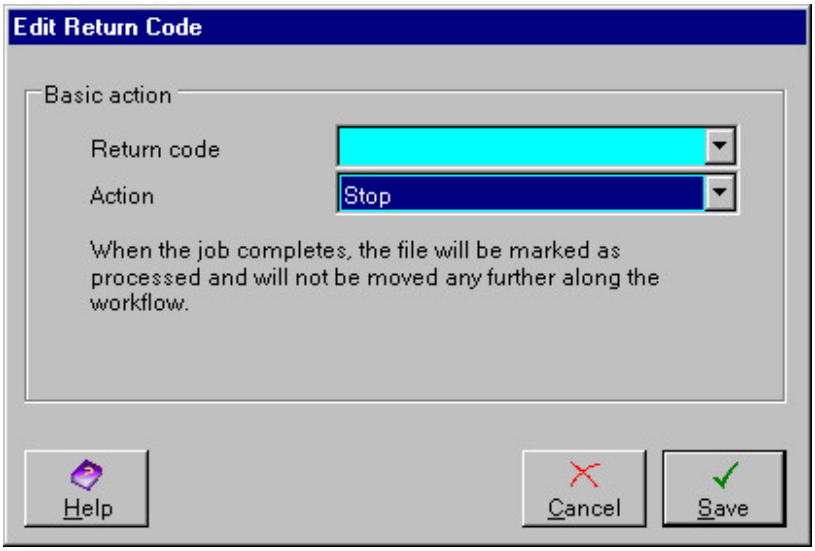
If the selected Action is 'Move to error workflow', you will see the dialog shown below.



In the Details section at the bottom of the dialog you must select the Error workflow for the file to be moved to if the return code matches the one selected at the top of the dialog.

Stop

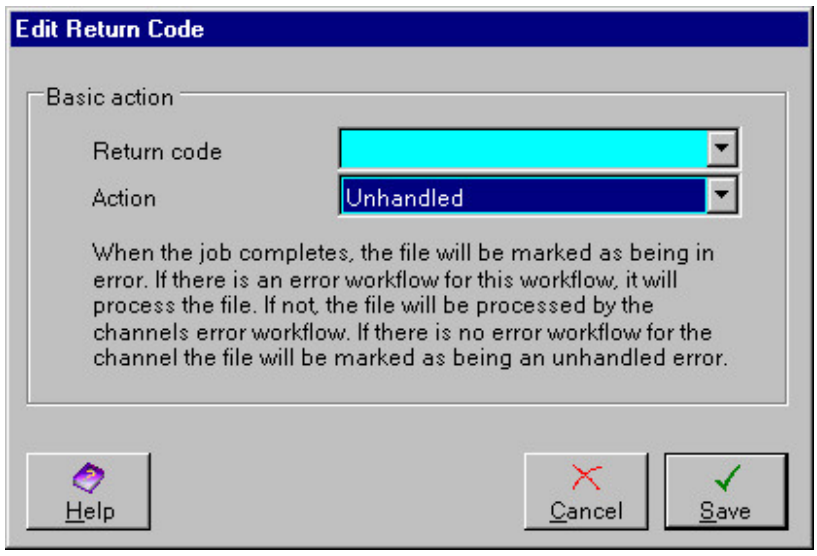
If the selected Action is ‘Stop’, you will see the dialog shown below.



There are no further selections to make on this dialog. If the return code matches the one selected at the top of the dialog, the file will not be processed any further.

Unhandled

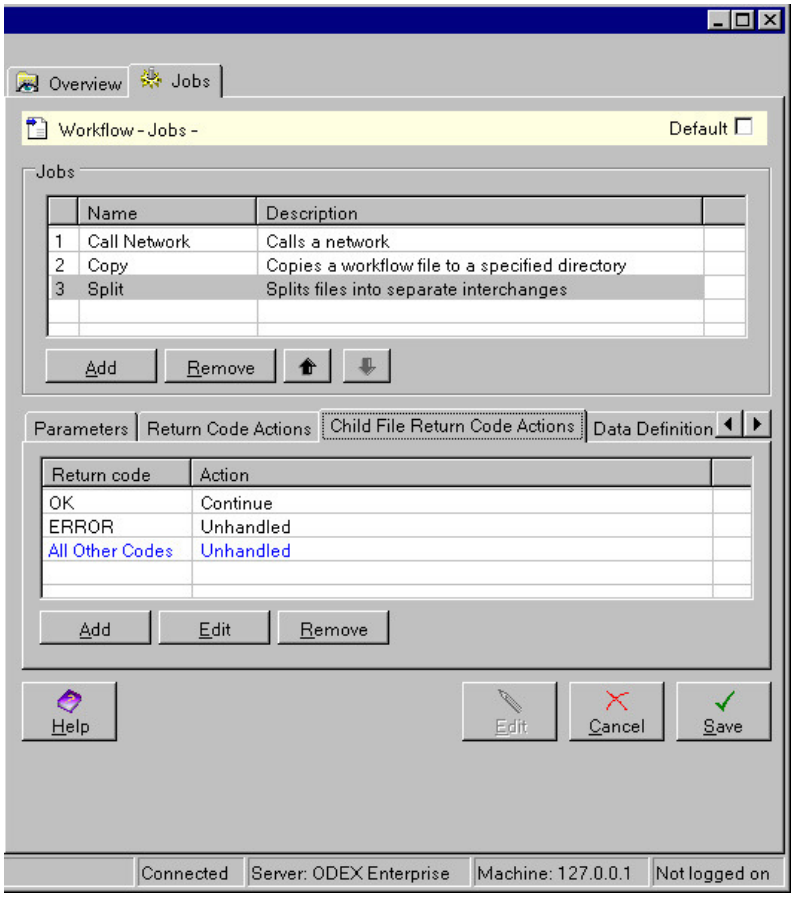
If the selected Action is ‘Unhandled’, you will see the dialog shown below.



There are no further selections to make on this dialog. If the return code matches the one selected at the top of the dialog, the file will be marked as being in error. Any further processing will be as described on this dialog.

Jobs – Child File Return Code Actions

If you have included Split as a job in this Workflow, you will see an extra page tab at the bottom of the Jobs page when you highlight the Split job. This is the Child File Return Code Actions page tab, shown below.



You can set the child file return code actions to be different from those of the parent file (also called a source file), whose return codes are dealt with on the Return Code Actions page tab. There is a wider range of return code actions for a child file than for a parent file.

If you remove a return code action for the Split job, this will also remove the corresponding child file return code action.

Likewise, if you remove a child file return code action for the Split job, this will also remove the corresponding source file return code action.

Jobs – Data Definition Conditions

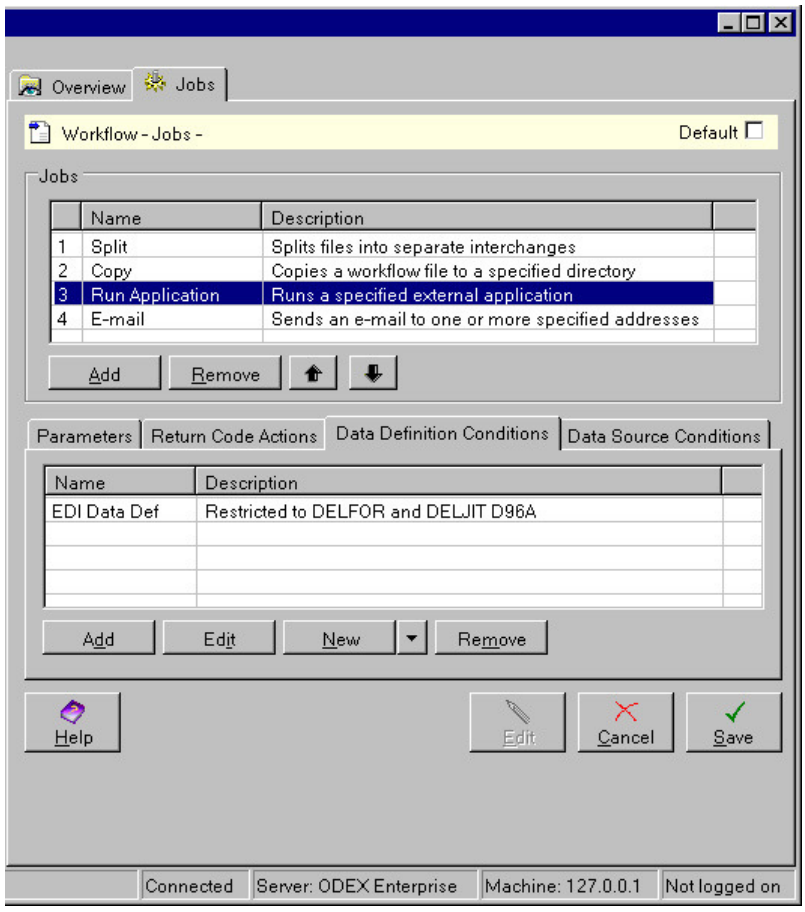
The Data Definition Conditions page tab allows you to set conditions against one or more of the jobs in a workflow, so that they will only be performed if the condition is met.

Although you can set data definition conditions for a Channel, setting conditions here means that you can avoid having to create numerous channels, where the channels all use the same workflow but for different data definitions.

For example, if you had selected jobs to Split, Copy, Translate and Run Application for files handled by this workflow, you could restrict the Translate job to run only against specific EDI messages.

You may specify one or more conditions for any of your selected jobs.

Click on the Data Definition Conditions page tab to view or edit the Data Definition Conditions for a selected Job.



The example above shows that the Run Application job will only be performed if the workflow file matches the selected EDI Data Definition (which in this case specifies only DELFOR and DELJIT D96A message types).

In this example, for any file that is not a DELFOR or DELJIT D96A message, the Run Application job will be skipped. ODEX will then perform the next job in the list (E-mail) on this file, provided there are no conditions set for the E-mail job that prevent it from being executed.

Jobs – Data Source Conditions

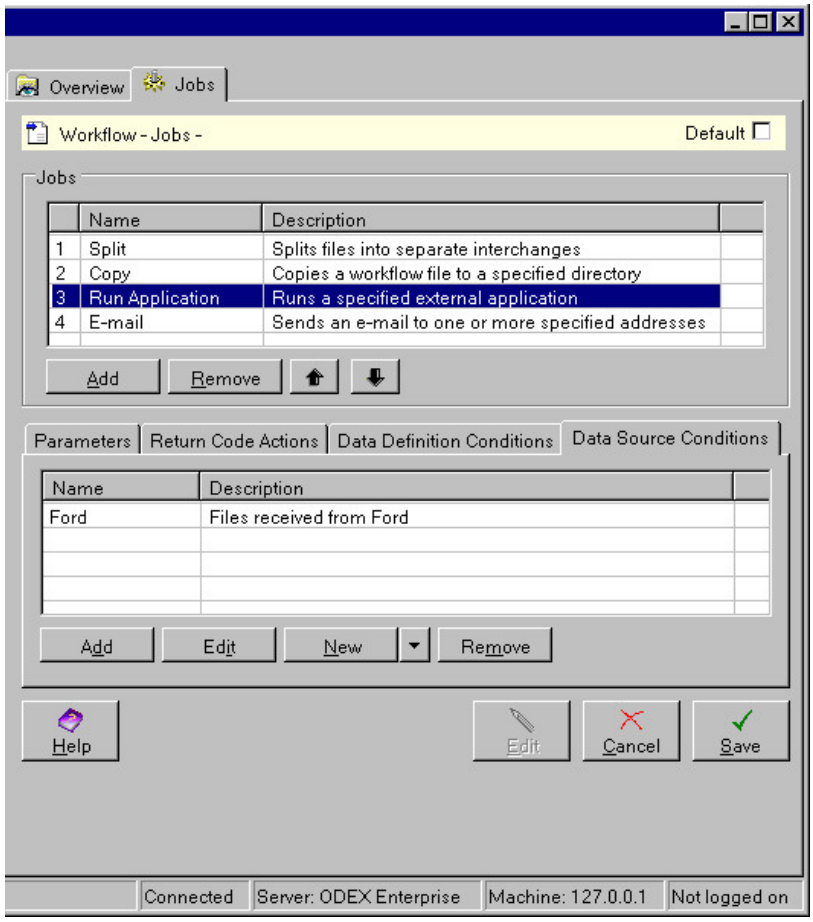
The Data Source Conditions page tab allows you to set conditions against one or more of the jobs in a workflow, so that they will only be performed if the condition is met.

Although you can set data source conditions for a Channel, setting conditions here means that you can avoid having to create numerous channels, where the channels all use the same workflow but for different data sources.

For example, if you had selected jobs to Split, Copy, Translate and Run Application for files handled by this workflow, you could restrict the Run Application job to run only against messages received from a specific communications data source.

You may specify one or more conditions for any of your selected jobs.

Click on the Data Source Conditions page tab to view or edit the Data Source Conditions for a selected Job.



The example above shows that the Run Application job will only be performed if the workflow file matches the selected data source (which in this case specifies only files received from Ford).

In this example, for any file that is not received from Ford, the Run Application job will be skipped. ODEX will then perform the next job in the list (E-mail) on this file, provided there are no conditions set for the E-mail job that prevent it from being executed.

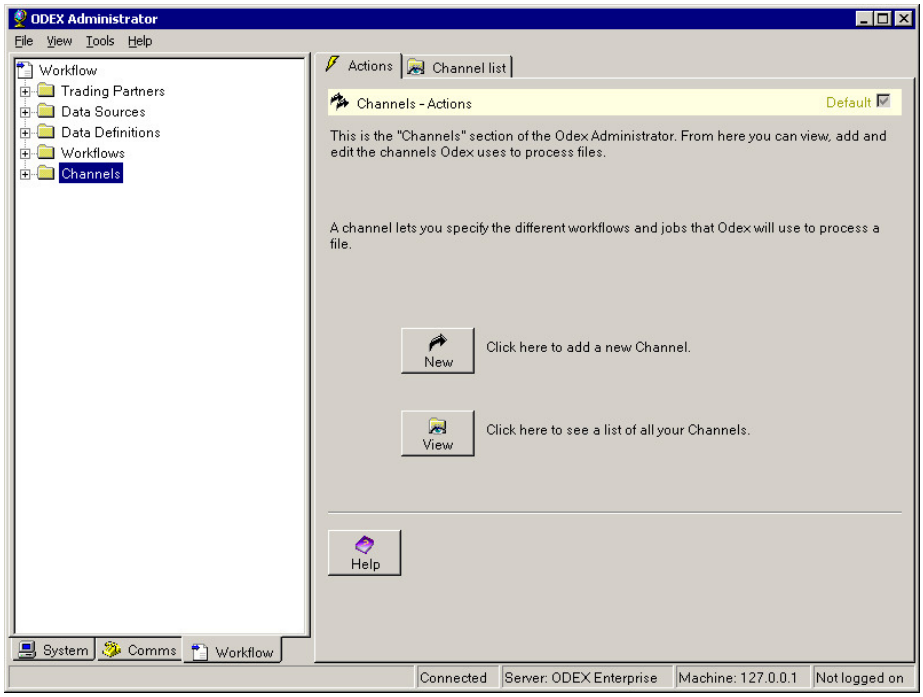
Channels

This section of the Administrator allows you to view and edit existing channels, and to create new channels. These channels are what ODEX uses to process

files. A channel allows you to specify the different workflows and jobs that ODEX will use to process a file.

You can create new data sources, new data definitions, new workflows and new error workflows from within this section, for use in new or existing channels. This saves you from having to switch between the different tree nodes unnecessarily.

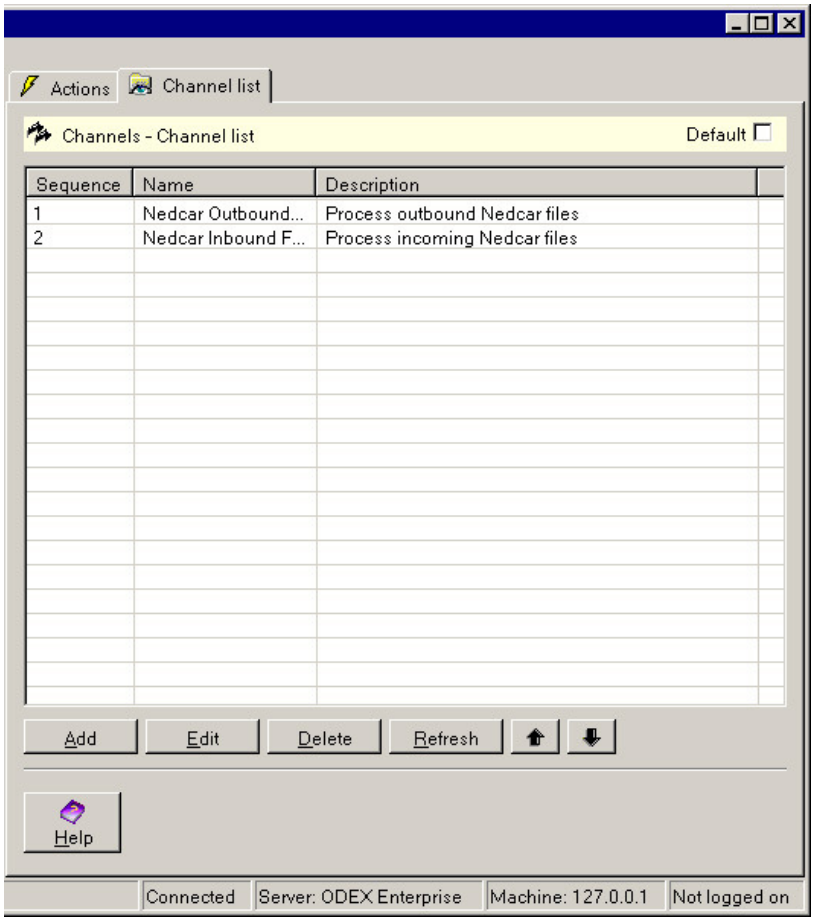
When you click on the Channels node in the tree view, you will see the following screen.



This is the Channels – Actions screen. From here you can add new channels or view and edit existing channels.

Viewing all your Channels

Click on the Channel list page tab to see the Channel list page, shown below. This page displays all the channels that you currently have defined in your ODEX system.



This page has three columns: Sequence, Name and Description.

The Name and Description were typed in by you when you created the channel.

Sequence field

The Sequence value is designated by ODEX when the channels are saved.

The Sequence value is very important, as it determines the order in which ODEX will check each channel to find one that matches the file to be processed.

ODEX will begin with the channel designated as Sequence 1. If the file matches the criteria in this channel, ODEX will not check any further channels but will use this channel to process the file.

If the file does not match the channel designated as Sequence 1, ODEX will then check the channel designated as Sequence 2, and so on.

If the file does not match any of the channels, it will be shown in the Workstation with the status "Processed" (since the Workflow Manager has done all the processing it can) and the error status “Unhandled Error”.

ODEX will allocate the next sequential number to each new channel you create. Therefore you should look very carefully at your list of channels to determine the order in which you want ODEX to check them to find one that matches the file to be processed. You should allocate the lowest sequence numbers, where 1 is the lowest, to the most restrictive channels. Having determined the order, use the up and down arrows to move the channels into the correct sequence.

To add a new channel

Click the **New** button to add a new channel, or open the Channel list page and click the **Add** button on that page.

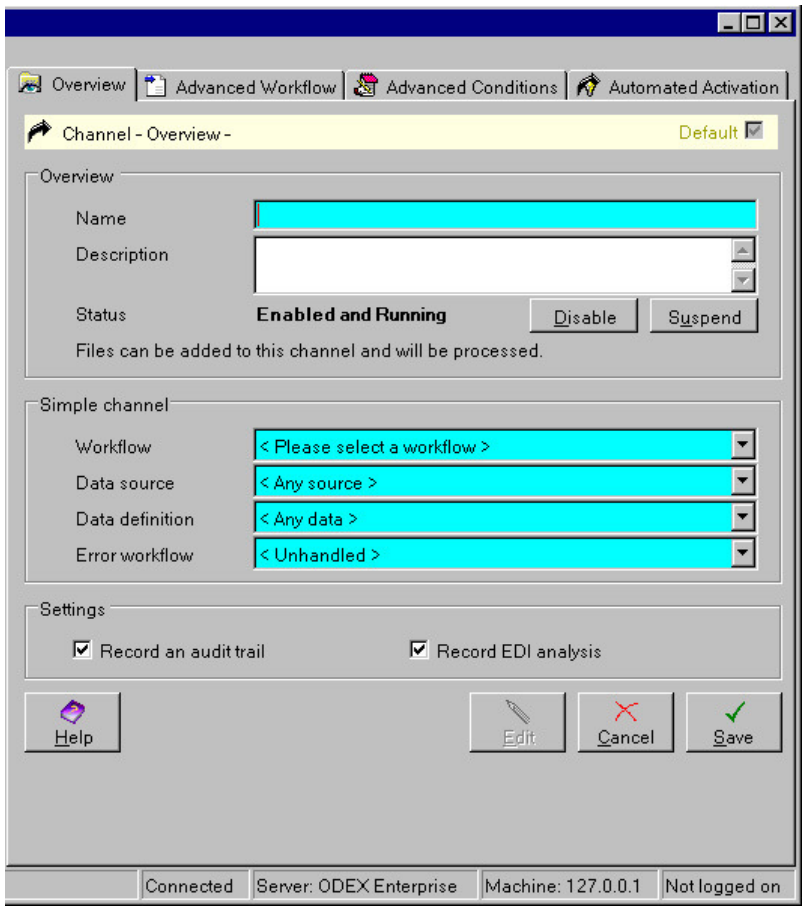
To view or edit an existing channel

Double-click on an existing channel in the tree view, or open the Channel list page, select an entry and click the **Edit** button.

The Channels section comprises four page tabs: Overview, Advanced Workflow, Advanced Conditions and Automated Activation.

Channel – Overview

The Channel – Overview page is shown below.



This page is divided into three sections: Overview, Simple channel and Settings.

If you want to include more than one workflow in this channel, use the Advanced Workflow page instead of the Workflow field.

If you want to include more than one data source in this channel, use the Advanced Conditions page instead of the Data source field.

If you want to include more than one data definition in this channel, use the Advanced Conditions page instead of the Data definition field.

You cannot select more than one error workflow for a channel, so you must use the Error workflow field to specify an error workflow or to leave any errors unhandled (the default).

Edit button

The **Edit** button on the four channel pages (alongside the **Cancel** and **Save** buttons) will only be enabled for Channels that have previously been saved.

If the **Edit** button is enabled, all other fields and buttons on these four pages (apart from the **Disable** and **Suspend** buttons) are disabled. Once you click the **Edit** button you can edit any of the fields and use any of the buttons on these four pages.

As you will appreciate, it would be dangerous to edit channels that might be in the middle of processing your files. The **Edit** button provides a safe way of editing channels without causing any disruption to current processing.

As soon as you click the **Edit** button, ODEX blocks access to the channel for any further files. It will finish processing any files that are already being handled by this channel, and will not allow you to save any changes that you have made until all these files have been processed. If you do attempt to save the changes before this, you will see a message telling you how many files remain to be processed before you can save your changes.

Overview – Name

This field requires a name for the channel.

Overview – Description

This field allows you to provide a description of the channel. This may be useful if you want to give more information than can be provided in the Name alone.

Overview – Status

Alongside this caption is the current status of the channel. Normally this will be "Enabled and Running". Alternatives are "Enabled and Suspended", "Disabled and Running" and "Disabled and Suspended", depending on whether you have clicked the **Disable** and **Suspend** buttons or not.

Below this caption is a description of the channel status. The four possibilities are:

- Enabled and Running – Files can be added to this channel and will be processed
- Enabled and Suspended – Files can be added to this channel but processing has been suspended
- Disabled and Running – Files cannot be added to this channel but existing files will be processed
- Disabled and Suspended – Files cannot be added to this channel and processing has been suspended

Overview – Disable/Enable

This toggle button allows you to disable or enable the channel. The effect of this button is immediate and does not require you to click the **Save** button to become effective.

If you disable the channel, files will not be added to it but existing files will be processed.

Overview – Suspend/Resume

This toggle button allows you to suspend or resume the channel. The effect of this button is immediate and does not require you to click the **Save** button to become effective.

If you suspend a channel, files may still be added to it, but processing of files within the channel will be suspended.

Simple channel – Workflow

Use this field to specify the workflow to include in this channel. If you want to include more than one workflow in this channel, use the Advanced Workflow page instead.

Simple channel – Data source

Use this field to specify the data source to include in this channel. If you want to include more than one data source in this channel, use the Advanced Conditions page instead.

Simple channel – Data Definition

Use this field to specify the data definition to include in this channel. If you want to include more than one data definition in this channel, use the Advanced Conditions page instead.

Simple channel – Error workflow

Use this field to specify the error workflow to be used by this channel.

Settings – Record an audit trail

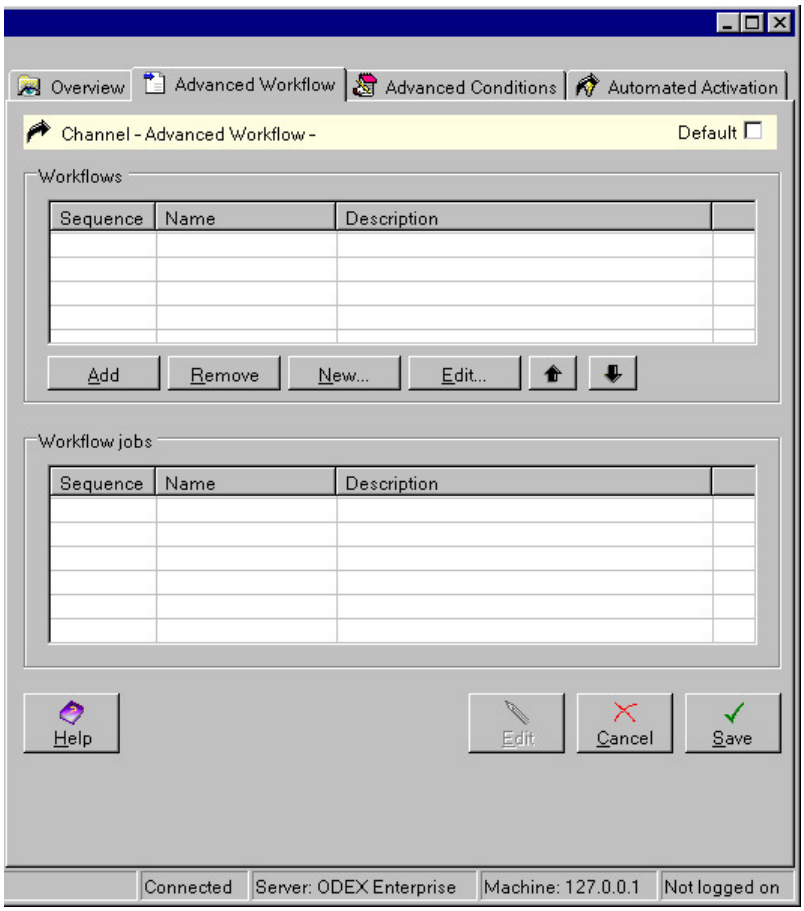
This checkbox will be selected by default, but you may deselect it if you wish. If this box is ticked, you will be able to see, in the Workstation application, the audit trail for the files processed by this channel.

Settings – Record EDI analysis

This checkbox will be selected by default, but you may deselect it if you wish. If this box is ticked, the results of any EDI analysis performed by this channel will be stored in the database. Even if you choose not to store the analysis results, you can still perform an EDI analysis manually from the Workstation application and see the results there.

Channel – Advanced Workflow

The Channel – Advanced Workflow page is shown below.



This page is divided into two sections: Workflows and Workflow jobs.

Use the Workflow section to add or edit existing workflows in this channel, to remove workflows from this channel, or to create a new workflow to be included in this channel.

If you highlight an entry in the Workflows section, its component jobs will be displayed in the Workflow jobs section.

Workflows section

The Sequence field is a feature of this section. Its purpose and the way it works is the same as for the sequence field on the Channel list page, except that it refers to workflows instead of channels.

The Sequence value is designated by ODEX when you add a workflow to the Workflows section.

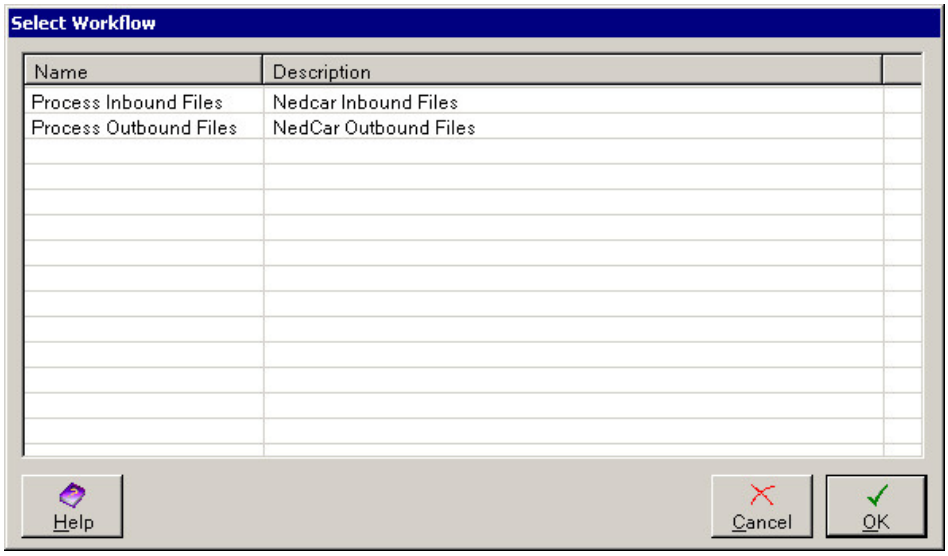
The Sequence value is very important, as it determines the order in which ODEX will perform the workflows.

ODEX will begin with the workflow designated as Sequence 1, will then perform the workflow designated as Sequence 2, and so on.

ODEX will allocate the next sequential number to each new workflow you add to the list within this channel. Therefore you should look very carefully at your list to determine the order in which you want ODEX to perform them. Having determined the order, use the up and down arrows to move the workflows into the correct sequence.

Adding an existing workflow

If you click the **Add** button you will see the Select Workflow dialog, shown below:



Simply highlight one or more workflows that you wish to add and click the **OK** button.

Workflow jobs section

The Sequence field is also a feature of this section. Its purpose and the way it works is the same as for the sequence field in the Workflows section, except that it refers to workflow jobs instead of workflows.

The Sequence value is designated by ODEX when you create the workflow, but you can alter it afterwards.

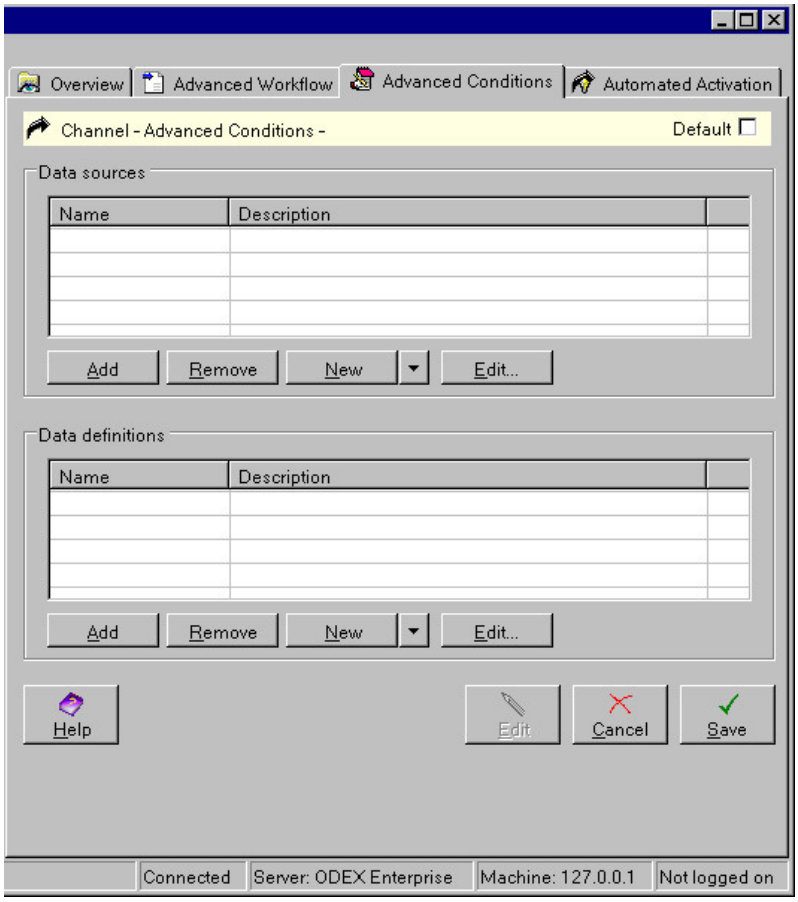
The Sequence value is very important, as it determines the order in which ODEX will perform the workflow jobs.

ODEX will begin with job 1, will then perform job 2, and so on.

Having determined the order in which you want ODEX to perform the jobs, use the up and down arrows to move the workflow jobs into the correct sequence.

Channel – Advanced Conditions

The Channel – Advanced Conditions page is shown below.



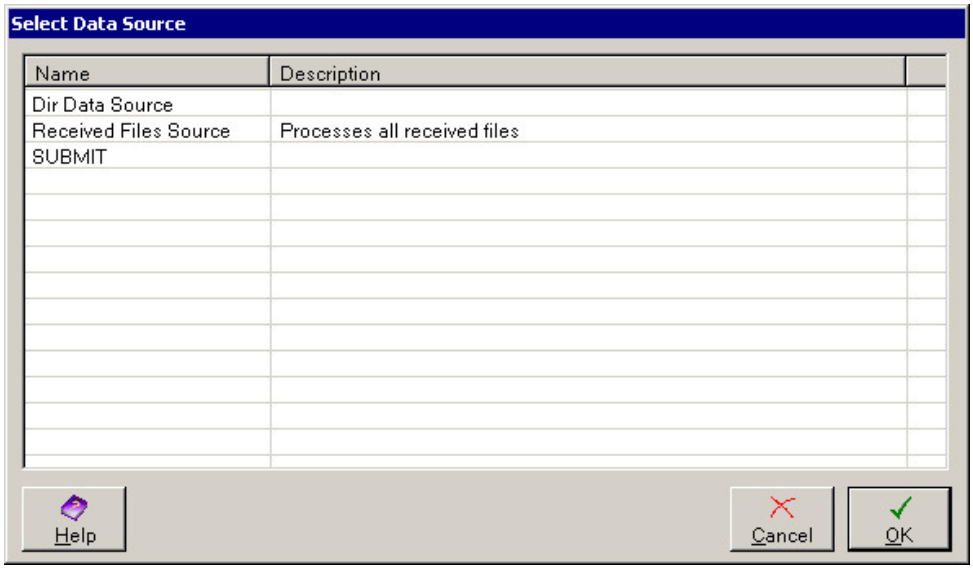
This page is divided into two sections: Data sources and Data definitions.

Use the Data sources section to add or edit existing data sources in this channel, to remove data sources from this channel, or to create one or more new data sources to be included in this channel.

Use the Data definitions section to add or edit existing data definitions in this channel, to remove data definitions from this channel, or to create one or more new data definitions to be included in this channel.

Add Data Source

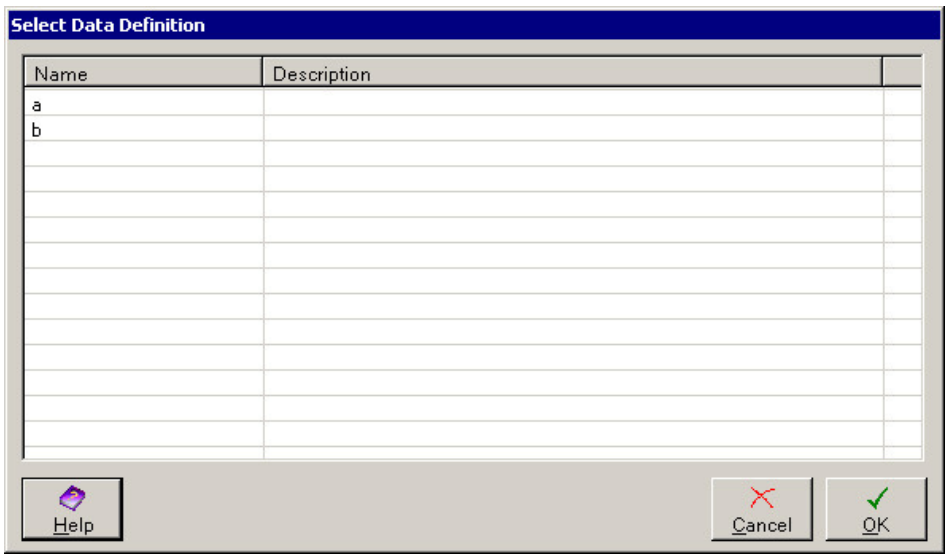
If you click the Data Sources **Add** button, you will see the following dialog.



Highlight one or more of the listed data sources and click **OK** to add them to your data sources for this channel.

Add Data Definition

If you click the Data Definitions **Add** button, you will see the following dialog.



Highlight one or more of the listed data definitions and click **OK** to add them to your data definitions for this channel.

Channel – Automated Activation

Automated activation is for those users who prefer to build up a collection of files for processing, rather than allowing each file to be processed as soon as it arrives in the system.

Activation can be triggered either by the number of files that have been collected, or by a specified event.

You can also deactivate the channel when the number of files falls to a specified number or when another specified event occurs.

You can use the two types of activation independently or in conjunction with each other. You may need to experiment a little to begin with, to see which type of activation and deactivation suits your system best, and which values or events are best used for the triggers.

How automated activation works

By default, once you have created and saved a channel it will be active, whether or not you have configured Automated Activation.

A channel will not become inactive until the deactivation threshold or event triggers deactivation. Therefore, if you set up activation, it is advisable to set up deactivation as well.

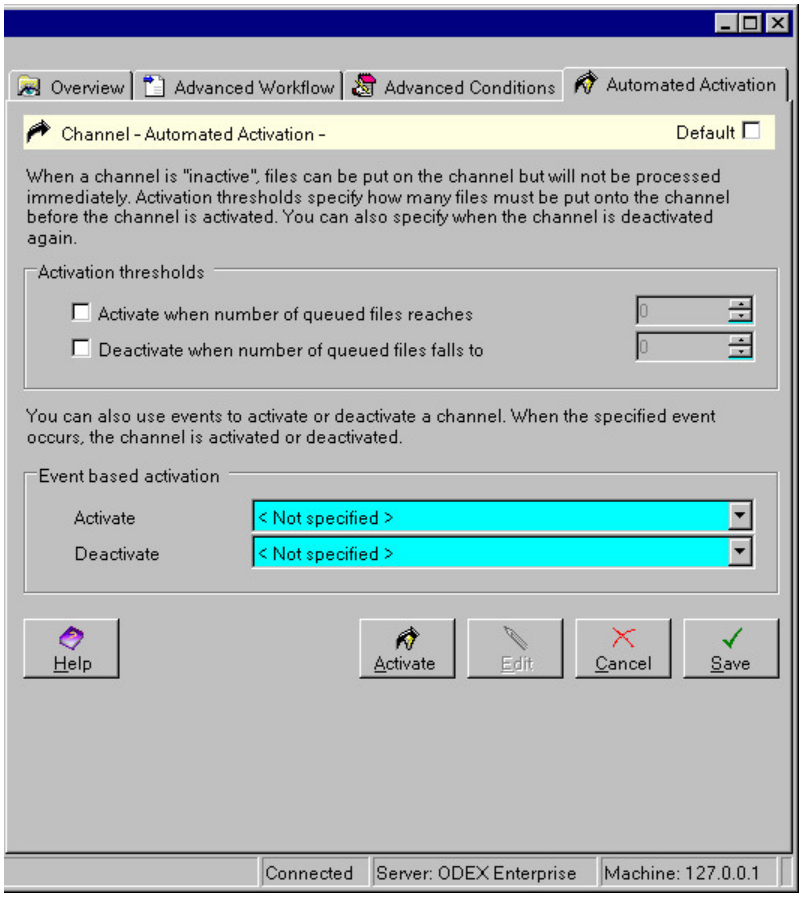
For example, if you set up an activation threshold of 25 files and a deactivation threshold of 0 files, **as soon as a file is placed on the channel, it will be processed, until the deactivation threshold is reached**. As soon as the number of files on the channel reaches zero, deactivation will be triggered. Once deactivation has been triggered, no more files will be processed by this channel until the number of files reaches 25. While active, the channel will continue to process files until the number of files reaches zero.

If you are using event-based activation, **all files placed on this channel will be processed until the deactivation event occurs**. Once deactivation has been triggered, no more files will be processed by this channel until the activation event occurs.

If you set up a threshold AND an event (for activation or deactivation), whichever situation occurs first will cause the activation or deactivation.

How to use the automated activation page

Initially the automated activation feature is not configured and will appear as shown below.



This page (not the channel) will also be disabled, with all fields and tickboxes greyed out, once the Channel to which it belongs has been saved. You will then have to enable the page for editing by clicking on the **Edit** button.

This page is divided into two sections: Activation thresholds and Event based activation.

Activation thresholds

This section allows you to trigger the activation of the channel according to the number of files that have been collected for processing by this channel.

Select the “Activate when number of queued files reaches” tickbox, then either type in a number in the field alongside, or use the up and down arrows, to set the number of queued files to your requirements.

To avoid the situation of too few files entering the system, meaning that activation will never be triggered, you should also set up a suitable event in the section below, which will serve as a failsafe mechanism.

For example, you could set the number of queued files to 50, to trigger activation. In case the number of files never reaches 50, you could select, or set up from new, an event that will activate the channel at a specific time each day.

If you wish, you can also deactivate the channel when the number of queued files falls to a certain number. To do this, Select the “Deactivate when number of queued files falls to” tickbox, then either type in a number in the field alongside, or use the up and down arrows, to set the number of queued files to your requirements. The value you choose does not have to be zero, but this is the most logical value to use.

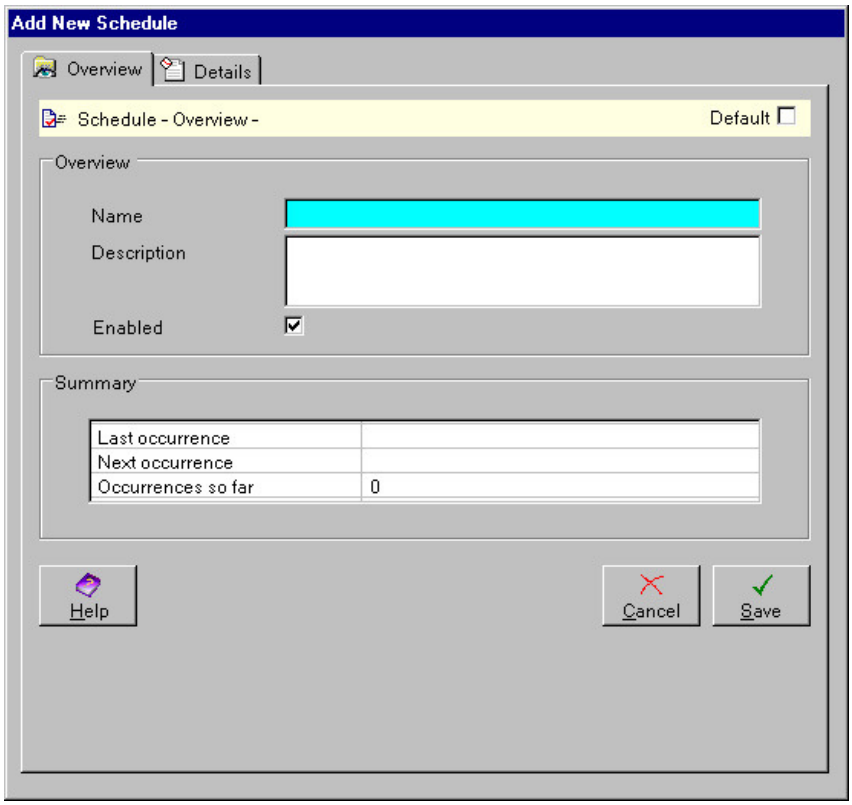
Event based activation

This section allows you to trigger the activation of the channel when a specified event or schedule occurs within ODEX. The channel can also be deactivated by another event or schedule.

Use the first dropdown list (Activate) to select the event or schedule you wish to trigger the activation of the channel. Of course, if the event you choose does not occur, then the channel will not be activated.

If required, use the second dropdown list (Deactivate) to select the event or schedule you wish to trigger the deactivation of the channel. Of course, if the event you choose does not occur, then the channel will not be deactivated.

In both the Activate and Deactivate fields is the option “Add new event schedule”. If you select this option, the following dialog will appear, allowing you to define a new schedule.



For full details of how to edit this dialog, please refer to the section entitled “Schedule – Overview”.

Activate button

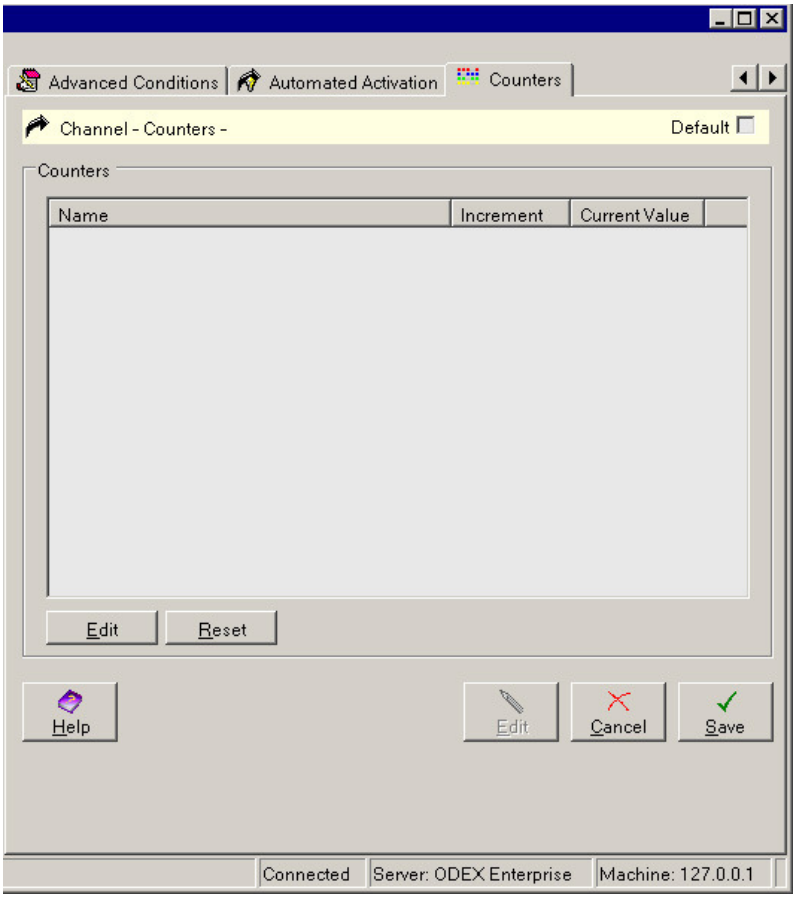
The **Activate** button has been provided for use in exceptional circumstances. For example, if you have set an activation threshold but the number of files has not yet reached the activation trigger level and you decide you want them to be

processed now anyway, you can click the **Activate** button to override the Automated Activation settings. The effect will be to activate the channel, just as if the automated activation trigger had occurred.

Channel – Counters

The Counters page displays all the different counters that are currently in use for Channels. These counters are created automatically by the system and are intended to be used as a source of basic statistical information.

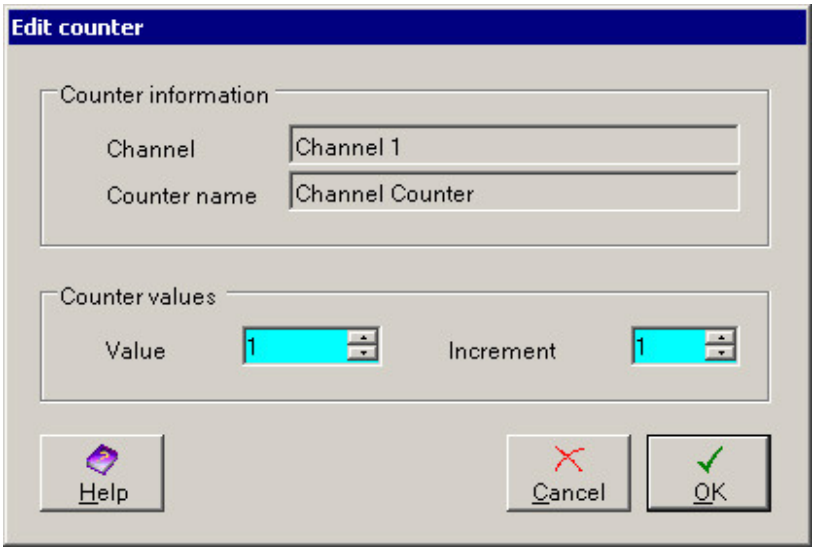
You cannot add any new counters, but you may edit or reset existing counters. However, you should be aware that editing or resetting counters may cause adverse effects. For example, changing the increment value of a counter will mean that counter values will no longer be consecutive. This would result in misleading statistics.



Each existing counter is displayed with its increment value and current value.

Edit

Highlight the counter you wish to edit and click the **Edit** button. This will bring up the following dialog.



Change the current value and/or increment value, being aware that editing counters may cause adverse effects as described above, and click the **OK** button to save your changes.

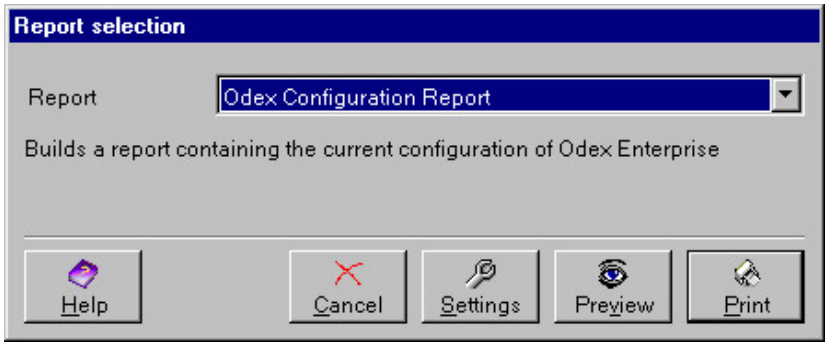
Reset

Highlight the counter you wish to reset and click the **Reset** button, being aware that resetting counters may cause adverse effects as described above. The counter will be reset to zero. Click **OK** to save your changes or **Cancel** to leave this page without saving your changes.

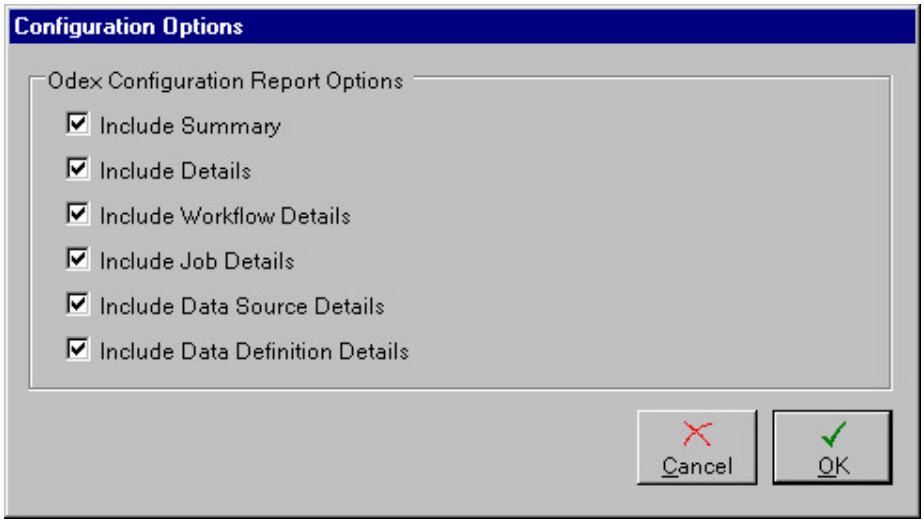
Channel configuration report

From the Tools menu option of the Administrator you can select the “Print Odex Configuration Report” option, which allows you to view, in a user-friendly way, the details of your Workflow Channels configuration.

Select **Tools >> Print Odex Configuration Report** to see the following dialog:

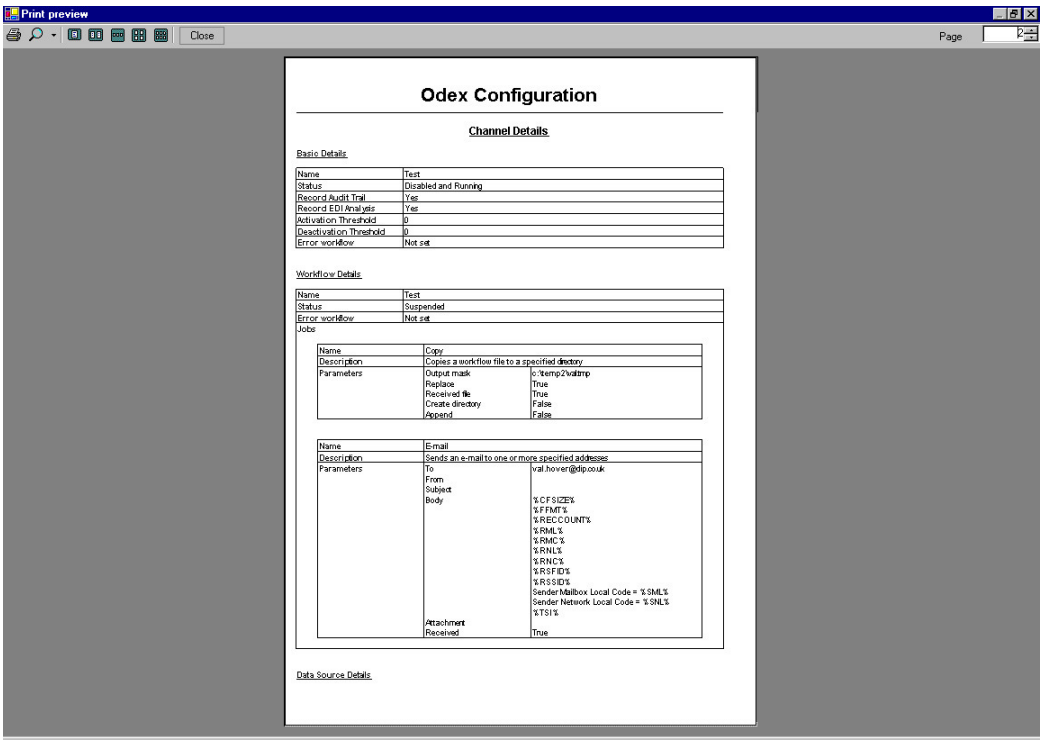


Click the **Settings** button to view or change the settings for the report. The Configuration Options dialog will appear, allowing you to change the settings if you wish.



The Odex Configuration Report can run to many pages, so it is always a good idea to select the Preview option before producing an actual printed copy. This will allow you to see how many pages the report entails and perhaps deselect some of the sections on the Configuration Options dialog.

A page from a sample Odex Configuration Report is shown below.



Routing Table

Through the routing table, ODEX allows you to choose the originator and destination mailboxes for a file, depending on characteristics of the file.

This allows files to be received from one trading partner and forwarded to another trading partner according to characteristics of the file. It is also possible to receive a file in one protocol and forward it using a different protocol.

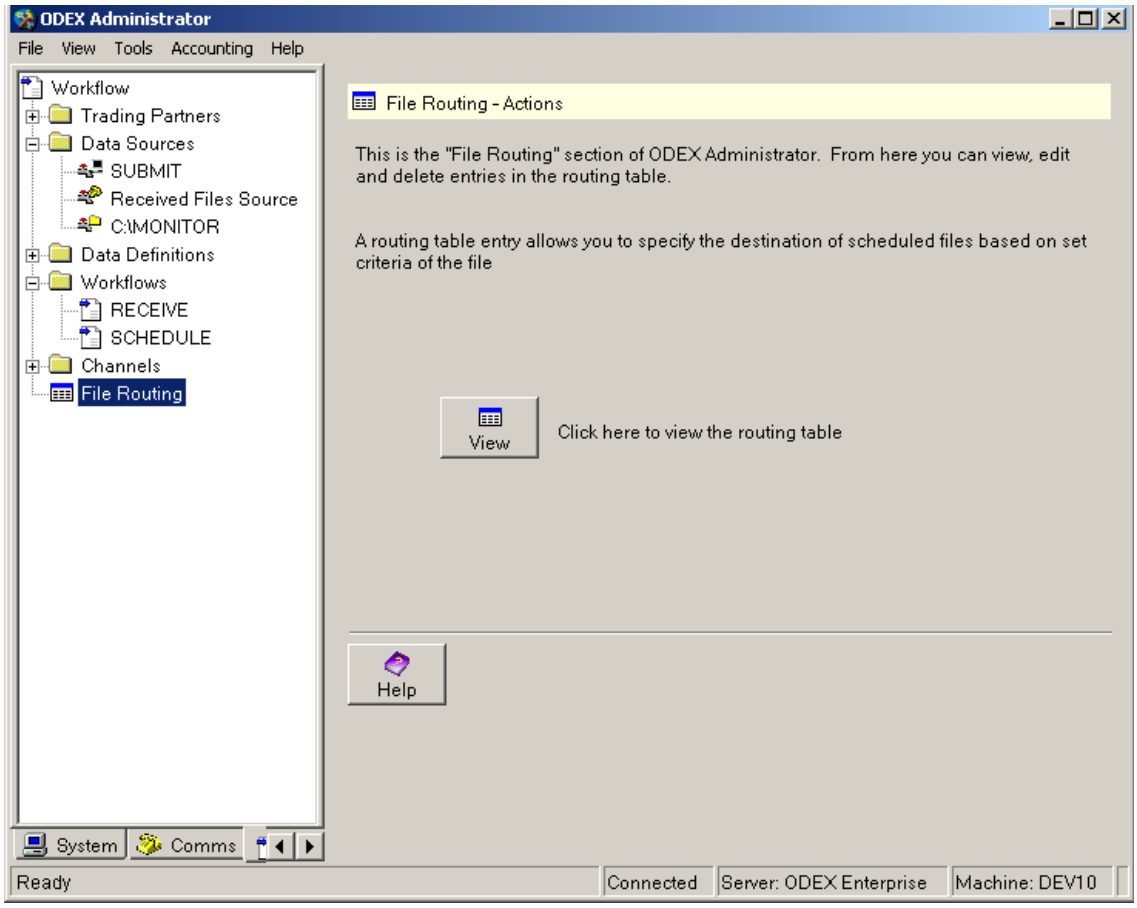
The routing table does not only have to be used for files that have been received – it is also possible to submit a file to the schedule job and change the originator or destination using the routing table, based on the file details detected by the schedule job.

The routing table consists of a number of rows. Each row contains a set of source file criteria and target file details.

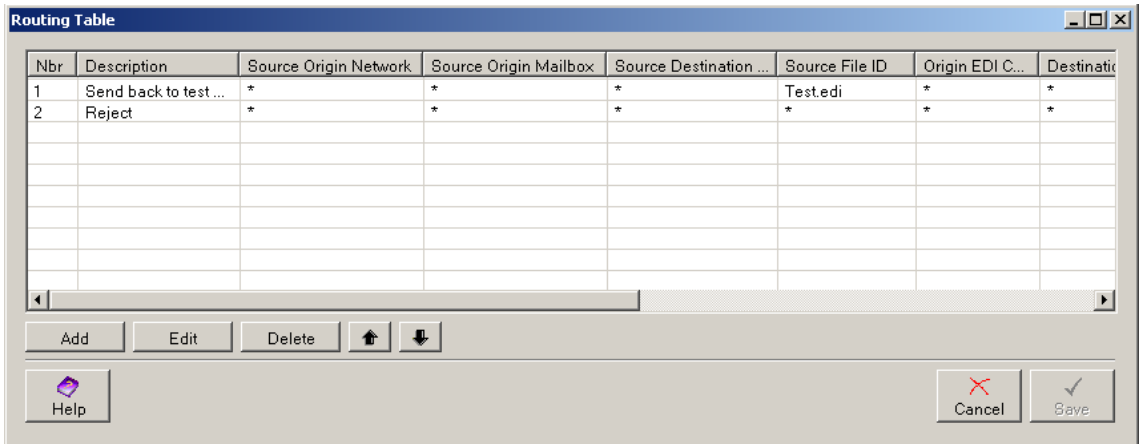
When a file is processed using the routing table, the routing table is searched from the top for a row with source file criteria that matches the given file. If a matching row is found, the target file details from the matching row are used to determine the originator and destination mailbox that will be used when scheduling the file.

Configuring The Routing Table

To view the routing table, select 'File routing' from the workflow administrator.



You will then see the File Routing actions view on the right hand side. To view the routing table, click the 'View' button. You will then be presented with a page similar to the following:



Each row in the routing table is displayed on the page. A column is displayed for each item of source file criteria and for each of the target file details. From here it is possible to add, edit, delete or change the sequence of rows.

Adding Or Editing Rows

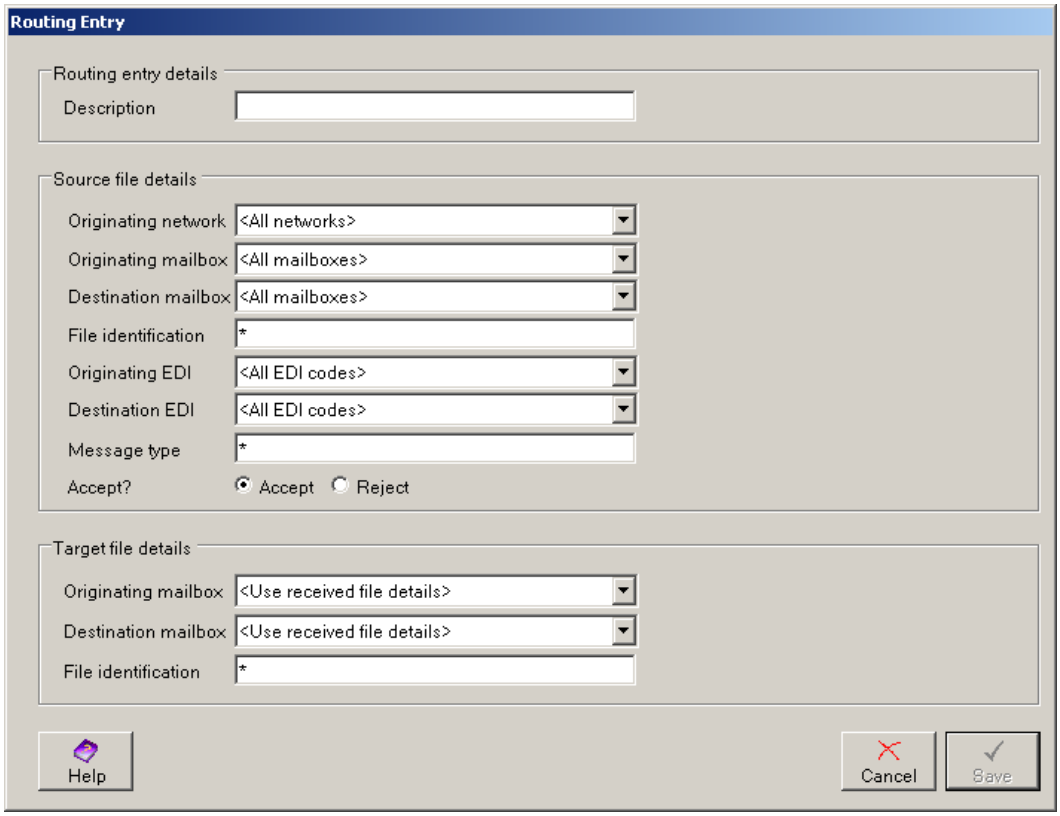
To add a row to the routing table, click the **'Add'** button, or press **Ctrl + A**.

If you select a row before adding the new row, the new row will be inserted into the table after the row that you have selected. If you do not select a row, the new row will be added to the end of the table.

To edit a row that is already present in the table you can:

- Double-click the row that you wish to edit
- Select the row and click the **'Edit'** button
- Select the row and press the **Ctrl + E** buttons

Whichever route you choose, you will now see a dialog box similar to the following example.



When adding a new entry, the dialog box will appear exactly as above. This is a blank routing table entry, which, if saved in its current state, will match to any file. The following describes each field in turn.

Once you have configured the routing table entry to your requirements, click the **Save** button to save the entry and return to the routing table. You can click **Cancel** at any time to undo your changes and return to the routing table.

Routing Entry Details – Description

This field allows you to add a description for this routing table row. The description is for your information only and is not used by ODEX.

Source File Details

The source file details are the criteria used to determine if a file matches to a routing table row.

Source File Details – Originating Network

This field allows you to restrict the files that this routing table row acts on to those that originate from a specific network. When scheduling a file that has been received from a trading partner through comms, the originating network is the trading partner network from which the file was received. For a file that was not received from a trading partner through comms, the originating network is the internal network from which the file is being scheduled.

The drop-down list contains an entry for every network defined in your ODEX system. The list contains:

- The SSID of each OFTP network
- The AS2 identifier of each AS2 network
- The name of each FTP client and FTP server network

If the default entry, 'All Networks' is selected, the row will act on files that originate from any network. To configure the row to act only on files from a specific network you may:

- Select an entry from the drop-down list
- Type in the SSID of an OFTP network
- Type in the AS2 identifier of an AS2 network

Source File Details – Originating Mailbox

This field allows you to restrict the files that this routing table row acts on to those that originate from a specific mailbox. For files that been received from a trading partner via comms, the originating mailbox is the external mailbox through which the file was received. For files that were not received from a trading partner via comms, the originating mailbox is the mailbox from which the file is being scheduled, as determined by the schedule job.

The drop-down list contains an entry for every mailbox defined in your ODEX system. The list contains:

- The SFID of each OFTP mailbox
- The local code of each FTP client and FTP server mailbox

Note that the concept of mailboxes does not exist in the AS2 protocol. However, an AS2 identifier will be shown for each AS2 network. Selecting an AS2 identifier will have the same effect as selecting an AS2 network from the Originating Network list.

If the default entry, 'All Mailboxes' is selected, the row will match to files that originate from any mailbox. To configure the row to act only on files received from a specific mailbox, you may:

Select an entry from the drop-down list

- Type in the SFID of an OFTP mailbox
- Type in the local code of an FTP mailbox

Source File Details – Destination Mailbox

This field works in the same way as the Originating Mailbox field, except this field allows you to restrict the files that this routing table row acts on, to those that are sent to a specific mailbox.

For files that have been received from a trading partner via comms, the destination mailbox is the internal mailbox through which the file was received. For files that that have not been received from a trading partner via comms, the destination mailbox is the external mailbox to which the file is being scheduled, as determined by the schedule job.

Source File Details – File Identification

This field allows you to restrict the files that this row acts on to those with specific file identifications. This field is only applicable to OFTP and FTP files. For OFTP files, the file identification is the virtual file name. For FTP files, the file identification is the file name.

You can match to all file identifications by entering an asterisk (*) in this field.

Source File Details – Originating/Destination EDI

This field allows you to restrict the files that this row acts on to those with a specific originating or destination EDI code. The EDI codes are determined by ODEX when analysing a file. It is therefore necessary to ensure that when restricting routing table rows to act on files with specific EDI codes, that the files being processed have been analysed.

You can restrict the row to act on files with specific EDI codes by:

- Selecting an EDI code from one of the lists
- Typing an EDI code into one of the lists

Source File Details – Message Type

This field allows you to restrict the files that this row acts on to those that only contain messages of a specific type, e.g. DELFOR, DELJIT. To match to all message types, enter an asterisk (*) in this field.

The message type is determined by ODEX when analysing a file. It is therefore necessary to ensure that when restricting routing table rows to act on files containing a specific message type, that the files being processed have been analysed.

Source File Details – Accept/Reject

The routing table can be used to prevent the system forwarding files with specified source file criteria.

When scheduling a file using the routing table, the routing table is searched from the top for a row with source file criteria that match the file. If the first row found has the ‘accept’ option set, the file will be scheduled. If the ‘reject’ option is set, a scheduling error will be raised and the file will not be scheduled.

Target File Details – Originating And Destination Mailbox

When scheduling a file using the routing table, if a matching row is found, the file will be scheduled from the mailbox selected in the originating mailbox field to the mailbox selected in the destination mailbox field.

The default value, ‘Use received file details’, means the originating or destination mailbox of the file will not be changed.

You can select a value by

- Selecting an entry from the drop-down list
- Typing the SFID of an OFTP mailbox
- Typing the local code of an FTP mailbox
- Typing the AS2 identifier of an AS2 network.

If an entry is selected from the list, the entries available in the destination mailbox drop-down list will be restricted to mailboxes of the same protocol.

Target File Details - Target File Identification

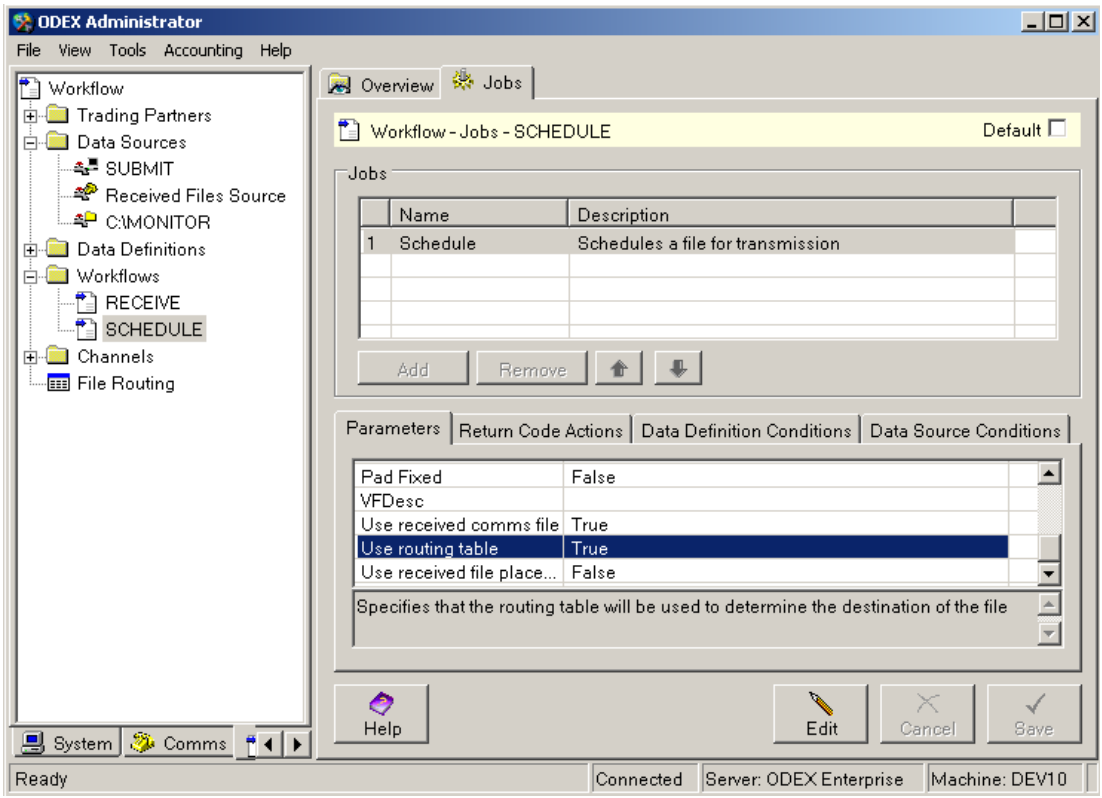
When scheduling a file using the routing table, if a matching row is found, entering a value in this field will change the file identification of the file. For OFTP files, this allows the virtual filename to be changed. For FTP files, this allows the filename to be changed. This field is ignored when scheduling an AS2 file.

To leave the identification of the file as the default value, or preserve the identification of the received file, enter an asterisk (*) in this field.

It is also permitted to enter placeholder values in this field. For more details on placeholders, see the section entitled 'Placeholders'.

Using The Routing Table

There are two different ways to configure the schedule job to use the routing table. The first is to set a parameter on the schedule job. The parameter 'Use routing table' must be set to true, as shown below.



When the job is configured in this way, the routing table will be searched from the top for a row with source file criteria that matches that of the file being scheduled. If a matching row is found, the origin, destination and file ID (OFTP virtual filename or FTP filename) of the scheduled file will be set according to the target file details of the routing table row. If no matching row is found, the file will be scheduled without using the routing table.

Another way to use the routing table is to configure an individual mailbox or network to use the routing table. Whether the mailbox or network can be configured to use the routing table depends on the protocol.

When receiving or sending files using OFTP or FTP, the originator mailboxes can be configured to pass files to the routing table. The concept of mailboxes does not exist in the AS2 protocol; it is therefore only possible to configure the network to use the routing table. For more information on configuring OFTP mailboxes, see the section entitled 'OFTP Mailbox'. For more information on configuring FTP mailboxes, see the section entitled 'FTP client Mailbox'.

If an external mailbox or network is configured to use the routing table, all files received through that mailbox or network that get passed to the schedule job will be routed using the routing table. If an internal network or mailbox is configured to use the routing table, all files scheduled from that network or mailbox would be routed using the routing table.

When the originator mailbox or network settings dictate that the routing table must be used when sending files, the routing table must contain a matching entry for each file submitted to the schedule job. If no matching entry is found in the routing table, this will cause the schedule job to generate an error.

Communications Monitor

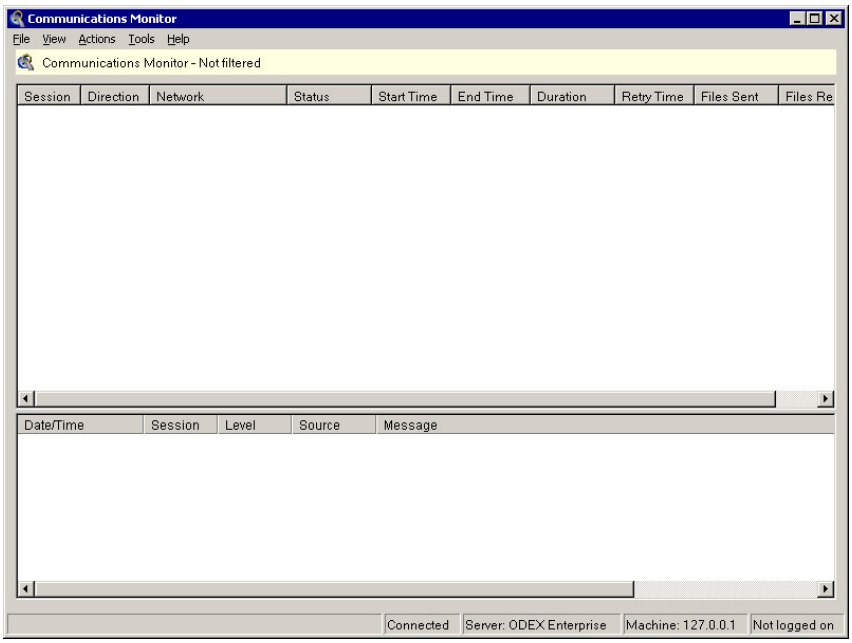
The Communications Monitor is a very simple client application that allows you to view details of your current log and all your current and recent communications sessions. Details of finished communications sessions are kept on the screen for 5 minutes, though this value can be configured if you wish, using the **Tools >> Options** menu option.

Please note that the contents of the Communications Monitor starts afresh each time you close and re-open the application.

The Communications Monitor allows you to see the current status of the communications within the system, including:

- The current status of each active session
- Log details for all sessions in the list
- A list of calls in retry mode, or recently failed.

Start the Communications Monitor to see the screen below.



The screen is divided into two: at the top are the details of your communications sessions, while below are details of your current system log. Note that the system log may contain log messages that are not connected with communications.

Each section is described below, together with the actions that can be performed upon it.

Menu options

The Communications Monitor has the following menu options and sub-options:

- File
- View
- Actions
- Tools

- Help

Selecting any of these options will present you with another list of options.

File option

The File option allows you to do the following:

- Log Off (only applicable if you are using ODEX security)
- Disconnect the comms monitor from the server. This will have the effect of freezing the contents of the screen until you reconnect to the server. To reconnect, simply click the **Connect** button on the Connection Lost dialog that will appear.
- Exit from the Communications Monitor

View option

The View option allows you to do the following:

- Filter the data content of the screen (see the section entitled "Comms Filter settings").
- Configure the columns on the screen (select which columns are displayed, their position and the sort order of data within each column). See the section entitled "Comms configure columns".
- Clear the log (clear the contents of the log as displayed on the screen).
- E-mail the log to the Data Interchange Plc support team
- Save the log to a file specified by you
- Enable/disable the log
- Select the log types to display (only available if the log is enabled)

Actions option

The Actions option allows you to do the following:

- Call selected networks
- Call a specific network
- Dismiss sessions manually
- Disconnect a selected session from the network

Tools option

The Tools option contains the following sub-options:

- Options
- Upgrade Settings
- Change Password

The Options dialog allows you to select the language in which you want to run the application, and lets you set up client-side logging. For full details of this dialog, please refer to the section entitled "Comms Monitor Options dialog".

The Upgrade settings option will only be available if you have any previous versions of ODEX Enterprise installed on your computer. This option allows you to copy settings, such as those from filters and display styles, from a previous

version to the current version. For full details of this option, please refer to the section entitled "Upgrade settings dialog".

The Change Password option will only be available if you are using ODEX User Security and have chosen to use passwords. This option allows you to change your password at any time while using the Communications Monitor. For full details of this option, please refer to the section entitled "Change password dialog".

Help option

The Help option gives you access to the following:

- the page(s) of the ODEX Enterprise on-line Help manual that describe and explain the Communications Monitor
- a dialog giving technical details about the Communications Monitor

Actions – Call Selected Networks

Use this option to make a call to one or more networks selected from the Comms Monitor view. Simply highlight the session lines relating to the network(s) you want to connect to and select this option.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Call Selected Networks**
- Using the 'Call Selected Networks' item on the context menu (right mouse click)
- Using the keyboard shortcut **Alt + A + C**

ODEX will immediately attempt to connect to the selected networks and you will see the new sessions appear in the list.

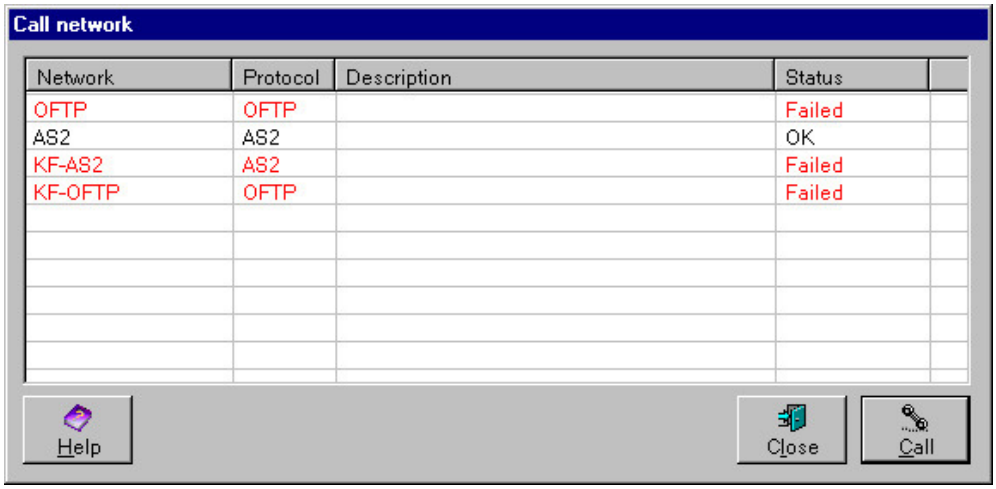
Actions – Call Network

The Call Network option allows you to make a manual call to a specified network. All files that have been scheduled to the selected network will be sent when the connection is made (subject to suspensions, retry limits etc).

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Call Network …**
- Using the 'Call Network' item on the context menu (right mouse click)
- Using the keyboard shortcut **Alt+A+N**

Any of these methods will bring up the following dialog:



This dialog shows all the external networks (i.e. for trading partners and clearing centres) you have defined in ODEX, with their associated protocol and the status of the last attempted call to each network.

Highlight the network(s) you want to call, then click the **Call** button. ODEX will attempt to make a connection to the selected network(s) and send any files that are scheduled to those networks.

Double-clicking on a network on this dialog will also result in a call being made to that network.

Actions – Dismiss

Use this option to dismiss sessions manually (i.e. remove them from the Comms Monitor view) before the expiry time specified in the **Tools >> Options >> View** dialog occurs.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Dismiss**
- Using the 'Dismiss' item on the context menu (right mouse click)
- Using the keyboard shortcut **Alt + A + I**

You will be asked if you are sure you want to dismiss the selected sessions. Click **Yes** to dismiss or **No** to cancel the request.

Actions – Disconnect

Use this option

- to terminate current sessions
- to terminate calls that are in Retry mode i.e. stop them from retrying

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Disconnect**
- Using the 'Disconnect' item on the context menu (right mouse click)
- Using the keyboard shortcut **Alt + A + D**

You will be asked if you are sure you want to disconnect the selected sessions. Click **Yes** to disconnect or **No** to cancel the request.

Communications Sessions

This part of the screen can display up to 18 columns. These columns are configurable i.e. you can select which columns are shown, the order they appear on the screen and the order of the data displayed in them.

The contents of each column is described in the following section. The default columns are listed first, followed by the remainder in alphabetical order.

Available columns

Default columns

Session – the ID of the communications session. This is allocated by ODEX Enterprise and is unique for the duration of the session.

Direction – the direction of the communication session. Its value will be either Incoming or Outgoing. Outgoing means that you instigated the communication session; Incoming means that your trading partner instigated the communication session.

Network – the name of the destination network for the session. This will be either a trading partner or a clearing centre, as set up in the Comms section of your Administrator.

Status – the status of the session, e.g. Connecting, Connected, Finished

Start Time – the time at which the session started.

End Time – the time at which the session ended.

Duration – the duration of the session in seconds (to 2 decimal places).

Retry Time – the time the connection was/will be retried. This can be interpreted in two ways. If the current status is Waiting to retry, then the time shown here is when the connection will be attempted again. Once it has commenced the retry, then the time shown here is the time it retried.

Files Sent – the number of files sent in the session. This is updated in real time as each file is sent.

Files Received – the number of files received in the session. This is updated in real time as each file is received.

Acks Sent – the number of acknowledgements sent in the session. This is updated in real time as each acknowledgement is sent.

Acks Received – the number of acknowledgements received in the session. This is updated in real time as each acknowledgement is received.

Remaining columns

Bytes Received – a count of the bytes received during this communications session so far. It is updated every second, though this time interval can be configured if you wish.

Bytes Sent – a count of the bytes received during this communications session so far. It is updated every second, though this time interval can be configured if you wish.

Connection – the connection type that is being used for the session, e.g. TCP.

File Direction – the direction of the file, i.e. either incoming or outgoing.

File Progress – this shows the transfer progress of the current file. Displayed as xxK / xxxK e.g. 15K / 250K.

Network Connection – the name of the destination network connection. It is only displayed for outgoing calls, as the connection name on an incoming call cannot be determined.

Protocol – the protocol that is being used for the session, e.g. OFTP, AS2.

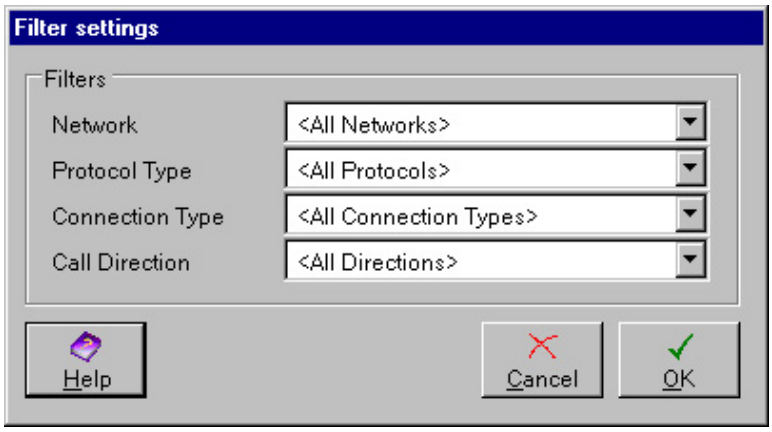
State – the current state of the protocol layer state machine e.g. WF_SSRM. This is an indication of what is happening during the exchange of protocol commands. WF_SSRM, for example, indicates Waiting For Start Session Ready Message. Contents of this column will be protocol-specific.

Comms Filter settings

The Filter settings dialog allows you to filter the log and session list to show only calls for a particular network, protocol type, connection type and/or call direction.

Use the dropdown arrow alongside each field to select the specific items or types of information you want to use for the filter.

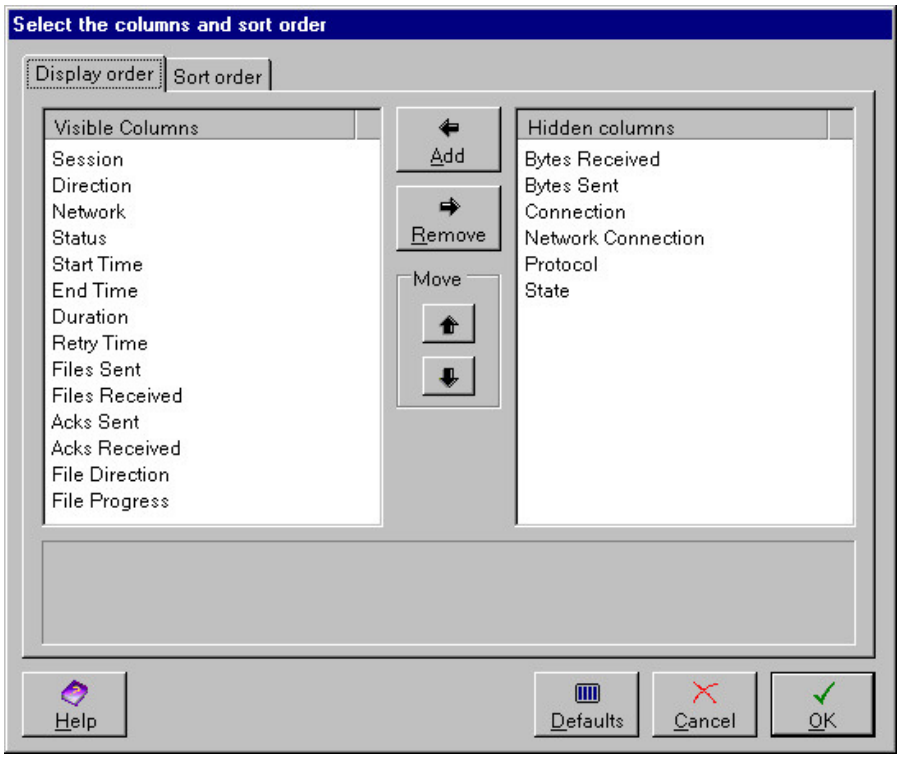
Click **OK** to save your selection and return to the main Communications Monitor screen, or click **Cancel** to leave the dialog without saving your changes.



The Filter settings are set to show all criteria by default, as shown in the example above.

Comms configure columns

To see all the available columns, select **View >> Columns** from the main menu, which will bring up the following dialog.



On the left-hand side of this dialog are the columns that are currently displayed on the Communications Monitor screen. These are the Visible columns.

On the right-hand side are the Hidden columns.

To make hidden columns visible, highlight the required Hidden column(s) and click the **Add** button.

To hide visible columns, highlight the required Visible column(s) and click the **Remove** button.

Once you have decided on your visible columns, you can alter the order in which they are displayed on the screen by using the **Move** buttons. Highlight one or more Visible columns and click the Up or Down **Move** button to move the

selected column(s) up or down one position in the list. Repeat until the column(s) are in the position in which you want them.

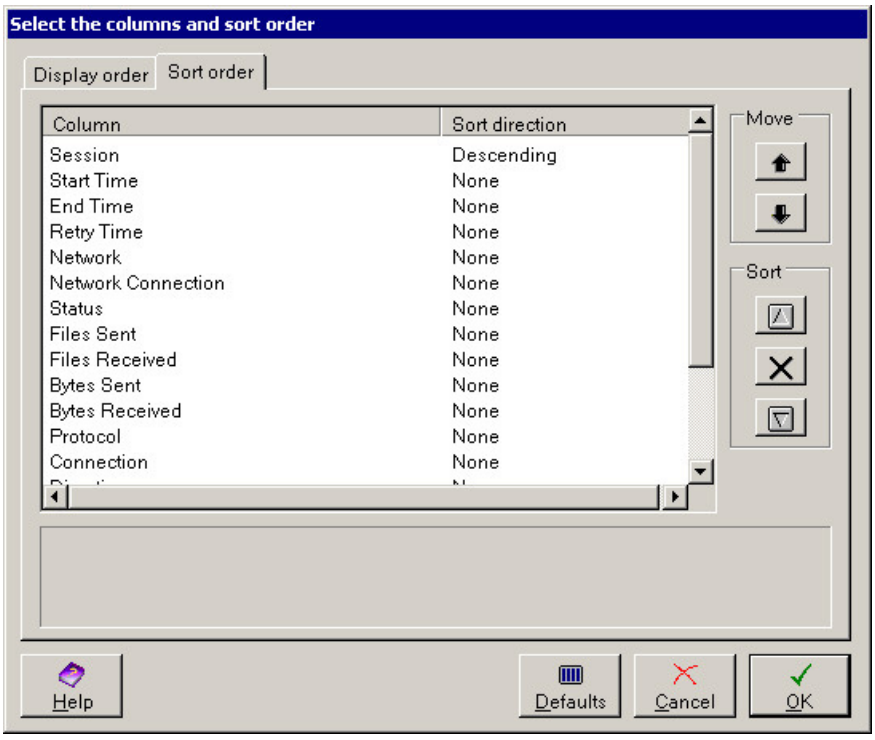
The top-to-bottom order of the columns in the list will be their left-to-right order when they are displayed on the screen.

To restore the default column setting for this view, simply click the **Defaults** button.

Select the Sort order page tab if you want to edit the sort order details. Otherwise click **OK** to save your changes and return to the Communications Monitor screen, or click **Cancel** to leave this dialog without saving your changes.

Choosing a sort order

Click the Sort order page tab to see the following dialog.



Here you can determine how the contents of the columns are to be sorted, if at all.

This dialog lists all the available columns, not just those that will be displayed on the screen. This means that the sort order of displayed columns can be affected by the sort order of hidden columns.

Use the three **Sort** buttons to determine whether columns are to be sorted in ascending order, descending order or not sorted at all. Highlight one or more items in the list and click the appropriate **Sort** button.

Use the two **Move** buttons to change the priority in which columns will be sorted. Highlight one or more items in the list and click the appropriate **Move** button to move the selected column(s) up or down one position in the list. Repeat until the column(s) are in the position in which you want them. N.B. This does not affect the order of the actual columns, but the data in the columns.

If you are not interested in sorting any columns by value, simply leave the Sort direction of all the columns as None (the default option). If all columns are set to None, the order of columns in the list will not have any effect on the way data is displayed on screen.

To restore the default column setting for this view, simply click the **Defaults** button.

Click **OK** to save your changes and return to the Communications Monitor screen. Alternatively, click **Cancel** to leave this dialog without saving your changes.

Log

The log window displays 5 columns, described below. No filter, column configuration or sort order is available here.

Date/Time – this is the date and time at which the logged event occurred.

Session – the unique identification of the communication session (only present if the message relates to communications)

Level – indicates the type of log message. The four possible types are: General, Protocol, Debug and Data.

- Protocol indicates a log message relating to the OFTP protocol that is an essential part of the communication session e.g. SSID or EFID.
- Debug messages are effectively trace messages, giving an indication of what is happening.
- Data indicates high-level logging, displaying the data contents of the received/sent protocol and files being exchanged.
- General indicates any other log information that is not covered by the other three categories. Such information is not necessarily related to communications.

Source – the code displayed here indicates the exact part of the internal program that produced the log message.

Message – this is the user-friendly log message, providing you with information on which you may want to act.

The log window shows the user the current communications log “as it happens” for the sessions in the list.

Colour coding

Each line of the log is colour-coded as follows:

Black – normal

Blue – trace messages

Orange – warning messages

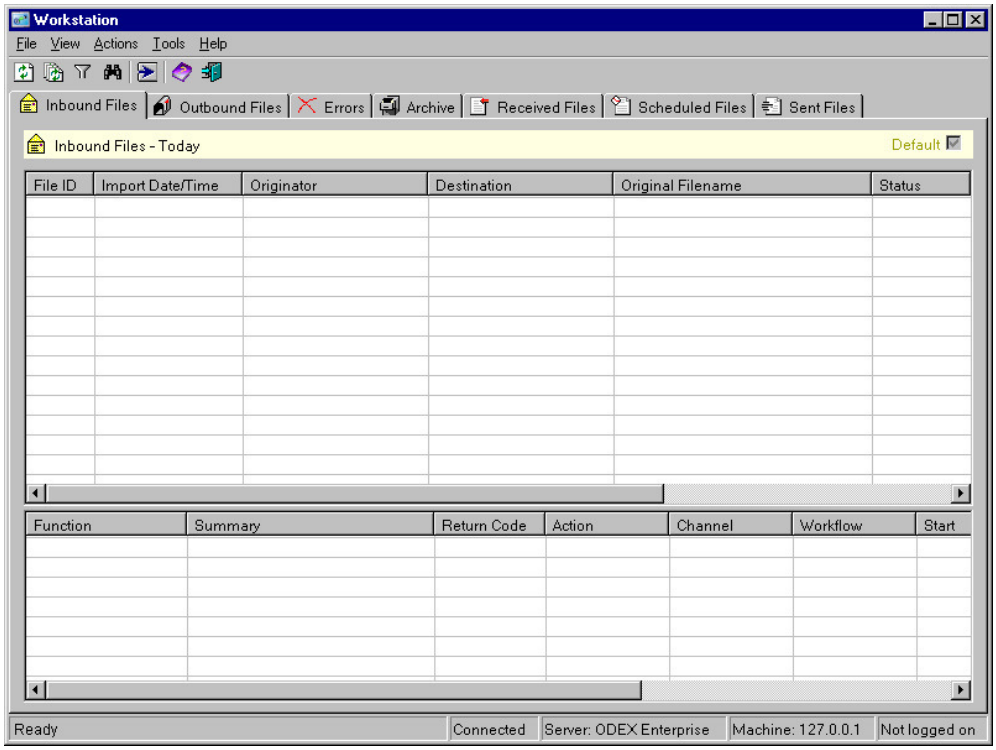
Red – error messages

ODEX Workstation

Introduction

The ODEX Workstation is the main ODEX application, used for day-to-day file exchange with trading partners and handling of these files.

When you first open the ODEX Workstation, you will see the following screen.



Workstation Views

There are seven views that you can see when you open the Workstation:

- Inbound files (files received via ODEX comms)
- Outbound files (files received via a Command data source or a Directory data source)
- Errors (files that have had an error during processing)
- Archive (files that have been archived)
- Received files (comms files that have been received by the system)
- Scheduled files (comms files that have been scheduled)
- Sent files (comms files that have been sent)

An additional view, the 'Forward files' view, may also be activated for use in a clearing centre environment. This view displays details of files that have been received and are due to be forwarded, or have been forwarded to another trading partner.

Workstation Files colour coding

You can see at a glance certain information about workstation files, depending on the colour coding that has been applied to them.

All workstation views

Pale blue/white = normal

Red/pink = error

Scheduled Files

Red/pink = has a status of “Send Failed” and will not be sent again

Yellow = suspended

Light orange = one of the following:

- Scheduled with attempts greater than 0
- Partly sent with attempts greater than 1 and a last error
- Partly sent with attempts greater than 2

Workflow Files

Workflow files include inbound files, outbound files, files containing errors and archived files. These are the first four views mentioned above. They are files that have been submitted to the workflow manager for automated processing. Files can be submitted in three ways:

- manually (via a command)
- when received via comms
- when detected in a monitored directory.

Although all files shown here are under the control of the workflow manager, you can intervene manually, if necessary, to perform a variety of actions on any file.

Each workflow file view is divided into two sections: the top section displays your files, while the bottom section displays an audit trail of all the actions that have been carried out by the workflow manager on a file highlighted in the top section.

Displaying Workflow File EDI Data

After of a known EDI format files have been analysed, usually automatically upon receipt by ODEX, additional data is available for display. To display Interchange and message data such as the EDI Code, Routing address, Interchange Control Reference and Document Number add the appropriate columns to the Workstation using the Column Picker. By default, only the first interchange and first message information for a particular file is shown. To view each message select ‘Show all messages’ from the view. This will show a single row per message; hence the file data will be repeated for messages in the same file.

Although files should be automatically analysed if they are sent to ODEX, to ensure that this EDI data is available files can be analysed using the ‘Analyse' job. If the ‘Condense Messages’ parameter on this job is set to ‘True’ then messages of the same type will be shown as a single message upon analysis. This can remove unique message data such as the Document Number.

Comms Files

The other three views (received, scheduled and sent files) of the workstation show comms files. Comms files are files that are under the control of the communications manager. These may have been scheduled automatically by

the workflow manager or manually by a user. Usually all received files will immediately be submitted to the workflow manager, but the communications manager will keep a copy of them.

Advanced users can add and remove views, and create named, customised views of the system with customised filters. This allows users to hide all the pre-defined views and set the system up to display the information in the way they want to see it.

Workflow and comms files

As well as being able to view all this data, users can interact with all the files. They can see the audit trail for each workflow file (a history of the jobs that have been performed on it) and bring up detailed information about the file and any jobs that have been performed (such as viewing the Xlate log if the file has been translated).

Users can also interact directly with the comms file, allowing them to schedule and extract files and to make calls to trading partners.

Before we describe these pages and how to use them, let's have a look at what the ODEX Workstation is for.

EDI Security Status

The workstation's workflow file and and comms file views indicate the EDI security status of a file using an appropriate icon to the far left of the line for that file. The icons used for each security status are indicated below:

- The security status 'Signature required' indicates that a file is awaiting signing on the client. It uses the icon  .
- The security status 'Signed' indicates that a file has been signed by the Sign EDI job ready for transmission. It uses the icon  .
- The security status 'Signed invalid' indicates that the signature associated with the file has been found to be invalid by the Verify or Process AUTACK jobs. It uses the icon  .
- The security status 'Signed valid' indicates that the signature associated with the file has been found to be valid by the Verify or Process AUTACK jobs. It uses the icon .
- The security status 'Signed, complete' indicates that the file was signed and sent and a positive response AUTACK has been received and processed. It uses the icon  .
- The security status 'Signed, response error' indicates that the file was signed and sent and a negative or invalid response AUTACK has been received and processed. It uses the icon  .
- The security status 'Signed, awaiting response' indicates that the file was signed redy for transmission and a response was requested, but the response AUTACK has not yet been received. It uses the icon  .
- The security status 'AUTACK response' indicates that the file was a response AUTACK. It uses the icon  .

What does the ODEX Workstation do?

The ODEX Workstation allows you to:

- View your received files, scheduled/sent files, files currently undergoing processing, processed files and archived files
- Schedule files to your trading partners
- Open files using any suitable application
- Submit and resubmit files to the workflow manager
- Suspend files from being processed by the workflow manager and resume processing when appropriate
- Copy files to another location
- Delete files
- Make calls to trading partners
- Archive files
- Add and remove views, and create named, customised views of the system (advanced users only)

You can use the ODEX Workstation to view the following information:

Files

- Workflow Files:
  - Inbound files
  - Outbound files
  - Error files
  - Archived files
- Communications Files:
  - Files received by the system
  - Files scheduled by the system
  - Files sent by the system
  - Files being forwarded by the system

For each file, you will be able to see its current status in the system, including the following information:

- File ID, as allocated by the workflow manager
- Data Source information
- Whether processing of the file has been suspended or not
- Import date/time
- Processing start date/time
- Processing end date/time
- Advanced information such as:
  - Filename
  - Original filename
  - Audit information

- Whether the file has been analysed or not
- Analysis information
- Parent file ID

In addition to being able to view all the files in each of the above categories, you will also be able to view files based on the following filters:

- To/From specific networks
- To/From specific mailboxes
- Files on specific channels
- Files that had errors when being processed by the workflow manager
- Communications files that have reached the retry limit

Errors

From an error tracking and catching point of view, you will also be able to see:

- Calls that have reached a retry limit
- Calls that are in retry
- Any file processing errors that have occurred in the system

Actions

You can perform the following actions:

- Schedule an EDI file (the system will analyse it and schedule it to the correct place), bypassing the workflow manager
- Schedule a non-EDI file (specifying the network it is to be sent to), bypassing the workflow manager
- Extract files from the system
- Submit a file into the system (to be processed by the workflow manager)
- Suspend a file from being processed
- Make a call to a trading partner

Workflow Files tool bar

The Workflow Files tool bar contains the following icons:

 This is the Refresh option. This option shows the results of any updating or editing that has been done in this view.

 This is the Refresh All option. This option refreshes all the views in the Workstation.

 This is the Filter option. This option allows you to select specific criteria for the files you want to see displayed in the data area.

 This is the Search option. This option allows you to look for one or more files in the ODEX system, using the file ID or the filename (or part thereof), and limiting the search to certain areas if required.

 This is the Submit option. This option allows you to place a file manually into a workflow channel.

 This is the Help option. The Help option takes you to the page(s) of the ODEX on-line Help manual that describe and explain the window or dialog you are currently looking at.

 This is the Exit option. The Exit option closes the ODEX Workstation.

Workstation View options

All views in the Workstation have a View menu option whose sub-options work in the same way, whether used for a Workflow file or for a Comms file. Most of them share common dialogs, so we have described them here. Others, such as the Filter dialogs, differ according to the view they are accessed from, and are described in the appropriate section.

Refresh

The Refresh option shows the results of any updating or editing that has been done in this view. It can be accessed in the following ways:

- From the main menu, using **View >> Refresh**
- Using the keyboard shortcut **F5**
- Using the toolbar icon 

Use any of these methods to refresh the contents of the view you are currently looking at.

Refresh All

The Refresh All option refreshes all the views in the Workstation. It can be accessed in the following ways:

- From the main menu, using **View >> Refresh All**
- Using the keyboard shortcut **Shift + F5**
- Using the toolbar icon 

Use any of these methods to refresh the contents of all the views in the Workstation.

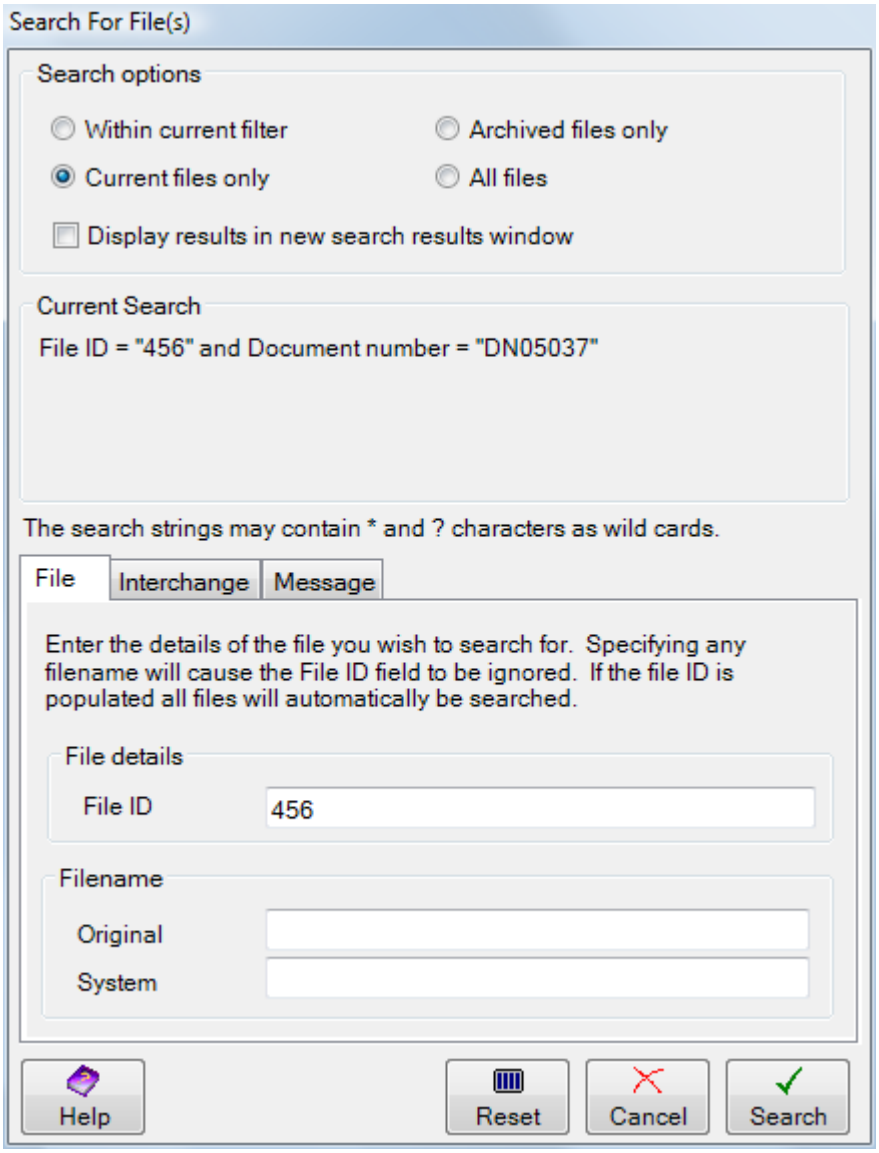
Search

The Search option allows you to look for one or more files in the ODEX system, using the file ID or the filename (or part thereof), and limiting the search to certain areas if required.

It can be accessed in the following ways:

- From the main menu, using **View >> Search**
- Using the keyboard shortcut **Ctrl + S**
- Using the toolbar icon 

Any of these methods will bring up the following dialog:



Search Options

This section of the dialog allows you to choose where ODEX is to conduct its search. The choices are:

- Within current filter – ODEX will only search through those files that are displayed as a result of the filter you currently have set
- Archived files only – ODEX will only search through archived files
- Current files only – ODEX will only search through files that have not yet been archived
- All files – ODEX will search through all files in the ODEX system

Additionally you can decide whether to open the search results in a new window or use the current search window. The first time you perform a search, the results will appear on a new tab page called Search Results, whether this tickbox is selected or not.

Current search

In this section you will see the search that will be executed. It will show combined searches from across the File, Interchange and Message tabs. If you wish to remove an item, simply clear its relevant text box.

In each tab view you can use the characters * and ? as wild characters, as for normal Windows searches.

- * represents zero or more wild characters
- ? represents exactly one wild character

File searches

This section allows you to select a specific file ID or Filename to search for. File ID refers to the ID allocated to the file by the Workstation, as shown on the Current Files views.

When searching for Filename you can type in either the original name of the file or the system name i.e. the name given to it by ODEX once it entered the ODEX system.

Interchange searches

This section allows you to search for an Interchange Control Reference and EDI codes.

When searching for EDI codes you can additionally search for Qualifiers, Routing Addresses and Sub-Routing Addresses by separating by ':'. For example, if you wanted to search for an EDI code and a specific Sub-Routing Address use 'CODE:::SUBADD' where there is nothing between the semi-colons of the fields you do not wish to search for.

Message searches

This section allows you to search for a Document Number of specific Message Type. Document Numbers are extracted from messages when they are analysed. Message Type is the specific format of the message such as 'INVOIC' for Edifact invoice messages. You should not specify versions here.

Search Window

Click the **Search** button to perform the search.

The Search Results page and the files displayed on it can be dealt with in the same way as for the other pages, using the available menu items, toolbar icons and keyboard shortcuts.

Once the search view is open, you can filter it as normal, but the filter will always include the filename filters from the search dialog.

The Search Results page is a workflow files view with its own column configuration. Initially it gets the default columns (for the view), but as soon as it has been used once it remembers the columns settings (which can be changed in the column picker).

Every time a search is invoked, the view is re-populated with the results of the new search.

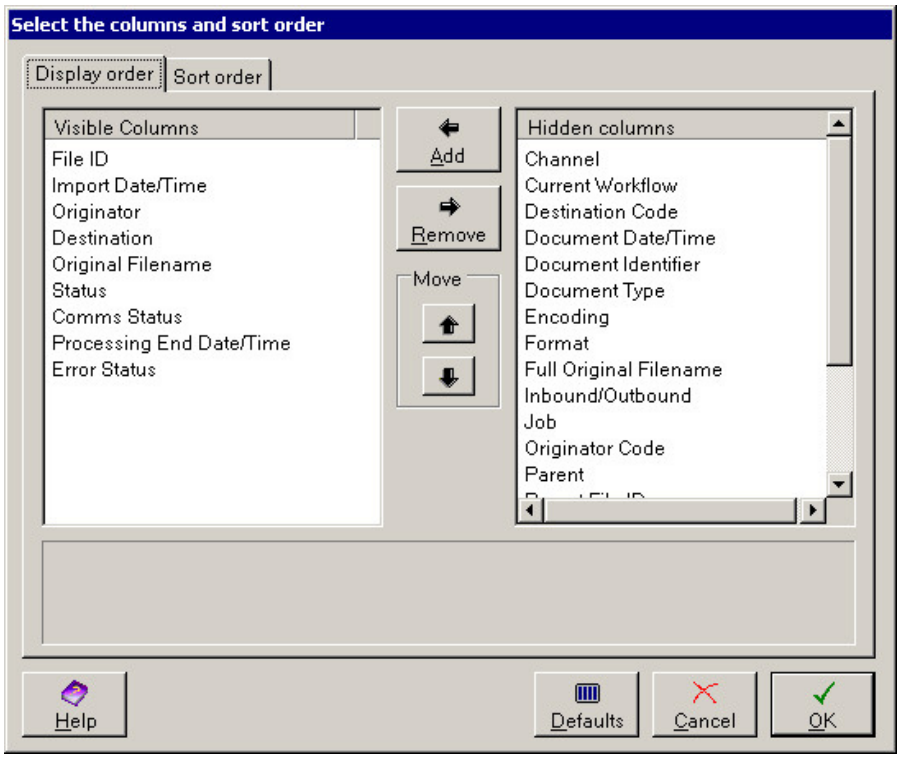
To close the Search Results page, select **View >> Close Search Results** (or **CTRL + R**) or **View >> Close All Search Results** (or **CTRL + Shift + R**).

Columns

The Columns option allows you to choose the columns you want to be displayed in this view, and the order in which you want to display them. It can be accessed in the following ways:

- From the main menu, using **View >> Columns**
- Using the keyboard shortcut **Ctrl + C**

Either of these methods will bring up the dialog shown below.



On the left-hand side of this dialog are the columns that are currently displayed on the Current Files page. These are the Visible columns.

On the right-hand side are the Hidden columns.

To make hidden columns visible, highlight the required Hidden column(s) and click the **Add** button.

To hide visible columns, highlight the required Visible column(s) and click the **Remove** button.

Once you have decided on your visible columns, you can alter the order in which they are displayed on the screen by using the **Move** buttons. Highlight one or more Visible columns and click the Up or Down **Move** button to move the selected column(s) up or down one position in the list. Repeat until the column(s) are in the position in which you want them.

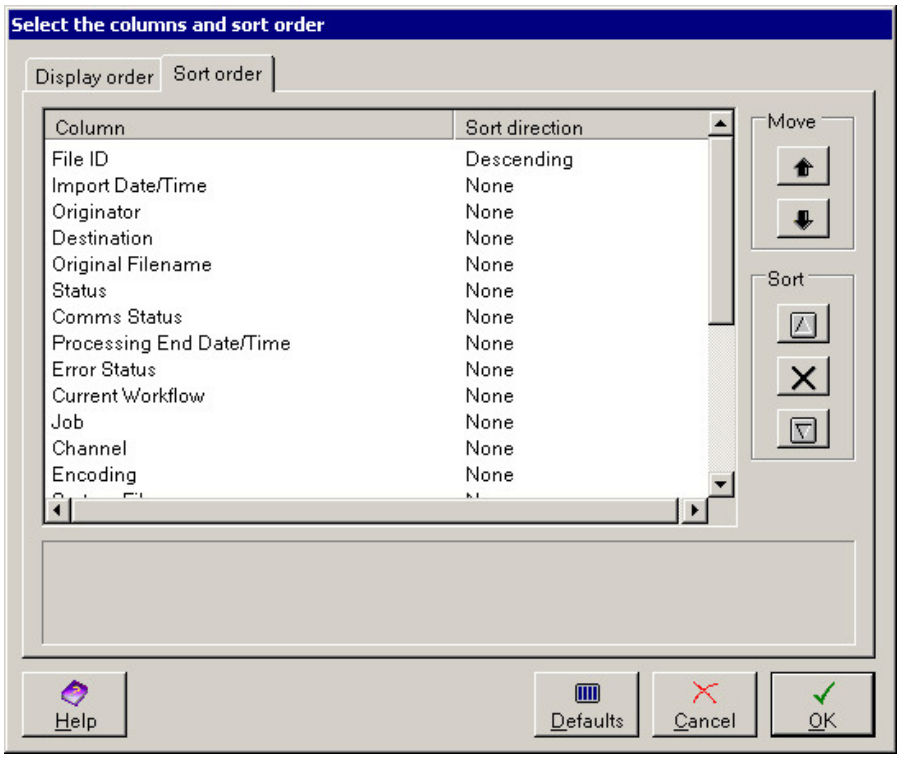
The top-to-bottom order of the columns in the list will be their left-to-right order when they are displayed on the screen.

If you want to restore the default column settings for the view, simply click the **Defaults** button.

Select the Sort order page tab if you want to edit the sort order details. Otherwise click **OK** to save your changes and return to the Current Files page, or click **Cancel** to leave this dialog without saving your changes.

Choosing a sort order

Click the Sort order page tab to see the following dialog.



Here you can determine how the contents of the columns are to be sorted, if at all.

This dialog lists all the available columns, not just those that will be displayed on the screen. This means that the sort order of displayed columns can be affected by the sort order of hidden columns.

Use the three **Sort** buttons to determine whether columns are to be sorted in ascending order, descending order or not sorted at all. Highlight one or more items in the list and click the appropriate **Sort** button.

Use the two **Move** buttons to change the priority in which columns will be sorted. Highlight one or more items in the list and click the appropriate **Move** button to move the selected column(s) up or down one position in the list. Repeat until the column(s) are in the position in which you want them. N.B. This does not affect the order of the actual columns, but the data in the columns.

If you are not interested in sorting any columns by value, simply leave the Sort direction of all the columns as None (the default option). If all columns are set to None, the order of columns in the list will not have any effect on the way data is displayed on screen.

If you want to restore the default column settings for the view, simply click the **Defaults** button.

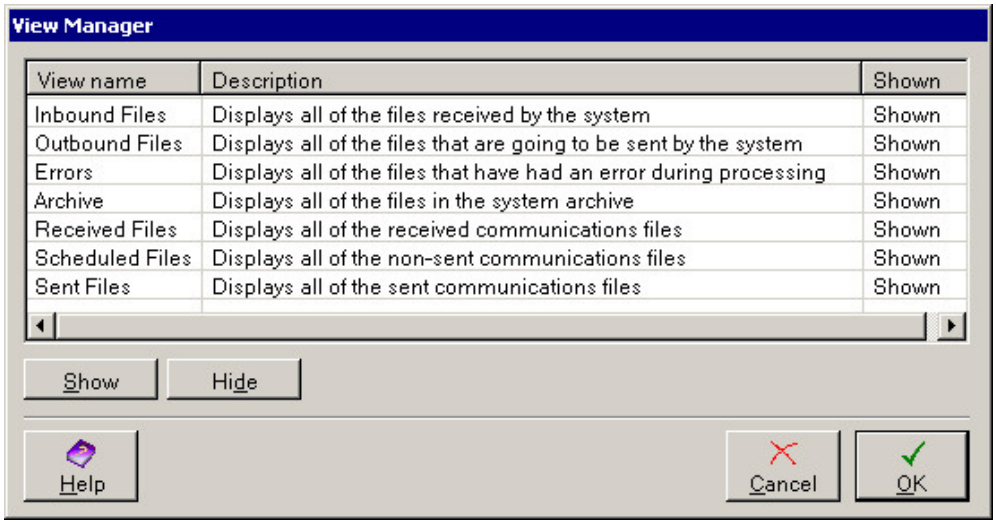
Click **OK** to save your changes and return to the Current Files page. Alternatively, click **Cancel** to leave this dialog without saving your changes.

Views

This option allows you to show or hide any of the views in the Workstation. It can be accessed in the following ways:

- From the main menu, using **View >> Views**
- Using the keyboard shortcut **Ctrl + V**

Either of these methods will bring up the View Manager dialog shown below.



This dialog lists all the available views for the Workstation, together with a description of what each displays and whether the view is currently Shown or Hidden. By default, all views will be shown.

To Show or Hide any of the views, highlight the appropriate line and click the Show or Hide button, as appropriate. The value in the Shown column will indicate the change you have made.

Click **OK** to save the changes and return to the Current Files view, or **Cancel** to quit the dialog without saving your changes.

Close Search Results

This option will only be available if you have one or more Search Results pages open, and one of them is the currently selected page. Selecting this option will close the currently selected Search Results page.

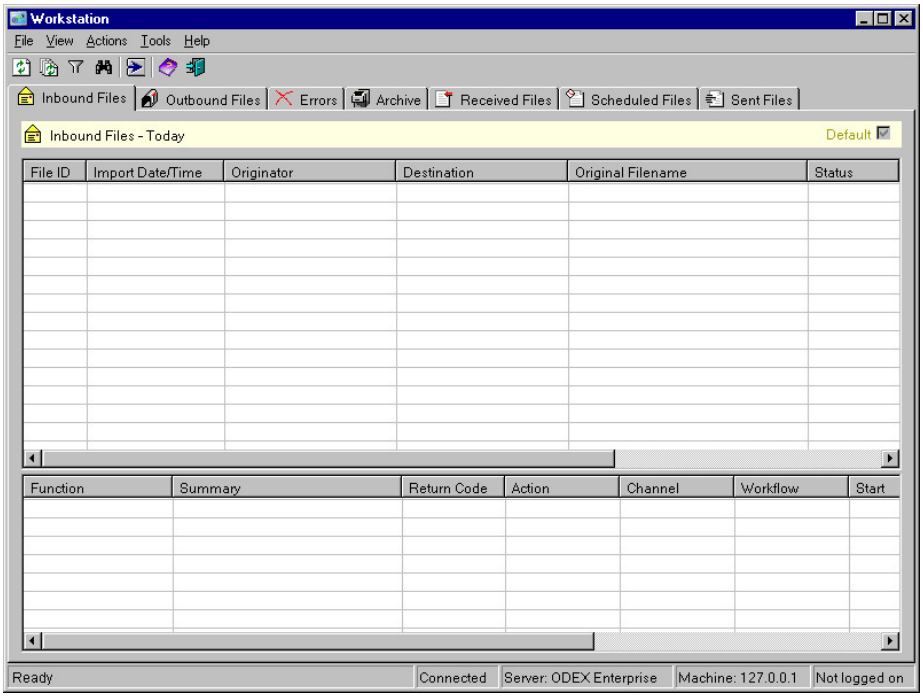
Close All Search Results

This option will only be available if you have one or more Search Results pages open. Selecting this option will close all the Search Results pages.

Workflow Files – File Details

The upper section of this page shows you a list of all workflow files available to you in your system. It also highlights any files that are in error, by displaying them in red on a pink background.

If you are logged on as a user that is a member of one or more communities, you will only be able to see files that have origin or destination companies that are associated with your communities.



This section of the page is configurable i.e. you can select which columns are shown, the order they appear on the page and the order of the data displayed in them.

Columns for Inbound, Outbound and Error pages are the same. There are a few different columns for the Archived page, which are indicated in the following section.

The contents of each column is described in the following section. The default columns are listed first, followed by the remainder in alphabetical order. Interchange and Message columns are also available. Information in this will be displayed from the first interchange and first message of this file unless 'Show All Messages' is turned on.

File columns

Default columns

File ID – the unique ID given to the file by the workflow manager. This will be a simple integer, incremented for each new file that is imported into ODEX.

Archived Date/Time – the date and time at which the file was archived (applicable only to archived files).

Import Date/Time – the date and time at which the file was imported into ODEX.

Originator – The trading partner that this file came from (this will be an internal network for outbound files). The trading partner is determined based on the EDI code and will only be known if the file has been analysed.

Destination – The trading partner that this file will be or has been sent to (this will be an internal network for inbound files). The trading partner is determined based on the EDI code and will only be known if the file has been analysed.

Original Filename – the name of the file that was originally imported into the system. If it was received via comms, this will be the VFN of the file. If it was imported from a monitor directory, this will be the name of the file that was put into the monitor directory.

Status – the current status of the file. Possible values are:

- Current
- Suspended
- Processed
- Archived

Comms Status – the current status of the comms session for this file, if applicable. If there is no comms file for this file, the status will be 'No Comms File'. If there is more than one comms file for this file, the status will be 'Multiple Comms Files'. If there is one comms file for this file, the status will be the status of the comms file.

Processing End Date/Time – the date and time at which the system finished processing the file.

Error Status – indicates whether the file had any errors during processing. Will also indicate if they were handled (by a user defined workflow) or unhandled (no error workflows defined).

Remaining columns

Channel – the name of the channel in which the file is currently being processed or, for archived files, was processed.

Current Workflow – the name of the workflow the file is currently in (not applicable to archived files)

Destination Code – the destination's identifier for the document e.g. EDI code for EDI documents

Document Date/Time – the date and time of the documents in the file e.g. interchange date and time in an EDI file

Document Identifier – the identifier of the documents in the file e.g. the interchange control reference in an EDI document

Document Type – the type of document in the file e.g. DESADV D96A for an EDI document

EDI Security – the EDIFACT security status of the file.

EDI Acknowledgement – the EDI functional acknowledgement status of the file.

Encoding – indicates the encoding used for this file e.g. ASCII, EBCDIC. If the type of coding is unrecognised or if the file is not encoded, the value in this column will be 'Unknown'.

Format – indicates the format of the data in the file. Among possible values are EDI, non-EDI and XML.

Full Original Filename – the full file path of the file that was originally imported into the system. If it was received via comms, this will be the VFN of the file. If it was imported from a monitor directory, this will be the full file path of the file that was put into the monitor directory.

Inbound/Outbound – indicates whether the file has been received into the system or whether it will be sent by the system. Inbound is a file you have received. Outbound is a file you are sending. If the file was not received via the communications component of the system, it is assumed to be outbound.

Job – the name of the job that is currently being performed on the file (not applicable to archived files)

Originator Code – the originator's identifier for the document e.g. EDI code for EDI documents

Parent – Yes or No indicates whether the file is a parent or not. A file containing one or more interchanges can be split into several files, each of which contains one of those interchanges. The original file is then deemed to be a parent, and each file it was split into is deemed to be a child of that parent.

Parent File ID – the ID of the file that this file was created from, if this file is a child resulting from a file split.

Previous Job – the name of the last job that was performed on the file.

Previous Workflow – the name of the last workflow which processed the file.

Processing Start Date/Time – the date and time at which processing began on this file.

Sub File Index – used if this is a "child" file resulting from a split file. This value indicates the original position of the "child" file in the parent file. The index starts at 0.

System Filename – the disk filename given to the file by the ODEX system when it is imported.

Test Indicator – the test indicator of the documents in the file. This is in the UNB segment in an EDI document.

User Data – This is data attached to the file by the user when the file was submitted to the system.

Interchange columns

From EDI code - The originator EDI code of the interchange

From EDI Code Qualifier - The originator EDI code qualifier of the interchange

From Routing Address - The originator routing address of the interchange

From Routing Sub-Address - The originator routing sub-address of the interchange

To EDI code - The destination EDI code of the interchange

To EDI Code Qualifier - The destination EDI code qualifier of the interchange

To Routing Address - The destination routing address of the interchange

To Routing Sub-Address - The destination routing sub-address of the interchange

Application Reference - The Application reference of the interchange, if present

Interchange Control Reference - The interchange control reference specified in the interchange

Syntax - The syntax that interchange follows

Interchange Syntax Version - The syntax version of the interchange

Interchange Transmission Time - The transmission time of the individual interchange

Interchange Message Count – The number of messages in this interchange

Message columns

Message Reference - The message reference number that was collected from the message

Message Version - The syntax version of this message

Message Release - The release of the syntax of this message

Message Type – The syntax type of the message

Document Number – The document number specified in the message

Workflow Files – Audit Log

The lower section of this page shows you an audit log of all the actions that have been performed on a highlighted file in the upper section.

This section of the page displays 6 columns – these are not configurable.

The contents of each column is described in the following section.

Columns

Function – the action that was performed on the file at the given time

Summary – if available, some extra information about the action. For example, for a file that has been copied, it will show where it has been copied to.

Return Code – the program code returned at the end of processing. A return code of 0 (zero) indicates that the action was successful. For any other value of return code you should check the Action column for further details of a possible failure.

Action – the action that was taken as a result of the return code value e.g. Continue or Unhandled.

Channel – the channel that is currently processing the file.

Workflow – the workflow that the file is currently in.

Start – the date and time when the action began.

End – the date and time when the action ended.

Duration (ms) – the length of time (in milliseconds) that the action lasted.

Child Action – the action that was performed on the child file, if applicable

Workflow Files – View option

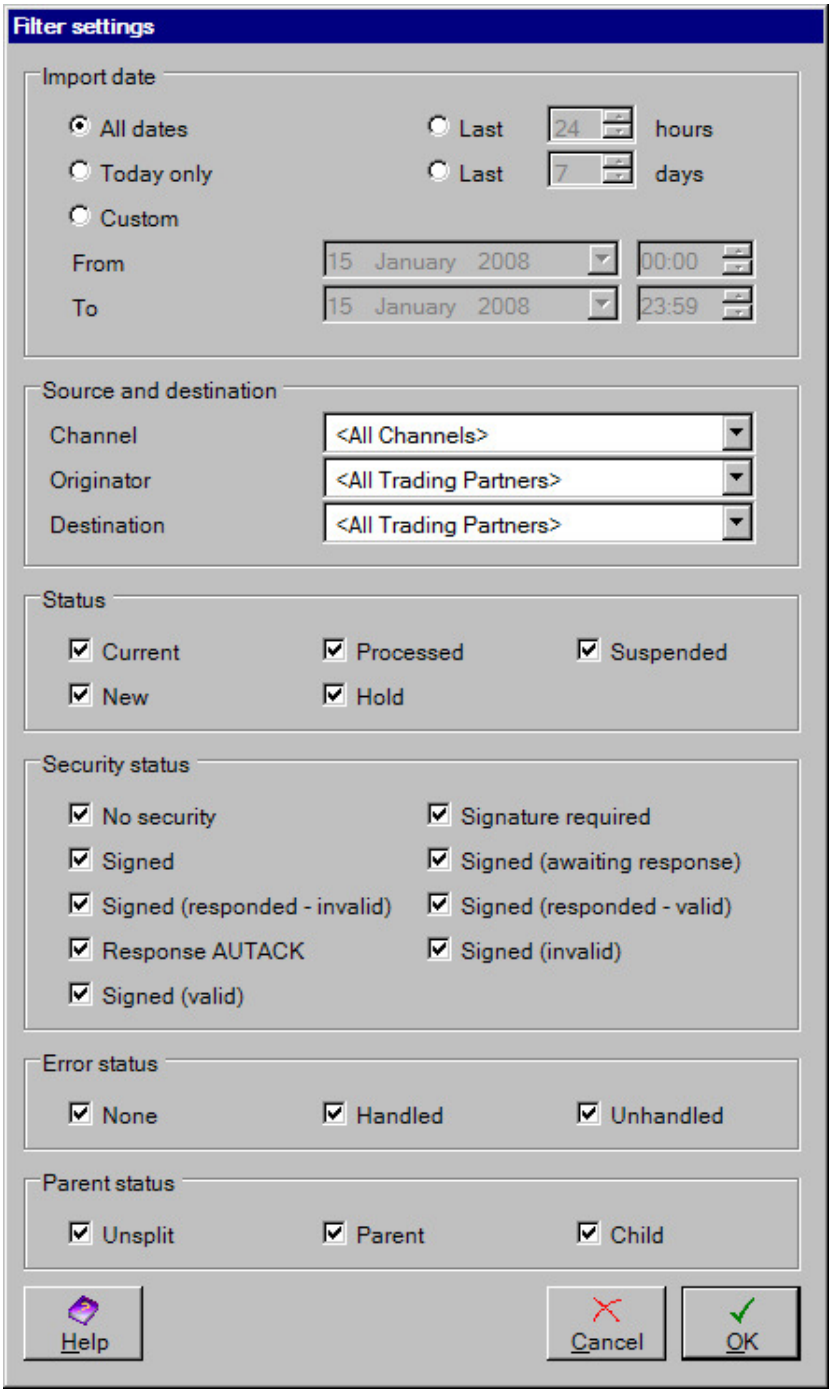
The View menu option contains the following sub-options:

Filter

The Filter option allows you to select specific criteria for the files you want to see displayed in the data area. It can be accessed in the following ways:

- From the main menu, using **View >> Filter**
- Using the keyboard shortcut **Ctrl + F**
- Using the toolbar icon 

Any of these methods will bring up the dialog shown below. (For the Error Files Filter dialog please see "Error Files Filter". For the Archived Files Filter dialog please see "Archived Files Filter").



Please bear in mind that filtering may result in no entries being shown in the data area if no files meet the filter criteria.

Import date

The default Import date setting for the filter is All dates. To limit the dates, select one of the other radio buttons.

Selecting "Today only" means that only files imported today will be displayed.

Selecting the Last n hours or Last n days will allow you to specify the number of hours or days to which the filter is to be restricted.

Selecting Custom will enable the From and To date and time fields. Use the arrow buttons alongside these fields to select a date and time range for the filter. To change the time value, click on the hours or minutes part of the time and then use the up and down arrows to change the hours and minutes respectively.

If you need help to select a new From or To date for the Custom option, please refer to the section entitled "Custom".

Source and destination

These fields allow you to restrict any or all of the given criteria to a single value. An Originator is a trading partner that has sent you one or more files. A Destination is a trading partner to whom you have sent one or more files. "Channel" refers to the logical data groupings you have set up in the ODEX Workflow Manager.

The community field will only be displayed if security is enabled, you are using communities and the user that you are logged on as can access multiple communities.

If you are logged on as a user that is a member of one community, this field is hidden as only files related to one community can be displayed.

Select a community to restrict the visible files to those where the origin or destination company is associated with the selected community.

Status

In this section you can select which status of files you want to see displayed.

Please note that you must select at least one option from this section.

'Current' will display files that are currently being processed by a user-defined workflow.

'Processed' will display files that have completed processing.

'Suspended' will display files that have been suspended by the user i.e. they have been stopped by the user during normal processing and are awaiting user intervention to resume processing.

'New' will display files that have arrived in the system but have not yet begun to be processed.

Security status

In this section you can filter the files to be displayed on the basis of EDIFACT security status. The supported values are listed below:

‘No security’. The file does not use EDIFACT security.

‘Signature required’. The file is on hold, waiting to be signed on the client.

‘Signed’. The file has been signed.

‘Signed (awaiting response)’. The file has been signed and we are awaiting an AUTACK response.

‘Signed (responded – invalid)’. The file has been signed and we have received and AUTACK response indicating that the signature was not valid.

‘Signed (responded – valid)’. The file has been signed and we have received and AUTACK response indicating that the signature was valid.

‘Response AUTACK’. The file contained a response AUTACK.

‘Signed (invalid)’. The file was signed and the signature has been found to be invalid.

‘Signed (valid)’. The file was signed and the signature has been found to be invalid.

Error status

In this section you can select which files will be displayed on the basis of the status of errors they have encountered.

Please note that you must select at least one option from this section.

'Handled' will display files whose errors have been handled by a user-defined error workflow.

'Unhandled' will display files for which no error workflows have been defined.

'None' will display files that have no errors.

Parent status

In this section you can select which files will be displayed on the basis of whether they have been split or not.

Please note that you must select at least one option from this section.

A file containing one or more interchanges can be split into several files, each of which contains one of those interchanges. The original file is then deemed to be a parent, and each file it was split into is deemed to be a child of that parent.

'Unsplit' will display files that have not been split into children. This will include non-EDI files, files that contain a single EDI interchange so cannot be split, files that contain more than one interchange but have not been split, and files that are themselves children and so cannot be split further.

'Parent' will display all those files that have been split into children, but in their original form i.e. still containing their children.

'Child' will display all files that have resulted from being split from their original parent file.

Even though the descriptions above mean that files can belong to more than one parent status, files displayed will never be duplicated.

Show Audit Trail

This option allows you to show or hide the audit trail section at the bottom of the Current Files views. It can be accessed in the following ways:

- From the main menu, using **View >> Show Audit Trail**
- Using the keyboard shortcut **Ctrl + T**

Show All Messages

This option allows you to display all messages in a file as separate rows. This enables unique data in the interchange and message columns to be displayed. It can be accessed in the following ways:

- From the main menu, using **View >> Show All Messages**
- Using the keyboard shortcut **Ctrl + M**

Workflow Files – Actions

This section lists all the actions that you can perform manually on individually selected files or, in some cases, audit lines.

Please note that any actions you perform manually on files in the Workstation will NOT be listed in the Audit Trail in the lower section of the screen.

Workflow File Details

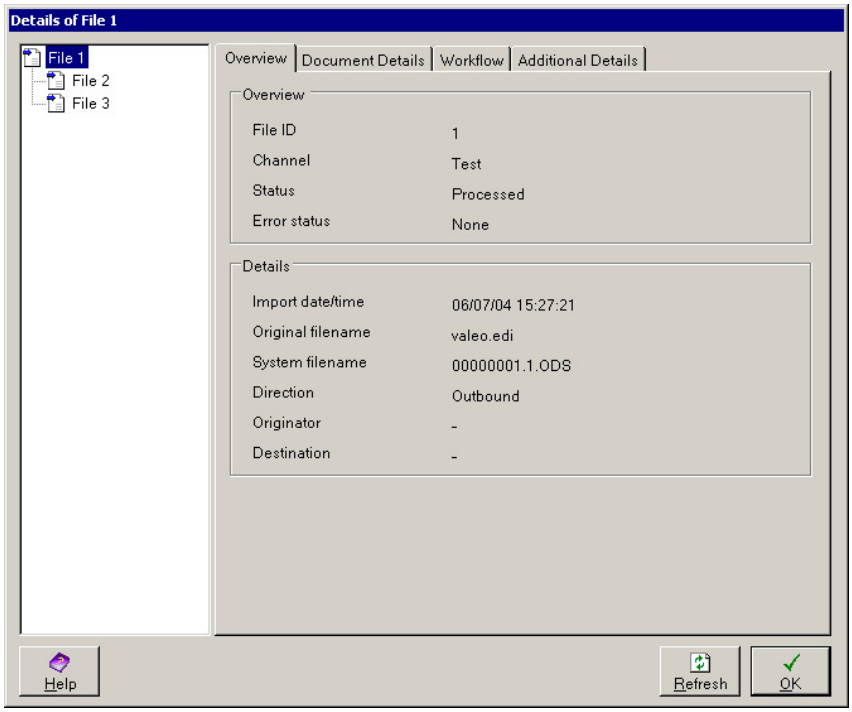
The Workflow File Details option allows you to view all the available details about any workflow file. First select the file with a single left-mouse click.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Workflow File Details**
- Double-clicking on a file line in the upper list view
- Using the keyboard shortcut **Alt+A+W**
- Using the 'Workflow File Details' item on the context menu (right mouse click)

Any of these methods will bring up the File Details dialog. The File Details dialog has two forms, depending on whether the file is associated with a split file or not.

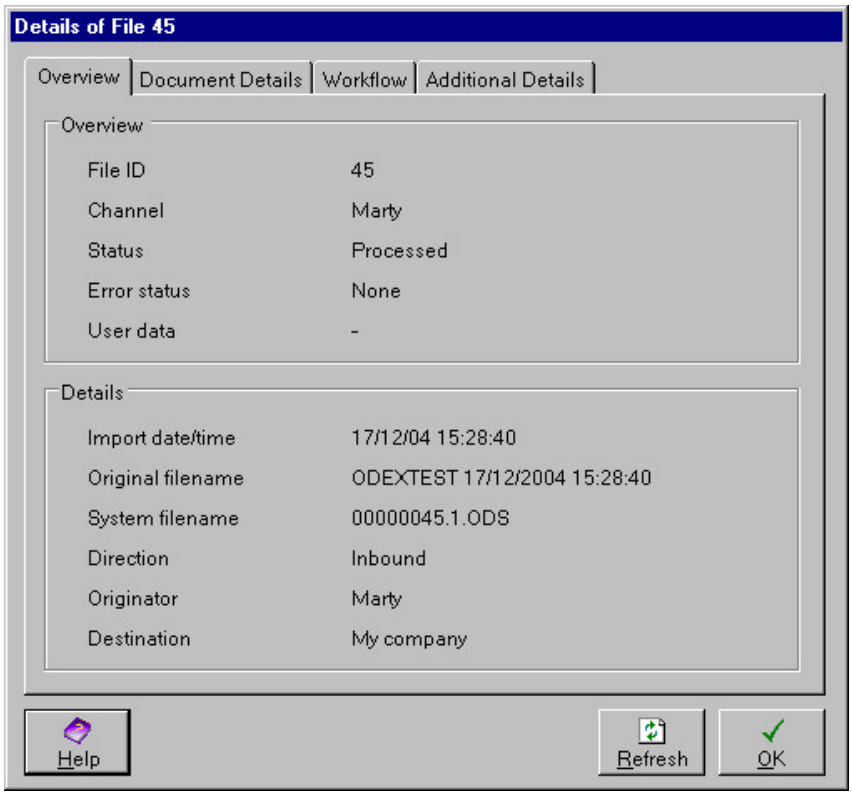
If the file is associated with a split file (i.e. it is either the original file containing two or more EDI interchanges, or it is one of the files into which the original file has been split), the dialog will look like the one below.



As you can see, for split files the dialog has a tree view on the left-hand side, showing the original file at the top (in this case File 3) and the child files below (Files 4 and 5 in our example).

For simple files, the dialog will look just the same but without the tree view.

The page tabs in each case have identical contents, as described below.



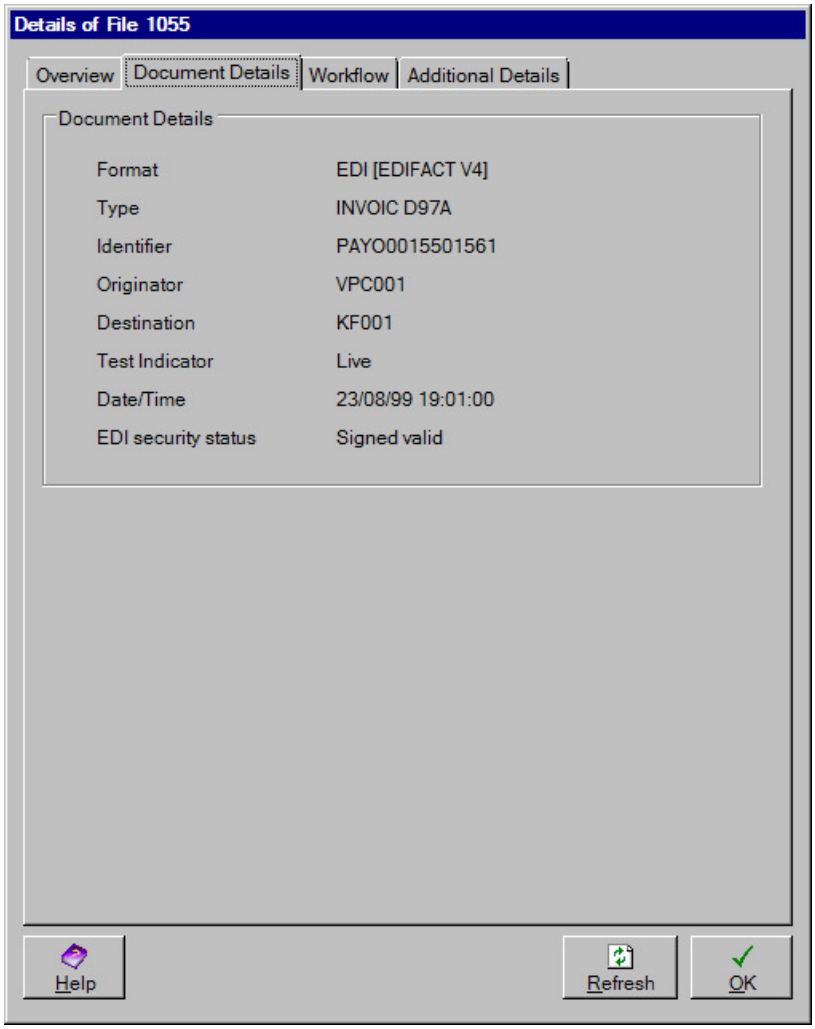
The File Details dialog consists of four pages: Overview, Document Details, Workflow and Additional Details. Together, these pages provide all the known information about a file.

The Overview page, shown above, shows which channel the file is being processed in and the file's status, together with other file information.

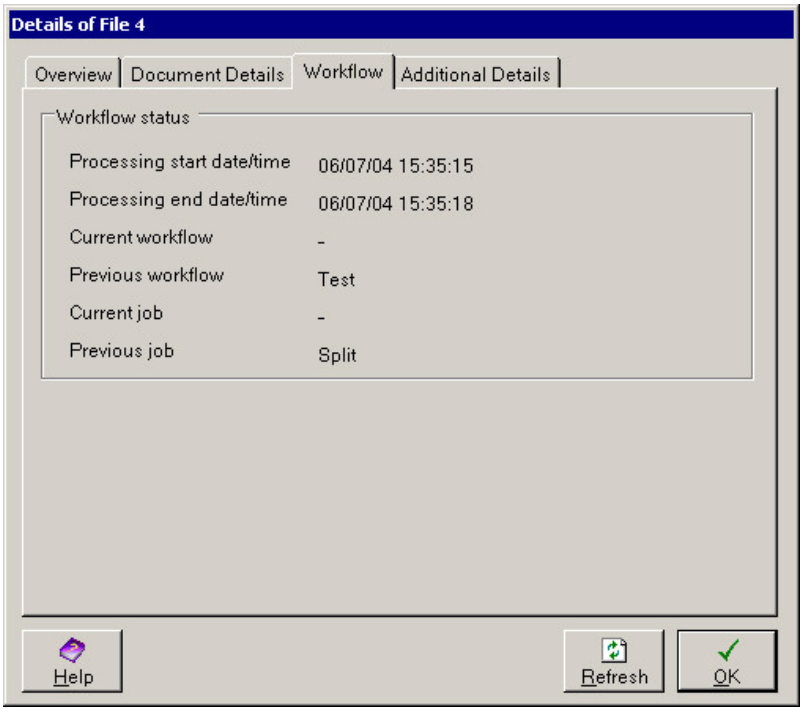
The Document Details page, shown below, is only relevant to EDI files and recognised non-EDI files (such as SAP files). This page gives the analysis-specific details of the file, such as the codes of the originator and destination and the format and type of the file.

The Test Indicator shows whether the file has a status of Live or Test.

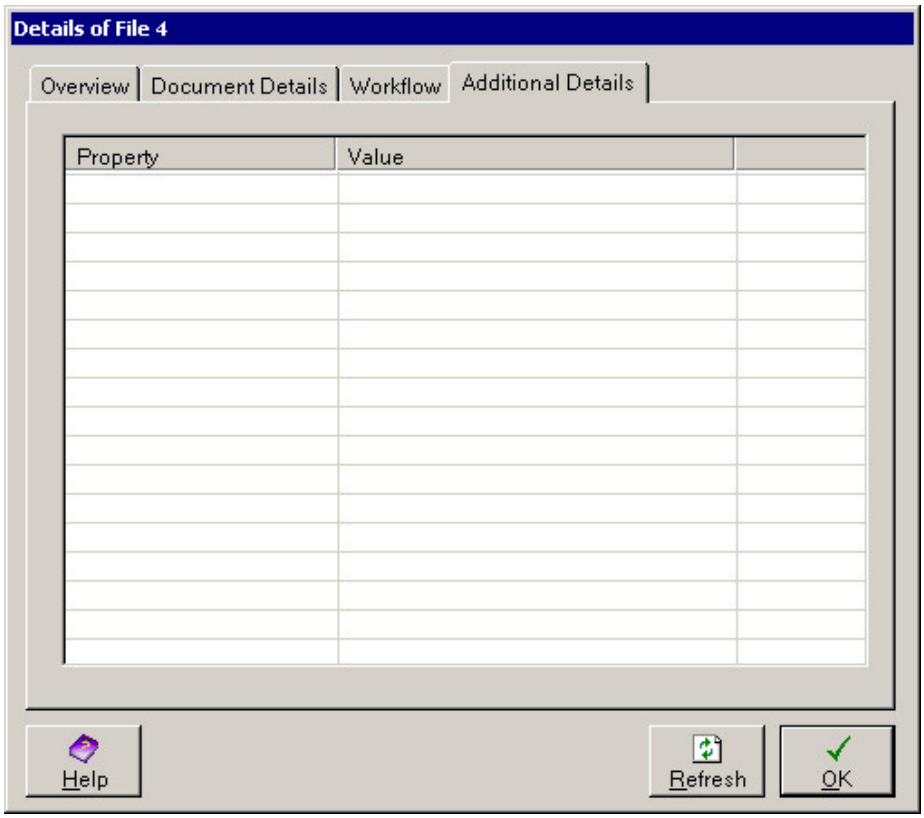
The EDI security status indicates the security status of the file where it includes EDIFACT security.



The Workflow page, shown below, displays information about the jobs that have been carried out on the file. Current workflow and Current job will only be shown if the file is still being processed.



The Additional Details page, shown below, shows a list of properties associated with the file, and the value of each property. These fields are currently only used for SAP files and will contain information about the IDoc in the file.



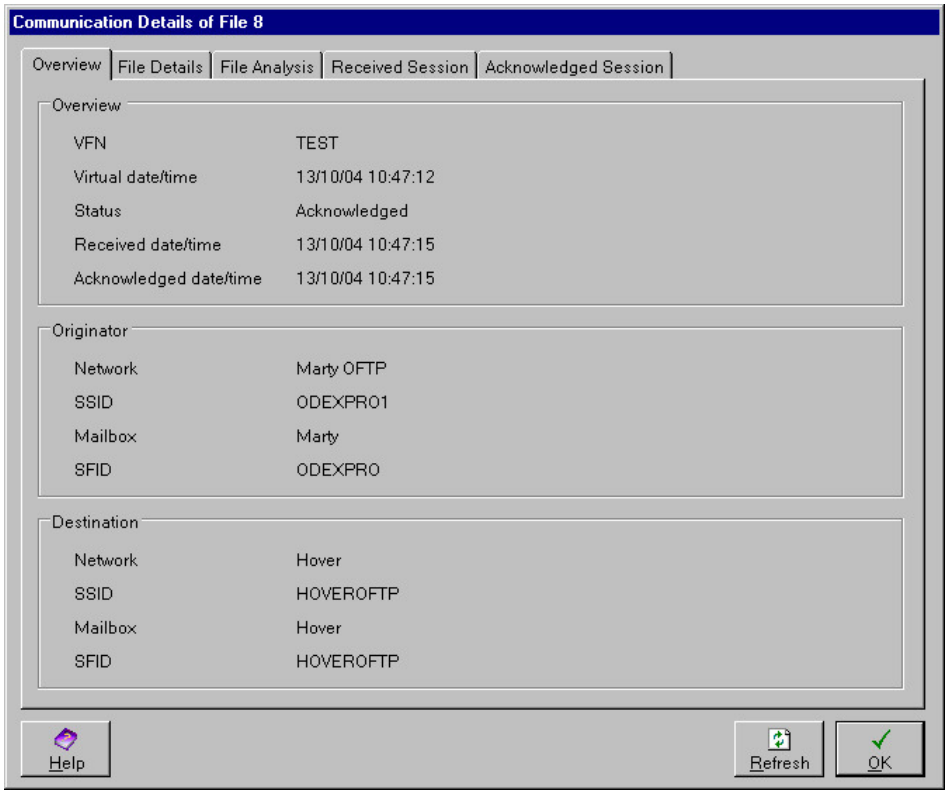
Comms Details

The Comms Details option allows you to view all the available communication details about any file. First select the file with a single left-mouse click.

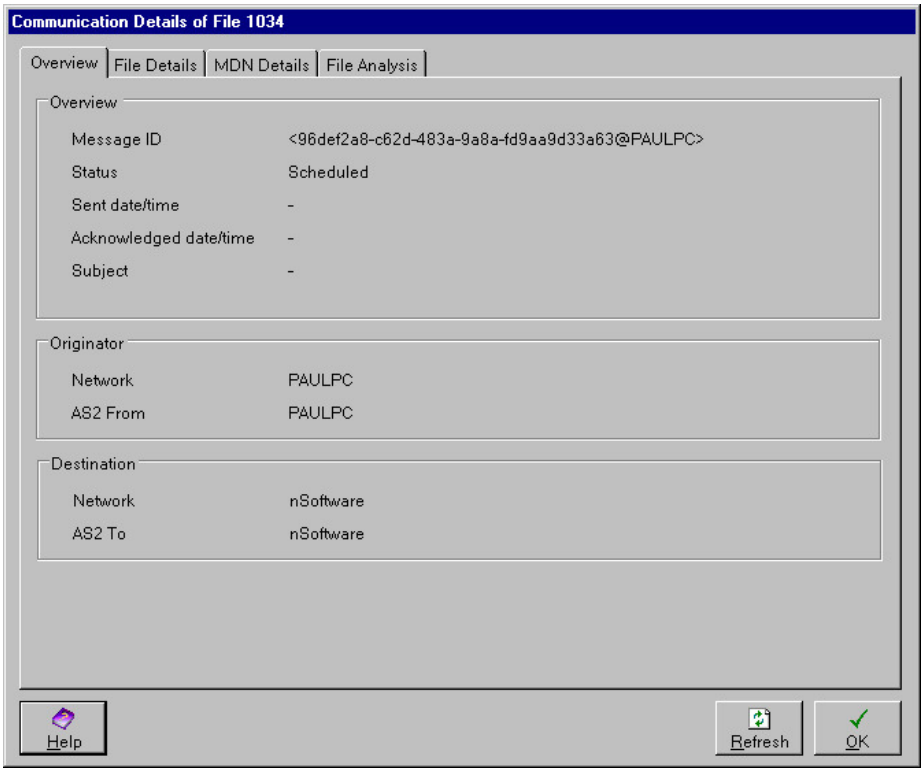
This option can be accessed in the following ways:

- From the main menu, using **Actions >> Comms Details**
- Using the keyboard shortcut **Alt+A+F**
- Using the 'Comms Details' item on the context menu (right mouse click)

Any of these methods will bring up a dialog similar to the one below, for an OFTP file:



or similar to the one below, for an AS2 file:



The Comms Details dialog consists of up to seven pages, depending on the type of comms session associated with the file. The Overview, File Details and File Analysis pages will always be present. In addition, there may be a VF Description, Received Session, Scheduled Session or Sent Session page, and an Acknowledged Session page. For an AS2 file, there will be an MDN Details page. Together, these pages provide all the known information relating to the communication details of the selected file.

If you have extracted a file that has been received via a communications session, you will be able to see the date and time at which it was extracted, and the location it was extracted to, on the File Details page tab, in the File Status section.

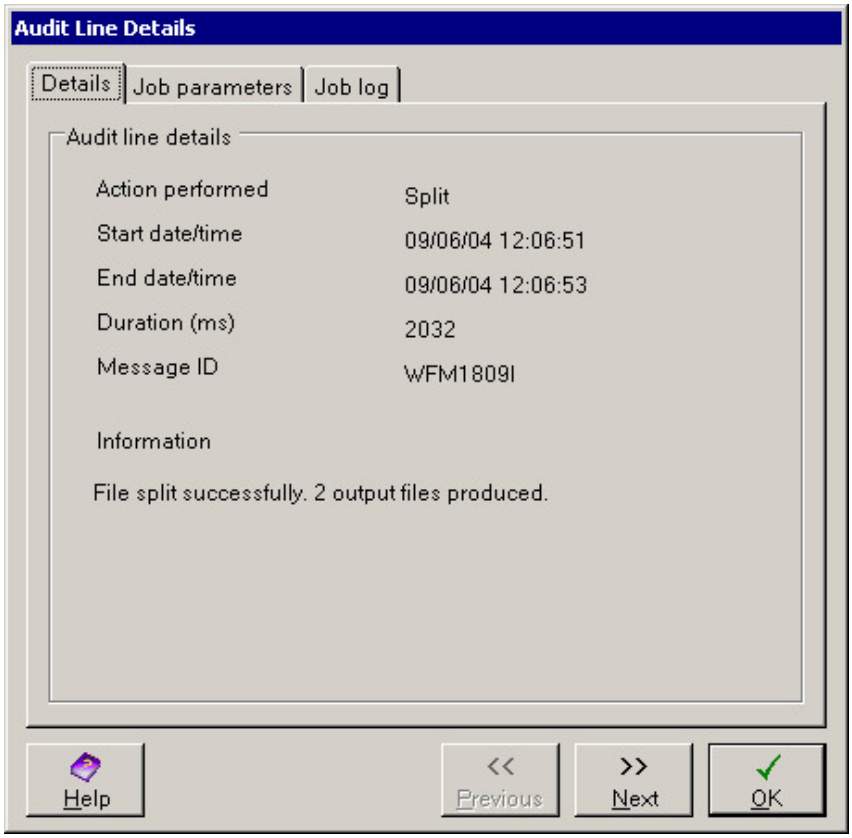
Audit Details

The Audit Details option allows you to view the available details about any line in the audit log. First select the audit line with a single left-mouse click.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Audit Details**
- Double-clicking on an audit line in the lower list view
- Using the keyboard shortcut **Alt+A+A**
- Using the 'Audit Details' item on the context menu (right mouse click)

Any of these methods will bring up the following dialog:



The Details page provides all the known information about the selected audit line.

If the audit line represents a map job and there were validation errors then the information section will include a list of the errors.

The **Previous** and **Next** buttons at the bottom of the dialog allow you to step through all the Audit Lines associated with the selected file. If there is only one Audit Line associated with the file, then both the **Previous** and **Next** buttons will be disabled.

The Job parameters page lists all the parameters that were provided for the action to be performed.

If the Job which generated the audit line produced a job log, this will be accessible on a further page tab, entitled Job Log.

File Analysis

The File Analysis option allows you to view the analysis details for any EDI file or IDoc file. First select the file with a single left-mouse click.

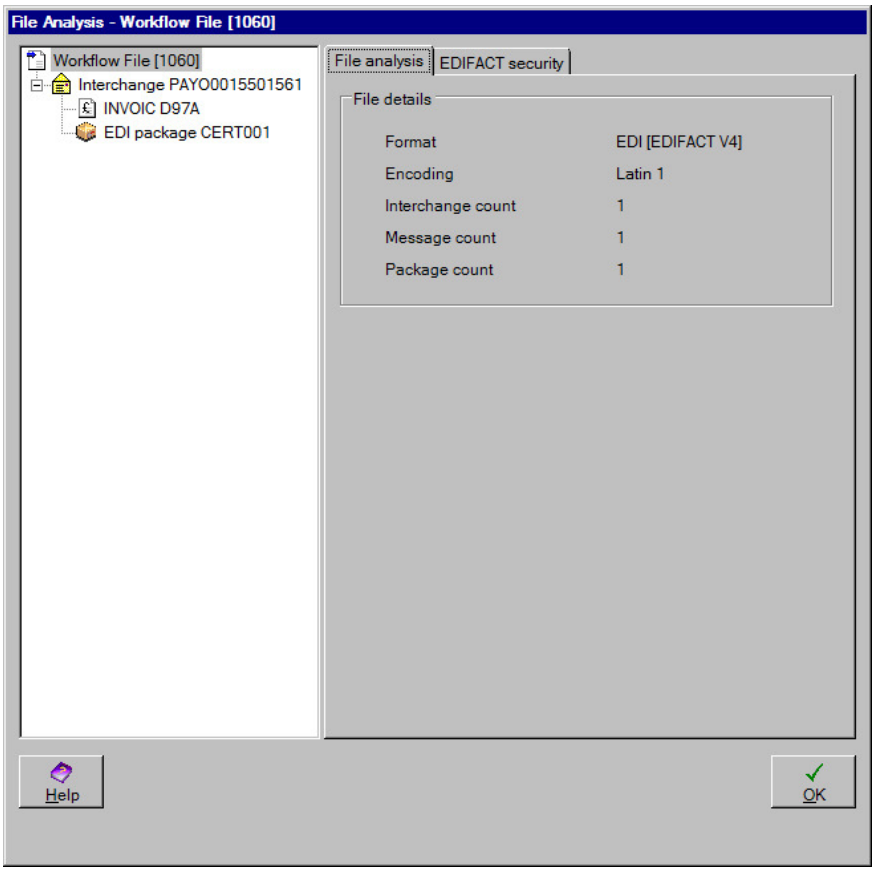
This option can be accessed in the following ways:

- Select the **Actions >> File Analysis** main menu option
- For Workflow files, using the keyboard shortcut **Alt+A+F**
- For Comms files, using the keyboard shortcut **Alt+A+L**
- Using the 'File Analysis' item on the context menu (right mouse click)

Any of these methods will bring up a dialog containing the file details, together with a tree view on the left-hand side that shows a hierarchical representation of the file split into its component parts.

File Analysis is applicable only to EDI files and IDoc files. The dialogs and descriptions below refer to EDI file analysis. IDocs do not have a hierarchical structure.

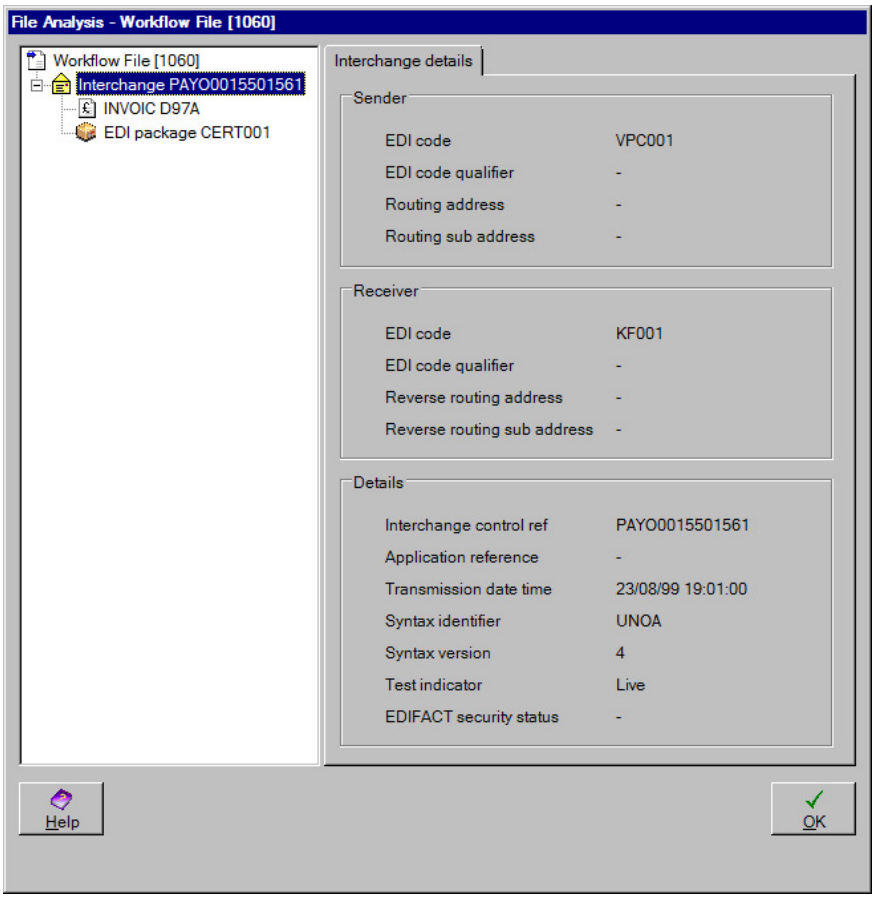
Each node below the file node represents an interchange (intermediate hierarchical level) or a message or package (lowest hierarchical level).



The example above shows a file containing one interchange, one message and one package in that interchange.

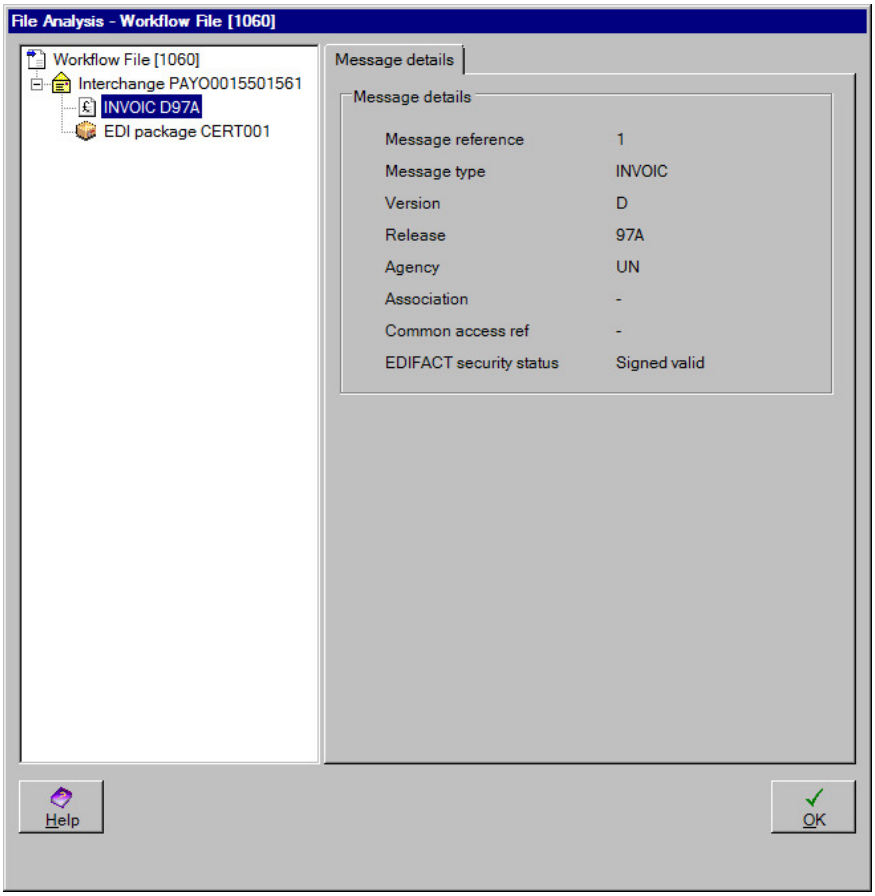
Interchanges will be shown with a plus or minus sign on their left. Click on the plus sign to see the messages and/or packages in the interchange. Click on the minus sign to hide these.

Highlight an interchange node to see its details on the right-hand side of the dialog, as shown below.



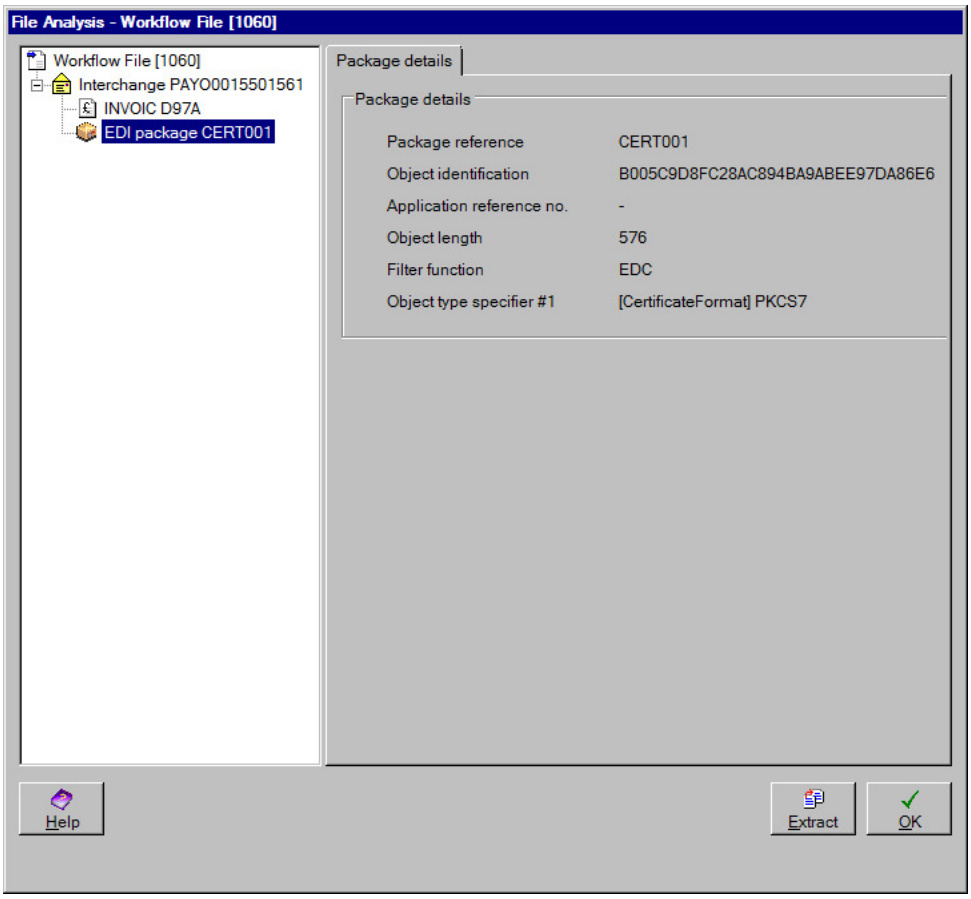
This shows the details from the UNB segment of the selected interchange.

Highlight a message node to see its details on the right-hand side of the dialog, as shown below.



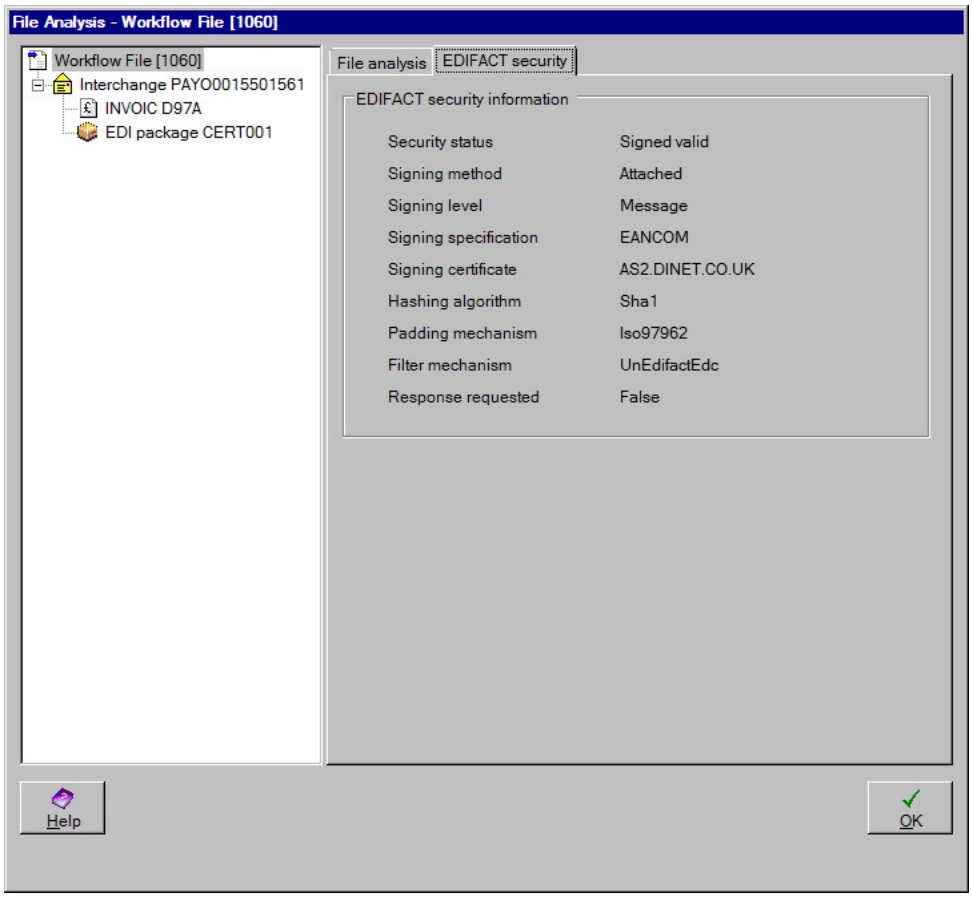
This shows the details from the UNH segment of the selected message.

Highlight a package node to see its details on the right-hand side of the dialog, as shown below.



This shows the details from the UNP segment of the selected package. The extract button is shown whenever a package is displayed. Click this button to extract the packaged object to a location on disk.

Where there is EDIFACT security information available as part of the file analysis, this is shown on a separate tab when the file node is selected in the tree view, as shown below:



Archive

The Archive option allows you to archive a selected file. First select the file with a single left-mouse click.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Archive**
- Using the keyboard shortcut **Alt+A+H**
- Using the 'Archive' item on the context menu (right mouse click)

Any of these methods will archive the selected file. Works on any file that is not yet archived.

Delete

The Delete option allows you to delete a selected file. First select the file with a single left-mouse click.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Delete**
- Using the keyboard shortcut **Alt+A+D**

- Using the 'Delete' item on the context menu (right mouse click)

Any of these methods will display an “Are you sure” dialog. If you click **Yes**, ODEX will delete the file.

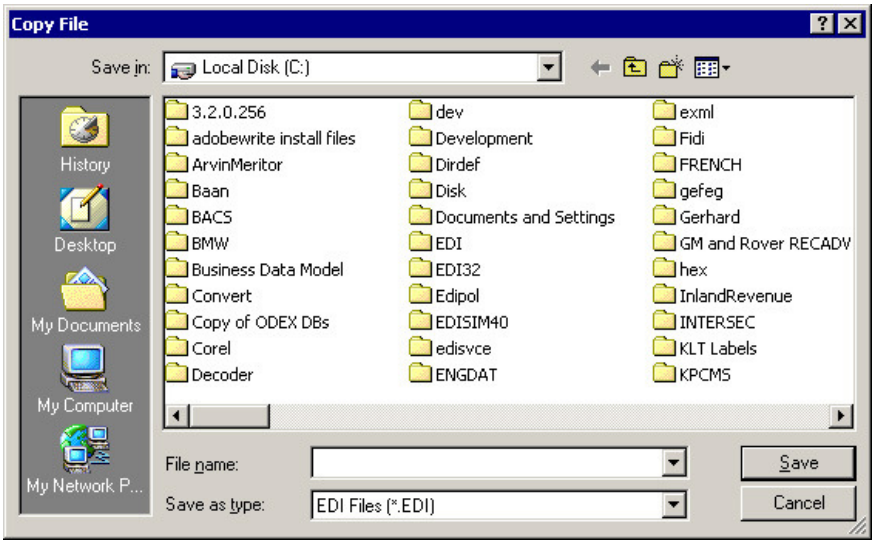
Extract

The Extract option allows you to extract a selected file into a new location, leaving the original in its original location. First select the file with a single left-mouse click.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Extract**
- Using the keyboard shortcut **Alt+A+X**
- Using the 'Extract' item on the context menu (right mouse click)

Any of these methods will bring up the following dialog:

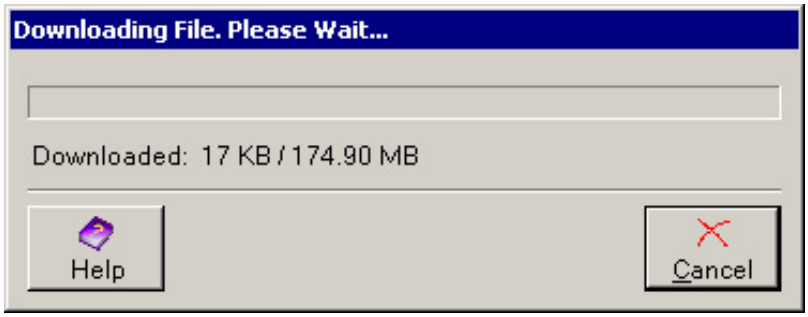


This dialog works in the same way as the Windows Browse dialog.

- Select the directory in which to save the file
- Type the new name of the file in the File name field. Omit the file extension unless you choose All Files (*.*) in the Save as type field.
- Use the dropdown arrow alongside the Save as type field to select a file type for this file (the default type shown in this field will match the type of file you are extracting).

Extracting a large file

If the file you are extracting is very large, you may see the following dialog during the time it takes to download it.



If you do not want to wait for the extraction to complete, you may click the **Cancel** button. This will cancel the Extract operation and return you to the Workstation view.

Extract Pre-Job File

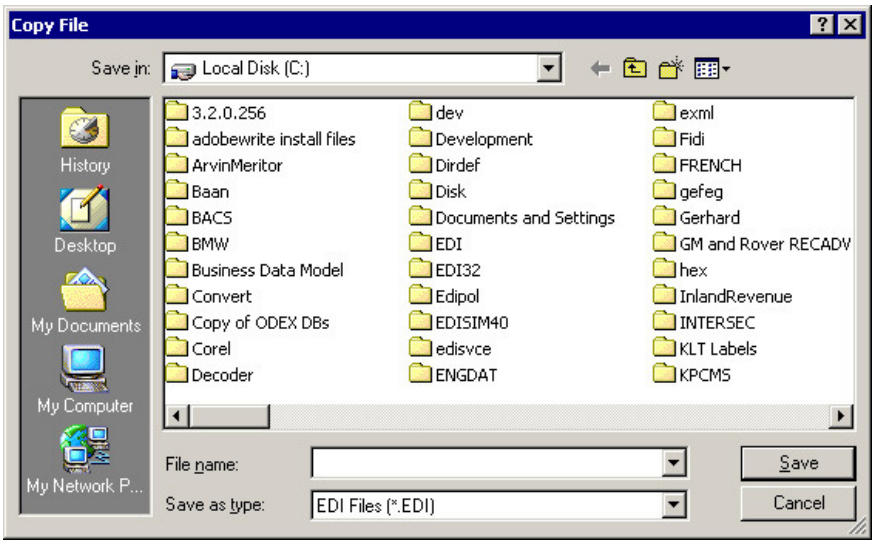
This option works on the Audit Line section.

The Extract Pre-Job File option allows you to extract a file, *as it existed before a specific audit line job was performed on it*, into a new location, leaving the original in its original location. First select the audit line with a single left-mouse click.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Extract Pre-Job File**
- Using the keyboard shortcut **Alt+A+T**
- Using the 'Extract Pre-Job File' item on the context menu (right mouse click)

Any of these methods will bring up the following dialog:

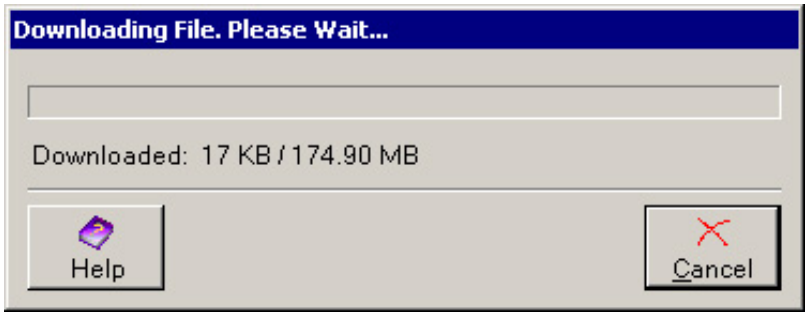


This dialog works in the same way as the Windows Browse dialog.

- Select the directory in which to save the file
- Type the new name of the file in the File name field. Omit the file extension unless you choose All Files (*.*) in the Save as type field.
- Use the dropdown arrow alongside the Save as type field to select a file type for this file (the default type shown in this field will match the type of file you are copying).

Extracting a large pre-job file

If the file you are extracting is very large, you may see the following dialog during the time it takes to download it.



If you do not want to wait for the extraction to complete, you may click the **Cancel** button. This will cancel the Extract operation and return you to the Workstation view.

Open With

The Open With option allows you to open a selected file using an application of your choice. First select the file with a single left-mouse click.

This option can be accessed in the following ways:

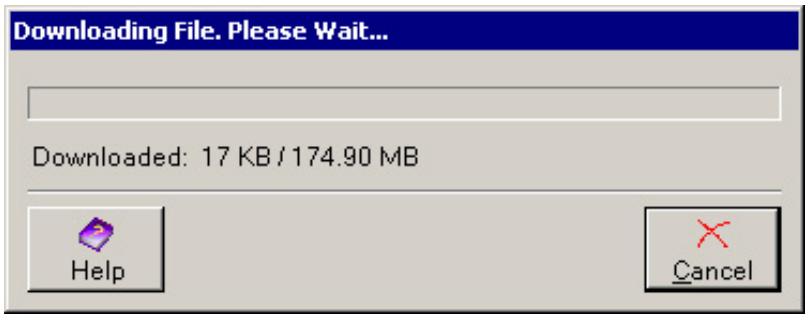
- From the main menu, using **Actions >> Open With**
- Using the keyboard shortcut **Alt+A+O**
- Using the 'Open With' item on the context menu (right mouse click)

Any of these methods will offer you a sub-menu containing applications with which to open the file, depending on what applications you have installed and used before. You can also use the Browse option it offers, to select an application that is not in the list.

If no applications have been used before, it will simply start up the "Open With" dialog. The “Open With” dialog is just a browse dialog for *.exe programs. When you select an application to open with, the file is retrieved from the server (creating a temporary copy locally) and then opened with the specified application.

Opening a large file

If the file you are opening is very large, you may see the following dialog during the time it takes to download it.



If you do not want to wait for the Open operation to complete, you may click the **Cancel** button. This will cancel the Open operation and return you to the Workstation view.

Open Pre-Job File With

This option works on the Audit Line section.

The Open Pre-Job File With option allows you to open a file, *as it existed before a specific audit line job was performed on it,* using an application of your choice. First select the audit line with a single left-mouse click.

This option can be accessed in the following ways:

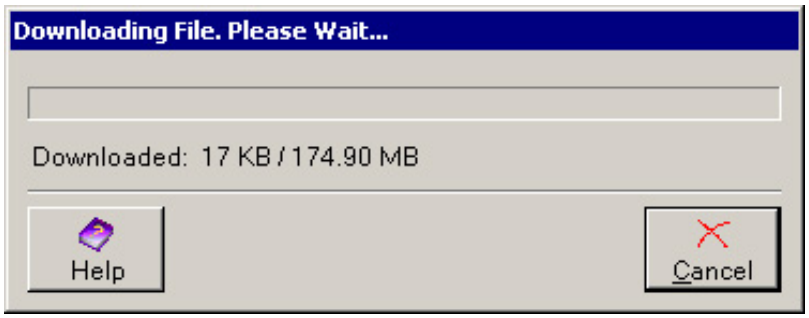
- From the main menu, using **Actions >> Open Pre-Job File With**
- Using the keyboard shortcut **Alt+A+P**
- Using the 'Open Pre-Job File With' item on the context menu (right mouse click)

Any of these methods will offer you a sub-menu containing applications with which to open the file, depending on what applications you have installed and used before. You can also use the Browse option it offers, to select an application that is not in the list.

If no applications have been used before, it will simply start up the "Open With" dialog. The “Open With” dialog is just a browse dialog for *.exe programs. When you select an application to open with, the file is retrieved from the server (creating a temporary copy locally) and then opened with the specified application.

Opening a large pre-job file

If the file you are opening is very large, you may see the following dialog during the time it takes to download it.



If you do not want to wait for the Open operation to complete, you may click the **Cancel** button. This will cancel the Open operation and return you to the Workstation view.

Submit and Resubmit Overview

There are 4 different submit and resubmit options, which are described.

Submit

The Submit option allows you to place a file manually into a workflow channel.

Submit Workflow File

The Submit Workflow File option allows you to place a selected processed workflow file manually into a workflow channel.

This option takes the file as it is now, with all of its audit lines and data and submits it to the Workflow Manager. This will cause an audit line to be added for the re-submission, and the file will be marked as **Current** again. The file keeps the same ID.

Resubmit

The Resubmit option allows you to resubmit the selected processed workflow files manually to a workflow channel.

The current underlying data files (as they are at the end of current processing) will be copied and submitted to the Workflow Manager as brand new workflow files with new IDs and no current audit lines.

Resubmit Original

The Resubmit Original option allows you to resubmit a selected processed workflow file manually to a workflow channel.

The original workflow file will be copied and submitted to the Workflow Manager as a brand new workflow file with a new ID and no current audit lines.

Submit

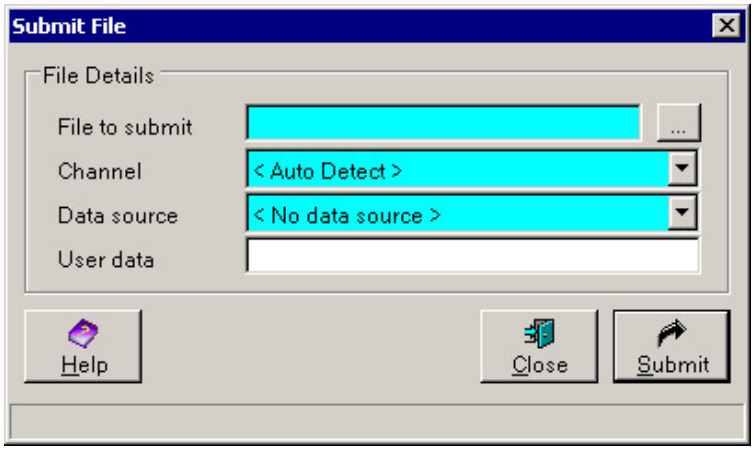
The Submit option allows you to place a file manually into a workflow channel. You can either choose a specific channel yourself, or allow ODEX to select the first channel which meets the criteria for the selected file.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Submit**
- Using the keyboard shortcut **Alt+A+U**
- Using the toolbar icon 

There is no context menu item for this option.

Any of these methods will bring up the following dialog:



Use the Browse button to select the file to be submitted (or type in the full path and filename).

In the Channel field, select the channel that this file should be processed by. Alternatively, you can leave the Channel field set to < Auto Detect > and ODEX will select the first channel which meets the criteria for the selected file.

In the Data source field, select the data source for this file. If there is no data source, leave the field set to < No data source >.

The User data field may be used for any information you want to keep with the file. The User data stays with the file for its lifetime.

Click the **Submit** button to submit the file.

If the submission is successful, you will see the message "File submitted successfully" appear at the bottom of the dialog.

The dialog will remain open, allowing you to submit more files if required.

Click the **Close** button when you have finished.

Submit Workflow File

The Submit Workflow File option allows you to place a selected processed workflow file manually into a workflow channel.

This option takes the file as it is now, with all of its audit lines and data and submits it to the Workflow Manager. This will cause an audit line to be added for the re-submission, and the file will be marked as **Current** again. The file keeps the same ID.

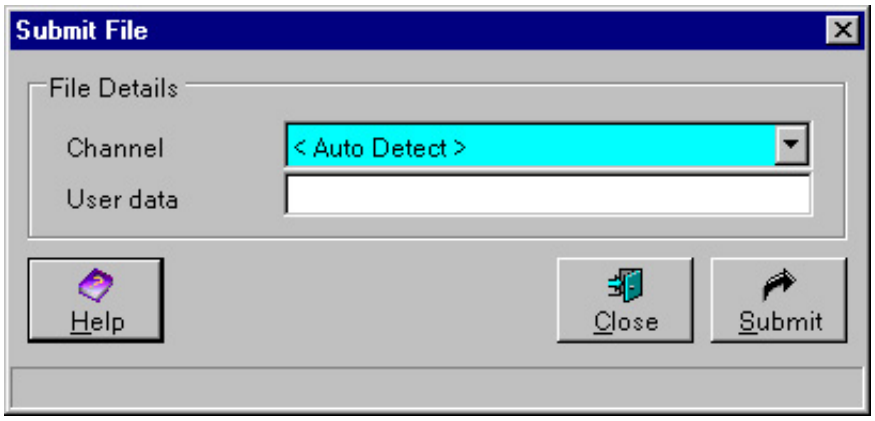
You can either choose a specific channel yourself, or allow ODEX to select the first channel which meets the criteria for the selected file. First select the file with a single left-mouse click.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Submit Workflow File**
- Using the keyboard shortcut **Alt+A+K**
- Using the 'Submit Workflow File' item on the context menu (right mouse click)

There is no toolbar icon for this option.

Any of these methods will bring up the following dialog:



In the Channel field, select the channel that this file should be processed by. Alternatively, you can leave the Channel field set to < Auto Detect > and ODEX will select the first channel which meets the criteria for the selected file.

The User data field may be used for any information you want to keep with the file. The User data stays with the file for its lifetime.

Click the **Submit** button to submit the file.

If the submission is successful, you will see the message "File submitted successfully" appear at the bottom of the dialog.

The dialog will remain open, allowing you to submit more files if required.

Click the **Close** button when you have finished.

Resubmit

The Resubmit option allows you to resubmit a selected processed workflow file manually to a workflow channel.

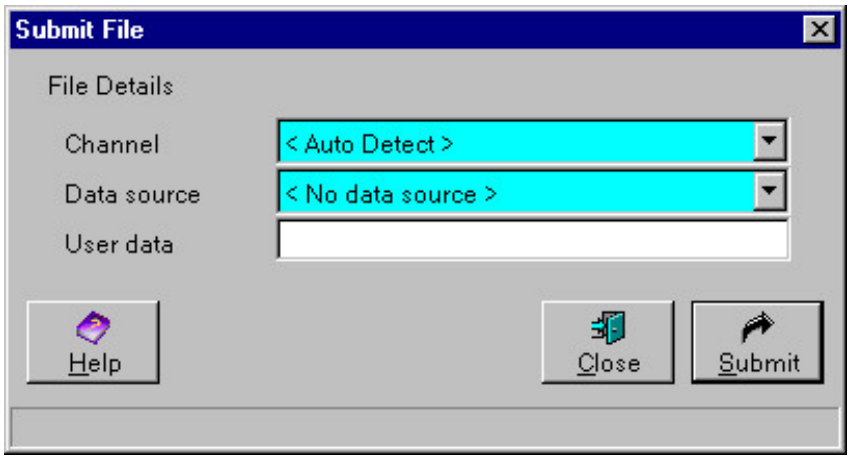
The current underlying data file (as it is at the end of current processing) will be copied and submitted to the Workflow Manager as a brand new workflow file with a new ID and no current audit lines.

You can either choose a specific channel yourself, or allow ODEX to select the first channel which meets the criteria for the selected file. This option can be accessed in the following ways:

- From the main menu, using **Actions >> Resubmit**
- Using the keyboard shortcut **Alt+A+E**
- Using the 'Resubmit' item on the context menu (right mouse click)

There is no toolbar icon for this option.

Any of these methods will bring up the following dialog:



In the Channel field, select the channel that this file should be processed by. Alternatively, you can leave the Channel field set to < Auto Detect > and ODEX will select the first channel which meets the criteria for the selected file.

In the Data source field, select the data source for this file. If there is no data source, leave the field set to < No data source >.

The User data field may be used for any information you want to keep with the file. The User data stays with the file for its lifetime.

Click the **Submit** button to submit the file.

If the submission is successful, you will see the message "File submitted successfully" appear at the bottom of the dialog.

The dialog will remain open, allowing you to submit more files if required.

Click the **Close** button when you have finished.

Resubmit Original

The Resubmit Original option allows you to resubmit a selected processed workflow file manually to a workflow channel.

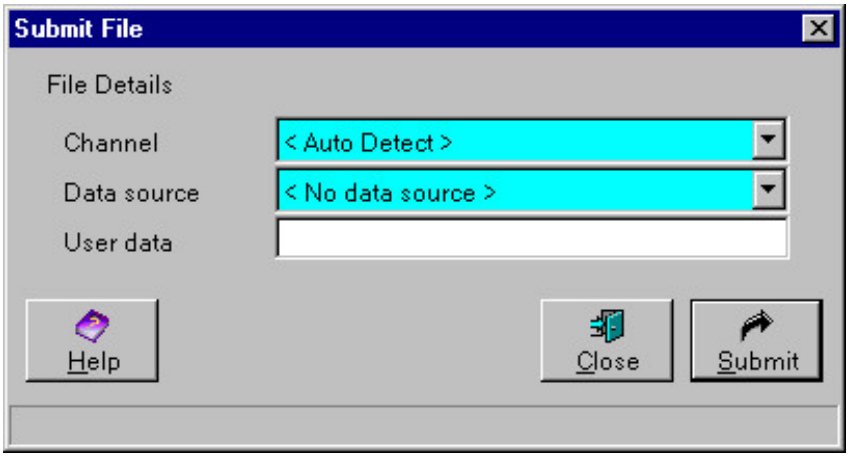
The original workflow file will be copied and submitted to the Workflow Manager as a brand new workflow file with a new ID and no current audit lines.

You can either choose a specific channel yourself, or allow ODEX to select the first channel which meets the criteria for the selected file. This option can be accessed in the following ways:

- From the main menu, using **Actions >> Resubmit Original**
- Using the 'Resubmit Original' item on the context menu (right mouse click)

There is no toolbar icon or keyboard shortcut for this option.

Any of these methods will bring up the following dialog:



In the Channel field, select the channel that this file should be processed by. Alternatively, you can leave the Channel field set to < Auto Detect > and ODEX will select the first channel which meets the criteria for the selected file.

In the Data source field, select the data source for this file. If there is no data source, leave the field set to < No data source >.

The User data field may be used for any information you want to keep with the file. The User data stays with the file for its lifetime.

Click the **Submit** button to submit the file.

If the submission is successful, you will see the message "File submitted successfully" appear at the bottom of the dialog.

The dialog will remain open, allowing you to submit more files if required.

Click the **Close** button when you have finished.

Export to SAP

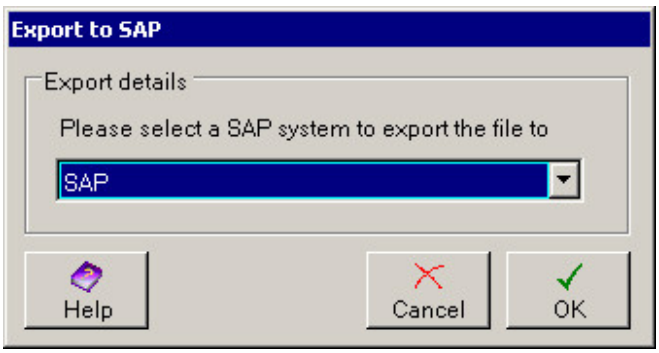
The Export to SAP option allows you to export a file to your SAP system. First select the file with a single left-mouse click.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Export to SAP**
- Using the 'Export to SAP' item on the context menu (right mouse click)

There is no keyboard shortcut or toolbar icon for this option.

Any of these methods will bring up the following dialog:



Use the dropdown arrow to select the SAP system to which you want to export the file, then click **OK**. You will be returned to the main Workstation screen.

Requeue SAP status records

The Requeue SAP status records option allows you to requeue any failed status records to the SAP system. First select the file with a single left-mouse click.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Requeue SAP status records**
- Using the 'Requeue SAP status records' item on the context menu (right mouse click)

There is no keyboard shortcut or toolbar icon for this option.

If there are any failed status records associated with this file, they will be requeued.

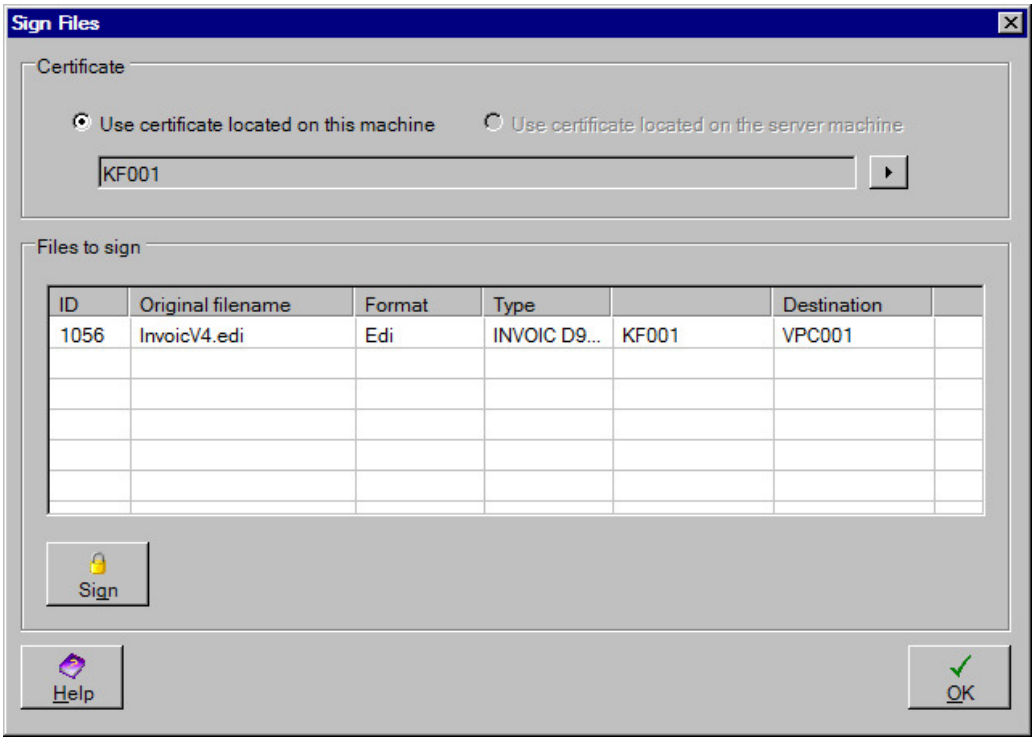
Sign EDI

The Sign EDI workflow job has an option to allow signing of data on the client. This means that instead of workflow files coming into the job being signed straight away on the server, they are held on the job to be signed in the Workstation.

The Sign EDI option allows you to sign held files and release them back to the workflow manager. It can be accessed in the following ways:

- From the main menu, using **Actions >> Sign EDI** .
- Using the **Sign EDI** item on the context menu (right mouse click).

You can select multiple files to sign, but they must all be EDIFACT files with a workflow status of 'Hold' and a security status of 'Awaiting signature'. When you select the option the following dialog will be shown:



The dialog lists the files selected for signing. You cannot change the files to be signed at this point. To change the selection you need to dismiss the dialog and make a new selection from the workflow files view.

If the client is running on the same machine as the server then the certificate option displayed is to select a certificate from the current machine. If the client

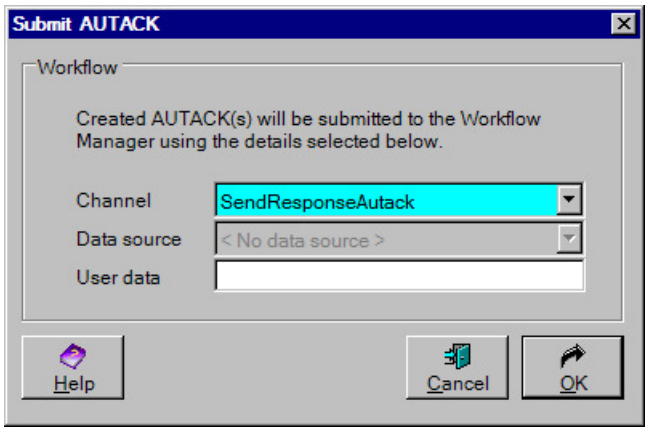
and server are running on different machine the option to pick a certificate from the server is enabled. Once you have selected a certificate, click the **Sign** button. The files shown will be signed one-at-a-time and released from the 'Hold' status. Note that if you have selected the option to release in sequence, some files may still be held after signing if older files are still held too.

Create and submit AUTACK

The 'Create and submit AUTACK' option allows you to create an AUTACK response message in respect of a signed EDI file and submit it to the Workflow Manager. It can be accessed in the following ways:

- From the main menu, using **Actions >> Create and submit AUTACK**.
- Using the **Create and submit AUTACK** item on the context menu (right mouse click).

You can select multiple files, but they must all be EDIFACT files with a digital signature that have been verified in either the 'Verify Signed EDI' or the 'Process AUTACK' workflow job. When you select the option the following dialog will be shown:



Select either a channel or data source, enter optional user data, and click OK to create the AUTACK response and submit it to the Workflow Manager. Typically you will submit it to a channel that contains a job to schedule to the file by EDI code.

Error Files

The error files page is used in exactly the same way as the inbound and outbound files pages, but it displays details of files that contain errors detected by the ODEX software.

When you highlight an error file (whether on the Error Files page or elsewhere) the Audit Line related to the error may tell you to see the Job Log for more information. The Job Log is accessible as follows:

- Right-click on the Audit Line which tells you to look at the job log
- Select Audit Details from the context menu
- Open the Job Log page of the dialog that is shown.

For most details of how to use the error files page, please refer to the "Workflow Files – View option" and the "Workflow Files – Actions" section. Any differences will be mentioned there.

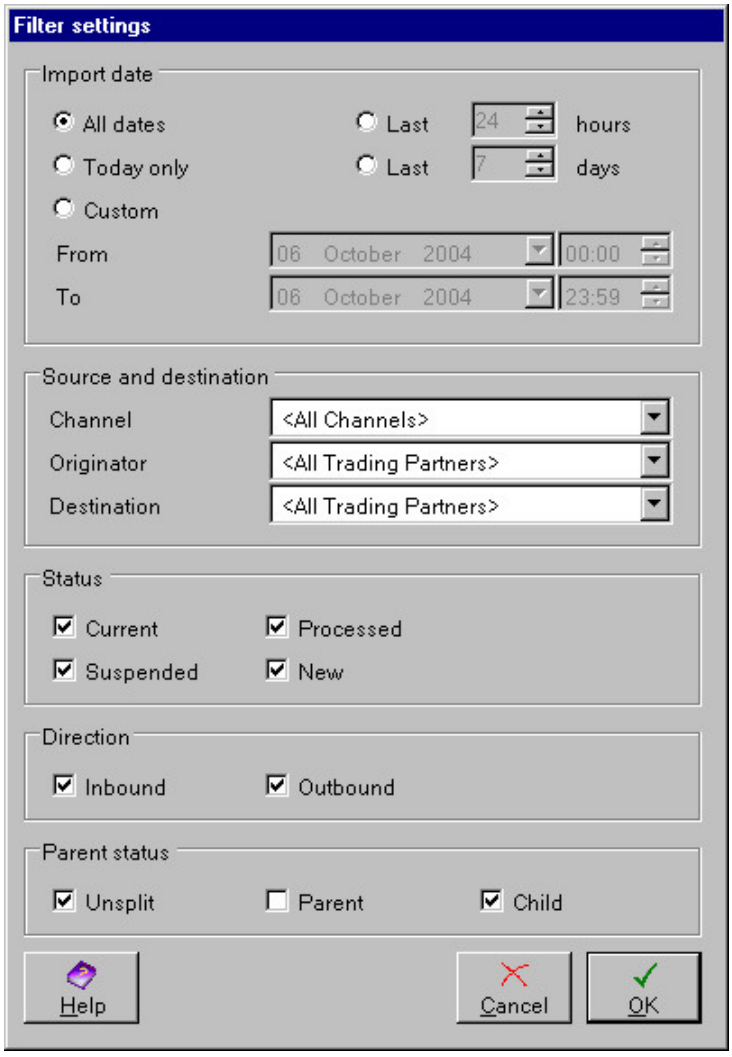
This section contains details of the Error Files Filter options.

Error Files Filter

The Error Files Filter option allows you to select specific criteria for the files you want to see displayed in the data area. It can be accessed in the following ways:

- From the main menu, using **View >> Filter**
- Using the keyboard shortcut **Ctrl + F**
- Using the toolbar icon 

Any of these methods will bring up the dialog shown below.



Please bear in mind that filtering may result in no entries being shown in the data area if no files meet the filter criteria.

Import date

The default Import date setting for the filter is All dates. To limit the dates, select one of the other radio buttons.

Selecting "Today only" means that only files imported today will be displayed.

Selecting the Last n hours or Last n days will allow you to specify the number of hours or days to which the filter is to be restricted.

Selecting "Custom" will enable the From and To date and time fields. Use the arrow buttons alongside these fields to select a date and time range for the filter.

If you need help to select a new From or To date for the Custom option, please refer to the section entitled "Custom".

Source and destination

These fields allow you to restrict any or all of the given criteria to a single value. An Originator is a trading partner that has sent you one or more files. A Destination is a trading partner to whom you have sent one or more files. "Channel" refers to the logical data groupings you have set up in the ODEX Workflow Manager.

The community field will only be displayed if security is enabled, you are using communities and the user that you are logged on as can access multiple communities.

If you are logged on as a user that is a member of one community, this field is hidden as only files related to one community can be displayed.

Select a community to restrict the visible files to those where the origin or destination company is associated with the selected community.

Status

In this section you can select which status of files you want to see displayed.

Please note that you must select at least one option from this section.

'Current' will display files that are currently being processed by a user-defined workflow.

'Processed' will display files that have completed processing.

'Suspended' will display files that have been suspended by the user i.e. they have been stopped by the user during normal processing and are awaiting user intervention to resume processing.

'New' will display files that have arrived in the system but have not yet begun to be processed.

Direction

In this section you can select which files will be displayed on the basis of their direction.

Please note that you must select at least one option from this section.

'Inbound' will display files that have been sent to you by your trading partners.

'Outbound' will display files that have been or will be sent by you to your trading partners.

Parent status

In this section you can select which files will be displayed on the basis of whether they have been split or not.

Please note that you must select at least one option from this section.

A file containing one or more interchanges can be split into several files, each of which contains one of those interchanges. The original file is then deemed to be a parent, and each file it was split into is deemed to be a child of that parent.

'Unsplit' will display files that have not been split into children. This will include non-EDI files, files that contain a single EDI interchange so cannot be split, files

that contain more than one interchange but have not been split, and files that are themselves children and so cannot be split further.

'Parent' will display all those files that have been split into children, but in their original form i.e. still containing their children.

'Child' will display all files that have resulted from being split from their original parent file.

Even though the descriptions above mean that files can belong to more than one parent status, files displayed will never be duplicated.

Archived Files

The archived files page is used in exactly the same way as the current files page, but it displays details of files that have been archived, either automatically by the workflow manager or manually by a user.

Some of the menu options available for current files are not available for archived files, but otherwise the menu system works in the same way. The dialogs for the Filter and Columns options have different contents, but these are simply cut-down versions of the dialogs for current files.

Therefore, please refer to the "Workflow Files – View option" section or the "Workflow Files – Actions" section for details of how to use the archived files options. Any differences will be mentioned there.

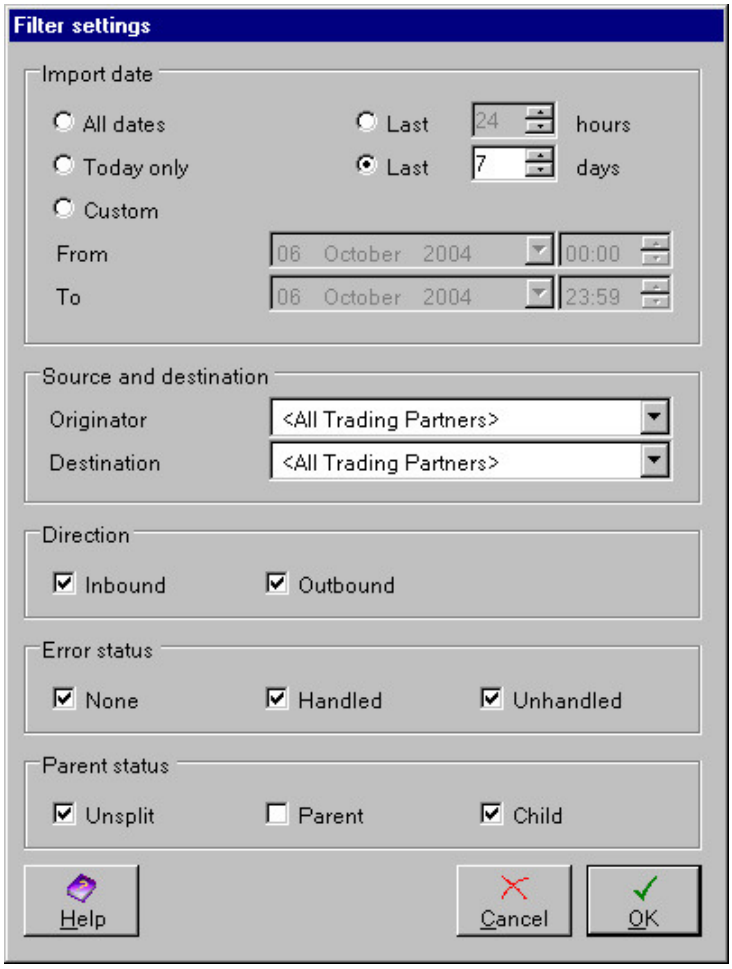
This section contains details of the Archived Files Filter options.

Archived Files Filter

The Archived Files Filter option allows you to select specific criteria for the files you want to see displayed in the data area. It can be accessed in the following ways:

- From the main menu, using **View >> Filter**
- Using the keyboard shortcut **Ctrl + F**
- Using the toolbar icon 

Any of these methods will bring up the dialog shown below.



Please bear in mind that filtering may result in no entries being shown in the data area if no files meet the filter criteria.

Import date

The default Import date setting for the filter is Last 7 days.

Selecting the Last n hours or Last n days will allow you to specify the number of hours or days to which the filter is to be restricted.

Selecting "All dates" means that date filtering will not be performed.

Selecting "Today only" means that only files imported today will be displayed.

Selecting Custom will enable the From and To date and time fields. Use the arrow buttons alongside these fields to select a date and time range for the filter.

If you need help to select a new From or To date for the Custom option, please refer to the section entitled "Custom".

Source and destination

These fields allow you to restrict any or all of the given criteria to a single value. An Originator is a trading partner that has sent you one or more files. A Destination is a trading partner to whom you have sent one or more files. "Channel" refers to the logical data groupings you have set up in the ODEX Workflow Manager.

The community field will only be displayed if security is enabled, you are using communities and the user that you are logged on as can access multiple communities.

If you are logged on as a user that is a member of one community, this field is hidden as only files related to one community can be displayed.

Select a community to restrict the visible files to those where the origin or destination company is associated with the selected community.

Direction

In this section you can select which files will be displayed on the basis of their direction.

Please note that you must select at least one option from this section.

'Inbound' will display files that have been sent to you by your trading partners.

'Outbound' will display files that have been or will be sent by you to your trading partners.

Error status

In this section you can select which files will be displayed on the basis of the status of errors they have encountered.

Please note that you must select at least one option from this section.

'Handled' will display files whose errors have been handled by a user-defined error workflow.

'Unhandled' will display files for which no error workflows have been defined.

'None' will display files that have no errors.

Parent status

In this section you can select which files will be displayed on the basis of whether they have been split or not.

Please note that you must select at least one option from this section.

A file containing one or more interchanges can be split into several files, each of which contains one of those interchanges. The original file is then deemed to be a parent, and each file it was split into is deemed to be a child of that parent.

'Unsplit' will display files that have not been split into children. This will include non-EDI files, files that contain a single EDI interchange so cannot be split, files that contain more than one interchange but have not been split, and files that are themselves children and so cannot be split further.

'Parent' will display all those files that have been split into children, but in their original form i.e. still containing their children.

'Child' will display all files that have resulted from being split from their original parent file.

Even though the descriptions above mean that files can belong to more than one parent status, files displayed will never be duplicated.

Comms Files – File Details

ODEX Comms files comprise Received, Scheduled and Sent files. Received files that are being forwarded to another trading partner are marked as forward files.

The Received Files page displays all files (subject to filter settings) that have been received from trading partners.

The Scheduled Files page displays all files (subject to filter settings) that are ready to be sent to trading partners.

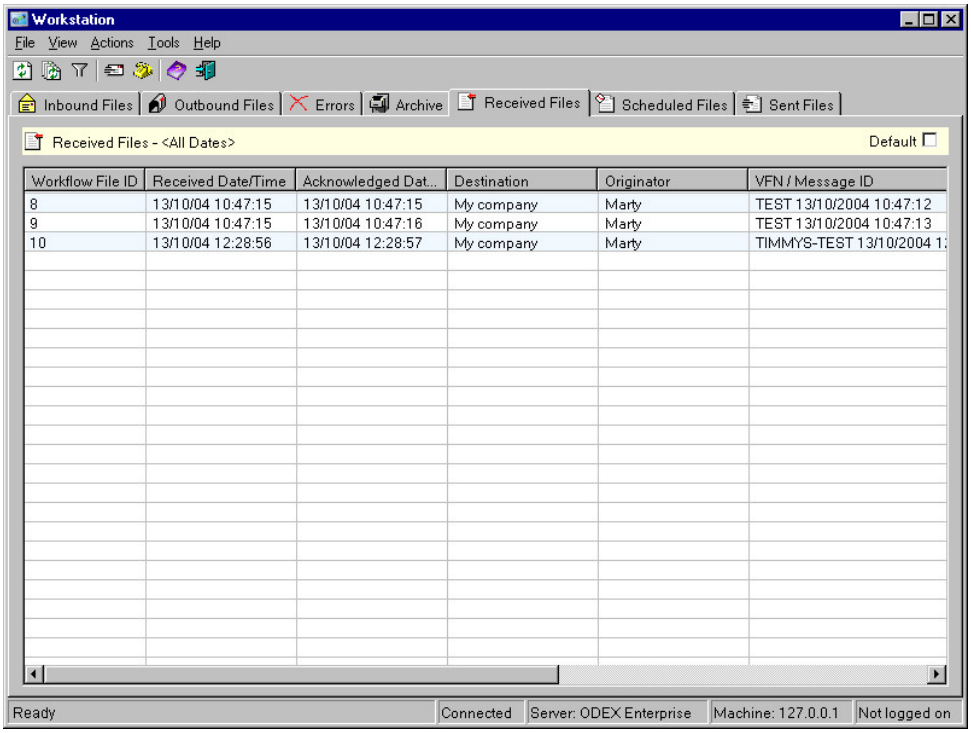
The Sent Files page displays all files (subject to filter settings) that have already been sent to trading partners.

The Forward Files page displays all files (subject to filter settings) that have been received and are about to be forwarded, files that have been received and are currently being forwarded and files that have been received and have been forwarded.

If you are using communities and security is enabled, each of the views restricts the visible data depending on which communities the logged on user is associated with.

If you log on as a user that is not associated with any communities, all comms files in the system are visible, subject to the chosen filter settings. If you log on as a user that is a member of one or more communities, only files will be visible where the origin or destination network or company is associated with one of the user's communities.

The screen will look like the example shown below.



Comms Files tool bar

The Comms Files tool bar contains the following icons:

 This is the Refresh option. This option shows the results of any updating or editing that has been done in this view.

 This is the Refresh All option. This option refreshes all views in the Workstation.

 This is the Filter option. This option allows you to select specific criteria for the files you want to see displayed in the data area.

 This is the Schedule option. This option allows you to schedule a file manually (EDI or non-EDI) and to specify details such as the file priority, earliest date/time to send and virtual filename.

 This is the Call Network option. This option allows you to make a call to a specified network.

 This is the Help option. The Help option takes you to the page(s) of the ODEX on-line Help manual that describe and explain the window or dialog you are currently looking at.

 This is the Exit option. The Exit option closes the ODEX Workstation.

Comms Files – View option

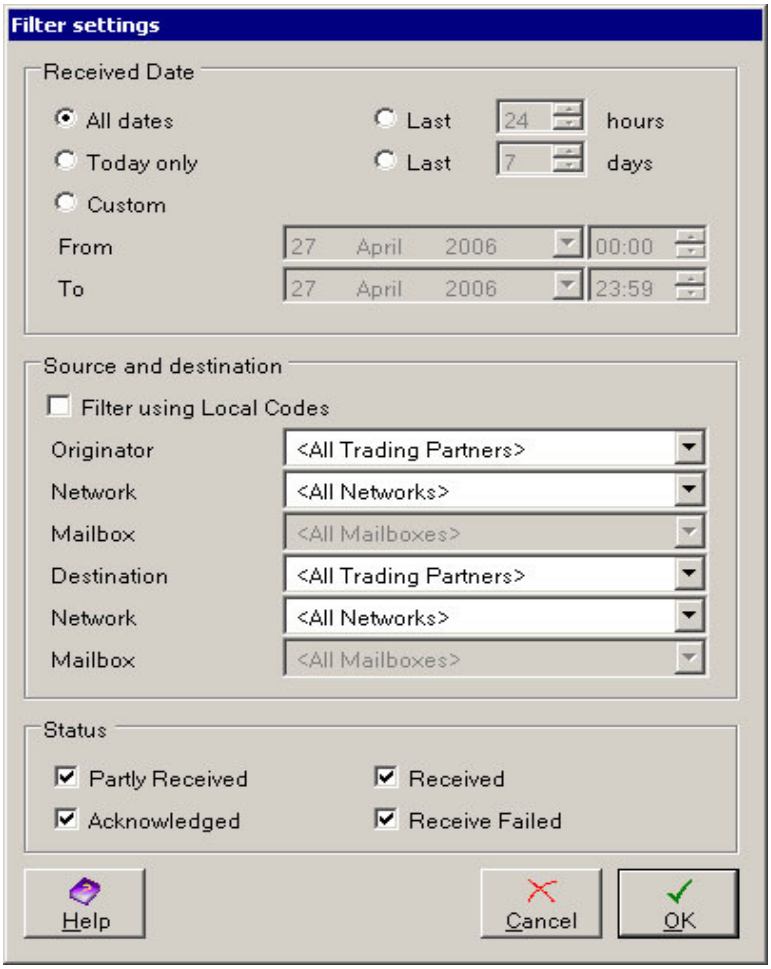
Most of the Comms Files View menu options are described in the section entitled "Workstation View options". This section describes the filter dialogs for each of the Comms File views.

Received Files Filter

The Received Files Filter option allows you to select specific criteria for the files you want to see displayed in the data area. It can be accessed in the following ways:

- From the main menu, using **View >> Filter**
- Using the keyboard shortcut **Ctrl + F**
- Using the toolbar icon 

Any of these methods will bring up the dialog shown below.



Please bear in mind that filtering may result in no entries being shown in the data area if no files meet the filter criteria.

Received date

The default Received date setting for the filter is All dates. To limit the dates, select one of the other radio buttons.

Selecting "Today only" means that only files received today will be displayed.

Selecting the Last n hours or Last n days will allow you to specify the number of hours or days to which the filter is to be restricted.

Selecting Custom will enable the From and To date and time fields. Use the dropdown arrows alongside these fields to select a date and time range for the filter.

If you need help to select a new From or To date for the Custom option, please refer to the section entitled "Custom".

Source and destination

These fields allow you to restrict any or all of the given criteria to a single value. An Originator is a trading partner or clearing centre that has sent you one or more files. A Destination is an internal network that has received one or more files.

If you are using communities and are logged on as a user that is a member of no communities or a member of more than one community, you can also filter the view by community. This will restrict the files to those where the origin or

destination network or company is associated with the community that you select.

Checking, ‘Filter using Local Codes’, allows you to enter the local codes of Networks and Mailboxes as your selection criteria. Un-checking this presents you with lists of names from which to select.

Status

In this section you can select which status of files you want to see displayed.

Please note that you must select at least one option from this section.

'Partly Received' will display files that, for whatever reason, have only been partly received.

'Received' will display files that have been completely received.

'Acknowledged' will display files for which an EERP (End-to-End-Response) has been sent to the sender of the file.

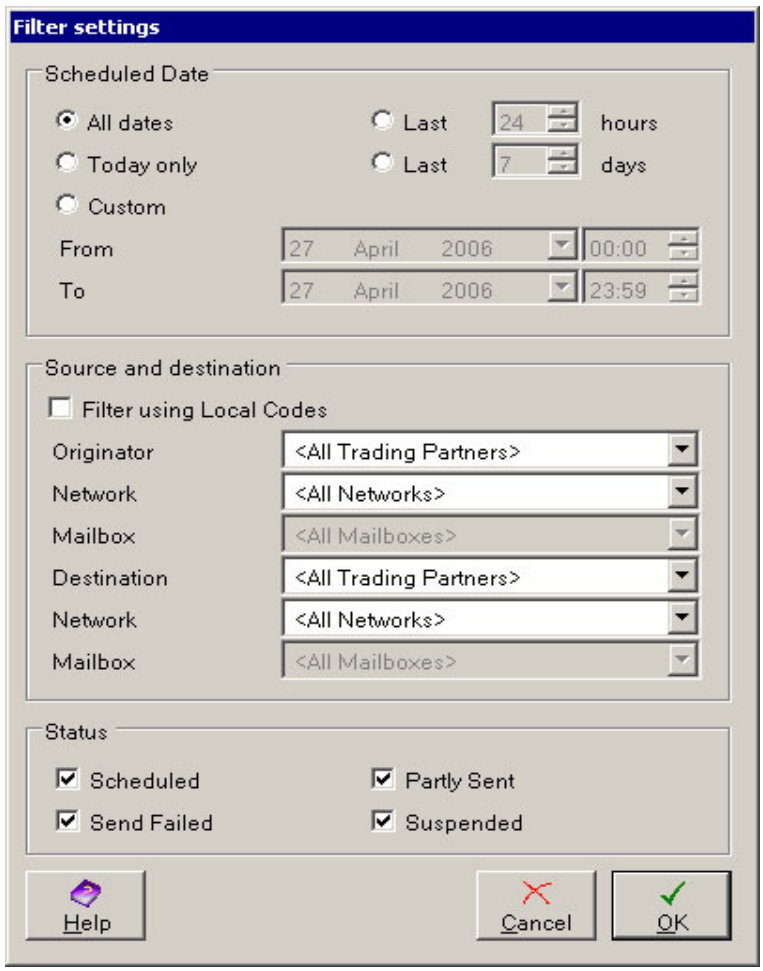
'Receive Failed' will display files that, for whatever reason, were not received successfully. This will include files that were not received at all and files that were rejected after receipt, but will not include partially received files (unless the maximum retries value has been reached).

Scheduled Files Filter

The Scheduled Files Filter option allows you to select specific criteria for the files you want to see displayed in the data area. It can be accessed in the following ways:

- From the main menu, using **View >> Filter**
- Using the keyboard shortcut **Ctrl + F**
- Using the toolbar icon 

Any of these methods will bring up the dialog shown below.



Please bear in mind that filtering may result in no entries being shown in the data area if no files meet the filter criteria.

Scheduled date

The default Scheduled date setting for the filter is All dates. To limit the dates, select one of the other radio buttons.

Selecting "Today only" means that only files scheduled today will be displayed.

Selecting the Last n hours or Last n days will allow you to specify the number of hours or days to which the filter is to be restricted.

Selecting Custom will enable the From and To date fields. Use the dropdown arrows alongside these fields to select a date range for the filter.

If you need help to select a new From or To date for the Custom option, please refer to the section entitled "Custom".

Source and destination

These fields allow you to restrict any or all of the given criteria to a single value. The Originator is the internal network that has scheduled one or more files. The Destination is the trading partner or clearing centre to whom the Originator has scheduled one or more files.

If you are using communities and are logged on as a user that is a member of no communities or a member of more than one community, you can also filter the view by community. This will restrict the files to those where the origin or destination network or company is associated with the community that you select.

Checking, ‘Filter using Local Codes’, allows you to enter the local codes of Networks and Mailboxes as your selection criteria. Un-checking this presents you with lists of names from which to select.

Status

In this section you can select which status of files you want to see displayed.

Please note that you must select at least one option from this section.

'Scheduled' will display files that are ready to be sent.

'Partly Sent' will display files that, for whatever reason, have only been partly sent.

'Send Failed' will display files that, for whatever reason, were not sent successfully.

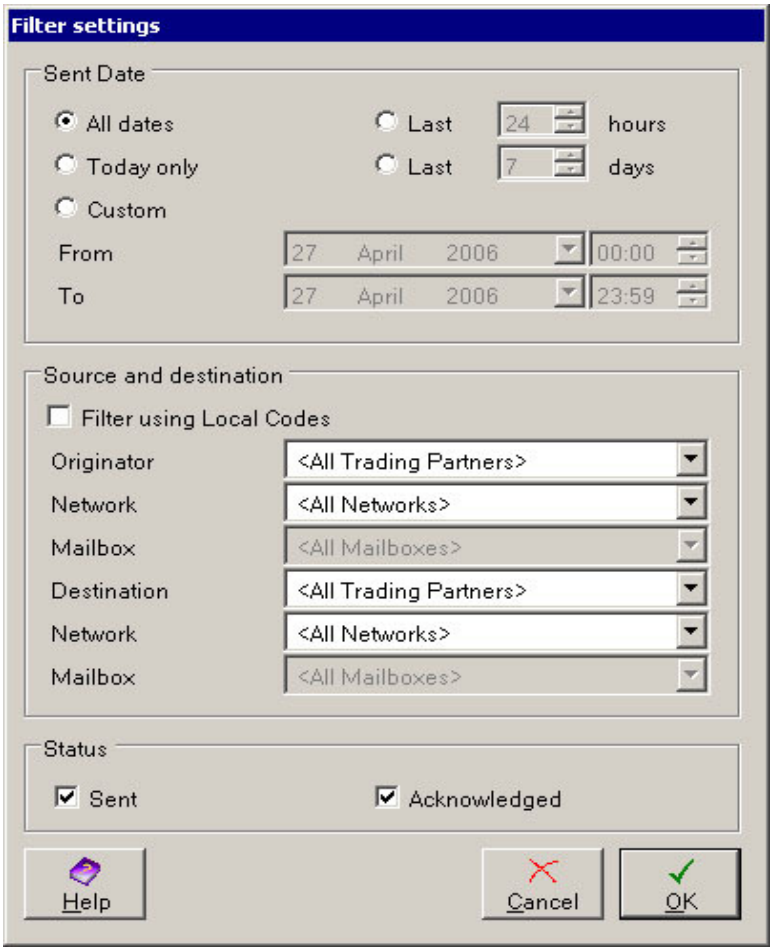
'Suspended' will display files that you have suspended before they could be sent.

Sent Files Filter

The Sent Files Filter option allows you to select specific criteria for the files you want to see displayed in the data area. It can be accessed in the following ways:

- From the main menu, using **View >> Filter**
- Using the keyboard shortcut **Ctrl + F**
- Using the toolbar icon 

Any of these methods will bring up the dialog shown below.



Please bear in mind that filtering may result in no entries being shown in the data area if no files meet the filter criteria.

Sent date

The default Sent date setting for the filter is All dates. To limit the dates, select one of the other radio buttons.

Selecting "Today only" means that only files sent today will be displayed.

Selecting the Last n hours or Last n days will allow you to specify the number of hours or days to which the filter is to be restricted.

Selecting Custom will enable the From and To date fields. Use the dropdown arrows alongside these fields to select a date range for the filter.

If you need help to select a new From or To date for the Custom option, please refer to the section entitled "Custom".

Source and destination

These fields allow you to restrict any or all of the given criteria to a single value. The Originator is the internal network that has sent one or more files. The Destination is the trading partner or clearing centre to whom the Originator has sent one or more files.

If you are using communities and are logged on as a user that is a member of no communities or a member of more than one community, you can also filter the view by community. This will restrict the files to those where the origin or destination network or company is associated with the community that you select.

Checking, ‘Filter using Local Codes’, allows you to enter the local codes of Networks and Mailboxes as your selection criteria. Un-checking this presents you with lists of names from which to select.

Status

In this section you can select which status of files you want to see displayed.

Please note that you must select at least one option from this section.

'Sent' will display files that have been sent.

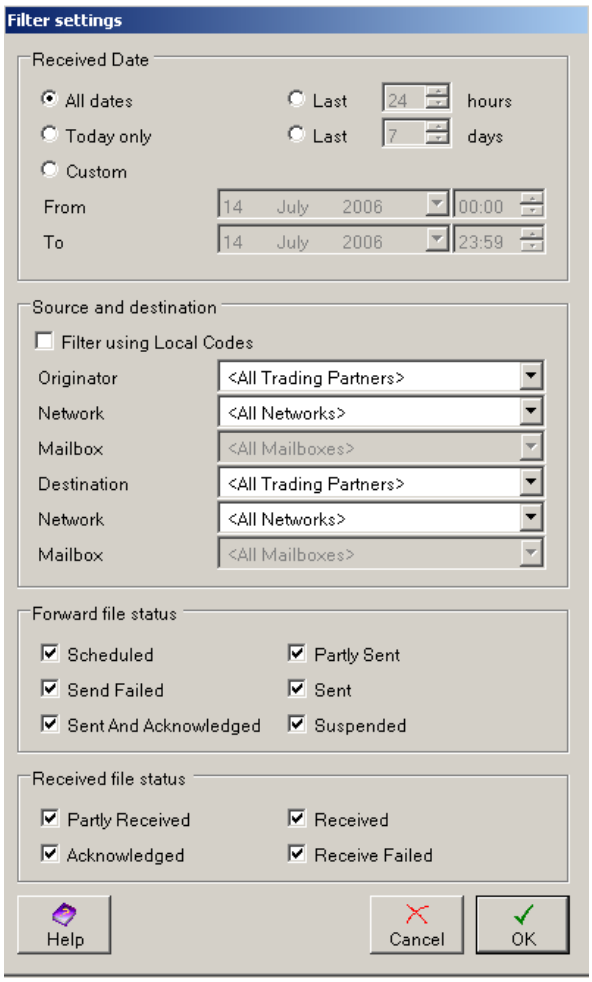
'Acknowledged' will display files for which you have received an EERP.

Forward Files Filter

The Forward Files Filter option allows you to select specific criteria for the files you want to see displayed in the data area. It can be accessed in the following ways:

- From the main menu, using **View >> Filter**
- Using the keyboard shortcut **Ctrl + F**
- Using the toolbar icon 

Any of these methods will bring up the dialog shown below.



Received Date

The default Received date setting for the filter is All dates. To limit the dates, select one of the other radio buttons.

Selecting "Today only" means that only files received today will be displayed.

Selecting the Last n hours or Last n days will allow you to specify the number of hours or days to which the filter is to be restricted.

Selecting Custom will enable the From and To date and time fields. Use the dropdown arrows alongside these fields to select a date and time range for the filter.

If you need help to select a new From or To date for the Custom option, please refer to the section entitled "Custom".

Source and destination

These fields allow you to restrict any or all of the given criteria to a single value. The Originator is the external network and mailbox from which the files were received. The Destination is the trading partner or clearing centre to whom the Originator has sent one or more files.

If you are using communities and are logged on as a user that is a member of no communities or a member of more than one community, you can also filter the view by community. This will restrict the files to those where the origin or destination network or company is associated with the community that you select.

Checking, ‘Filter using Local Codes’, allows you to enter the local codes of Networks and Mailboxes as your selection criteria. Un-checking this presents you with lists of names from which to select.

File Status

In this section you can select which status of files you want to see displayed. The status can be selected for the file that has been received and for the file that is being forwarded.

Please note that you must select at least one option from each of the status sections.

‘Received’ will display files that have been received. The status of the file that is being sent, is determined by the option in the ‘forward file status’ section.

‘Partly received’ will display files that are in the process of being received from a trading partner.

'Receive Failed' will display files that, for whatever reason, were not received successfully. This will include files that were not received at all and files that were rejected after receipt, but will not include partially received files (unless the maximum retries value has been reached).

‘Acknowledged’ will display files where the file received from the trading partner has been acknowledged. For OFTP, this means an EERP has been sent. In AS2, this means an MDN has been sent to the trading partner.

‘Scheduled’ will display files that have been received from a trading partner and are due to be forwarded.

'Sent' will display files that have been received from a trading partner and forwarded to another trading partner, but the forwarded file has not yet been acknowledged.

'Sent and Acknowledged' will display files that have been received from a trading partner, the file has been forwarded to another trading partner and an acknowledgement (EERP or MDN) has been received for the sent file.

'Partly Sent' will display files that have been received but for whatever reason, the file being forwarded has only been partly sent.

'Send Failed' will display files that have been received but for whatever reason, the file being forwarded was not sent successfully.

'Suspended' will display files that have been received but you have suspended before they could be forwarded.

Received Files – Available columns

The Received Files page displays columns which are configurable i.e. you can select which columns are shown, the order they appear on the page and, in some cases, the order of the data displayed in them.

The contents of each column is described in the following section. The default columns are listed first, followed by the remainder in alphabetical order.

Default columns

Workflow File ID – the unique ID of the workflow file with which this comms file is associated.

Received Date/Time – the date and time at which the file was received.

Acknowledged Date/Time – the date and time at which an acknowledgement (an EERP) was sent to the sender of the file. If this column is blank, no acknowledgement has been sent.

Destination – The internal network that this file has been sent to.

Originator – The trading partner that this file came from.

VFN/Message ID – the virtual filename and virtual date/time (OFTP) or unique message ID (AS2) of the file.

File Status – the current status of the file from a communications point of view. Possible values differ according to which comms file view you are looking at:

- **Received Files** – Partly Received, Received, Acknowledged, Received, Failed

File Progress – an estimate of how much of the file has been transmitted (as a percentage).

Remaining columns

Bytes received – the number of bytes of the file that have been received so far.

Content Type – this column is only applicable to AS2. This is the MIME content type string, which indicates the type of data sent or received.

Destination Mailbox – the SFID of the destination mailbox.

Destination Mailbox Name – the name of the destination mailbox.

Destination Network – the SSID of the destination network.

Destination Network Name – the name of the destination network.

Document Type – the type of document in the file e.g. a DESADV D96A for an EDI document.

EDI Security – the EDIFACT security status of the file.

Encoding – the encoding of the file e.g. ASCII.

Encrypted – this column is only applicable to AS2. Indicates whether the data was encrypted.

Extracted – indicates whether the file has been extracted or not.

Extraction Date/Time – shows the last date and time that the file was extracted.

Extraction Destination – shows the last location the file was extracted to.

File Name – the disk name of the file as it is stored in the system.

File Size – the size of the file in bytes.

Format – the format of the data in the file e.g. EDI.

Last Error – the error that stopped the file being received last time it was attempted.

Maximum Record Size – the OFTP maximum record size (for F or V format files).

MDN Description – this column is only applicable to AS2. This is the MDN disposition description, which accompanies the response to a transmission of AS2 data.

MDN Disposition – this column is only applicable to AS2. This is the MDN disposition type. It indicates the response to a transmission of AS2 data.

MDN Modifier – this column is only applicable to AS2. This is the MDN disposition modifier. It gives more information about the response to a transmission of AS2 data.

MDN Settings – this column is only applicable to AS2. It indicates how the response to a transmission of AS2 data was or is to be sent.

Number Of Attempts – the number of times the system has tried to receive the file.

OFTP File Format – the OFTP file format i.e. F (Fixed),T (Text), U (Unformatted) or V (Variable).

Originator Mailbox – the SFID of the originator mailbox.

Originator Mailbox Name – the name of the originator mailbox.

Originator Network – the SSID of the originator network.

Originator Network Name – the name of the originator network.

Protocol – the protocol used to receive the file.

Records – the number of OFTP records in the file (for F or V format files).

Session Acknowledged – the unique ID of the session in which the file was acknowledged.

Session Received – the unique ID of the session in which the file was received.

SFID User Data – the OFTP SFID User Data associated with the file.

Signature – this column is only applicable to AS2. Indicates whether the data was signed and, if so, whether the signature was valid.

Subject – this column is only applicable to AS2. Contains the subject of the message.

VF Description – this column is only applicable to OFTP and only if the sender used OFTP 2 or higher. The description of the virtual file.

Virtual Date/Time – this column is only applicable to OFTP. This is the virtual date and time of the file. Although this information is also present in the VFN/Message ID column, the virtual date/time has also been included separately in case you prefer to use this.

Scheduled Files – Available columns

The Scheduled Files page displays columns which are configurable i.e. you can select which columns are shown, the order they appear on the page and, in some cases, the order of the data displayed in them.

The contents of each column is described in the following section. The default columns are listed first, followed by the remainder in alphabetical order.

Default columns

Workflow File ID – the unique ID of the workflow file with which this comms file is associated.

Scheduled Date/Time – the date and time at which the file was scheduled.

Destination – The trading partner that this file has been scheduled to.

Originator – The internal network that this file was scheduled from.

VFN/Message ID – the virtual filename and virtual date/time (OFTP) or unique message ID (AS2) of the file.

File Status – the current status of the file from a communications point of view. Possible values differ according to which comms file view you are looking at:

- **Scheduled Files** – Scheduled, Partly Sent, Send Failed, Suspended

File Progress – an estimate of how much of the file has been transmitted (as a percentage).

Remaining columns

Bytes sent – the number of bytes of the file that have been sent so far.

Content Type – this column is only applicable to AS2. This is the MIME content type string, which indicates the type of data sent or received.

Description – A description of the file, which may have been added by the system or a user.

Destination Mailbox – the SFID of the destination mailbox.

Destination Mailbox Name – the name of the destination mailbox.

Destination Network – the SSID of the destination network.

Destination Network Name – the name of the destination network.

Document Type – the type of document in the file e.g. a DESADV D96A for an EDI document.

Earliest Date/Time – the earliest date and time when the file will be sent.

EDI Security – the EDIFACT security status of the file.

Encoding – the encoding of the file e.g. ASCII.

Encrypted – this column is only applicable to AS2. Indicates whether the data was encrypted.

File Name – the disk name of the file as it is stored in the system.

File Size – the size of the file in bytes.

Format – the format of the data in the file e.g. EDI.

Last Error – the error that stopped the file being sent last time it was attempted.

Maximum Number Of Tries – the maximum number of times the system will try to send the file

Maximum Record Size – the OFTP maximum record size (for F or V format files).

MDN Description – this column is only applicable to AS2. This is the MDN disposition description, which accompanies the response to a transmission of AS2 data.

MDN Disposition – this column is only applicable to AS2. This is the MDN disposition type. It indicates the response to a transmission of AS2 data.

MDN Modifier – this column is only applicable to AS2. This is the MDN disposition modifier. It gives more information about the response to a transmission of AS2 data.

MDN Settings – this column is only applicable to AS2. It indicates how the response to a transmission of AS2 data was or is to be sent.

Number Of Attempts – the number of times the system has tried to send the file.

OFTP File Format – the OFTP file format i.e. F (Fixed),T (Text), U (Unformatted) or V (Variable).

Originator Mailbox – the SFID of the originator mailbox.

Originator Mailbox Name – the name of the originator mailbox.

Originator Network – the SSID of the originator network.

Originator Network Name – the name of the originator network.

Priority – the transmission priority of the file.

Protocol – the protocol used to send the file.

Records – the number of OFTP records in the file (for F or V format files).

Session Attempted – the unique ID of the session in which the file was last attempted to be sent.

SFID User Data – the OFTP SFID User Data associated with the file.

Signature – this column is only applicable to AS2. Indicates whether the data was signed and, if so, whether the signature was valid.

VF Description – this column is only applicable to OFTP and the value will only be used if the receiver uses OFTP 2 or higher. The description of the virtual file.

Virtual Date/Time – this column is only applicable to OFTP. This is the virtual date and time of the file. Although this information is also present in the VFN/Message ID column, the virtual date/time has also been included separately in case you prefer to use this.

Sent Files – Available columns

The Sent Files page displays columns which are configurable i.e. you can select which columns are shown, the order they appear on the page and, in some cases, the order of the data displayed in them.

The contents of each column is described in the following section. The default columns are listed first, followed by the remainder in alphabetical order.

Default columns

Workflow File ID – the unique ID of the workflow file with which this comms file is associated.

Transmission Date/Time – the date and time when the file was transmitted.

Acknowledged Date/Time – the date and time when the file was acknowledged.

Destination – The trading partner that this file has been sent to.

Originator – The internal network that this file was sent from.

VFN/Message ID – the virtual filename and virtual date/time (OFTP) or unique message ID (AS2) of the file.

File Status – the current status of the file from a communications point of view.

Remaining columns

Content Type – this column is only applicable to AS2. This is the MIME content type string, which indicates the type of data sent or received.

Description – A description of the file, which may have been added by the system or a user.

Destination Mailbox – the SFID of the destination mailbox.

Destination Mailbox Name – the name of the destination mailbox.

Destination Network – the SSID of the destination network.

Destination Network Name – the name of the destination network.

Document Type – the type of document in the file e.g. a DESADV D96A for an EDI document.

EDI Security – the EDIFACT security status of the file.

Encoding – the encoding of the file e.g. ASCII.

Encrypted – this column is only applicable to AS2. Indicates whether the data was encrypted.

File Name – the disk name of the file as it is stored in the system.

File Size – the size of the file in bytes.

Format – the format of the data in the file e.g. EDI.

Maximum Record Size – the OFTP maximum record size (for F or V format files).

MDN Description – this column is only applicable to AS2. This is the MDN disposition description, which accompanies the response to a transmission of AS2 data.

MDN Disposition – this column is only applicable to AS2. This is the MDN disposition type. It indicates the response to a transmission of AS2 data.

MDN Modifier – this column is only applicable to AS2. This is the MDN disposition modifier. It gives more information about the response to a transmission of AS2 data.

MDN Settings – this column is only applicable to AS2. It indicates how the response to a transmission of AS2 data was or is to be sent.

Number Of Attempts – the number of times the system tried to send the file.

OFTP File Format – the OFTP file format i.e. F (Fixed),T (Text), U (Unformatted) or V (Variable).

Originator Mailbox – the SFID of the originator mailbox.

Originator Mailbox Name – the name of the originator mailbox.

Originator Network – the SSID of the originator network.

Originator Network Name – the name of the originator network.

Protocol – the protocol used to send the file.

Records – the number of OFTP records in the file (for F or V format files).

Scheduled Date/Time – the date and time at which this file was scheduled.

Session Acknowledged – the unique ID of the session in which the file was acknowledged.

Session Sent – the unique ID of the session in which the file was sent.

SFID User Data – the OFTP SFID User Data associated with the file.

Signature – this column is only applicable to AS2. Indicates whether the data was signed and, if so, whether the signature was valid.

VF Description – this column is only applicable to OFTP and the value will only have been used if the receiver used OFTP 2 or higher. The description of the virtual file.

Virtual Date/Time – this column is only applicable to OFTP. This is the virtual date and time of the file. Although this information is also present in the VFN/Message ID column, the virtual date/time has also been included separately in case you prefer to use this.

Forward Files – Available Columns

Default columns

Workflow File ID – the unique ID of the workflow file with which this comms file is associated.

Transmission Date/Time

Received Date/Time – the date and time at which the file was received.

Forward File Acknowledged Date – the date and time at which an acknowledgement (an EERP) was sent to the sender of the file. If this column is blank, no acknowledgement has been sent.

VFN/Message ID – the virtual filename and virtual date/time (OFTP) or unique message ID (AS2) of the file.

Received File Status

Forward File Status

Virtual Date/Time

Destination Mailbox – The internal network that this file has been sent to.

Originator Mailbox – The trading partner that this file came from.

Remaining Columns

Bytes Received – The number of bytes received.

Bytes Sent – The number of bytes of the forward file sent.

Destination – The name of the trading partner that the file is being forwarded to.

Destination Mailbox Local Code – The local code of the mailbox to which the file is being forwarded.

Destination Mailbox Name – The name of the mailbox that to which the file is being forwarded.

Destination Network Local Code – The local code of the network that to which the file is being forwarded.

Document Type – The type of document in the file, e.g. DESADV D96A for an EDI document.

Earliest Date/Time – The earliest date and time at which the file will be forwarded.

Encoding – The encoding of the received file.

Extracted – Indicates whether the file has been extracted or not.

Extraction Date/Time – If the file has been extracted, this column will show the date and time at which the extraction took place.

Extraction Destination – The last location that the file was extracted to.

File Size – The size of the file, in bytes.

Format – The format of the file, e.g. EDI.

Forward File Acknowledgement Error Code – If a negative acknowledgement was received for the forward file, this is the error code from the acknowledgement.

Forward File Description – A description of the forward file. This could be added by the system or a user.

Forward File Destination Network – The identification of the network to which the file is being forwarded. This is the SSID for OFTP networks or the AS2 identifier for AS2 networks.

Forward File Destination Network Name – The name of the network to which the file is being forwarded.

Forward File Last Error - If an error occurred on the last attempt to forward the file, this is the error that prevented the file being forwarded.

Forward File Name – The disk name of the forward file.

Forward File Progress – An estimate of how much of the file has been forwarded, as a percentage.

Forward File Protocol – The protocol being used to transmit the file.

Forward File Session Acknowledged – The unique ID of the session in which the forwarded file was acknowledged.

Forward File Virtual Date – The virtual date and time of the file being forwarded. This only applies to files being forwarded using OFTP.

Last Error – If an error occurred while receiving a file, this is the error that prevented the file from being received.

Maximum Number Of Tries – The maximum number of times the system will try to forward the file.

Maximum Record Size – The OFTP maximum record size, for fixed length record format or variable length record format files.

Number Of Attempts – The number of times the system has tried to forward the file.

OFTP File Format – The OFTP file format (Fixed Length, Text, Unformatted or Variable Length).

Originator – The trading partner from which the file was received.

Originator Mailbox Local Code – The local code of the mailbox through which the file was received.

Originator Mailbox Name – The name of the mailbox through which the file was received.

Originator Network Local Code – The local code of the external network from which the file was received.

Priority – The transmission priority of the forward file.

Received File Acknowledged Date – The date and time at which the original received file was acknowledged.

Received File Name – The disk name of the received file.

Received File Originator Network – The identification of the external network from which the file was received. For OFTP networks, this is the SSID. For AS2 networks, this is the AS2 identifier of the network.

Received File Originator Network Name – The name of the external network from which the file was received.

Received File Progress – An estimate of how much of the file has been received, as a percentage.

Received File Protocol – The protocol used to receive the file.

Received File Session Acknowledged – The unique ID of the session in which the received file was acknowledged.

Records – The number of OFTP records in the file.

Scheduled Date/Time – The date and time at which the forward file was scheduled.

Session Attempted – The unique ID of the session in which an attempt was made to send the file. This only applies to files that have not yet been forwarded.

Session Received – The unique ID of the session in which the file was received.

Session Sent – The unique ID of the session in which the file was forwarded.

SFID User Data – The OFTP SFID user data associated with the received file.

VF Description – The virtual file description.

Comms Files – Actions

This section lists all the actions that you can perform manually on individually selected comms files. Some of these options are only applicable to certain types of comms file. This will be indicated where necessary.

Comms File Details

The Comms File Details option allows you to view all the available details about any file. First select the file with a single left-mouse click.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Comms File Details**
- Double-clicking on a file line in the upper list view
- Using the keyboard shortcut **Alt+A+F**
- Using the 'Comms File Details' item on the context menu (right mouse click)

Any of these methods will bring up the dialog that is described in the "Comms Details" section.

Workflow File Details

The Workflow File Details option allows you to view all the available workflow details about any file. First select the file with a single left-mouse click.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Workflow File Details**
- Using the keyboard shortcut **Alt+A+W**
- Using the 'Workflow File Details' item on the context menu (right mouse click)

Any of these methods will bring up the dialog that is described in the "Workflow File Details" section.

Session Details

The Session Details option allows you to view the Attempted, Sent or Acknowledged session details for any file. First select the file with a single left-mouse click.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Session Details >> Attempted** or **Actions >> Session Details >> Sent** or **Actions >> Session Details >> Acknowledged**
- Using the keyboard shortcut **Alt+A+S+P** or **Alt+A+S+S** or **Alt+A+S+A**
- Using the **Session Details >> Attempted** or **Session Details >> Sent** or **Session Details >> Acknowledged** item on the context menu (right mouse click)

Any of these methods will bring up the appropriate session details page of the Comms Details dialog.

File Analysis

The File Analysis option allows you to view the file analysis details for any file. First select the file with a single left-mouse click.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> File Analysis**
- Using the keyboard shortcut **Alt+A+L**
- Using the 'File Analysis' item on the context menu (right mouse click)

Any of these methods will bring up the dialog that is described in the "File Analysis" section.

Delete

The Delete option allows you to delete a selected file. First select the file with a single left-mouse click.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Delete**
- Using the keyboard shortcut **Alt+A+D**
- Using the 'Delete' item on the context menu (right mouse click)

Any of these methods will displays an “Are you sure” dialog. If you click **Yes**, ODEX will delete the file.

Acknowledge

This option is only available for Received Files.

The Acknowledge option allows you to send a negative or positive acknowledgement to the sender of the selected file. First select the file with a single left-mouse click.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Acknowledge**
- Using the keyboard shortcut **Alt+A+A**
- Using the 'Acknowledge' item on the context menu (right mouse click)

If an acknowledgement has already been sent for the selected file, you will be asked if you still want to acknowledge this file.

Suspend

This option is only applicable to Scheduled Files.

The Suspend option allows you to suspend processing on a selected file. First select the file with a single left-mouse click.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Suspend**
- Using the keyboard shortcut **Alt+A+U**
- Using the 'Suspend' item on the context menu (right mouse click)

Only works on files that are not currently suspended. Once suspended, the file will be displayed in orange.

Resume

This option is only applicable to Scheduled Files.

The Resume option allows you to resume processing on a selected file. First select the file with a single left-mouse click.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Resume**
- Using the keyboard shortcut **Alt+A+R**
- Using the 'Resume' item on the context menu (right mouse click)

Only works on files that are currently suspended.

Reschedule

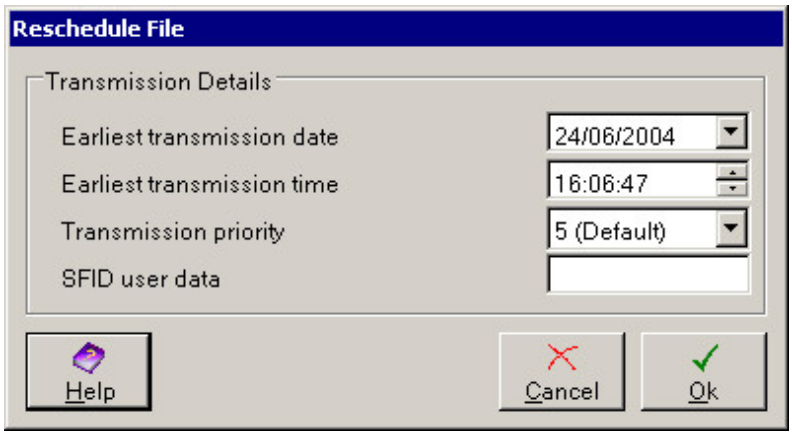
This option is only applicable to Scheduled Files and Sent Files.

The Reschedule option allows you to reschedule a file. First select the file with a single left-mouse click.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Reschedule**
- Using the keyboard shortcut **Alt+A+E**
- Using the 'Reschedule' item on the context menu (right mouse click)

Any of these methods will bring up the following dialog



On this dialog you can specify the earliest transmission date and time (the default is the current date and time).

You can also select the transmission priority, where 1 is the highest priority and 10 is the lowest. The default priority is 5.

If necessary, you can also provide SFID user data. This should be agreed with your trading partner beforehand.

Click the **OK** button to reschedule the file, or click **Cancel** to quit the dialog without rescheduling the file.

Reset Attempts

This option is only applicable to Scheduled Files.

The Reset Attempts option allows you to reset to zero the number of attempts that have been made to send the file. This means that ODEX will be able to try and send the file again. First select the file with a single left-mouse click.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Reset Attempts**
- Using the keyboard shortcut **Alt+A+M**

- Using the 'Reset Attempts' item on the context menu (right mouse click)

Any of these methods will bring up a message box asking if you are sure you want to reset the number of attempts for the selected file. Click **Yes** to reset or **No** to cancel the request.

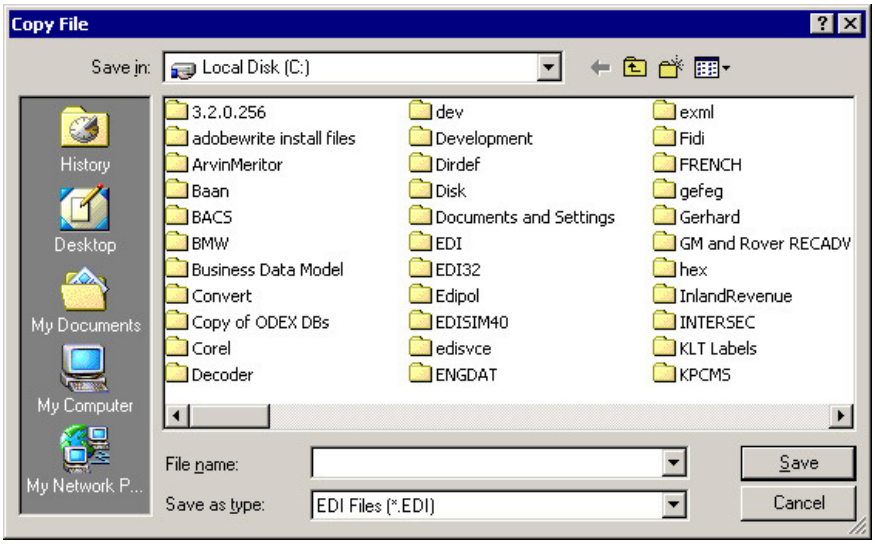
Extract

The Extract option allows you to extract a selected file into a new location, leaving the original in its original location. First select the file with a single left-mouse click.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Extract**
- Using the keyboard shortcut **Alt+A+X**
- Using the 'Extract' item on the context menu (right mouse click)

Any of these methods will bring up the following dialog:

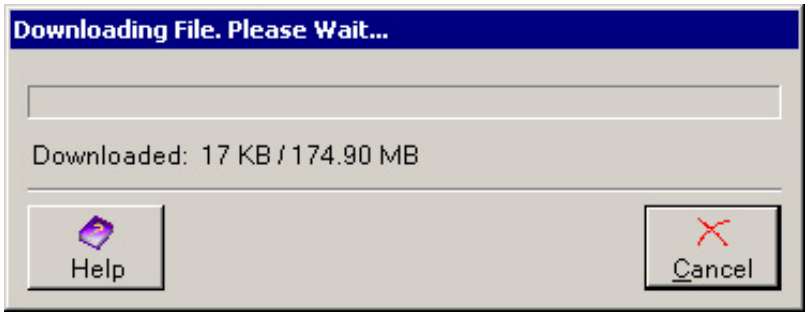


This dialog works in the same way as the Windows Browse dialog.

- Select the directory in which to save the file
- Type the new name of the file in the File name field. Omit the file extension unless you choose All Files (*.*) in the Save as type field.
- Use the dropdown arrow alongside the Save as type field to select a file type for this file (the default type shown in this field will match the type of file you are extracting).

Extracting a large file

If the file you are extracting is very large, you may see the following dialog during the time it takes to download it.



If you do not want to wait for the extraction to complete, you may click the **Cancel** button. This will cancel the Extract operation and return you to the Workstation view.

Open With

The Open With option allows you to open a selected file using an application of your choice. First select the file with a single left-mouse click.

This option can be accessed in the following ways:

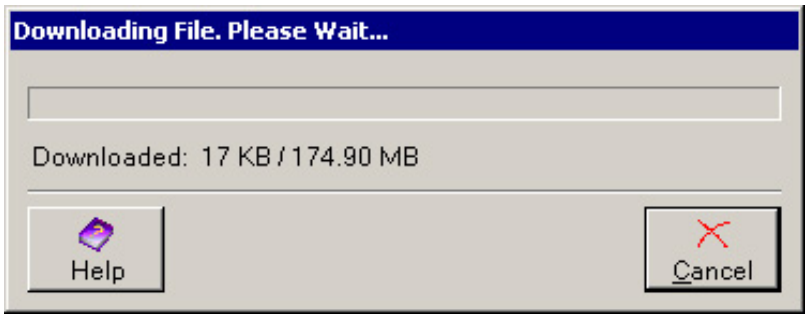
- From the main menu, using **Actions >> Open With**
- Using the keyboard shortcut **Alt+A+O**
- Using the 'Open With' item on the context menu (right mouse click)

Any of these methods will offer you a sub-menu containing applications with which to open the file, depending on what applications you have installed and used before. You can also use the Browse option it offers, to select an application that is not in the list.

If no applications have been used before, it will simply start up the "Open With" dialog. The “Open With” dialog is just a browse dialog for *.exe programs. When you select an application to open with, the file is retrieved from the server (creating a temporary copy locally) and then opened with the specified application.

Opening a large file

If the file you are opening is very large, you may see the following dialog during the time it takes to download it.



If you do not want to wait for the Open operation to complete, you may click the **Cancel** button. This will cancel the Open operation and return you to the Workstation view.

Submit

This option is only applicable to Received Files.

The Submit option allows you to submit a selected comms file manually to a workflow channel.

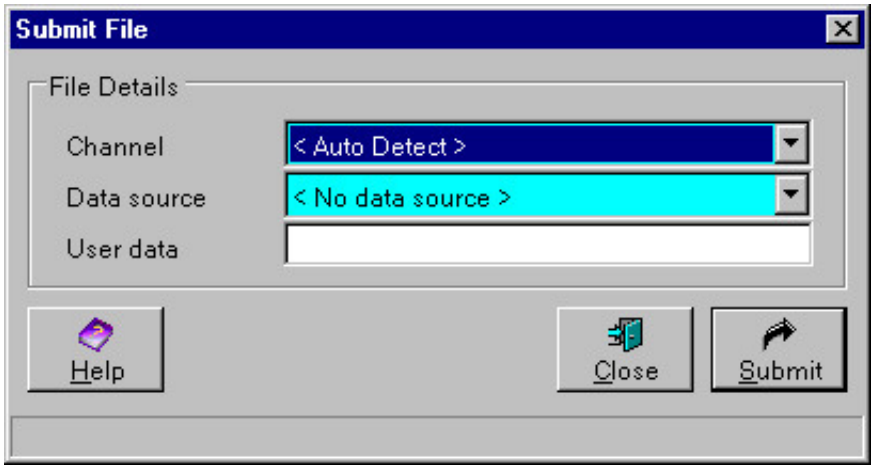
The actual comms file will be given to the Workflow Manager and submitted as a brand new workflow file with a new ID and no current audit lines. If the comms file is already associated with a workflow file, you will be warned that the previous link will be broken and that the comms file will only be linked to the new workflow file.

You can choose to submit the workflow file from its original data source or you can choose a channel for the file to be submitted to directly. You can either choose a specific channel, or allow ODEX to select the first channel which meets the criteria for the selected file.

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Submit**
- Using the keyboard shortcut **Alt+A+T**
- Using the 'Submit' item on the context menu (right mouse click)

Any of these methods will bring up the following dialog:



In the Channel field, select the channel that this file should be processed by. Alternatively, you can leave the Channel field set to < Auto Detect > and ODEX will select the first channel which meets the criteria for the selected file.

In the Data source field, select the data source for this file. If there is no data source, leave the field set to < No data source >.

The User data field may be used for any information you want to keep with the file. The User data stays with the file for its lifetime.

Click the **Submit** button to submit the file.

If the submission is successful, you will see the message "File submitted successfully" appear at the bottom of the dialog.

The dialog will remain open, allowing you to submit more files if required.

Click the **Close** button when you have finished.

Schedule File

The Schedule File option allows you to schedule a file manually (EDI or non-EDI) and to specify details such as the file priority, earliest date/time to send and virtual filename.

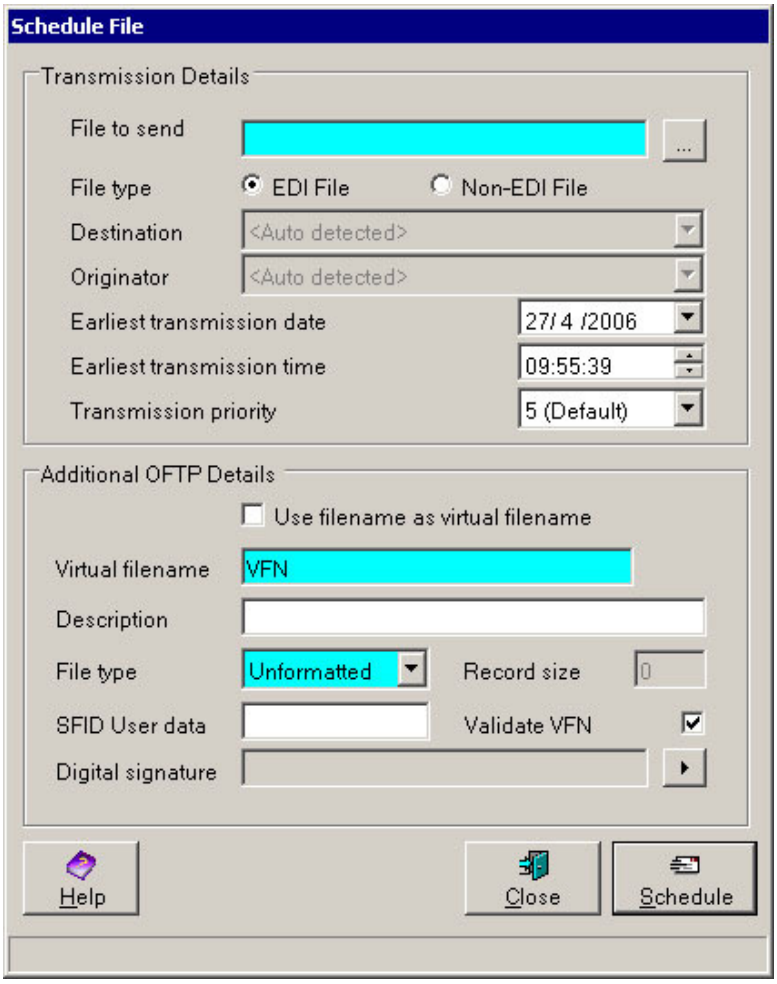
It can be accessed in the following ways:

- From the main menu, using **Actions >> Schedule File**

- Using the keyboard shortcut **Alt+A+H**
- Using the toolbar icon 

There is no context menu item for this option.

Any of these methods will bring up the following dialog:



The dialog is divided into two sections: Transmission Details and Additional OFTP Details.

Transmission Details – File to send

Use the Browse button alongside this field to select the full file path of the file you want to send.

Transmission Details – File type

Select the appropriate file type for the file you are scheduling. If you select EDI File, the Destination and Originator fields will become disabled, as ODEX can automatically detect from the contents of the file what these two values should be.

If you select non-EDI File, you must provide a value in the Destination field. If the Destination you select is an AS2 network, the Originator field and the Additional OFTP details section will become disabled, as these fields are not applicable to AS2 communications.

Transmission Details – Destination

Only applicable if you have selected non-EDI as your file type. Use the dropdown arrow alongside this field to select the appropriate destination for this

file. If the destination you want is not in the list, you must add it using the ODEX Comms Administrator.

Transmission Details – Originator

Only applicable if you have selected non-EDI as your file type and the Destination you have selected is an OFTP network. Use the dropdown arrow alongside this field to select the appropriate originator mailbox for this file. If the mailbox you want is not in the list, you must add it using the ODEX Comms Administrator.

Transmission Details – Earliest transmission date

This is the earliest date that the file will be sent to the trading partner. The default value in this field is the current date. If you wish to postpone the sending of the file, select a later date using the dropdown calendar on the right-hand side of this field.

Transmission Details – Earliest transmission time

This is the earliest time that the file will be sent to the trading partner. The default value in this field is the current time. If you wish to send the file later in the day, perhaps overnight, then select a later time using the arrows on the right-hand side of this field.

Transmission Details – Transmission Priority

Files due for sending to the same destination at the same time are sent in order of priority. The files with the highest priority, 1, are sent first, and then the next highest, and so on, down to the lowest priority of 10.

The transmission priority affects the sequence in which files will be sent. By default, the transmission priority is set to 5, neither high nor low. If this file is of high priority, use the dropdown arrow to select a priority higher than 5 (i.e. a number less than 5). If this file is of low priority, use the dropdown arrow to select a priority lower than 5 (i.e. a number greater than 5).

Additional OFTP Details – Use filename as virtual filename

If you select this tickbox (it is selected by default), ODEX will use the same name as the source file (but excluding the drive and pathname). For example, a filepath of C:\PRO04022004104630.edi in the File to send field will result in a virtual filename of PRO04022004104630. You will see this name appear in the Virtual filename field when you select it or type it in the File to send field.

If you deselect this tickbox, the Virtual filename field will become enabled, allowing you to specify the virtual filename to be used.

Additional OFTP Details – Virtual filename

This field will only be enabled if you have deselected the "Use filename as virtual filename" tickbox.

Type in the name to be used as the virtual filename.

This is the Virtual Filename of the transmitted file. The name must be meaningful to both you and the file's receiver, and is often agreed at the start of a trading partner relationship. Only certain specified characters may be used in this field up to a maximum of 26 characters. These are A to Z (uppercase), 0 to 9 and the special characters / - . & ( ) and space.

Please note – Although it is possible to schedule and send files with virtual filenames that include space characters, the OFTP standards state that

this is not an accepted practice. It is supported in ODEX by popular request, but you should clear its use with your trading partner because some OFTP software will reject the file.

Additional OFTP Details – Description

The description is only used when scheduling a file to a trading partner using a version of OFTP 2 or higher. The description consists of up to 999 characters that are passed with the file identification and may be used for whatever purpose you and the destination agree. If you are in any doubt as to a value to specify, leave this as spaces.

Additional OFTP Details – File type

Four types of file may be scheduled. These may be selected by using the drop down arrow to the right of the field:

- Fixed – This stipulates that the file is to be sent as fixed length records, with the record length specified in the Record size field. The size of the file must be a multiple of the record size given in the next field. If you select this option for an EDI file, the scheduler will increase the size of the EDI file if necessary, so that its length is a multiple of the record size. For a non-EDI file, the scheduler will validate that it is a multiple of the record length.
- Variable – This file type is not supported on PCs, but is used for files that originate from an IBM mainframe.
- Unformatted – This option can usually be selected for most files, meaning that the data will be sent as one long string of information without formatting.
- Text – This means that the file will be sent in text mode and may be reformatted when it reaches its destination. A text file requires a 'carriage return, line feed' character every 2K bytes.

Additional OFTP Details – Record size

Only required when the file is made up of fixed length or variable length records. For variable length records, type in the maximum record length appearing in the file.

Additional OFTP Details – SFID User data

SFID User data, if used, consists of 8 characters which are passed with the file identification, and may be used for whatever purpose you and the destination agree. If you are in any doubt as to the contents, leave this as spaces.

Additional OFTP Details – Validate VFN

This tickbox is selected by default, which means that the virtual filename will be checked for invalid characters before the file is scheduled. If any invalid characters are found, a message box will inform you of the characters that may be used.

If your trading partner insists that you use characters that are not part of the virtual filename character set, you should uncheck this tickbox so that ODEX will not prevent you from scheduling files to him.

Please see the description of the Virtual filename field above, for details of the characters that may be used.

Additional OFTP Details – Digital signature

If you need to enter a PIN number to sign the file, click the arrow button at the side of the field and choose the “Select” option. This will bring up the “Common

Dialogs - Select Certificate" dialog (see the section entitled "Common Dialogs - Select Certificate"). Choose the private key certificate with which to sign the file.

Close

Click the **Close** button to close the dialog without scheduling the file and without saving any changes you made to the dialog.

Schedule

Click the **Schedule** button to schedule the file. If it is scheduled successfully, a message to that effect will appear at the bottom of the dialog.

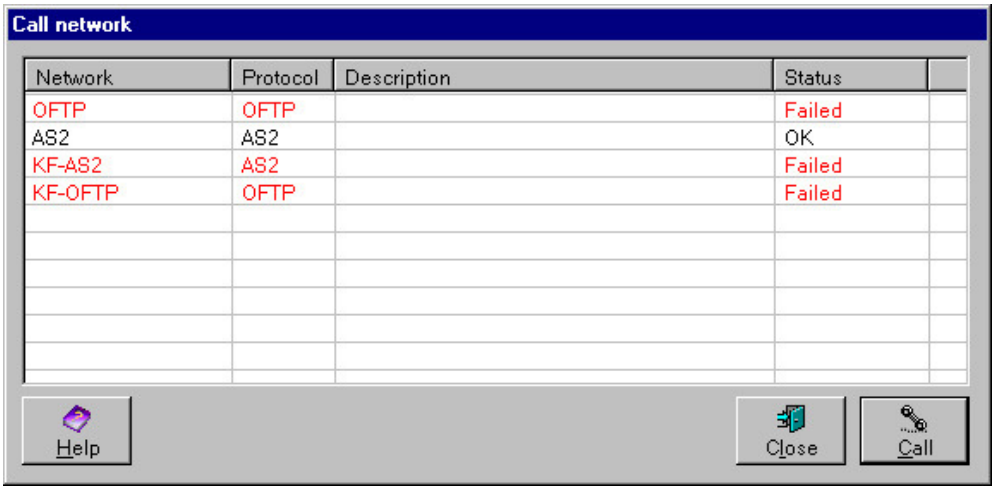
Call Network

The Call Network option allows you to make a manual call to a specified network. You do not need to select any files to use this option, as all files that have been scheduled to the selected network will be sent when the connection is made (subject to suspensions, retry limits etc).

This option can be accessed in the following ways:

- From the main menu, using **Actions >> Call Network**
- Using the keyboard shortcut **Alt+A+C**
- Using the toolbar icon 

Any of these methods will bring up the following dialog:



This dialog shows all the external networks (i.e. for trading partners and clearing centres) you have defined in ODEX, with their associated protocol and the status of the last attempted call to each network.

Highlight the network(s) you want to call, then click the **Call** button. ODEX will attempt to make a connection to the selected network(s) and send any files that are scheduled to those networks.

Double-clicking on an entry in this dialog will also result in a call being made to that network.

ODEX ENGDAT Workstation

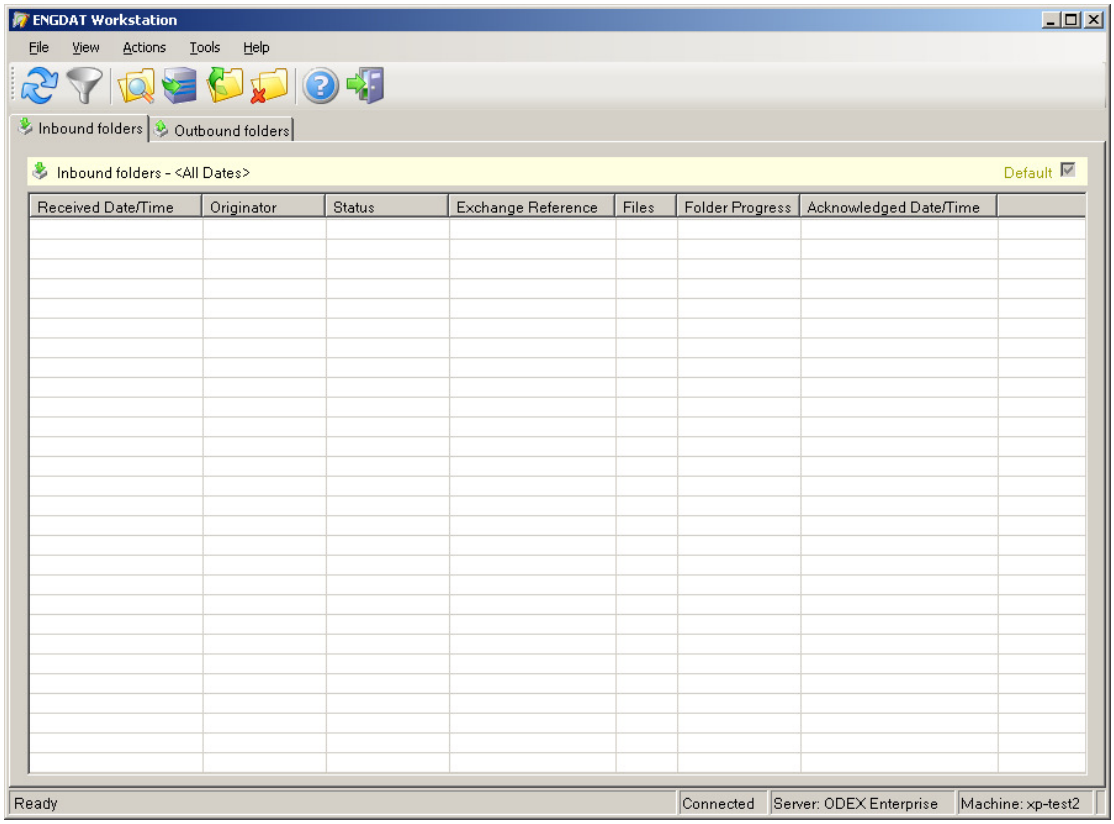
Introduction

The ENGDAT Workstation is a specialised version of the ODEX Workstation, designed for the day-to-day exchange and handling of ENGDAT folders between trading partners.

From the ENGDAT Workstation, you can view received ENGDAT folders, as well as extracting them or submitting them to the workflow manager. You can also edit, delete and create new ENGDAT folders and schedule the folders for transmission. Both views can be customised with filtering, column ordering and sorting. Individual files in received or scheduled folders can be viewed within the ODEX Workstation.

The status bar at the bottom will inform you if the list of files is out of date and the view needs to be refreshed, as well as giving details on whether and to whom the client application is connected.

When you first open the workstation, you will see the following screen:



Workstation Views

There are two possible views in the workstation:

Inbound folders

The inbound folder view shows folders received from your trading partners.

Folders shown on the inbound view may be in one of the following states:

Partly Received – ODEX has started to receive the folder, but some of the files have not yet been received.

Received – All of the files in the folder have been received, but ODEX has not yet sent acknowledgements for each file.

Acknowledged – All of the files in the folder have been received and ODEX has sent a file acknowledgement (EERP) for each file in the folder.

Outbound folders

The outbound folder view shows folders created in ODEX. These may have been scheduled for transmission to a trading partner, or sent to a trading partner.

Folders shown on the outbound view may be in one of the following states:

Created (valid) – The folder has been created but has not been scheduled for transmission to the destination trading partner. If the folder contains an ENGDAT message, the message passes the validation requirements of the validation profile (all mandatory fields have a value).

Created (invalid) – The folder has been created but has not been scheduled for transmission to the destination trading partner. One or more mandatory fields are missing in the ENGDAT message – it is therefore not possible to schedule this folder until values are entered in the missing fields. Once the mandatory field values have been provided, the status will be changed to 'Created (valid)'.

Scheduled – All of the files in the folder have been scheduled for transmission to the destination trading partner. Once a folder has been scheduled, a date and time will be shown in the 'Scheduled Date/Time' column. If you are using security, the name of the user that scheduled the folder will be shown in the 'Scheduled By' column.

Partly Sent – ODEX has started sending the folder to the destination trading partner, but not all of the files have been sent yet. When a folder is in this state, the 'progress' column will show an estimate of how much of the folder has been sent, as a percentage.

Sent – ODEX has sent all of the files in the ENGDAT folder to the destination trading partner, but the trading partner has not yet acknowledged receipt of all of the files. Once the folder has been sent, a date will be shown in the 'Transmitted Date/Time' column.

Acknowledged – ODEX has sent all of the files in the ENGDAT folder to the destination trading partner and has received a file acknowledgement (EERP) from the destination trading partner for all of the transmitted files. Once a folder has been acknowledged, a date will be shown in the 'Acknowledged Date/Time' column.

Workstation Toolbar

Some buttons on the toolbar are dependent on which tab has been selected, as the actions that they trigger are only applicable to inbound or outbound folders. However, there are four buttons that appear on both tabs:

This is the **Refresh** button. When pressed, it shows the results of any updates that have been made to the display. This can also be done by pressing the F5 key or accessing the Refresh option in the View menu.

This is the **Filter** button. When pressed, it brings up the (Filter settings) dialogue, from where the user can alter the criteria for visible folders.

This is the **Help** button. When pressed, it brings up the root page of this help section.

This is the **Close** button. When pressed, it immediately closes the program.

This is the Extract button. When pressed, you will be presented with a browse dialog from which you can select a directory. The files in the ENGDAT folder can then be extracted to the selected directory.

Workstation View Options

The view menu allows you to customise how the currently selected view is displayed, and what data is displayed. On each view, the same three options are given: Refresh, Filter and Columns. These function in exactly the same way, though dealing with different sets of columns and status values depending on the view.

Filter

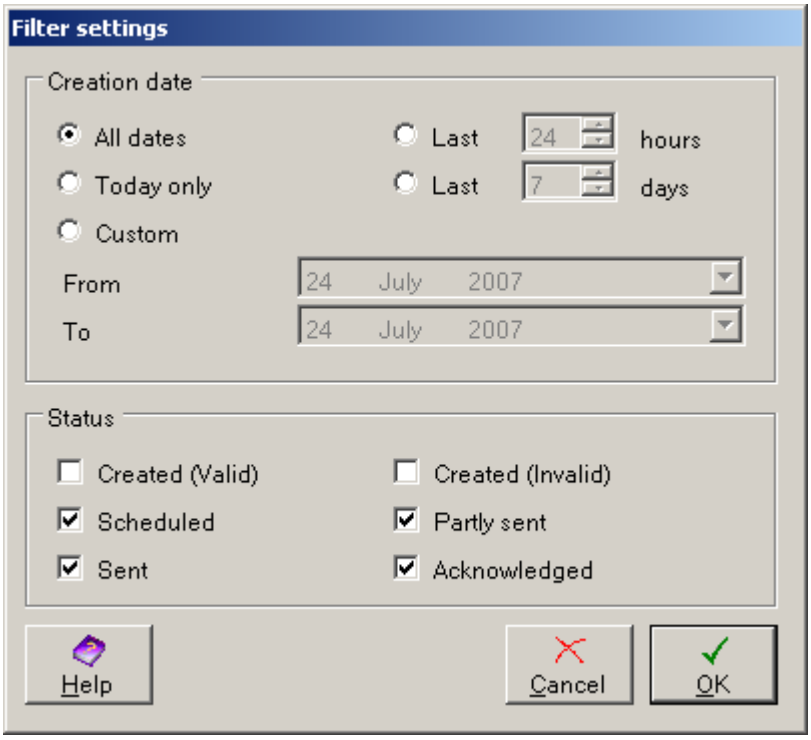
The filter option allows you to restrict the folders that will be displayed in the Inbound or Outbound views, depending on selected folder criteria. This page can be accessed in any of the following ways:

From the main menu, using **View >> Filter**

Using the keyboard shortcut **Ctrl + F**

Using the toolbar icon 

Below is an example of what this page will look like. Although they both work in the same way, the Inbound and Outbound filter options are separate and have different sets of status values.



Please bear in mind that filtering may result in no folders being shown in the folder list if no folders meet the filter criteria.

Creation Date

Here you can specify the range of dates in to which a folder's creation date must fall in order to be displayed. Only one radio button can be selected at any one time; by default, the radio button **All dates** is shown, which is fairly self-explanatory. **Today only** shows only folders created on the current day. Choosing one of the **Last** radio buttons will enable the corresponding entry field for hours or days, allowing you to specify how long before the current date and time the cut-off date should be. You can also use **Custom** to specify the earliest and latest creation date.

Status

Here you can specify one or more status flags to filter by. In order to pass through the filter, a folder must have one of the checked values for its status.

Help

This page can be reached by clicking the **Help** button.

Cancel

Clicking the **Cancel** button with unsaved changes will quit the dialogue, discarding those changes.

Save

To apply the filter settings, click the **Save** button.

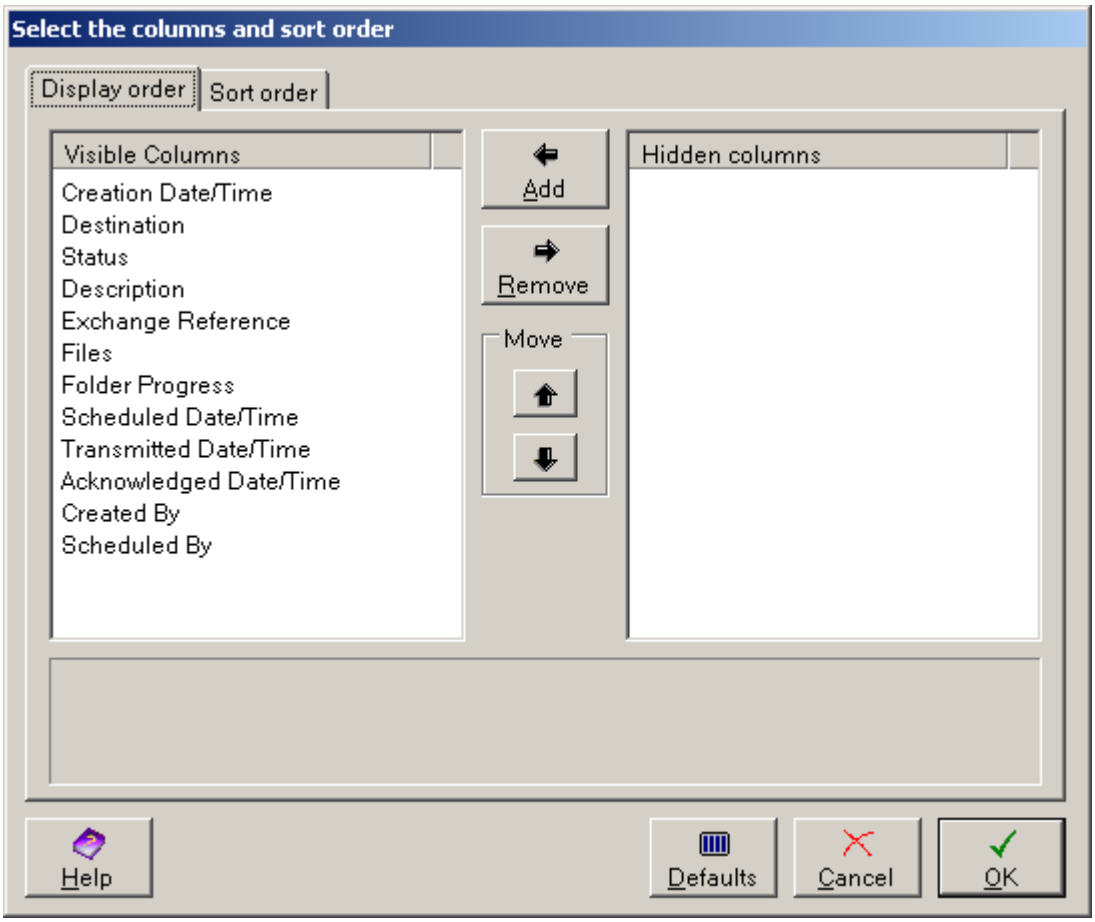
Columns

The columns dialogue allows you to set which columns should be visible in the currently selected view, as well as how the data should be sorted. This dialogue can be accessed in one of the following ways:

- From the main menu, using **View >> Columns**

- Using the keyboard shortcut **Ctrl + C**

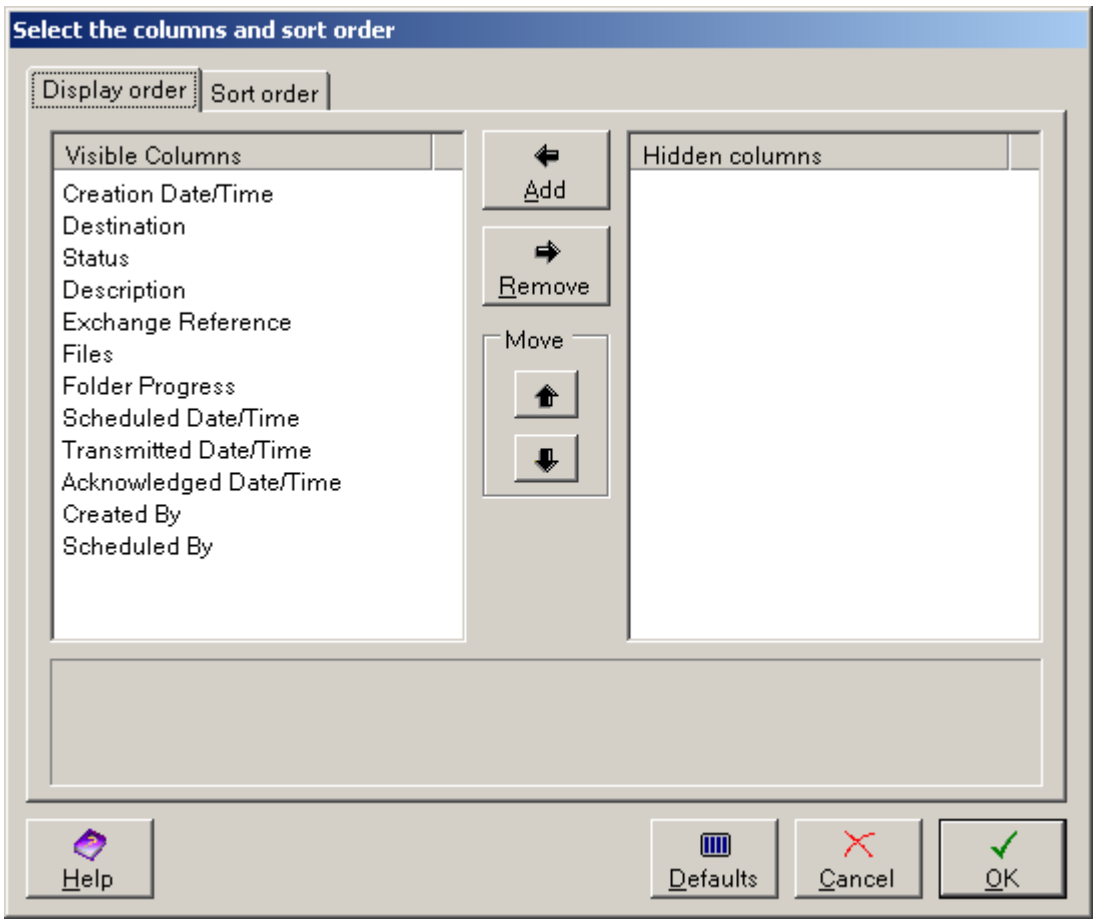
Both of these methods will bring up a dialogue resembling the example below:



There are two tabs: the **Display order** tab is shown here, which provides the ability to specify which columns should be visible. The other tab, the **Sort order** tab, provides the ability to specify how folders should be sorted.

Columns – Display Order

The Display Order tab in the Columns dialogue, shown below, provides the ability to specify exactly which columns should be visible in the currently selected view, by moving column titles between the Visible and Hidden groups and changing their display order when visible.



The left-hand section lists the Visible columns, which by default contains all possible columns. The right-hand section lists the Hidden columns.

Add

Hidden columns can be made visible by highlighting one or more columns from the Hidden columns list and clicking the **Add** button, which will transfer those selected columns to the Visible list.

Remove

Conversely, you can make visible columns hidden by highlighting one or more from the Visible columns list and clicking the **Remove** button.

Move

You can also alter the order by which visible columns are displayed on the screen, using the **Move** buttons. Highlight one or more columns and press the up or down button to change its position in the ordering. Note that the top-to-bottom order of the columns in the list represents the left-to-right order of the columns as they are displayed in the view.

Help

This page can be reached by clicking the **Help** button.

Defaults

All of the settings in this dialogue can be restored to their original values at any time by clicking the **Defaults** button. A confirmation dialogue will be shown; click **Yes** to proceed with the restoration, or **No** to abort.

Cancel

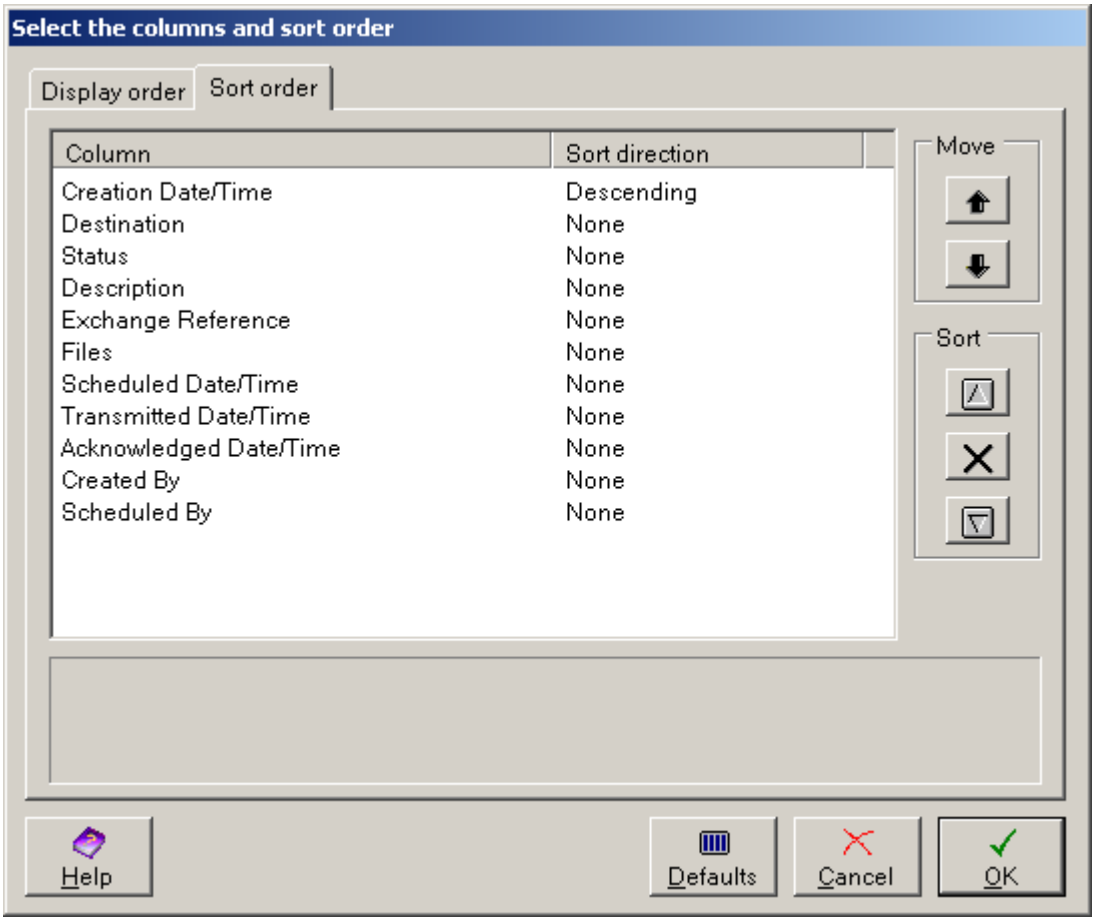
Clicking the **Cancel** button with unsaved changes will quit the dialogue, discarding all changes made in both tabs.

OK

To save all unsaved changes that you have made in this dialogue, click the **OK** button.

Columns – Sort Order

The second tab in the Columns dialogue is the Sort Order tab, shown below. From here, you can alter how the folders are sorted by choosing for each column whether to sort Ascending, Descending or not at all, as well as the order or precedence if sorting by multiple columns. You can also alter the sorting of the columns at a more basic level by clicking the column heading you want to sort by in the main view. Changes made in this manner will be saved and reflected in this dialogue.



The main feature of this panel is the columns list, which shows each column and the sort direction – if any – assigned to it.

Move

You can change the order of precedence by which the columns are sorted by using these buttons with one or more columns selected. Folders will be sorted first by the column at the top, then by the next column down, and so on. Note that to change the actual display order of the columns you should go to the 'Display Order' tab.

Sort

There are three available sort buttons allowing you to alter the sort direction of the selected column(s): ascending order, descending order, and none.

Help

This page can be reached by clicking the **Help** button.

Defaults

All of the settings in this dialogue can be restored to their original values at any time by clicking the **Defaults** button. A confirmation dialogue will be shown; click **Yes** to proceed with the restoration, or **No** to abort.

Cancel

Clicking the **Cancel** button with unsaved changes will quit the dialogue, discarding all changes made in both tabs.

OK

To save all unsaved changes that you have made in this dialogue, click the **OK** button.

Workstation – Common Actions

From the ENGDAT Workstation, there are many different actions that can be performed on folders. Those that are specific to the Inbound or Outbound views will be detailed in the relevant section. In the following section are the actions available to you from both the inbound and outbound views.

Workstation – Common Actions – Extract Folder

This option allows all of the files contained within an ENGDAT folder to be downloaded from the ODEX server and copied to a directory of your choice.

There are different ways that you can extract a folder. It is possible to extract an ENGDAT folder and decompress the ENGDAT files. It is also possible to extract an ENGDAT folder and name the extracted files according to the filenames used in the ENGDAT message.

With this extraction method, none of the files in the ENGDAT folder will be changed. Any compressed files will remain compressed.

When the files are extracted to the output directory, the files will be given the same filename that is used by the ODEX server. The ODEX server names ENGDAT files using a unique numeric filename with a filename extension of '.ENG', giving a filename such as 00000001.ENG.

ENGDAT files that have been received from a trading partner or ENGDAT files that have been scheduled for transmission to a trading partner are given numeric filenames with a filename extension of '.CMS', to indicate that the file is a communications file.

With a folder selected, this action can be accessed in the following ways:

- From the main menu, using **Actions >> Extract Folder**
- By right-clicking on the desired folder and clicking the **Extract Folder** action
- Using the toolbar button 

When you select the action, a standard browse dialogue will let you browse for a directory in which to place the files, or you may create a new one. Once you have selected a directory, click 'OK' to extract the ENGDAT files to the directory. Alternatively, You may select 'Cancel' to abort the action.

Workstation – Common Actions – Extract Folder with ENGDAT Filenames

This action is similar to the 'Extract Folder' action, but the extracted files will be named according to the filenames used in the ENGDAT message. As with the 'Extract Folder' option, no files will be decompressed.

With a folder selected, this action can be accessed in the following ways:

- From the main menu, using **Actions >> Extract Folder with ENGDAT Filenames**
- By right-clicking on the desired folder and clicking the Extract Folder with ENGDAT Filenames action.

When you select the action, a standard browse dialogue will let you browse for a directory in which to place the files, or you may create a new one. Once you have selected a directory, click 'OK' to extract the ENGDAT files to the directory. Alternatively, you may select 'Cancel' to abort the action.

Workstation – Common Actions – Extract and Decompress Folder

This action is similar to the 'Extract Folder with ENGDAT filenames' option, but this action will additionally decompress any compressed zip files in the folder.

There are three different ways that you can extract a folder. This method will rename each file to its original name and extension, if available in the ENGDAT message. It will also automatically extract any file it finds that is a compressed (ZIP) file. Note that directory structure within the zip file is not preserved.

With a folder selected, this action can be accessed in the following ways:

- From the main menu, using **Actions >> Extract and Decompress Folder**
- By right-clicking on the desired folder and clicking the Extract and Decompress Folder option

When you select the action, a standard browse dialogue will let you browse for a directory in which to place the files, or you may create a new one. Once you have selected a directory, click 'OK' to extract the ENGDAT files to the directory. Alternatively, You may select 'Cancel' to abort the action.

Workstation – Common Actions – Delete Folder

In either the inbound or the outbound view, you can delete one or more folders from the system, if you have the permissions to do so. Note that once a folder is deleted it cannot be retrieved, and all of its stored exchanged files are also deleted. When a received, scheduled or sent folder is deleted, this will remove the communications files that are associated with the folder.

With a folder selected, this option can be accessed in the following ways:

- From the main menu, using **Actions >> Delete**
- By right-clicking on the desired folder and clicking the **Delete** action
- By pressing the Delete key
- Using the toolbar button 

When you choose to delete a folder, a confirmation dialogue is displayed to ensure that a mistake is not being made. Click **Yes** to proceed with deletion, or **No** to abort.

Workstation – Common Actions – Print Report

For any folder with an ENGDAT message, a human-readable report containing all the information stored in the message can be generated. This report can be previewed and printed. When you click on this option, a dialogue like the one below will be shown:

Report

This dropdown box allows you to choose from the possible report definitions installed, displaying a short description of the chosen definition below.

Help

The **Help** button brings up this help page.

Cancel

The **Cancel** button quits the dialogue without generating, previewing or printing a report.

Settings

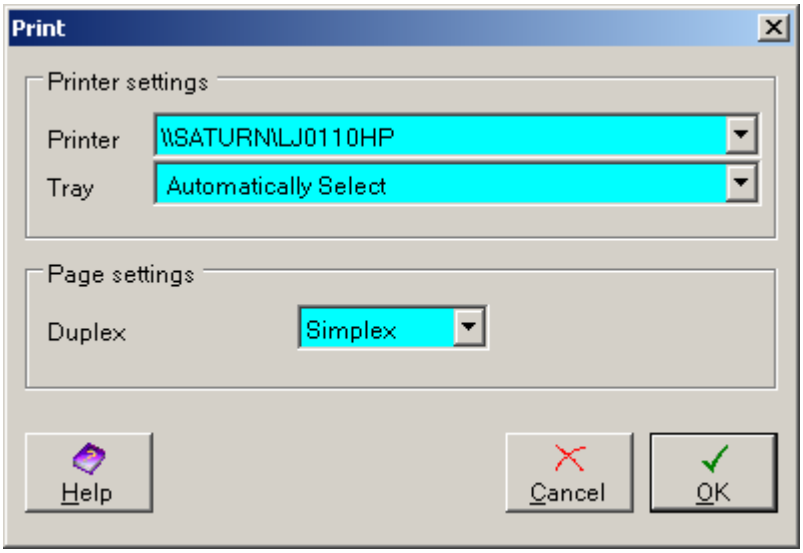
The ENGDAT message report does not currently have any settings that can be changed. This button is therefore disabled.

Preview

The **Preview** button will generate a report and allow you to view a representation of it having been printed, without actually printing it.

Print

The **Print** button will bring up the printing dialogue shown below:



From here you can use the dropdown boxes to choose a printer and a tray to which to send the print job. You can also alter how the document is actually printed with the Duplex setting.

Help

The **Help** button brings up this help page.

Cancel

The **Cancel** button quits the dialogue without generating or printing anything.

OK

The **OK** button generates the report and sends it to the chosen printer with the chosen settings.

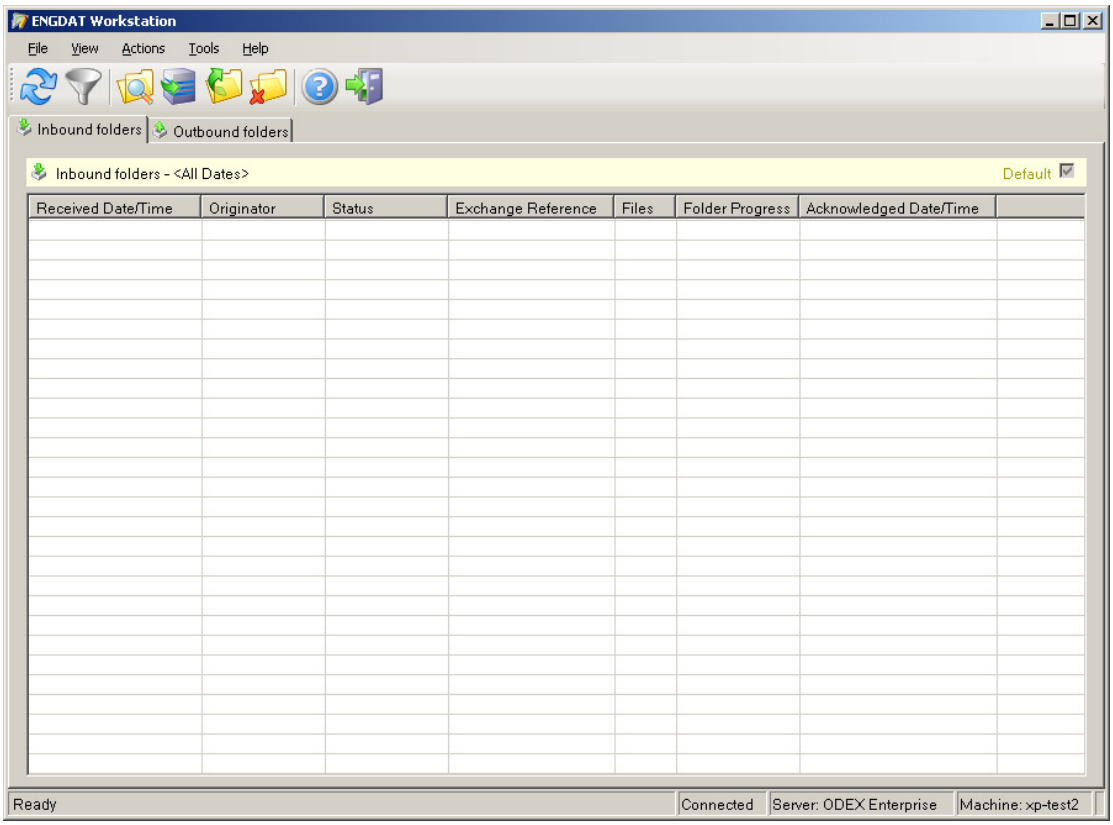
Inbound Folders

The first of the two views in the ENGDAT Workstation is the Inbound Folders section. The list will show all folders that have been received, or are in the process of being received.

How these folders are shown depends on view options that you can customise in the View menu. With the options in this menu you can change the order the columns are displayed, as well as how the folders are sorted and filtered.

You can click on the **Default** check box here to set or reset this tab to the default visible tab at start-up. A similarly labelled check box exists in the Outbound folders section, which you can use to set that tab to the default one.

Below is what the view should look like when you see it for the first time.



You can alter how the folders are sorted by clicking on the column headers, or in greater detail through the Columns dialogue.

Inbound Folders – Available Columns

Received Date/Time – The date and time that the folder was received.

Originator – The ENGDAT relationship to which the folder belongs.

Status – The status of the folder. Possible values are:

- Partly received
- Received
- Acknowledged

Exchange Reference – The exchange reference of the folder, generated by the sender on creation. This uniquely identifies folders received from this sender.

Files – The number of files in the folder, not including the ENGDAT message itself.

Folder Progress – Shows how many out of the total number of files in the folder have been fully transferred. This file count includes the ENGDAT message.

Acknowledged Date/Time – The date and time the folder was acknowledged by the ODEX server. This column will be blank if receipt of the folder has not been acknowledged.

Inbound Folders – Toolbar

There is 1 toolbar button specific to the Inbound Folders view.

This is the **View** button. When pressed, this will display the ENGDAT folder editor, though none of the fields can be changed.

Inbound Folders – Actions

There are many actions that can be performed at the Inbound Folders view, generally on specific folder(s). Most, such as extraction or deletion, are not specific to this view. Actions available from both views are described in the section entitled 'Workstation – Common Actions'. The following section details those actions that are specific to the inbound view.

Inbound Folders – Actions – View Folder

This option will open up the selected folder with the ENGDAT Folder Editor. When viewing inbound folders, all of the fields in the editor can be viewed, but not modified.

With a folder selected, this option can be accessed the following ways:

- From the main menu, select **Actions >> View Folder**
- By right-clicking on the desired folder and choosing the **View Folder** action
- By pressing the Enter key
- By double clicking the desired folder
- Using the toolbar button 

Any of these methods will bring up the folder editor. Please see the section entitled 'ENGDAT Folder Editor' for more information on the folder editor.

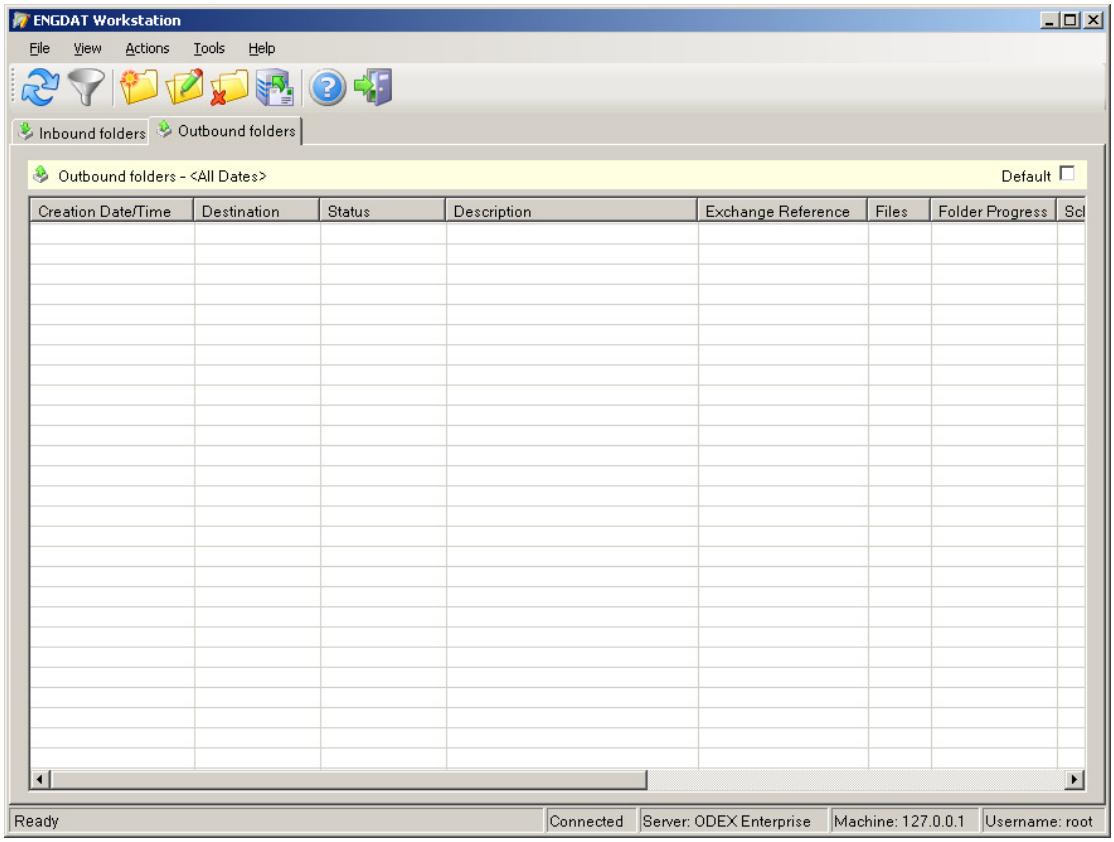
Outbound Folders

The second view available to you is the Outbound Folders section, accessible through the tab. The list will show all ENGDAT folders that have been created on the ODEX server machine for the purposes of scheduling and transmission, provided that they meet the filter criteria.

How these folders are shown depends on view options that you can customise in the View menu. With the options in this menu you can change the order the columns are displayed, as well as how the folders are sorted and filtered.

You can click on the **Default** check box here to set or reset this tab to the default one on start-up. A similarly labelled check box exists in the Inbound view, which you can use to set that view to the default one on program start-up.

Below is what the view should look like when you see it for the first time.



You can alter how the folders are sorted by clicking on the column headers, or in greater detail through the Columns dialogue. You can view the columns dialogue by clicking **View >> Columns** or by pressing **Ctrl + C.**

Some folders will be displayed in a different colour to highlight their state. Folders that contain invalid data are shown with red text and cannot be scheduled. Folders that have run into errors during transmission have a red background. For folders with transmission errors, view the Scheduled Files view in the ODEX workstation for further details.

Outbound Folders – Available Columns

Creation Date/Time - This is the date and time that the folder was originally created.

Destination - This is the ENGDAT relationship (link) being used by the folder, which contains details on the sender, recipient, communications settings, data defaults and so on. You can view, create, edit and delete relationships in the Comms section of the ODEX Administrator.

Status - The status of the folder. Possible values are:

- Created (valid)
- Created (invalid)
- Scheduled
- Partly sent
- Sent
- Acknowledged

Description - This is the optional description that was entered on creation of the folder for easy identification.

Exchange Reference - The exchange reference of the folder, generated on creation according to the settings in the ENGDAT relationship.

Files - The number of files in the folder, not including the ENGDAT message itself.

Folder Progress – Shows an estimate of how much of the folder has been transmitted, as a percentage.

Scheduled Date/Time - The date and time the folder was scheduled to be transmitted, if applicable.

Transmitted Date/Time - The date and time the folder was transmitted to the destination server, if applicable.

Acknowledged Date/Time – For folders where all files have in the folder have been acknowledged, this is the date and time at which the folder was marked as acknowledged.

Created By - The ODEX user who created the folder, if security is being used. If security is disabled, this column will be blank.

Scheduled By - The ODEX user who scheduled the folder, if security is being used and it has been scheduled. If security is not being used, or the folder has not been scheduled, this column will be blank.

Outbound Folders – Toolbar

There are four toolbar buttons specific to the Outbound Folders view. They correspond to certain available actions, which are discussed in detail in the next section and in the common actions section.

This is the **Create Folder** button. When pressed, it will ask you to choose an ENGDAT relationship, create a new blank folder according to the relationship settings, then open up ENGDAT Folder editor. From here files and an ENGDAT message can be added to the new folder.

This is the **View or Edit** button. When pressed, the selected ENGDAT folder will be displayed in the ENGDAT folder editor. If the folder has already been scheduled, then the editor will be read-only.

This is the **Schedule** button. When pressed, it will schedule the selected folder for transmission, or ask you if you want to re-schedule the folder if it has already been scheduled. The folder will not actually be transmitted until the trading partner's network has been called.

Outbound Folders – Actions

There are many actions that can be performed with the Outbound Folders view. Actions that are also available on the Inbound Folders view are described in the section entitled 'Workstation – Common Actions'. The following section details those actions that are specific to the outbound view only.

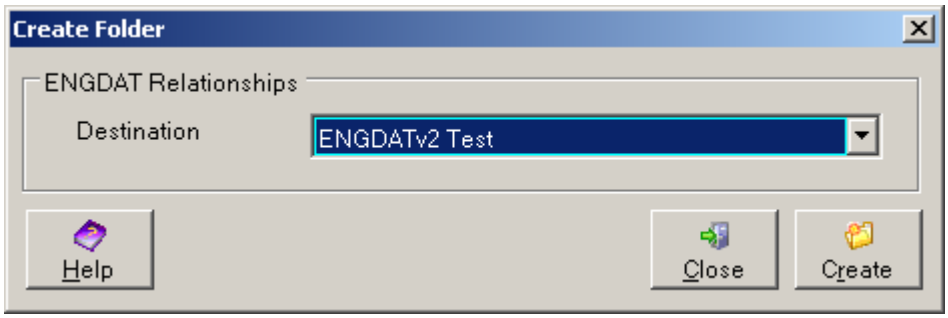
Outbound Folders – Actions – Create Folder

This action can be accessed the following ways:

- From the main menu, select **Actions >> Create Folder**

- By right-clicking in the area of the table and choosing the **Create Folder** action
- Using the toolbar icon 

Any of these actions will cause the following dialogue box to be shown:



ENGDAT Relationships

This dropdown list contains all of the ENGDAT relationships set up in your system. The ENGDAT relationship determines the origin and destination company details, the ENGDAT message version etc.

Please refer to the section entitled 'ENGDAT Relationships' for information on ENGDAT Relationships.

Help

The **Help** button brings up this help page.

Close

The **Close** button quits the dialogue without creating a new folder or opening the editor.

Create

The **Create** button will create a new empty folder using the settings from the chosen relationship and display it in the ENGDAT Folder editor. From here you will be able to add files to the folder and optionally an ENGDAT message.

Outbound Folders – Actions – Edit Folder

With a folder selected, this option can be accessed the following ways:

- From the main menu, select **Actions >> Edit Folder**
- By right-clicking on the desired folder and choosing the **Edit Folder** action
- By pressing the Enter key
- By double clicking on the desired folder
- Using the toolbar icon 

Any of the above actions will display the selected folder in the ENGDAT Folder Editor. If the folder has not been scheduled or sent, you will be able to modify its contents.

For further information on the ENGDAT folder editor, please refer to the following section:

Outbound Folders – Actions – Schedule Folder

With a folder selected, this action can be accessed the following ways:

- From the main menu, select **Actions >> Schedule Folder**
- By right-clicking on the desired folder and choosing the **Schedule Folder** action
- Using the toolbar icon 

This action will schedule the selected folder for transmission. If the selected folder has already been scheduled or sent, you will be asked to confirm if you want to re-schedule the folder.

When the folder is scheduled for the first time, for each file in the folder a new communications file will be created and scheduled for transmission to the destination trading partner.

If you reschedule a folder that has already been scheduled or sent, the existing scheduled or sent files that were created the first time the folder was scheduled will be rescheduled. New communications files will not be created.

The scheduled files will be transmitted when a call is made to the destination trading partner. The call will be made automatically, provided the trading partner network settings allow this and the network is not in 'retry' mode.

You can monitor the progress of the scheduled files in the 'Scheduled Files' tab of the ODEX workstation. The newly scheduled ENGDAT files can be identified by the VFN shown in the 'VFN/Message ID' column and the 'Scheduled Date/Time'. The ODEX Communications Monitor may also be used to monitor the progress of the files as they are transmitted.

When rescheduling a folder, if the existing scheduled or sent files have been removed, it will not be possible to reschedule the folder. This can be overcome by creating a copy of the folder and updating the files on the server.

Outbound Folders – Actions – Copy Folder

With a folder selected, this option can be accessed the following ways:

- From the main menu, select **Actions >> Copy Folder**
- By right-clicking on the desired folder and choosing the **Copy Folder** action

This action will produce a newly created copy of the selected folder, with a newly generated exchange reference and creation date. The new folder will be immediately visible in the list of folders. Copies of the files included in the folder will be made on the ODEX server. Note that the files stored by the server will not be updated from their original locations.

Outbound Folders – Actions – Copy and Refresh Folder

With a folder selected, this option can be accessed the following ways:

- From the main menu, select **Actions >> Copy and Refresh Folder**
- By right-clicking on the desired folder and choosing the Copy and Refresh Folder action

This action will produce a newly created copy of the selected folder, with a newly generated exchange reference and creation date, including all of the exchanged files contained in the original folder.

The difference between this and the standard copy action is that all files contained in the folder are sent from their original locations to the server.

For an example of where this action is useful, consider the scenario where revisions of the same CAD drawing are being sent to a trading partner. The CAD drawing is created and added to a new ENGDAT folder. When the folder is saved, the CAD drawing file is copied and sent from the ODEX ENGDAT Workstation client to the ODEX Server and stored by the server.

The folder containing the first version of the CAD drawing is then scheduled and transmitted. At a later date, revisions are made to the CAD drawing and the new version must be sent to the trading partner in a new folder.

Rather than creating a brand new folder for the revised CAD drawing and entering all of the details again, the existing folder can be copied and any necessary changes to the ENGDAT message details can be made.

Using the standard folder copy action would result in a new folder being created that contained a copy of the original CAD file before the revisions were made, since the file is copied from the version stored by the ODEX Server.

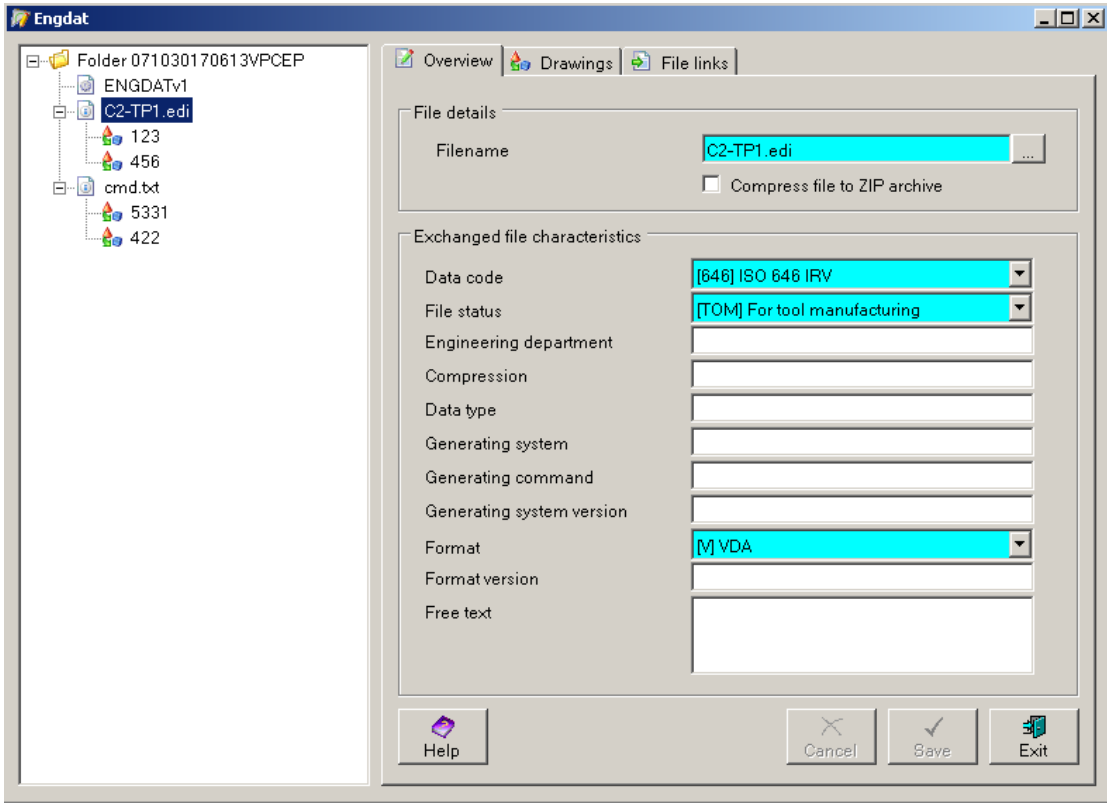
Using the ‘Copy and Refresh Folder’ action, the folder is copied in the same way, but the updated CAD file is re-sent to the server from its original location. This results in a new copy of the folder being created ready for editing, that contains the updated CAD file.

ENGDAT Folder Editor

The ENGDAT Folder Editor is the part of the ENGDAT Workstation that provides the ability to view and manipulate the contents of the ENGDAT message in an ENGDAT folder, as well as adding, removing or updating the files within the folder.

There are generally two possible modes that the folder editor can be in, depending on whether the folder is inbound, scheduled, sent or outbound. In the former cases, all fields will be disabled and the data in the message can only be viewed. In the latter case, you are able to modify the data in the folder, by for example adding a file or changing the contents of the fields.

There are two parts to the folder editor: the navigation panel on the left, where a graphical representation of the viewed folder is displayed; and the information panel on the right, where details of the entry selected in the navigation panel are displayed. Below is an example of a typical situation in the folder editor.



ENGDAT Folder Editor – Navigation Panel

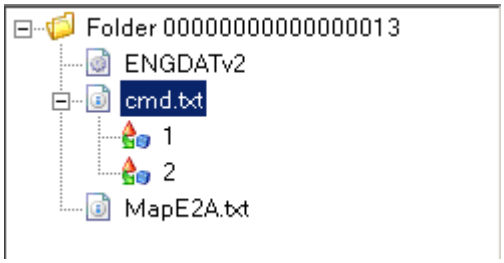
The navigation panel is on the left hand side of the ENGDAT folder editor. From here, you can use the mouse to navigate between some of the different entries within the folder and the ENGDAT message if present.

Clicking on the expand buttons marked by **+** signs will show you what is contained within an entry; clicking the collapse buttons marked by **–** signs will hide this information. You can also expand or collapse the entries by double clicking on that entry.

To display detailed information about an entry in the information panel on the right, select an entry in the navigation panel. If the selected entry is a data file included in the folder that does not have any detailed information, the information panel will revert to showing information applicable to the ENGDAT folder.

Clicking onto another entry in the navigation panel while there are unsaved changes in the information panel will cause the editor to ask you if you wish to save or discard the changes before proceeding.

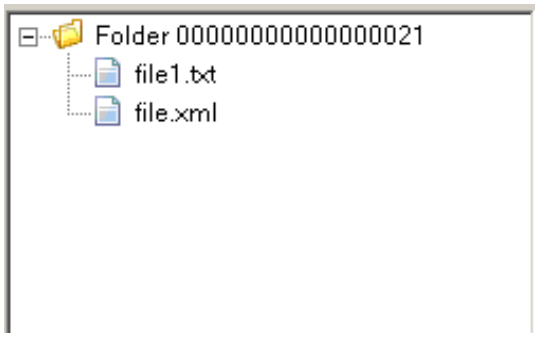
The navigation panel will contain entries for the folder, the ENGDAT message if present, exchanged files, contained files and drawings. Below is an example of how the navigation panel looks with a simple folder.



This example shows an ENGDAT folder with the exchange reference '00000000000000013'. The folder contains an ENGDAT version 2 message, as indicated by the ENGDATv2 entry. The folder also contains 2 data files, named 'cmd.txt' and 'MapE2A.txt' as indicated by the 2 file entries underneath the folder entry. The section in the ENGDAT message describing the file 'cmd.txt' contains 2 drawing descriptions, with drawing numbers '1' and '2'.

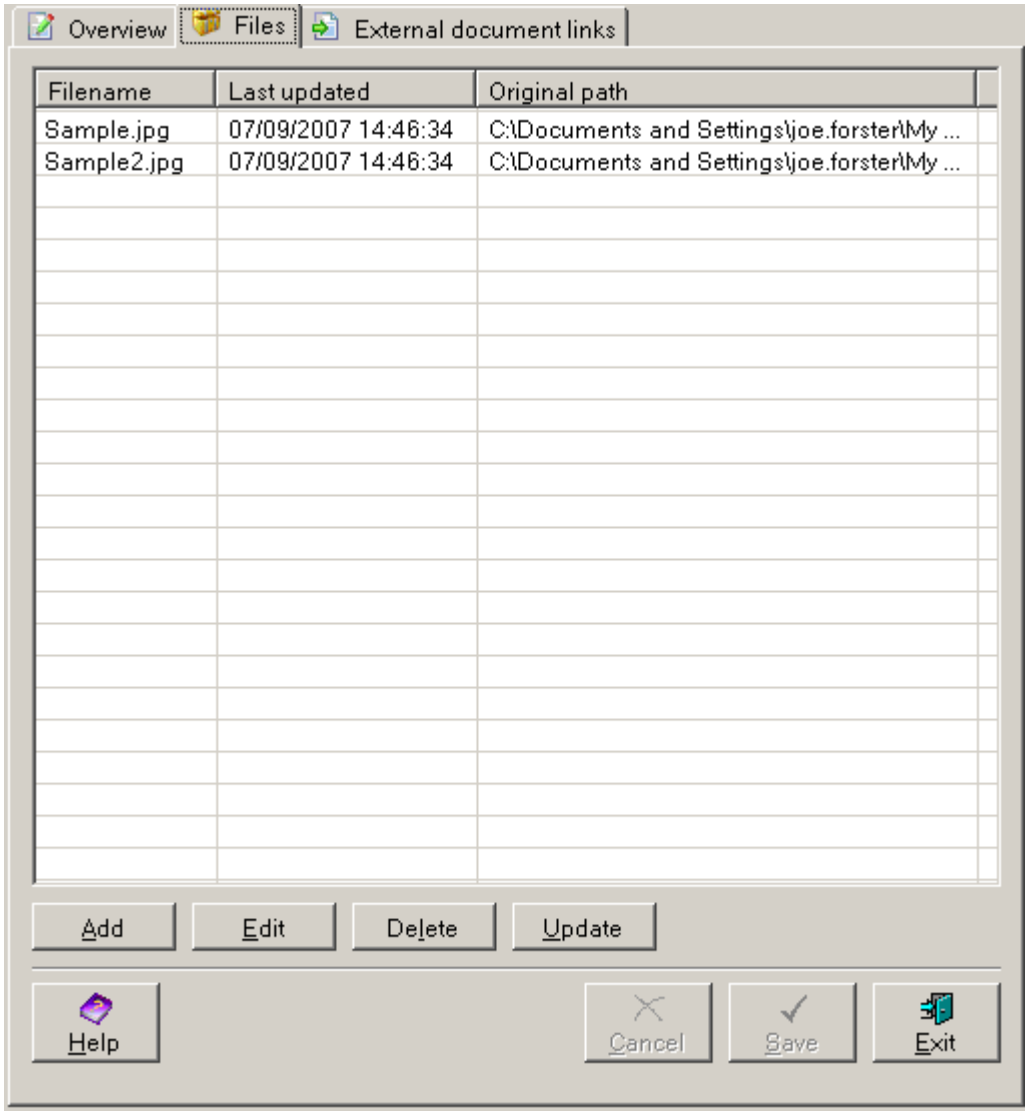
Both of the files in this example are described in the ENGDAT message, as indicated by the icon next to each. Files that are contained in the folder and described in the ENGDAT message are always shown with an 'information' symbol.

The following example shows an ENGDAT folder that contains 2 files, but no ENGDAT message. Where there is no ENGDAT message, the files are shown with an icon that does not show the information symbol.



ENGDAT Folder Editor – Information Panel

The information panel in the folder editor is situated on the right hand side of the dialogue. This panel is where the viewing and editing of data in the ENGDAT folder is done. The tabs at the top can be navigated to view different pages of information for the entry that is being viewed. Below is an example of a typical situation in the information panel.



There are some differences in each tab page that make them warrant their own help pages. However, the following buttons are common to all pages:

Help

Clicking on the **Help** button will send you to the most relevant page within these help pages for the tab that you are currently on.

Cancel

The **Cancel** button will be enabled if unsaved changes are present on the page. Note that in this case all data on each tab is discarded, not just the tab currently selected. Whenever unsaved changes are about to be discarded, you will be asked for confirmation to prevent accidental loss of changes. Click **Yes** to discard the changes or **No** to do nothing and leave the page as it is.

When viewing the folder details (the folder is selected in the navigation panel), the **Cancel** button behaves slightly differently. Since this is the 'top level' of the ENGDAT folder, clicking the **Cancel** button will close the editor without saving changes to the folder.

Save

The **Save** button will be enabled if any part of the current entry has been changed. Note that, as with the **Cancel** button, all unsaved changes across all tabs will be saved upon clicking this button.

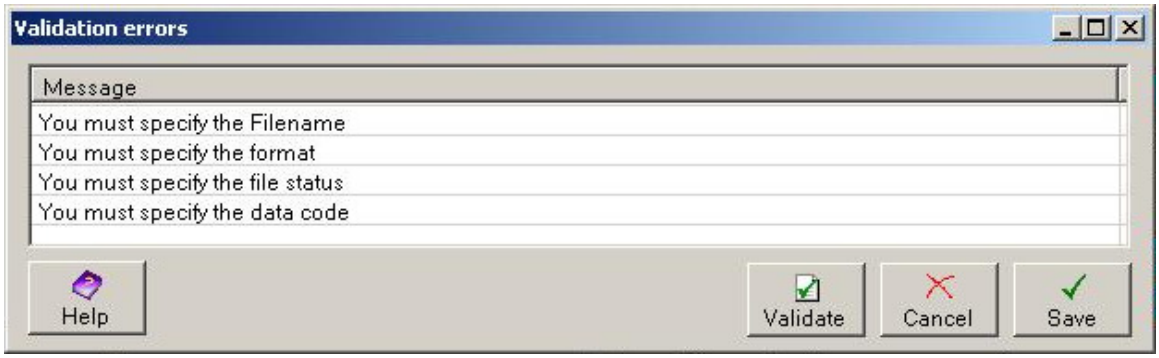
When viewing the top level of the folder, the **Save** button behaves slightly differently. This will save the folder and exit from the editor.

Exit

The **Exit** button is visible in most tabs, except at the root where both the **Save** and **Cancel** buttons will exit the editor if clicked. The **Exit** button is essentially the equivalent of the **Save** button at the root of the folder; you will be asked for confirmation on saving and quitting, then the editor will close.

ENGDAT Folder Editor – Validation

The validation profile determines which fields in the editor require a value before the ENGDAT folder can be saved. If you attempt to save the details of a file when a required field is missing, you will see a dialogue box like that shown below.



You can double-click an entry in the list to bring the relevant field into focus, where you may then enter the required value.

Once you have made changes, click the '**Validate'** button to re-validate the page. If you have corrected all of the errors, the dialogue box will close and you will be able to save your changes.

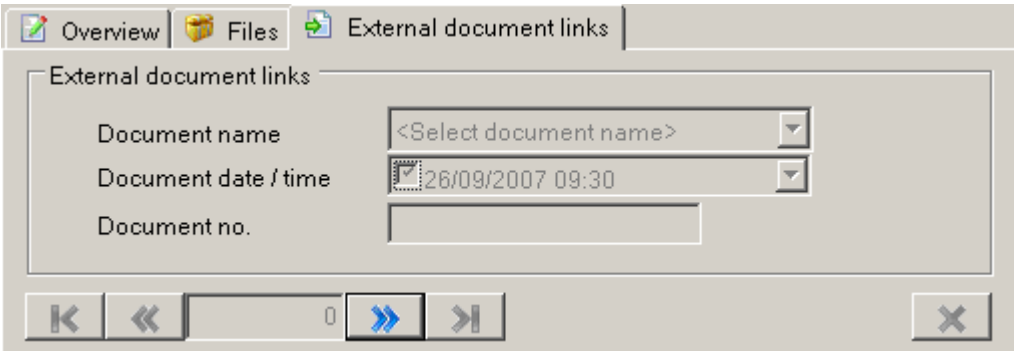
At any time, you can click the '**Save'** button, which will save the page and bypass the validation checks. However, this will result in the ENGDAT folder being flagged as invalid and you will not be able to schedule the folder.

Alternatively, you can click '**Cancel**' to return to the page and make changes further changes.

ENGDAT Folder Editor – Navigation

In some areas of the ENGDAT Folder Editor, the information panel on the right allows you to navigate through a collection of entries of some kind, such as external document references, drawings or links to other files.

This section describes how to use these navigation buttons. Shown below is the external document references page for ENGDAT version 1 and version 2 messages.



This is how the page will look when you first view the page in a new ENGDAT message. As you can see, all of the fields are disabled because the ENGDAT message does not contain any document reference entries. These will be enabled once an entry has been added.

The buttons at the bottom of the page are used to add new entries, remove entries and navigate through the entries. The following summarises the function of each of the buttons used to control adding, removing and viewing/editing document references in the collection.

Displays the first entry.

Displays the previous entry.

If the entry currently being displayed is not the last entry, this button will advance to the next entry. If the entry being displayed is the last entry in the collection, a new entry will be added.

Displays the last entry.

Deletes the entry currently being displayed. If there is only one entry, the fields on the page will be disabled, as shown above. To enable the fields again, you must add another entry by clicking the button.

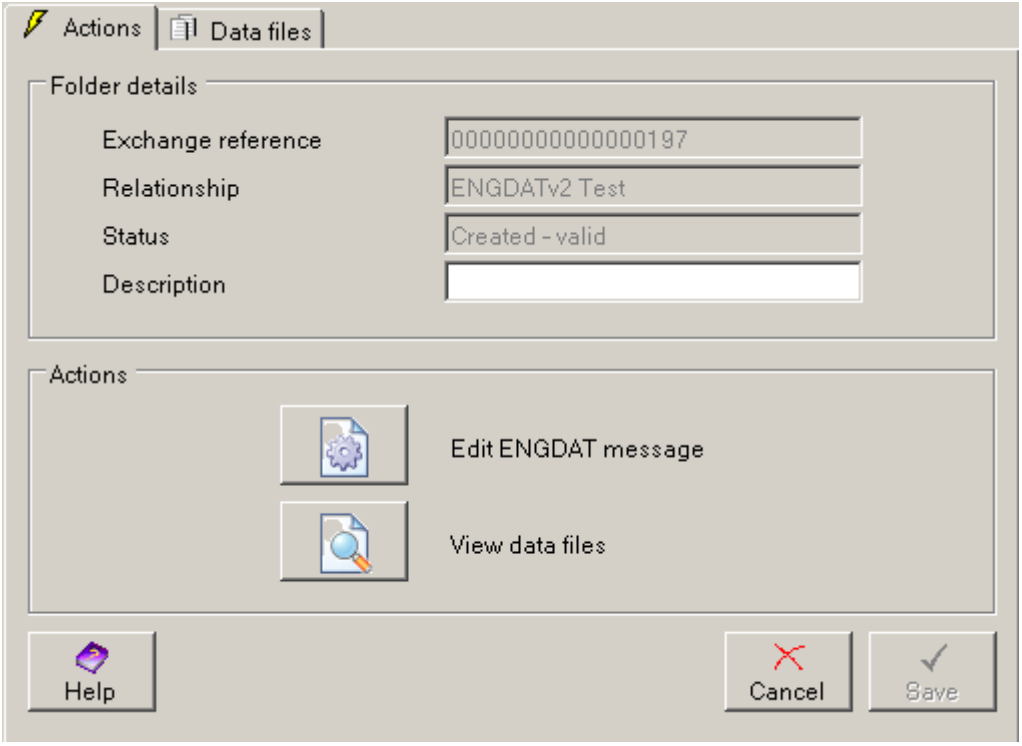
While navigating through the collection of entries, you may modify the field values. Any changes that you make are not committed until you click the **Save** button. You may edit several entries before you save your changes – changes are not lost when you navigate to a different entry. This means that when you click the **Save** button, all of your changes across all of the entries are saved – not just changes to the entry that is currently being displayed.

When you navigate through the entries, or add a new entry, the entry that is currently displayed will be validated to ensure that all mandatory fields have a value entered. If you attempt to move to another entry when a mandatory field has no value, a message will be displayed requesting a value for the field.

The set of navigation buttons are used in several different areas of the ENGDAT folder editor. Wherever you see these buttons, they will behave in the same way, whether you are dealing with external document links, drawings, contained files or links to other files.

ENGDAT Folder Editor – Folder Actions Tab

When the editor is displayed, the first page that you will see is the actions tab of the folder view, shown below. This page provides the starting point when creating or viewing a folder.



Folder Details – Exchange Reference

This contains the exchange reference that has been allocated to this folder. This is generated when the folder is created and cannot be changed.

Folder Details – Relationship

This field gives the name of the ENGDAT relationship that is being used, which determines the origin and destination companies being used and the ENGDAT message settings. This cannot be changed once a folder has been created.

Folder Details – Status

This contains the status of the folder. For a new folder, this will always be 'Created – valid'.

Folder Details – Description

This field is where you can enter a description of the folder to assist in identifying it. The description will be shown in the 'Description' column in the workstation. This field is for information only – it is not transmitted with the folder.

Actions – Add ENGDAT Message

This button allows you to add a new ENGDAT message to the folder or view/edit an existing ENGDAT message. If the folder already contains an ENGDAT message, the button text will be 'Edit ENGDAT message' or 'View ENGDAT Message', depending on whether the folder can be edited.

Click this button if you would like to add an ENGDAT message to the folder. You will see that an entry will be added for the ENGDAT message in the navigation panel, underneath the folder and the message details will be displayed in the information panel on the right.

Actions – Edit ENGDAT Message

You will only see this button if the folder already contains an ENGDAT message. Clicking this button will select the ENGDAT message entry in the navigation panel and show the message details in the information panel on the right.

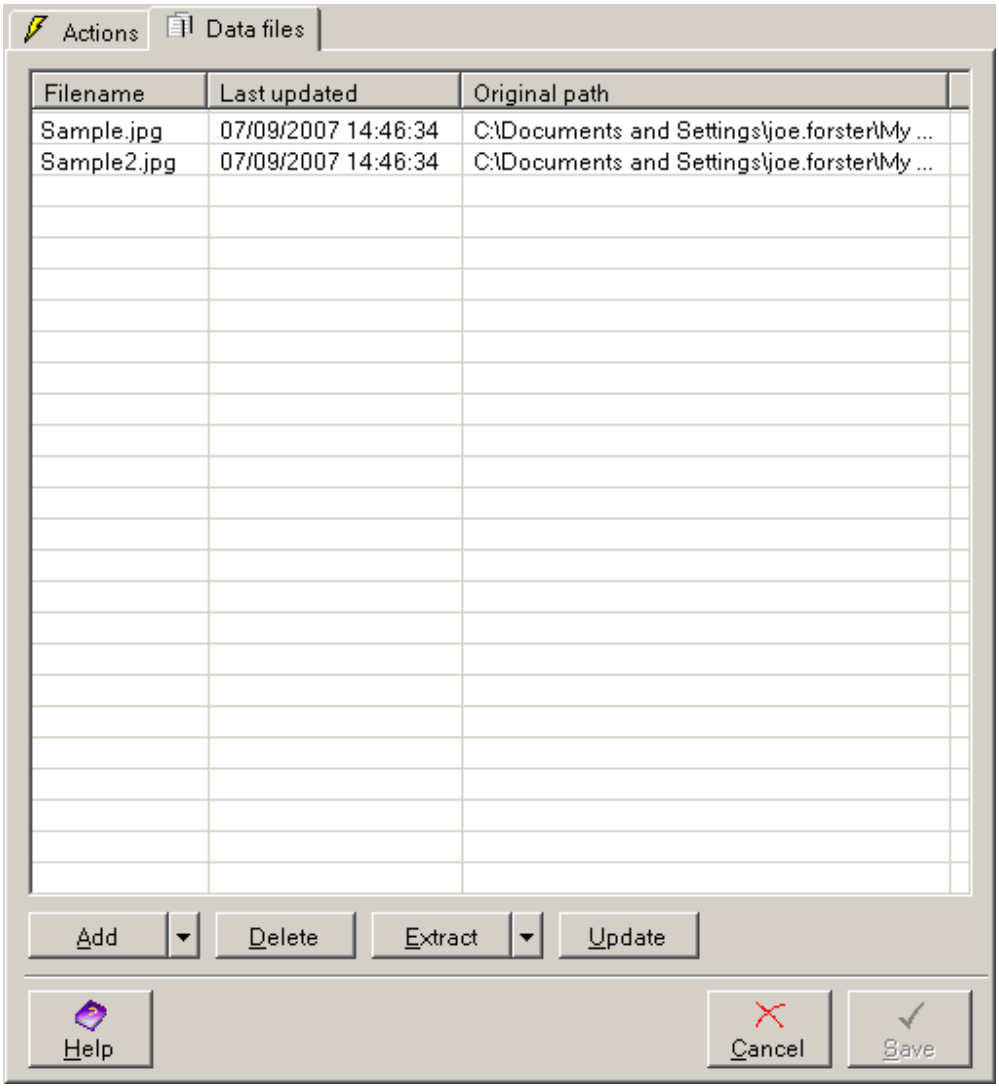
Actions – View Data Files

Clicking on this button will send you to the Data Files tab. Equivalently, clicking on the tab at the top will also send you there.

ENGDAT Folder Editor – Folder Data Files Tab

The Data Files tab lists the files that are contained in the folder. This includes all files, regardless of whether they are described in the ENGDAT message. You can use the buttons to add, delete, extract or update files from this view. However, if you want to view the details of a file that is included in the ENGDAT message, you must click on the entry for that file in the navigation panel under the ENGDAT message.

All of the buttons on the page will be enabled for folders created in ODEX that have not been scheduled or sent. All buttons except for the extract button will be disabled for folders that have been received, scheduled or sent.



Add

Clicking on the **Add** button will show a pop-up menu providing you with two options: **Add file** will simply add the uncompressed file to the folder. **Add and**

compress file will compress the file to a zip file before adding the file to the folder.

Delete

Clicking on the **Delete** button with one or more files selected in the table will result in a confirmation dialogue being shown. Clicking **Yes** will remove that file and clicking **No** will abort the action. However, after deleting files it is still possible to undo the changes by clicking cancel and discarding changes to the folder.

Extract

Clicking on the **Extract** button with a file selected in the table will show a pop-up menu providing you with two options. **Extract** will simply extract the file with the directory and file name of your choice. **Extract and decompress** will also decompress the file if it is a compressed (ZIP) file.

Update

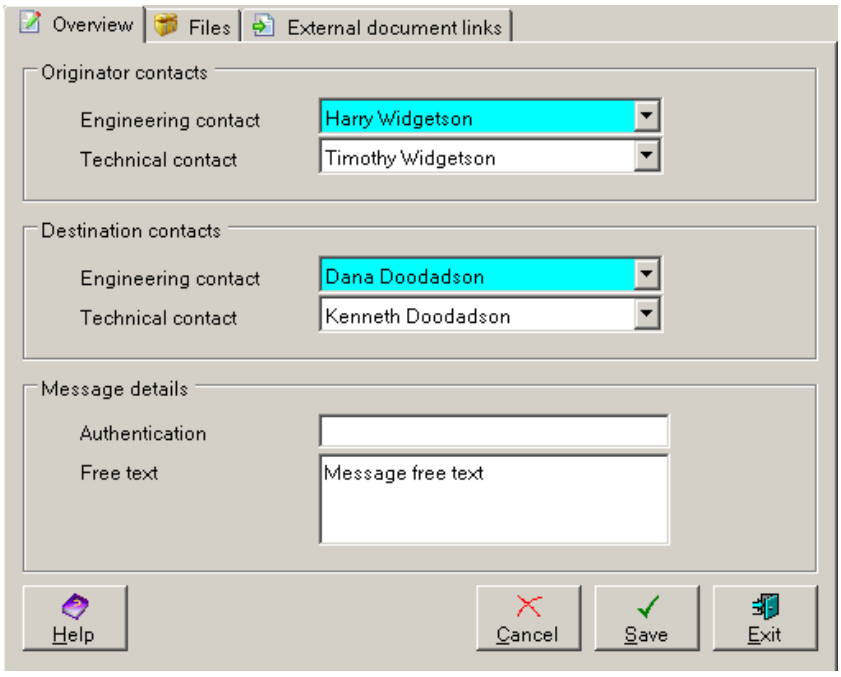
Clicking on the **Update** button will resend the file from its original path to the server, thus updating the file if it has been changed. Once the file has been updated, the last updated date will change.

ENGDAT Folder Editor – ENGDAT Message Overview Tab

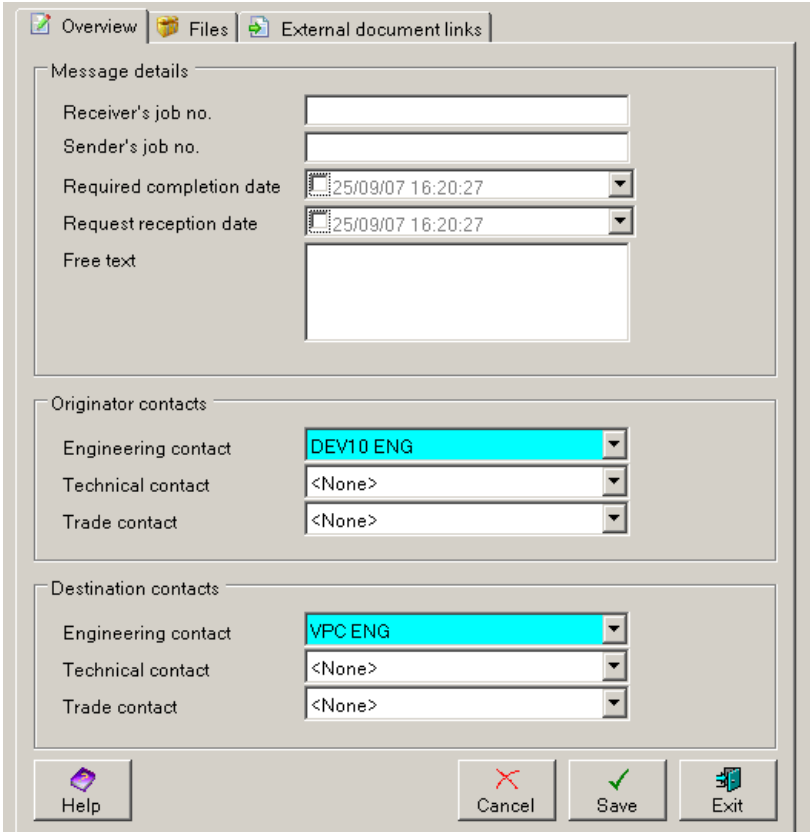
This is the first page that you will see after adding an ENGDAT message, clicking the view ENGDAT message button.

The overview contains general information on the contacts and details associated with the message itself. From here you can view and change this information. The available fields on the tab differ slightly depending on whether the ENGDAT version being used is 1, 2 or 3.

Below is an example of this tab in use. The example shows the overview of an ENGDAT version 2 message. Note that if you are viewing an inbound folder or a folder that has been scheduled, all of these fields will be disabled.



The following example shows the message overview for an ENGDAT version 3 message.



As you can see, the ENGDAT version 3 message includes some additional fields that are not present in ENGDAT versions 1 and 2.

Some fields may also be disabled, depending on the validation profile that is in use. This is to prevent values being entered in fields that are not used by the destination trading partner. The generic validation profiles included with ODEX allow values to be entered for all fields. Some manufacturer-specific validation profiles are more restrictive – for example, the Swedish OEM profile does not allow technical contact details to be selected, because the Swedish manufacturers supported in the profile do not require technical contact details.

Contacts

The drop-down lists of contacts allow you to specify which contact details will be included in the ENGDAT message. Subject to validation profile restrictions, ENGDAT message versions 1 and 2 allow you to select engineering contact and technical contact details. With ENGDAT message version 3 you can additionally select trade contact details.

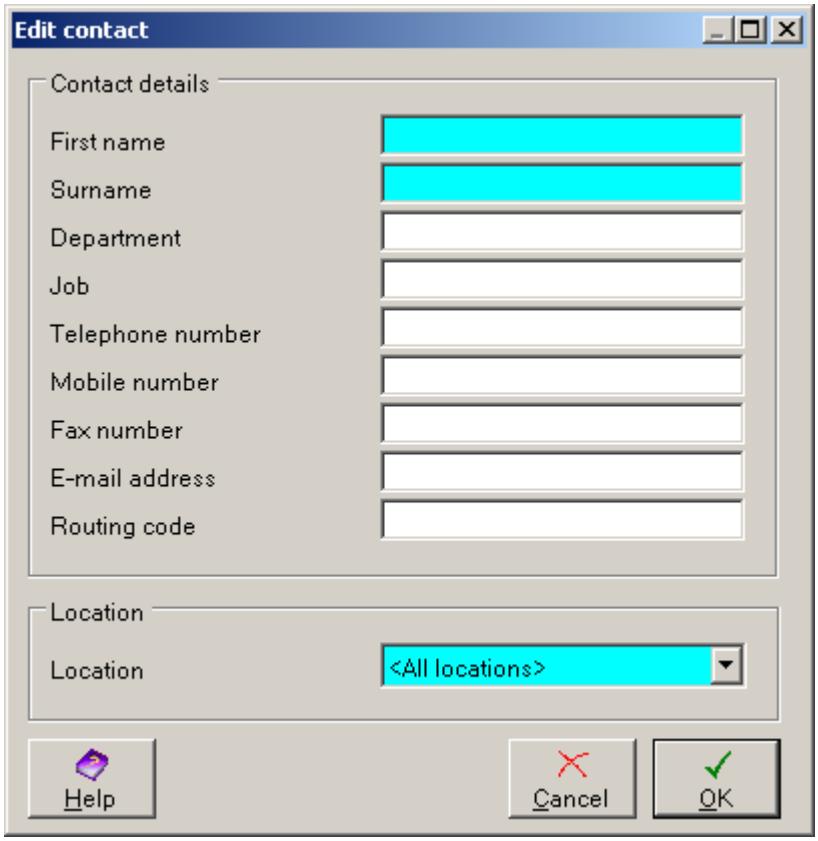
For an outbound ENGDAT message, the originator contact details will be included in the 'Sender Details' section and the destination contact details will be included in the 'Receiver Details' section of the ENGDAT message. (Referred to as the SDE and RDE segments respectively, in ENGDAT versions 1 and 2).

When a message is added to a folder, some contacts will already be selected. The selected contacts are those that were chosen as default contacts when setting up the ENGDAT relationship. The values can be changed here if necessary.

Adding Contacts

If you need to add new contacts, select <Add contact> from any of the drop-down lists to create a new contact. The contact will be stored as a contact of the

origin or destination company, depending on whether you choose a drop-down list in the origin or destination contacts group.



The above dialogue is the same in form and function as the edit contact dialogue in the ODEX Administrator. Please refer to the section entitled 'Contacts' for further details. If you save the contact, it will be selected in the list upon returning from the dialogue box.

Message Details – Authentication (ENGDATv1 and ENGDATv2 only)

This field corresponds to the Authentication field in the ENGDAT Message Identification (referred to as the MID segment). Only enter a value in this field if your trading partner has indicated that this is required.

Message Details – Free Text

This field is for the entry of free-form text regarding the message or folder as a whole.

Receiver's Job No (ENGDATv3 only)

Unique number of the job, as given by the receiver.

Sender's Job No (ENGDATv3 only)

Unique number of the job, as given by the sender.

Required Completion Date (ENGDATv3 only)

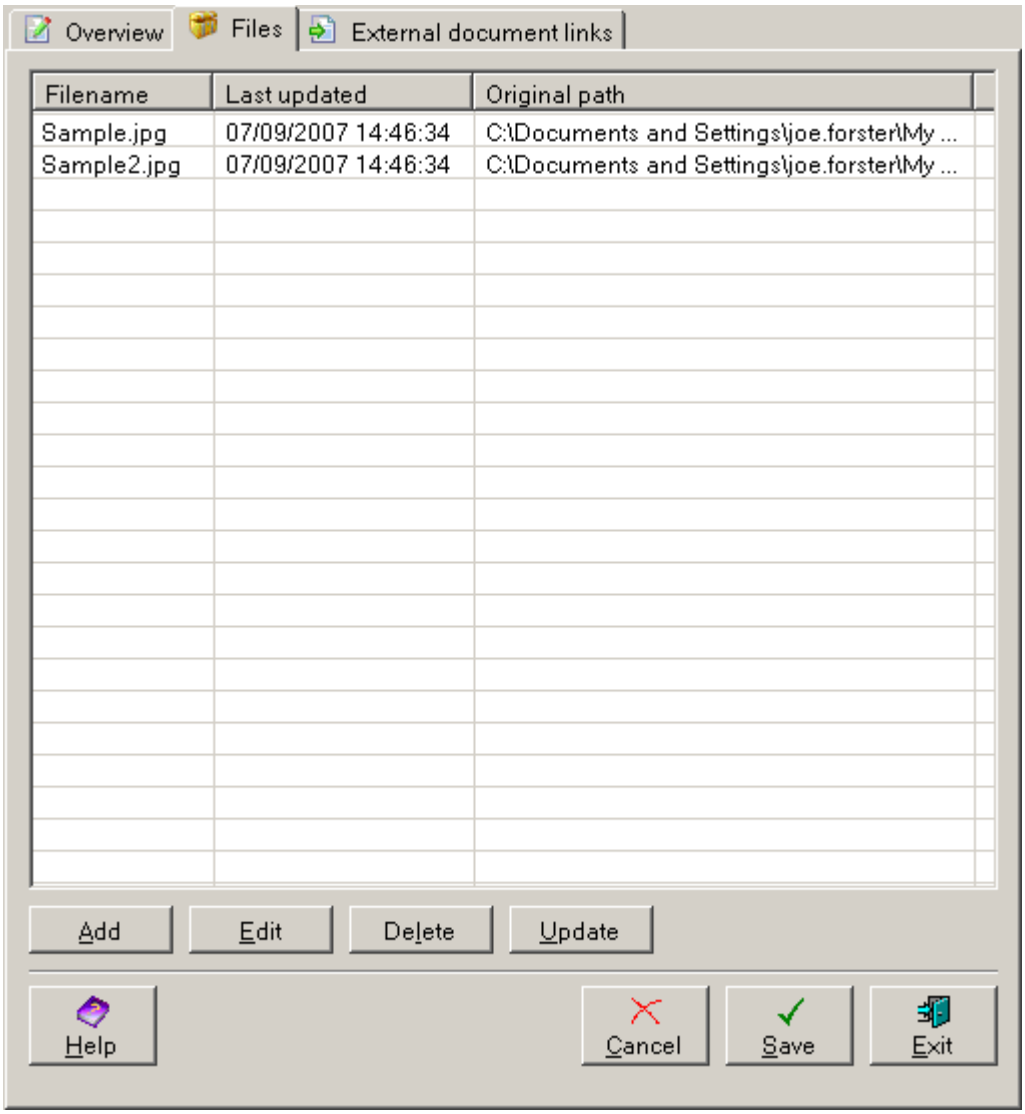
Date, and optionally time, of the deadline for supplying data. To omit this value, uncheck the checkbox to the left of the date.

Request Reception Date (ENGDATv3 only)

Date, and optionally time, when the sender's technical department receives the sending request from the receiver. To omit this value, uncheck the checkbox to the left of the date.

ENGDAT Folder Editor – Message Exchanged Files

The exchanged files page is the same regardless of which ENGDAT version is being used. It is quite similar to the Data Files tab in the root folder entity, but only the files referred to in the ENGDAT message are listed here. It is also possible to navigate into a file entry from here as well as with the tree view.



Add

Clicking on the **Add** button will add a new blank exchanged file to the message, sending you to its Overview tab. You will notice that new entries will be added to the navigation panel for the new file – one under the ENGDAT message, corresponding to the file details in the message and one under the folder, corresponding to the physical file itself within the folder.

Edit

With a file selected in the list, clicking on the **Edit** button will send you to the Overview of the details for that file. You can also do this by selecting an entry in the list and pressing **Enter.**

Delete

With one or more files selected in the list, clicking on the **Delete** button will bring up a confirmation dialogue. If you click **Yes**, the file will be removed. If you click **No**, this action will be aborted. Note that removing the file from the ENGDAT message completely removes the file from the folder.

Update

Clicking on the **Update** button uploads the file to the server from its original location, updating the file on the server. Once the file has been uploaded, the last updated date will change to the current date and time.

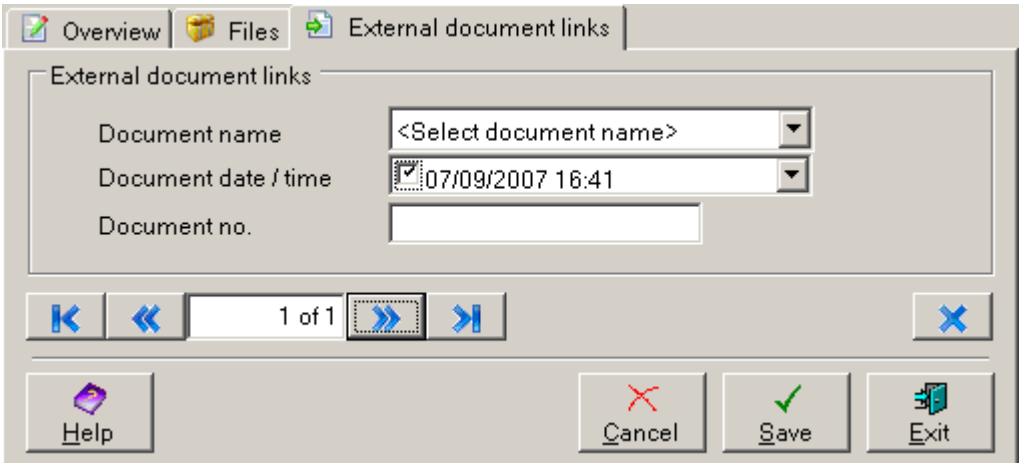
ENGDAT Folder Editor – External Document Links

This page allows you to add references in the ENGDAT message to documents or files that are not contained in the folder. External document references are written to the DAN segment in ENGDAT version 1 and 2 messages and the DAN element group in the ENGDAT version 3 message.

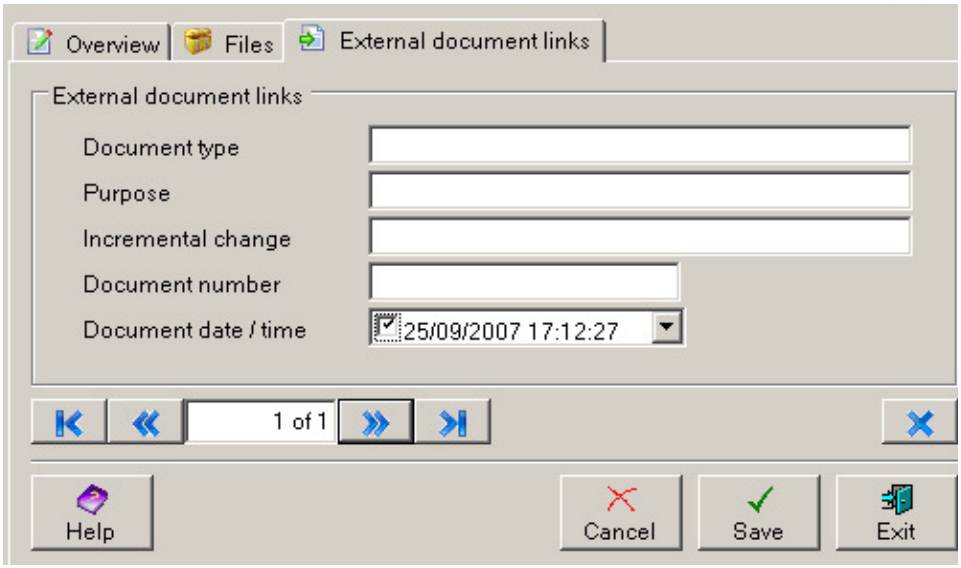
You will only be able to select this page if the validation profile in use allows external document references to be included in the ENGDAT message. With some validation profiles, such as the Swedish OEM profile, this tab is hidden because the destination trading partner does not support external document references.

The available fields differ slightly between ENGDAT message versions. ENGDAT versions 1 and 2 are the same, while ENGDAT Version 3 includes some additional fields.

The following shows what the page looks like when working with a version 1 or version 2 ENGDAT message.



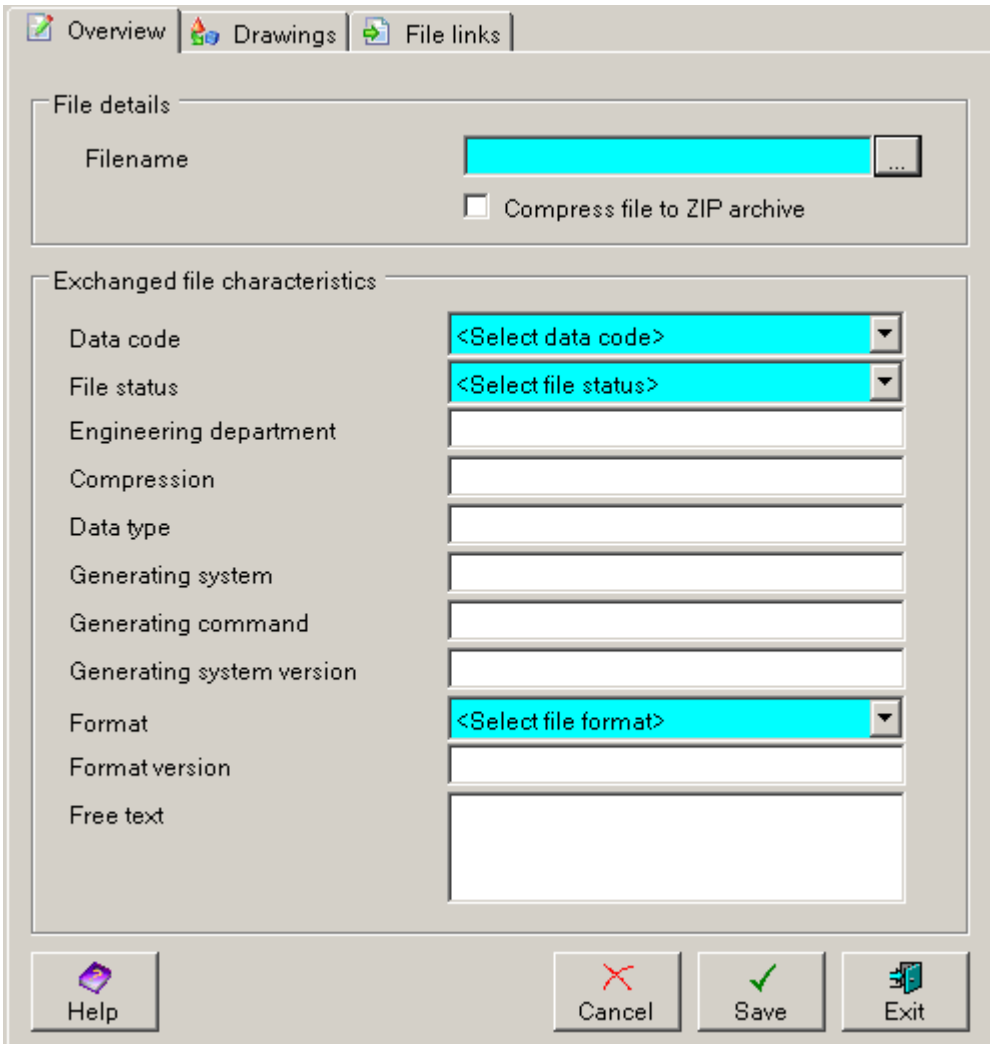
The following shows what the page looks like when working with an ENGDAT version 3 message.



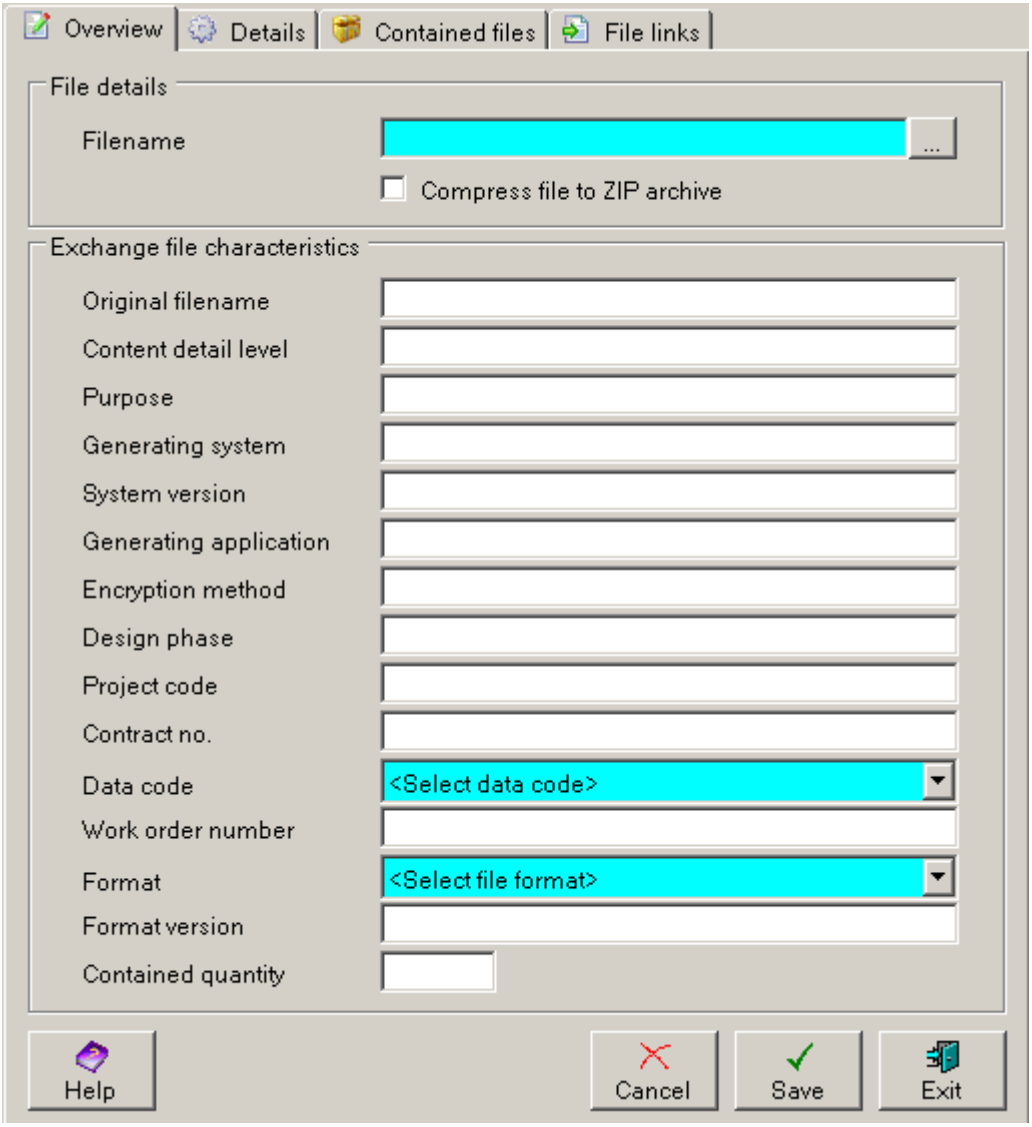
Use the navigation buttons to add, remove and navigate the document links. For more information on how the navigation buttons work, please refer to the section entitled 'ENGDAT Folder Editor – Navigation'.

ENGDAT Folder Editor – Exchanged File Overview

This page allows you to view or edit the details that are included in the ENGDAT message for a file. The exchanged file details overview pages vary slightly between ENGDAT message versions. The following shows how the overview looks for ENGDAT version 1 and ENGDAT version 2 folders when you add a new file.



The following shows what the exchanged file overview looks like for ENGDAT version 3 folders. As you can see, ENGDAT version 3 includes some additional fields.



In both of the above screenshots, every field is blank. If you configured default field values on the ENGDAT relationship, the fields with default values will contain the default values.

File details – Filename

To select a file to add to the folder and ENGDAT message, click the button to the right of the Filename field. You will then be presented with a browse dialog, from which you can locate the file. Once you have selected a file and clicked OK, you will be returned to the overview. The filename will then be shown in the Filename field.

When you save the ENGDAT folder, the file will be copied and sent to the ODEX server, where it will be stored.

File details – Compress file to zip archive

Select this checkbox if you would like to compress the file into a zip file. The file will be compressed before it is sent to the ODEX server. You should only

compress exchanged files if your trading partner has agreed to receive compressed ENGDAT files.

If you are editing the details of an existing file that has already been saved, you may still change this value. If the file was previously compressed and you uncheck this box, the file will be sent to the server again, without compression. If the file was previously uncompressed and you check this box, the file will be compressed before it is sent to the server and saved.

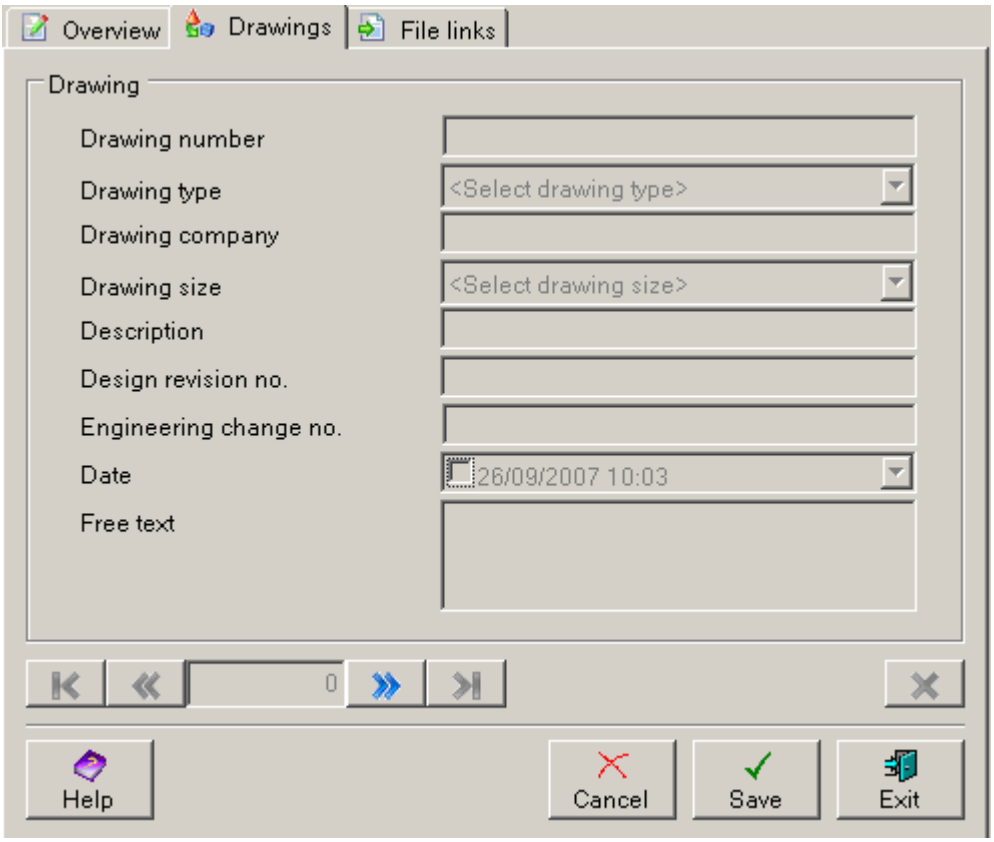
Exchanged file characteristics – Other fields

All of the fields within the exchanged file characteristics section are fields included in the ENGDAT message. The fields on the overview are used in the EFC segment in ENGDAT version 1 and version 2 messages. In ENGDAT version 3, the details are placed in the EFC element group.

he fields that are available and fields that are mandatory will vary depending on which validation profile is in use.

ENGDAT Folder Editor – Drawing Details

Below is the drawing details page. This page is only available for ENGDAT version 1 and version 2 folders. You can reach this page by selecting the 'Drawings' tab at the top of the exchanged file details view, or by selecting an existing drawing in the navigation panel on the left.

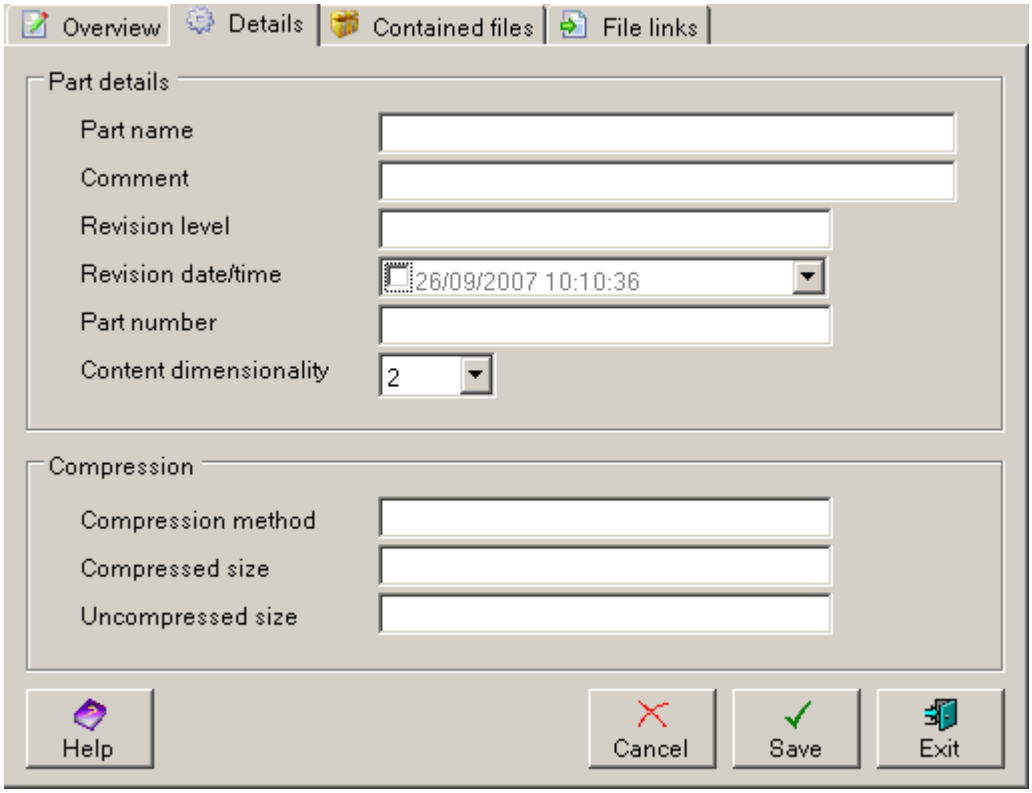


To add a new drawing description entry, click the  button. This will enable the fields on the page. You may then enter values for the fields and use the navigation controls to add more drawing descriptions if necessary.

Please refer to the section entitled 'ENGDAT Folder Editor – Navigation' for information on using the navigation buttons.

ENGDAT Folder Editor – File Details

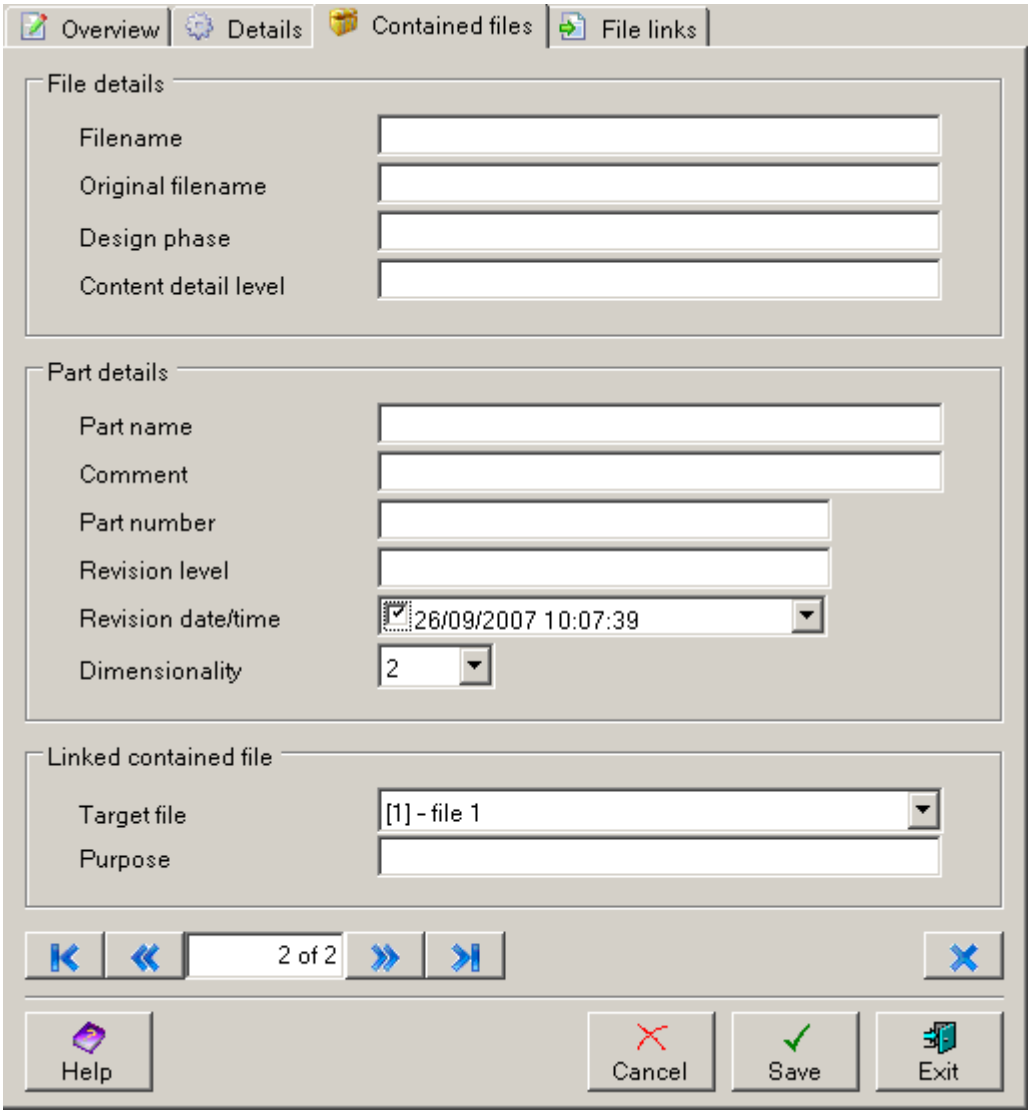
Below is the file and part details page. This page is only available for ENGDAT version 3 folders.



To specify part details, fill in the fields that you require. You may also specify the compression method, compressed file size and uncompressed file size. Note that file sizes should be in kilobytes.

ENGDAT Folder Editor – Contained Files

The contained files page is shown below. This page is only available in ENGDAT version 3 folders. It allows you to add description to the ENGDAT message for files that are contained within other files.



Use the navigation buttons to add, remove and navigate through the collection of contained files. You can also select contained files from the navigation panel on the left.

For more information on how the navigation buttons work, see the section entitled ‘ENGDAT Folder Editor – Navigation’.

File details

The file details section contains details concerning the physical file, such as the filename and original filename.

Part details

The part details section contains fields that describe the part detailed in the file. These fields are the same as the Part details section on the File Details page.

Linked contained file

It is possible to describe the relationship between files within a contained file by adding links between the contained files. However you can only link contained file to one other contained file. With files that are not contained files, multiple links to other files can be added.

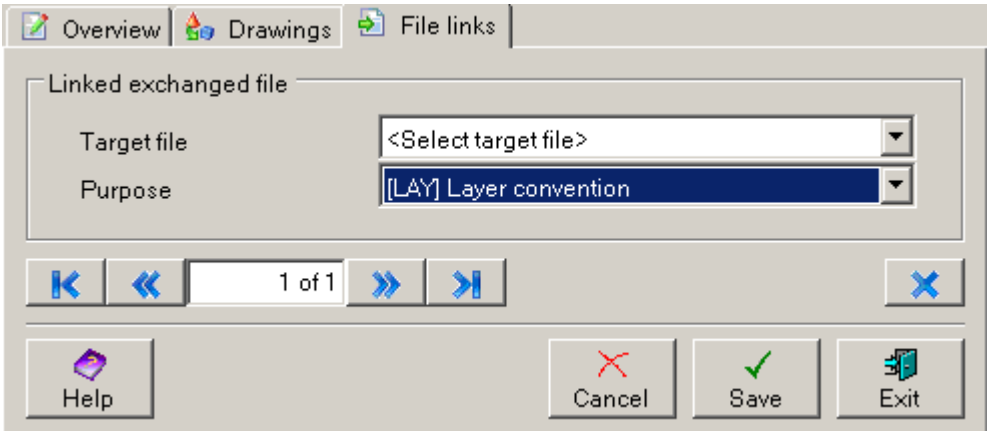
If your container file only contains a single file, the fields in the Linked contained file section will be disabled, because there are no other contained files to link to. As soon as 2 or more contained files are present, these fields will be enabled. Note that you can only link contained files that are contained in the same file.

To add a link, select a target contained file from the drop-down list and optionally enter the link purpose.

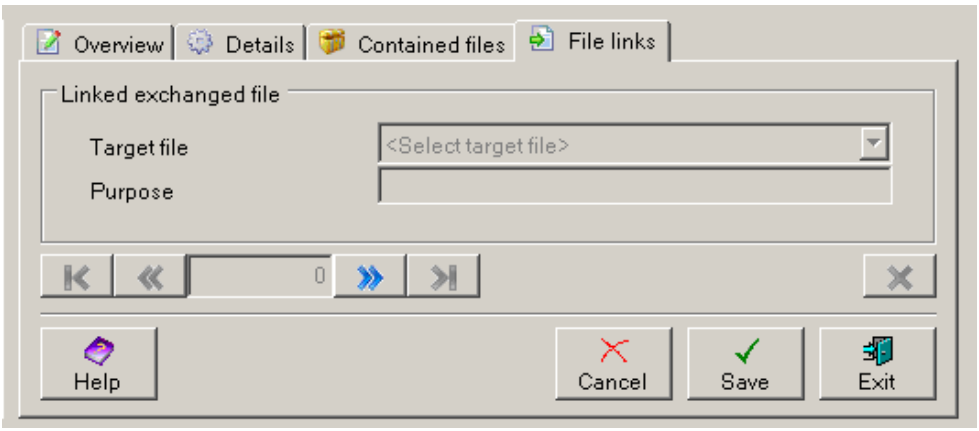
ENGDAT Folder Editor – File Links

Links to other files are used in ENGDAT messages to describe the relationship between exchanged files. Links to other files are stored in the LOF segment in ENGDAT version 1 and 2 messages and the LOF element group in ENGDAT version 3 messages.

Below is the File Links page for ENGDAT versions 1 and 2.



The following shows the File Links page for ENGDAT version 3.



As you can see, the pages are almost identical for all of the ENGDAT message versions. The only difference between ENGDAT version 3 and the other ENGDAT versions is that the link purpose field is a free-form text field in ENGDAT version 3, while ENGDAT versions 1 and 2 use a set of coded values.

To add, remove and navigate the file links, use the navigation buttons. For more information on how the navigation buttons work, please refer to the section entitled ‘ENGDAT Folder Editor – Navigation’.

ODEX Batch Administrator

Introduction

If you have a sequence of operations to be performed regularly or if you want ODEX to be run by non-computer personnel, you may automate it by setting it to run in batch mode. Batch mode operation requires you first to set up a file of commands to run the functions you would otherwise have invoked from the keyboard.

As it runs, ODEX produces a file of all the commands it has run and its responses to those commands. This response file, named ODEXPC.RSP, can be examined later by operators or by another program to find the results of your commands and take the necessary actions.

Configuration

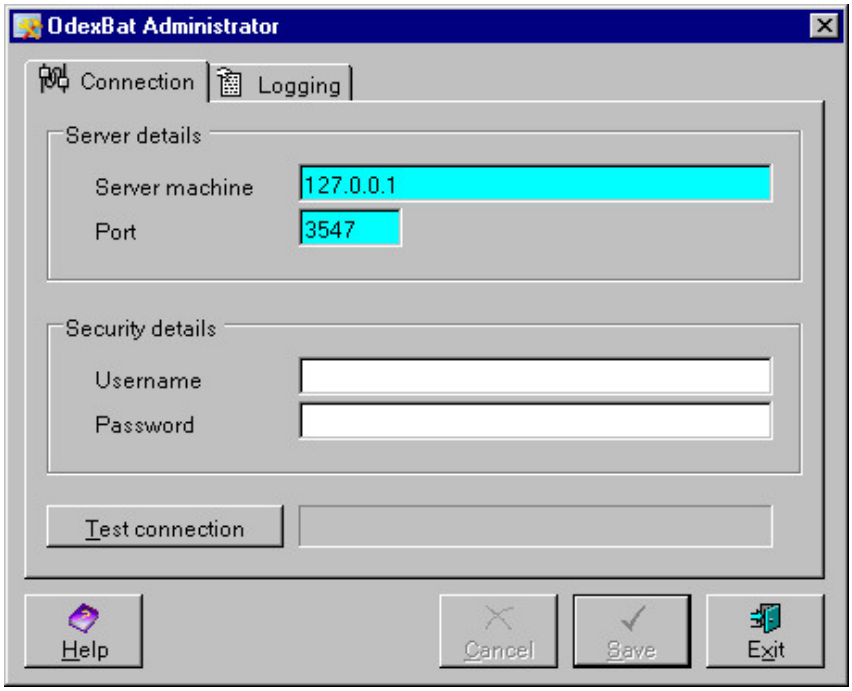
You only need to configure the Batch Interface if you do not want to use the default settings.

Open the ODEX Batch Administrator to see the ODEX Batch Configuration dialog.

The dialog has two pages – Connection and Logging.

Connection and Logging

This page allows you to provide the details of the server machine on which the ODEX Server is running.



There are two sections – Server details and Security details. It also allows you to test the connection.

Server details – Server machine

This must be set to the IP address of the machine on which the ODEX Server is installed.

The default value in this field will be the IP address of your local machine. You may change it to the address of another machine if necessary.

Server details – Port

This must be set to the port number used by the ODEX Server.

Security details – Username

You only need to provide a value in this field if you are using ODEX security.

Security details – Password

You only need to provide a value in this field if you are using ODEX security.

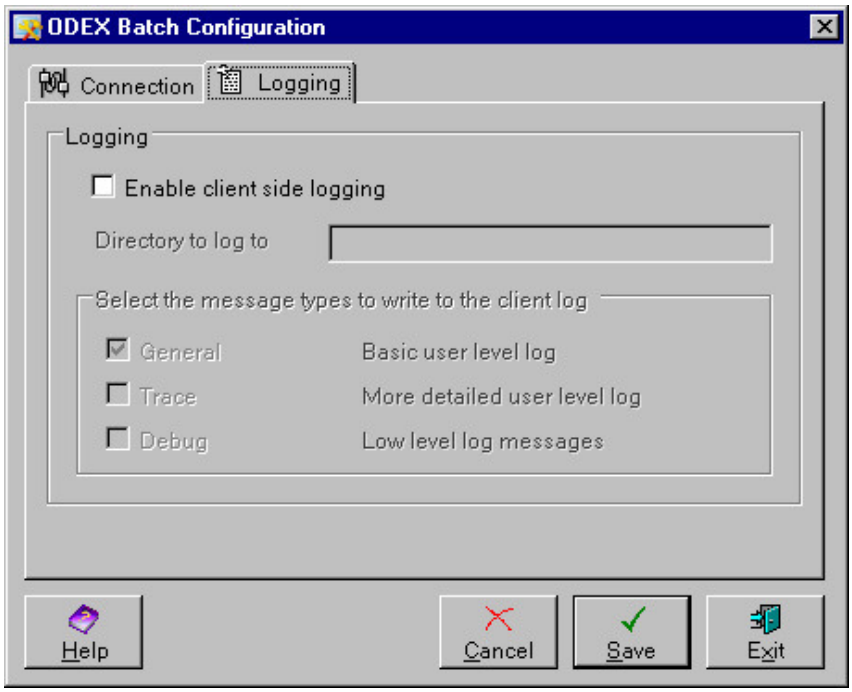
Test connection

The **Test Connection** button may be used to check out that the TCP/IP connection works, but please note that the ODEX server must be started before you can use this test facility otherwise the connection will fail.

The box alongside will show a progress bar and, if the connection is successful, you will then see a “Connection successful” message box. Click **OK** to close the message box.

This feature can be used at any time, not just when doing the initial configuration.

Logging



This page allows you to enable client side logging. Select the tickbox to enable the rest of the page.

You can now type in the directory to which you want the client-side logging to be written, and select the message types to write to the client log.

Click **Save** to save all the changes you have made and close the dialog, or **Cancel** to close the dialog without saving your changes.

Running the ODEX Batch Interface

Once you have configured the Batch Interface, or left it with its default settings, you can run the odexbat program using the command file(s) you have written.

For more information on batch invocation, please refer to the section entitled “Running a Batch Command File”.

The ODEX Batch Language

Introduction

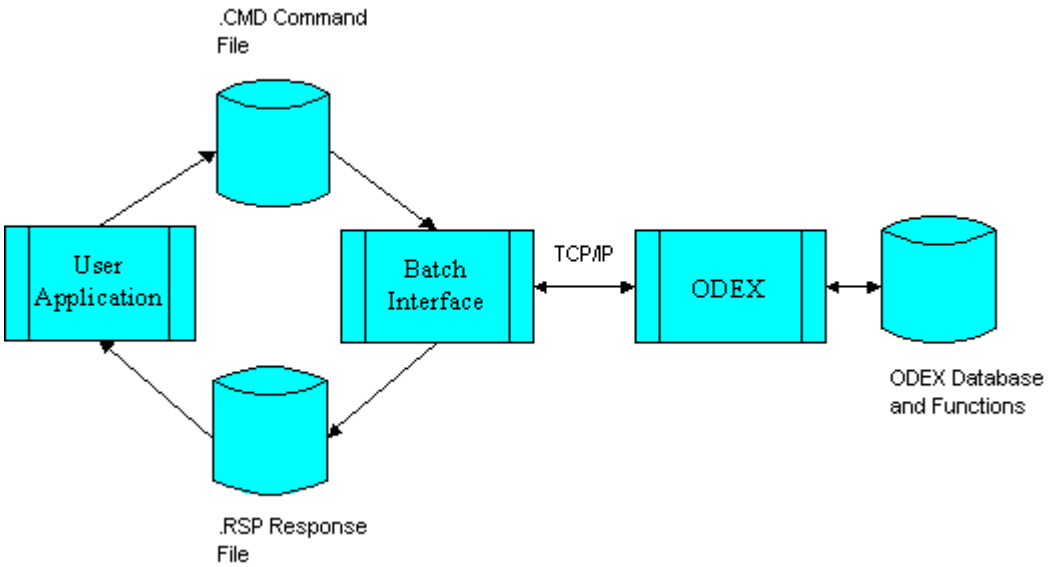
ODEX has, as we have already seen, some very sophisticated automation functions which will allow most, if not all, of your automation to be set up without recourse to any programming. However, when an even higher degree of automation is required you may use the Batch Language to perform tasks such as setting up new Comms entries, scheduling files for sending immediately and many other tasks.

The command scripts that ran on your old ODEX system will be compatible with the new one and will minimise the amount of set up required to get your ODEX system upgraded.

Please note that the Batch Interface only acts on files that have been received into ODEX via ODEX comms or are to be sent via ODEX comms.

The Batch Interface

If you have a sequence of operations to be performed regularly or if you want ODEX to be run by non-computer personnel, you may automate it by setting it to run in batch mode. Batch mode operation requires you first to set up a file of commands to run the functions you would otherwise have invoked from the keyboard. As it runs, ODEX produces a file of all the commands it has run and its responses to those commands. This response file, named ODEXPC.RSP, can be examined later by operators or by another program to find the results of your commands and take the necessary actions.



The batch interface program uses TCP/IP to communicate its commands and actions to ODEX. You can run it without any prior set-up if you want to use the default settings. To view or change the default settings, open the ODEX Batch Administrator client.

The advantages of using TCP/IP are that the ODEX system can be located on one machine on a local area network and the batch scheduling may be

performed from several others on that same network as well as by the local machine itself. This allows the ODEX system to be used as an EDI gateway from a network to the outside world.

The batch command processor, ODEXBAT, can be invoked from an operating system "Batch" file. The system could therefore easily be set to schedule several files, to make a call out to all the necessary trading partners and then to extract any received files into an area where they can be processed by in-house systems. The DOS batch command for such a process could look something like the following:

```
ODEXBAT SENDIT.CMD
```

The command shown above will start the process by actioning the ODEX command file SENDIT.CMD. This file may contain the batch commands necessary to schedule the files for transmission. It may look something like the following:

```
-SNDFILE
LOCAL=TRAD
PCFILE=C:\DATA\INVFILE.DAT
VIRTFILE=INVOICES
-END
-DIRUPDAT
LOCAL=TR02
MAKECALL=Y
-END
```

The first command (-SNDFILE) of this file will schedule a Non-EDI data file called "C:\DATA\INVFILE.DAT" to be sent to a trading partner whose local code is "TRAD". The virtual filename for the transfer will be "INVOICES". The "-END" statement ends the current command.

The next command is "-DIRUPDAT" which will update the user directory of the local code TR02 entry, setting the MAKECALL indicator to "Y". In other words, although there is nothing to schedule for this user, we still wish to make the call in case they have files scheduled for us to receive. The final "-END" ends the "-DIRUPDAT" command.

This is a very simple example. In real life the files may be much larger and user-written programs may be run, scanning the response file for particular events and taking the necessary action on them. In certain sophisticated systems even the commands file itself may be created by a program before being obeyed, as its format is very simple.

Commands File

The commands file, as we have seen above, is really just an ASCII text file that contains an exact description of the sequence of events that ODEXBAT is required to go through in this particular session. You can create as many command files as required for use, as and when necessary. There is no limit to the size of the commands files and they can take any name acceptable to the operating system.

The commands file input to batch ODEX has the following technical characteristics :

- Variable length records each terminated by a carriage return and line feed combination (Hex 0D,0A) i.e. a normal ASCII text file.

- Maximum length of records (excluding **C**/**R** & **L**/**F**) should not exceed 79 bytes
- Commands all start with a hyphen (**-**)
- Comments, which are ignored by ODEX, start with an asterisk (*****). It is suggested that comments are used to document the functioning of the command file. Make the comments clear and easy to read as it will assist any later amendments to the system.
- Leading spaces on each line are ignored. It is therefore possible to indent each command's parameters, improving the human readability of the file.
- Wholly blank lines are ignored. It may be useful to leave blank lines between logical groups of commands, again improving the human readability of the file and easing the task of maintenance.
- The first non-comment record of the commands file need not be a command. If the first non-comment line does not start with the character (**-**), then ODEX treats it as a header or identity record, which it copies unchanged to the response file. Use this record to give a name to your commands file (possibly the same name as the commands file itself) and to relate the responses generated to the commands file that produced them.
- If you create your commands file from within a program, we recommend you include a time stamp in the header record (the first non comment line not starting with (**-**) character) so that commands and their responses are uniquely related.

For each function to be performed, include the relevant command line, and on separate, subsequent lines, the parameters for the command identified by a keyword and the (**=**) character. The commands, their keywords and possible arguments are listed later on in this section. Any keywords and arguments defined as mandatory must be provided. Conditional keywords and arguments may be omitted.

The syntax of a typical command is shown below :

```
-command
keyword1=argument
keyword2=argument
.
.
keywordn=argument
-END
```

Note the following points on the syntax of the commands file.

- Each -command must have a matching **-END** command to terminate it.
- Keywords not supplied will take the default values specified in the command description section.
- Repeat as many -command / **-END** sequences as required. There is no limit.

Batch Invocation

Running a Batch Command File

Please note that the Batch Interface only acts on files that have been received into ODEX via ODEX comms or are to be sent via ODEX comms.

To run ODEX in batch, first make the ODEX directory the current one –

```
CD C:\Program Files\DIP\Odex Enterprise\n.n.n.nnn
```

Where n.n.n.nnn is the ODEX Enterprise installation directory

and then start the batch driver with:

```
ODEXBAT cmdfile [-h host] [-v BuildNumber] [-e]
```

Where the following values (not case-sensitive) are used:

cmdfile	The name of the command file to be executed. It is possible to use a fully qualified path if required. This must be the first parameter following the odexbat command.
host	Host name or TCP/IP address of the ODEX Enterprise server. If this parameter is not specified then the default host is taken from the information specified on the batch configuration dialog.
response	The name of the response file to be created. If not specified, the default file, ODEXPC.RSP will be used.
BuildNumber	Not used. This is only included for compatibility with existing users' systems.
-e	When specified, information is logged to the console as well as the log.

When running the command files, the Batch Interface connects to the server specified in the configuration dialog (or to that specified in the command line) and then logs on to that machine.

It then reads the command file whose name is given on the command line. For each command within the file, a response is written to the response file with the results in (the response file is called ODEXPC.RSP unless overridden by the command line).

Finally ODEXBAT logs off and disconnects from the server.

A simple example of such a batch invocation would be:

```
ODEXBAT CONNECT1.ODX
```

When the ODEXBAT program terminates, it returns an error level to the operating system. This will take the form of the highest return code encountered during the batch run and can be monitored by the operating system batch file or by the calling program. It will take one of the values zero, four, eight, or twelve. These return codes are indications of the seriousness of any problems

encountered during the batch run and are explained in the section on the batch response file (ODEXPC.RSP).

To monitor the return codes in an operating system batch file, use the ERRORLEVEL variable as in the following example, which checks the batch run for any problems.

```
ODEXBAT SENDIT.CMD
IF ERRORLEVEL 12 GOTO BADCOMMAND
IF ERRORLEVEL 8 GOTO SERIOUS
IF ERRORLEVEL 4 GOTO PROBLEM
IF ERRORLEVEL 0 GOTO ENDOK
:BADCOMMAND
ECHO **** A COMMAND WAS NOT ATTEMPTED ****
ECHO **** PLEASE CHECK THE RESPONSE ****
ECHO **** FILE FOR DETAILS ****
GOTO ENDRUN
:SERIOUS
ECHO **** A SERIOUS ERROR WAS ENCOUNTERED ****
ECHO **** PLEASE CHECK THE RESPONSE ****
ECHO **** FILE FOR DETAILS ****
GOTO ENDRUN
:PROBLEM
ECHO **** A PROBLEM WAS ENCOUNTERED ****
ECHO **** PLEASE CHECK THE RESPONSE ****
ECHO **** FILE FOR DETAILS ****
GOTO ENDRUN
:ENDOK
ECHO **** END OF SUCCESSFUL RUN ****
:ENDRUN
```

Batch Response File (ODEXPC.RSP)

In order to communicate its progress and problems to other programs and to monitoring personnel, ODEXBAT writes not only a log file, which contains all information on the system from all users, but also a response file. The function of this response file is to contain the commands and their results for easy analysis.

One point worth bearing in mind is that the response file is always called ODEXPC.RSP (unless the user specifies otherwise at run-time) and this file is cleared at the start of each ODEXBAT run. Information from previous runs will need to be copied into other files if it is to be preserved. For example, taking the batch file in the introduction, if the responses were to be preserved, the following amendment would be required to create a total response file called RESPONSE and print it.

```
ODEXBAT SENDIT.CMD
COPY ODEXPC.RSP RESPONSE
ODEXBAT PROCESS.CMD
COPY RESPONSE+ODEXPC.RSP RESPONSE
COPY RESPONSE PRN
```

Like the input commands file, the response file output by the batch driver comprises variable length records ending with C/R L/F, in other words it is a basic text file. The first record of the response file is the input header record echoed back, if it is present in the command file. Then, for each command that was input, a block of records like those following is generated -

```
-command
RETURN CODE nn
ppp response1
ppp response2
ppp response3
.
.
ppp responsen
```

Each response has a three character prefix (identified here as ppp) to identify the type of response for that particular input command. The responses produced depend upon how the command executed in that particular instance, so if you are using programs to examine the response file, process the responses according to their prefix type. The first character of the prefix will be one of the following characters:

I	Informational
E	Error
M	Message
O	Output
R	Report

The remaining two characters will be numeric.

The status of each command is indicated by the return code. This is logged as the second response file record for any command execution (the first is an echo of the command itself). The return code shows how successful the command was in operation. The possible return code values are -

00	Successful, no errors
04	Completed but with errors

08 Could not complete because of errors

12 Command not attempted (invalid command or operator bypassed it)

The highest return code generated by a run is returned to the operating system as an error level at the end of the batch run. Therefore it is possible to monitor the general success of a run and highlight runs that had problems. This is explained further in the section on batch invocation.

Taking the example command file given in our introduction to batch execution, the command file looked like this:

```
-SNDFILE
LOCAL=TRAD
PCFILE=C:\DATA\INVFILE.DAT
VIRTFILE=INVOICES
-END
-DIRUPDAT
LOCAL=TR02
MAKECALL=Y
-END
```

The output after running ODEXBAT with this file will look something like this:

```
-SNDFILE
RETURN CODE 00
I01 LOCAL=TRAD
I08 PCFILE=C:\DATA\INVFILE.DAT
I05 VIRTFILE=INVOICES
I99 -END
O46 TEST-EDI-CODE
O45 17/02/92 09:45:08 size = 000000424
O09 00000008.CMS
O48 92/07/23 10:23:19 INVOICES
M99 Request Completed Successfully
-DIRUPDAT
RETURN CODE 00
I01 LOCAL=TR02
I22 MAKECALL=Y
I99 -END
M99 Request Completed Successfully
Z99 BAT0006I End of command file reached
```

Note that the return codes of 00 in each command indicate that both functions were successful. Note also how the “I” entries echo the original command lines. On line O46, TEST-EDI-CODE is the EDI code of the local code TRAD.

Line O45 shows the date and time of creation of the C:\DATA\INVFILE.DAT file.

Line O09 shows the virtual filename that the data is stored in on the ODEX system, ready for transmission.

Line O48 shows the date and time and filename of the EDI Virtual file that will be transmitted.

The Interpretation of the M99 Request Completed Successfully message must not be misunderstood. It is simply saying is that the syntax of the command was understood and attempted. A failure to action because of an invalid parameter value will still cause this M99 line to be output, because the command could be attempted. The real indicator of success of the command is a return code of 00.

The following example shows a valid command with a valid parameter but an invalid parameter value :

```
-PRMUPDAT
RETURN CODE 04
```

```
I01 LOCAL=TRAD
I08 PCFILE=C:\Unknonwn.txt
I99 -END
E08 Invalid PC file name
M99 Request Completed Successfully
Z99 BAT006I End of command file reached
```

Note on the example above that M99 still appears. The only method of checking the failure is the response code of 04. In the next example the syntax of one of the parameters is incorrect, PCFILE has been intentionally changed to PCFOLE. This invalid syntax prevents the M99 message and prompts an M98 message.

```
-SNDFILE
RETURN CODE 08
E00 Invalid keyword follows
PCFOLE=C:\DATA\INVFILE.DAT
M98 Request Not Completed.
Z99 BAT0006I End of command file reached
```

Note that the error code has been upgraded to severity 08 showing a command syntax failure.

Commands

There are two types of command in the ODEX batch interface:– those which are the equivalent of an ODEX GUI function, and those which are the equivalent of normal script commands (currently –DOS is the only script command available).

The next section deals with all the ODEX batch commands, which are listed in alphabetical order.

ODEX batch commands and their responses

This section lists all the ODEX batch commands.

For each ODEX batch command we have provided a section entitled “Provided”. This is a table of the parameters that are associated with each particular batch command. The table has five columns, the command and its parameters, the format and length of the parameter, whether the parameter is mandatory or conditional, the default value of the parameter and a short description of its contents.

Where a default exists for a parameter, it is listed in the defaults column. If no default exists then the word ‘None’ appears.

If the command is required as is, i.e. there are no options for the command then nothing appears in the Format /length or Default value columns.

The section entitled “Returned” is a list of the responses that you may receive, having issued a set of batch commands. This is followed by an explained example of the use of the command and its normal responses.

The available ODEX batch commands are: -

-CNSTRUCT	This allows ODEX to construct a user’s in-house file into a named EDI file.
-CTLUPDAT	This updates a control file entry.
-DIRADD	This adds a new entry into a User Directory.
-DIRUPDAT	This updates a User Directory entry.

-RCVFILE	This displays received non-EDI file details.
-RCVODETT	This displays received EDI file details.
-REPRCV	This produces a report of received file details.
-REPSND	This produces a report of sent file details.
-SNDFILE	This is used to queue a non-EDI format file for sending.
-SNDODETT	This is used to queue an EDI format file for sending.
-STOPSERVER	This command can be used to stop ODEX running.
-TRNSLATE	This allows ODEX to translate a user's EDI file into a named in-house file.
-WRITELOG	This can be used to write a line to the ODEX log.

It is possible to enclose text fields in double or single quotes to signify the inclusion of spaces.

NOTE - ODEX will terminate each command line at the first encountered space character, so it is vital that quotes are used. Text entries such as COMPANY=Data Interchange will be interpreted as COMPANY=Data unless it is input as COMPANY="Data Interchange".

CUD=" " would set the CUD field to spaces.

In the following pages the "Provided" section Format / Length column uses a shorthand format similar to COBOL.

Examples of Format/Length column formats:

- X(12) is an alphanumeric field of up to 12 characters.
- 9(5) is a numeric field of maximum length 5 digits.
- 999 is a numeric field of maximum length 3 digits.
- XX is an alphanumeric field of maximum length 2 digits.

-CNSTRUCT – Construct an EDI File

The function of this command is to construct an in-house format file into an EDI format file. This command allows a file to be constructed without being scheduled for sending.

Examples of Format/Length column formats:

- X(12) is an alphanumeric field of up to 12 characters.
- 9(5) is a numeric field of maximum length 5 digits.
- 999 is a numeric field of maximum length 3 digits.
- XX is an alphanumeric field of maximum length 2 digits.

Provided

Command	Format/ Length	Mandatory/ Conditional	Default Value	Description/ Content
-CNSTRUCT				Command Name
IHS	X(255)	Mandatory	None	The name of the in-house format file to be constructed.
DEF	X(32)	Mandatory	None	The In-house ID identifying the contents of the file to be constructed. This should correspond with the name given in the translator index file's HSE statement
EDI	X(255)	Mandatory	None	The EDI output filename
-END				

Returned

```
-CNSTRUCT
RETURN CODE nn
I94 IHS=(drive:) (path)filename(.ext)
I95 DEF=InHouseId
I93 EDI=(drive:) (path)filename(.ext)
I99 -END
M03 Number of in-house records read  = X
M04 Number of segments written       = X
M99 Request Completed Successfully
M98 Request Not Completed
E99 Missing mandatory parameter IHS
E99 Missing mandatory parameter DEF
E99 Missing mandatory parameter EDI
E08 Invalid PC file name
E00 Invalid keyword follows
E60 CON0001A No HSE entry for (definition) on IDX file
E71 HIS value is longer than 255
E71 DEF value is longer than 32
E71 EDI value is longer than 255
```

-CTLUPDAT - Control File Record Update

Probably the largest usage of this command is to generate End to End ResPonses (EERPs) for files that have been received from trading partners whose network details indicate that the EERP should be generated manually.

The command will locate and change the first record that it encounters that satisfies all the specified criteria, the possible criteria parameters being TYPE, LOCAL, VIRTDATE, VIRTTIME, VIRTFILE, FTPFILE and ODETTE. Only this one record will be changed. It is therefore good practice to make the record selection criteria as specific as possible.

Possible unique permutations are to specify VIRTFILE with VIRTDATE and VIRTTIME or to specify FTPFILE on its own as it is always unique, or to specify ODETTE with VIRTFILE (and/or VIRTDATE and VIRTTIME). TYPE and LOCAL can be used to further identify the record required for update.

Only those change parameters specified are amended in the database. All other fields are left at their original values.

Important Note

In the Batch Interface, the PRIORITY parameter values range from 1 to 9, where 9 is the highest priority and 1 is the lowest. This is to ensure compatibility with users who have upgraded from ODEX Professional. This differs from the way Priority fields are handled in the rest of ODEX Enterprise, where 1 is the highest priority.

Examples of Format/Length column formats:

- X(12) is an alphanumeric field of up to 12 characters.
- 9(5) is a numeric field of maximum length 5 digits.
- 999 is a numeric field of maximum length 3 digits.
- XX is an alphanumeric field of maximum length 2 digits.

Provided

Command	Format/ Length	Mandatory/ Conditional	Default Value	Description / Content
-CTLUPDAT				Command Name
TYPE	X	Conditional	None	This states whether the selected record is to be a Received file (Value = **R**) or a Sent file (Value = **S**).
LOCAL	X(35)	Conditional	None	This is the local code to be selected.
ODETTE	X(35)	Conditional	None	This is the trading partner's EDI code to be selected.
VIRTFILE	X(26)	Conditional	None	This is the name of the virtual file to be selected.

VIRTDATE	9(6)	Conditional	None	This is the date of scheduling of the virtual file to be selected. The format is YYMMDD.
VIRTTIME	9(6)	Conditional	None	This is the time of scheduling of the virtual file to be selected. The format is HHMMSS.
FTPFILE	X(12)	Conditional	None	This is the name of the Comms file to be selected and is unique in itself.
DELETEREQ		Conditional		Use this parameter to delete the selected file entry from the database. The parameter has no value. This is actioned for Sent and Received files.
EERP		Conditional		Use this parameter to send End to End Responses for the selected Received file. This is necessary when the trading partners "Time to send EERP" is set to Manual. The parameter has no value. This is actioned for Received files only.
ATTEMPTS	9(3)	Conditional	None	This changes the number of possible attempts at connection before ODEX stops trying to make the call.
RETRY	X	Conditional	None	This changes the number of unsuccessful attempts so far at connection to the trading partner. Normally the value will be zero.
FLAG	XX	Conditional	None	Not used and not echoed to the

				response file. Provided for compatibility with ODEXPC
FLAGS	XX	Conditional	None	Not used and not echoed to the response file. Provided for compatibility with ODEXPLUS
NEWVIRTFILE	X(26)	Conditional	None	This is the new EDI Virtual File Name.
EARLYDATE	9(6)	Conditional	None	This is the new Earliest Date to send. In the format YYMMDD.
EARLYTIME	9(4)	Conditional	None	This is the new Earliest time to send. In the format HHMM.
PRIORITY	9(1)	Conditional	None	This is the new Priority. In the range **1** (Lowest) to **9** (Highest).
FORMAT	X	Conditional	None	This is the new file format. Valid values are **F** = Fixed length, **T** = Text, **U** = Unformatted, **V** = Variable length. ODEX cannot convert to or from **V** format
RECSIZE	9(5)	Conditional	None	If the database format is set to **F** then this is the new record length. For **V** format files this is the calculated max. record size which cannot be changed.
USERDATA	X(8)	Conditional	None	This is the new user data.
-END				End of Command

Returned

```
-CTLUPDAT
RETURN CODE 00
I51 TYPE=a
I01 LOCAL=aaaa
I29 ODETTE=aaaa
I03 VIRTDATE=yymmdd
I04 VIRTTIME=hhmmss
I05 VIRTFILE=file name
I09 FTPFILE=file name
```

```
I66 DELETEREQ
I99 EERP
I52 ATTEMPTS=nnn
I53 RETRY=a
I55 NEWVIRTFILE=file name
I10 EARLYDATE=yymmdd
I11 EARLYTIME=hhmm
I03 PRIORITY=n
I13 FORMAT=a
I14 RECSIZE=nnnnn
I15 USERDATA=aaaaaaaa
I99 -END

E00 Invalid Keyword Follows
E01 No control file entry found
E10 Invalid date / time
E13 File format not F, T, U or V
E71 Field size exceeded
E73 Invalid numeric value
E74 Parameter value not specified
E75 Argument should be Y or N

E88 BAT0007E Logon required
E90 No Authority to use this option

M04 CTL0510E May not update : FTP file not on disk
M98 Request Not Completed
M99 Request Completes Successfully
```

Example

Probably the most common use of this function is the sending of EERP's when the User Directory entry's Time to Send EERP is set to B (EERPs are then sent only at user request). The Command file for such an operation would look something like :

```
-CTLUPDAT
TYPE=R
LOCAL=UKTE
VIRTFILE=INVOICES
EERP
-END
```

This command file will set the first occurrence of the EDI file, whose Virtual filename is INVOICES, received from UKTE local code, to be EERP'd on the next communications session. The output ODEXPC.RSP will look like this :

```
-CTLUPDAT
RETURN CODE 00
I51 TYPE=R
I01 LOCAL=UKTE
I05 VIRTFILE=INVOICES
I99 EERP
I99 -END
M99 Request Completed Successfully
Z99 BAT0006I End of command file reached
```

-DIRADD – Add Directory Entries

The function of the command is to add new entries to the internal or external networks. Networks, Mailboxes and EDI Codes can be added. The command can only add entries, it does not update existing ones.

Mandatory fields vary slightly with the different entry types that may be created. All entry types require the DIRTYPE, LOCAL and ODETTE parameters. Networks require additional NUA and CAMP parameters; Mailboxes and EDI Codes require an additional REDIRECT parameter.

Some parameters are not applicable to certain entry types, for example the FILEDIR and CALLDIR parameters are only of use within the Network definition. If such parameters are included in other definitions they will not be marked as errors, merely ignored.

Examples of Format/Length column formats:

- X(12) is an alphanumeric field of up to 12 characters.
- 9(5) is a numeric field of maximum length 5 digits.
- 999 is a numeric field of maximum length 3 digits.
- XX is an alphanumeric field of maximum length 2 digits.

Provided

Command	Format/ Length	Mandatory/ Conditional	Default Value	Description/ Content
-DIRADD				Command Name
DIRTYPE	X	Mandatory	None	The type of entry to be created. **N** = Network, **F** = Mailbox, **M** = EDI Code.
LOCAL	X(35)	Mandatory	None	The local code reference
ODETTE	X(35)	Mandatory	None	The EDI code associated with this entry.
CAMP	X(35)	Conditional	None	Specifies the Subsystem to be used for the new Network. This parameter is mandatory when the entry type is **N** = Network but is ignored for **F** = Mailbox and **M** = EDI Code (but still echoed in the response file).
REDIRECT	X(25)	Conditional	Spaces	If DIRTYPE=**N** this is ignored, otherwise this is the EDI code of the associated network. Mandatory for Mailboxes or EDI Codes.
NUA	X(15)	Conditional	None	The Network User

				Address. Must be present if DIRTYPE=**N** and CALLDIR=**O** or **B**.
ALTNUA	X(15)	Conditional	Spaces	This parameter is not used. Provided only for compatibility with ODEXPC.
COMPANY	X(30)	Mandatory	Spaces	The company name associated with this entry.
CONTACT	X(20)	Conditional	Spaces	The contact name for this entry.
TEL	X(20)	Conditional	Spaces	The telephone number for the contact. This is used for information only.
INTEXT	X	Conditional	E	**I** = Internal network, **E** = External network. If the value is not I or E, the default value is assumed.
LOCKCODE	X(12)	Conditional	Spaces	This is the authorisation key and is required for new internal networks.
SENTPASS	X(8)	Conditional	Spaces	Password to be sent.
RECVPASS	X(8)	Conditional	Spaces	Password to be received.
CALLDIR	X	Conditional	B	If DIRTYPE=**N** this determines whether outgoing calls will be initiated. **I** = Incoming only, **O** = Outgoing only, **B** = Both.
FILEDIR	X	Conditional	B	If DIRTYPE=**N** this determines in which direction files may be exchanged. **O** = Send files only, **I** = Receive files only, **B** = Both.
DAILY	X	Conditional	N	If DIRTYPE=**N** this specifies whether to make a call at the given time every day. **Y** = make daily call, **N** = Do not.
EARLYTIME	9(4)	Conditional	Spaces	If DIRTYPE=**N** this is the earliest time to make an outgoing call to this entry. In the format HHMM.
FORMAT	X	Conditional	Spaces	If DIRTYPE=**N** or **F** this is the default file format. Permitted values are **F** = Fixed length, **T** = Text,

				U = Unformatted, **V** = Variable length.
RECSIZE	9(5)	Conditional	Spaces	If DIRTYPE=**N** or **F** this is the default record size.
CUD	X(48)	Conditional	Spaces	If DIRTYPE=**N** this is the Call User Data.
MAKECALL	X	Mandatory	N	If DIRTYPE=**N** then **Y** = make an outgoing call even if no files are scheduled to this node. **N** = do not make an outgoing call unless files are scheduled.
PRIORITY	9	Conditional	5	Not used. Provided for compatibility with ODEXPC
ATTEMPTS	999	Conditional	0	If DIRTYPE=**N** this is the number of attempts so far to contact this network.
MAXRETRY	999	Conditional	7	If DIRTYPE=**N** this is the maximum number of attempts that will be made to contact this network.
INTERVAL	9(4)	Conditional	10	If DIRTYPE=**N** this is the time period in minutes between each attempt to contact this network.
USERDATA	X(8)	Conditional	Spaces	If DIRTYPE=**N** this is the SSID user data to be used for whatever purpose the user requires.
THRESHOLD	9	Conditional	Spaces	Not used. Provided for compatibility with ODEXPC
WFDISC	X	Conditional	N	Not used. Provided for compatibility with ODEXPC
EERPTIME	X	Conditional	A	If DIRTYPE=**N** or **F** this is the time to send the end to end response. **A** = on file receipt, **B** = on user request, **C** = on file extraction.
ISDNNUM	9(25)	Conditional	Spaces	Not used. Provided for compatibility with ODEXPC. Use the appropriate CAMP name and NUA.
ISDNSUB	9(10)	Conditional	Spaces	Not used. Provided for compatibility with ODEXPC

-END		Mandatory		End of Command

Returned

```
-DIRADD
RETURN CODE nn
I95 DIRTYPE=N
I00 CAMP=CAMP
I29 ODETTE=TEST-EDI-CODE
I86 COMPANY=TEST
I87 CONTACT=TEST
I80 TEL=1234567890
I01 LOCAL=TEST
I97 NUA=23422120017020
I13 FORMAT=F
I14 RECSIZE=80
I89 SENTPASS=SENDPASS
I90 RECVPASS=RECVPASS
I91 CALLDIR=B
I92 FILEDIR=B
I88 INTEXT=E
I15 USERDATA=USERDATA
I22 MAKECALL=Y
I03 PRIORITY=1
I93 DAILY=Y
I11 EARLYTIME=1200
I52 ATTEMPTS=1
I25 MAXRETRY=10
I26 INTERVAL=1
I94 CUD='01'02'03ABC
I10 EERPTIME=A
I99 -END
E1 REDIRECT code must be specified for File and Message nodes
E1 CALLDIR must be ‘B’, ‘I’ or ‘O’
E1 FILEDIR must be ‘B’, ‘I’ or ‘O’
E1 EERPTIME must be ‘A’, ‘B’ or ‘C’
E01 LOCAL value already exists
E01 Unknown CAMP name
E10 Invalid early time. Use HHMM
E13 FORMAT=X value is Not ‘F’, ‘T’, ‘U’ or ‘V’
E14 XXXX must be specified for Network nodes
E16 DIRTYPE X is not ‘N’, ‘F’ or ‘M’
E21 Record Creation Failed
E22 Invalid entry code
E23 Invalid EDI Code
E24 Must be (I)nternal or (E)xternal
E25 Invalid local code
E26 Duplicate local code
E27 NUA not numeric
E28 File format not F,T,U or V
E29 Invalid record size
E30 Invalid send password
E31 Invalid received password
E32 Call direction not B, I or O
E33 File direction must be B, S or R
E34 User data format invalid
E35 Outgoing call request not Y or N
E36 Call request/call direction incompatible
E37 Priority not in range 0 to 9
E38 Daily call request not Y or N
E39 Daily call/call direction incompatible
E40 Invalid daily call time
E41 Call attempts not numeric
E42 Max. call attempts not numeric
E43 Call attempts interval not numeric
E44 Invalid call user data
E45 Only 16 bytes allowed
E46 Cannot be specified for internal
E47 Threshold not in range 1 to 8
E48 Wait for Disconnect must be Y or N
E49 EDI indirection code MUST be a Network Node
E49 EDI indirection code MUST be a Network or File node
E55 Duplicate EDI code
E71 XXXX value is longer than X
E72 Numeric field size exceeded
E73 KEYWORD=VALUE value is not numeric
E74 No parameter allowed
E75 KEYWORD=VALUE value is Not ‘Y’ or ‘N’
E90 No authority to use this option
E99 Missing mandatory parameter XXXX
```

Example

It is required to set up a new trading partner's network with the default options. The command file would look something like this :

```
-DIRADD
DIRTYPE=N
LOCAL=NEW1
ODETTE=EDI-CODE
CAMP=OFTP SUBSYSTEM
NUA=23422120017000
-END
```

The resultant response file would look like this:

```
-DIRADD
RETURN CODE 00
I95 DIRTYPE=N
I01 LOCAL=NEW1
I29 ODETTE=EDI-CODE
I00 CAMP=OFTP SUBSYSTEM
I97 NUA=23422120017000
I99 -END
M99 Request Completed Successfully
Z99 BAT0006I End of command file reached
```

The return code of 00 shows that the command was successful, otherwise there is just the echoing back of the commands and parameters followed by the M99 and Z99 lines.

-DIRUPDAT – Directory Update Command

The function of this command is to update an already existing Network or Mailbox. This command will not create new Networks or Mailboxes. Only those parameters that require change need be specified.

The LOCAL code must be specified for any amendment (Note that this code itself cannot be changed) and the entry with the given LOCAL code must already exist.

Some parameters are not applicable to certain entries, for example the FILEDIR and CALLDIR parameters are only of use within a Network. If such parameters are included in other definitions they will not be flagged as errors, merely ignored.

Examples of Format/Length column formats:

- X(12) is an alphanumeric field of up to 12 characters.
- 9(5) is a numeric field of maximum length 5 digits.
- 999 is a numeric field of maximum length 3 digits.
- XX is an alphanumeric field of maximum length 2 digits.

Provided

Command	Format/ Length	Mandatory/ Conditional	Default Value	Description / Content
-**DIRUPDAT**				Command Name
DELETEREQ				Include this parameter to delete the selected Network or Mailbox.
LOCAL	X(35)	Conditional	None	The local code. Either this or the ODETTE parameter must be specified for an existing Network or Mailbox entry.
ODETTE	X(35)	Conditional	None	The EDI code. Either this or the LOCAL parameter must be specified for an existing Network or Mailbox entry.
MAKECALL	X	Conditional	None	Only applicable to Networks. **Y** = make an outgoing call even if no files are scheduled to this network. **N** = do not make an outgoing call unless files are scheduled.
PRIORITY	9(1)	Conditional	None	This parameter is not used. It is included only for compatibility with ODEX/PC.

ATTEMPTS	9(3)	Conditional	None	Only applicable to Networks. This is the number of attempts so far to contact this network.
MAXRETRY	9(3)	Conditional	None	Only applicable to Networks. This is the maximum number of attempts that will be made to contact this network.
INTERVAL	9(4)	Conditional	None	Only applicable to Networks. This is the time period in minutes between each attempt to contact this network.
USERDATA	X(8)	Conditional	None	Only applicable to Networks. This is the SSID user data to be used for whatever purpose the user requires.
CAMP	X(35)	Conditional	None	Specifies the Subsystem to be used for the new Network. This parameter is mandatory for a Network but is ignored for Mailboxes and EDI Codes. CAMP must equate to a Subsystem name in ODEX Enterprise.
NUA	X(15)	Conditional	None	Only applicable to Networks. This is the Network User Address.
ALTNUA	9(15)	Conditional	None	This parameter is not used. Provided only for compatibility with ODEXPC.
COMPANY	X(30)	Conditional	None	The company name associated with this entry.
CONTACT	X(20)	Conditional	None	The contact name for this company.
TEL	X(20)	Conditional	None	The telephone number for this contact/company. (For information only).
LOCKCODE	X(12)	Conditional	Spaces	Required only for internal networks.

SENTPASS	X(8)	Conditional	None	Password to be sent.
RECVPASS	X(8)	Conditional	None	Password to be received
CALLDIR	X	Conditional	None	Only applicable to Networks. This determines whether outgoing calls will be initiated. **I** = Incoming only, **O** = Outgoing only, **B** = Both.
FILEDIR	X	Conditional	None	Only applicable to Networks. This determines in which direction files may be exchanged. **S** = Send files only, **R** = Receive files only, **B** = Both.
DAILY	X	Conditional	None	Only applicable to Networks. This specifies whether to make a call at the given time every day. **Y** = make daily call, **N** = Do not
EARLYTIME	9(4)	Conditional	None	Only applicable to Networks. This is the earliest time to make an outgoing call to this network. In the format HHMM.
FORMAT	X	Conditional	None	Not used. Provided for compatibility with ODEXPC
RECSIZE	9(5)	Conditional	None	Not used. Provided for compatibility with ODEXPC
CUD	X(48)	Conditional	None	Only applicable to Networks. This is the Call User Data.
THRESHOLD	9	Conditional	None	Not used. Provided for compatibility with ODEXPC
WFDISC	X	Conditional	None	Not used. Provided for compatibility with ODEXPC

EERPTIME	X	Conditional	None	Applicable to Networks and Mailboxes. This is the time to send the end to end response. **A** = on file receipt, **B** = on user request, **C** = on file extraction.
ISDNNUM	9(25)	Conditional	None	Not used. Provided for compatibility with ODEXPC. Use the appropriate CAMP name and NUA.
ISDNSUB	9(10)	Conditional	None	Not used. Provided for compatibility with ODEXPC.
-END		Mandatory		End of Command

Returned

```
-DIRUPDAT
RETURN CODE NN
I01 LOCAL=XXXX
I29 ODETTE=XXXX
I22 MAKECALL=Y
I52 ATTEMPTS=NNN
I25 MAXRETRY=NNN
I26 INTERVAL=NNNN
I27 USERDATA=XXXXXXXX
I86 COMPANY=CHANGED-NAME
I87 CONTACT=CHANGED TEST
I80 TEL=1111111111
I97 NUA=22222222222222
I13 FORMAT=V
I14 RECSIZE=2048
I89 SENTPASS=CHNDPASS
I90 RECVPASS=CHCVPASS
I91 CALLDIR=B
I92 FILEDIR=B
I93 DAILY=N
I11 EARLYTIME=1300
I94 CUD=CHANGEDTEXT
I10 EERPTIME=B
I66 DELETEREQ
I00 CAMP=XXX
I99 -END

E00 Invalid Keyword Follows
E01 No directory entry found
E1  PARAM must be 'X', 'Y' or 'Z'
E10 Invalid early date / time
E13 File format not F, T, U or V
E14 Either LOCAL or ODETTE must be specified
E71 Field size exceeded
E73 Invalid numeric value
E74 No parameter allowed
E75 Argument should be Y or N

M98 Request not completed.
M99 Request Completed Successfully
Z99 BAT006I End of command file reached
```

Example

The most commonly found example of the use of this command is in its ability to ask ODEX to make an outgoing call even if there is no file to send. This is very useful, especially for those DOS users who connect by an async method and

who therefore cannot be directly called by another X.25 user. This parameter means that they can call out to a trading partner even if they have no files to send.

The sample command file is extremely simple and looks something like this :

```
-DIRUPDAT
LOCAL=UKTE
MAKECALL=Y
-END
```

This will generate the following response file, as well as asking ODEX to make the outgoing call to the NUA of local code UKTE the next time that communications are loaded.

```
-DIRUPDAT
RETURN CODE 00
I01 LOCAL=UKTE
I22 MAKECALL=Y
I99 -END
M99 Request Completed Successfully
Z99 BAT0006I End of command file reached
```

The above response file needs little explanation. The return code of 00 says that the function was successful. The rest of the lines are just the echo back of the commands and parameters, and the termination lines (M99 and Z99).

-RCVFILE – Extract Data File

This command acts on non-EDI files received via ODEX comms. Its function is two-fold. Firstly it is designed to extract a non-EDI file from the ODEX system and write it to a PC file. Secondly it is able to extract EDI data from selected EDI format files on the ODEX system and write this data to a PC file. Unlike the -RCVODETT command, only one file at a time is concerned in this data extraction process.

Sufficient information must be given in the parameters to uniquely identify this file, otherwise ODEX will extract the first file matching the required criteria that it comes across. The output file is cleared before the extracted data is added.

Examples of Format/Length column formats:

- X(12) is an alphanumeric field of up to 12 characters.
- 9(5) is a numeric field of maximum length 5 digits.
- 999 is a numeric field of maximum length 3 digits.
- XX is an alphanumeric field of maximum length 2 digits.

Provided

Command	Format/ Length	Mandatory/ Conditional	Default Value	Description / Content
-RCVFILE				Command Name
LOCAL	X(35)	Conditional	None	The local code of the company that sent the file to be extracted.
VIRTDATE	9(6)	Conditional	None	The date of the virtual file to be extracted in the format YYMMDD.
VIRTTIME	9(6)	Conditional	None	The time of the virtual file to be extracted in the format HHMMSS.
VIRTFILE	X(26)	Conditional	None	The virtual filename of the file to be extracted.
FTPFILE	X(12)	Conditional	None	The disk name of the file to be extracted. Format will be nnnnnnnn.CMS
FILETYPE	X(1)	Conditional	None	B, O or C for both, old or current respectively.

PCFILE	X(255)	Mandatory	None	The PC filename in which to place the extracted data, in the format (drive:)(path)filename(.extension)
MSGTYPE	X(8)	Conditional	UNKNOWN	If a file contains EDI data, then a specified message type can be extracted from it. This parameter specifies that message type. The default parameter "UNKNOWN" specifies a non-EDI file.
NEW		Conditional		If this is specified then the latest non-EDI file (message type of "Unknown") is retrieved.
OLD		Conditional		If this is specified then the oldest non-EDI file (message type of "Unknown") is retrieved.
-END		Mandatory		End of Command

Notes

Three general parameter groups can be selected from the above table. The output PC filename is mandatory and will always be present so has been excluded from this commentary.

NEW or OLD is mandatory when combined with LOCAL or MSGTYPE or VIRTFILE, or a combination of these three.

If just OLD is specified, then the oldest non-EDI file (message type of "Unknown") is extracted.

If OLD and MSGTYPE parameters are specified then the oldest EDI message of that message type is extracted.

A similar process happens with the NEW parameter except that the latest file or message type is extracted.

The same functioning as MSGTYPE happens with LOCAL and VIRTFILE except that it will be the oldest or newest file for the specified local code or virtual filename that is extracted.

The parameters NEW and OLD obviously should not appear together in the same command set.

The parameters VIRTFILE, VIRTDATE, VIRTTIME, and LOCAL, when appearing together will specify a particular interchange for extraction.

The third method of extraction is to use the parameters FTPFILE and LOCAL. This obviously only applies when the disk file name of the Received file is known at the time of the batch run, which will be relatively rare.

Returned

```
-RCVFILE
RETURN CODE nn
I01 LOCAL=aaaa
I03 VIRTDATE=yymmdd
I04 VIRTTIME=hhmmss
I05 VIRTFILE=file name
I08 PCFILE= (drive:)(path)filename(.ext)
I02 MSGTYPE=aaaaaaaa
I16 FILETYPE=B
I10 NEW
I10 OLD
I99 -END

O47 SFID code of sender
O09 FTP filename
O02 MSGTYPE of file
O48 VDT VFN of file

E00 Invalid Keyword Follows
E74 No parameter allowed

M02 Invalid PC file name

M99 Request Completed Successfully

Z99 BAT0006I End of command file reached
```

Examples

The following example is a general search and extract of the DELINS messages on the oldest file containing DELINS messages sent from the trading partner whose local code is UKTE.

```
RCVFILE EXAMPLE HEADER
-RCVFILE
LOCAL=UKTE
MSGTYPE=DELINS
PCFILE=OUTPUT
OLD
-END
```

The response to this file, would be an output to the ODEXPC.RSP file of lines similar to the following.

```
RCVFILE EXAMPLE HEADER
-RCVFILE
RETURN CODE 00
I01 LOCAL=UKTE
I02 MSGTYPE=DELINS
I08 PCFILE=OUTPUT
I10 OLD
I99 -END
O47 UK-TEST
O09 00000003.CMS
O02 DELINS
O48 92/08/03/11:39:22 TEST.EDI
M99 Request Completed Successfully
Z99 BAT0006I End of command file reached
```

The first line of the response file shows the header from the input file and is only a text comment. The second line shows the command and is followed by the return code which shows a successful extraction. The following five lines are echoes of the batch file commands.

Line **O47** shows that the file extracted was sent by EDI code UK-TEST (local code UKTE).

Line **O09** states that the information retrieved was stored in disk file 00000003.CMS.

Line **O02** states that a DELINS message was retrieved.

Line **O48** details the date, time and filename of the Virtual file that was received. The date and time refer to the date and time that the file was scheduled for transmission and not the time of receipt.

Line **M99** shows that this request was completed successfully and Z99 indicates that this is the end of the Batch command file. The data extracted would have been written to a file called OUTPUT on the current directory.

-RCVODETT – Extract EDI Data

This command acts on EDI files received via ODEX comms. The function of this command is to extract EDI data from the ODEX system into a PC file which can then be translated and used. ODEX files that have been received via comms are stored in the ..\Data\Comms_In directory of the ODEX installation directory. These files are scanned by this command for data of the type given in the MSGTYPE parameter, and all data matching the descriptions is written to the output PC file. Only the files that have been received correctly are extracted. All others are left on the system until the next run of this command (or a manual extraction is performed).

This process allows the user to, for example, scan the incoming messages for all invoice data files so that the received invoices can be extracted, translated and fed into this period's purchase ledger run. The extraction is limited to a single trading partner.

The PC file used as the output file from this command will be cleared of all other data before being written to, thus giving the added security that the files' data from last month will not be used again.

Examples of Format/Length column formats:

- X(12) is an alphanumeric field of up to 12 characters.
- 9(5) is a numeric field of maximum length 5 digits.
- 999 is a numeric field of maximum length 3 digits.
- XX is an alphanumeric field of maximum length 2 digits.

Provided

Command	Format/ Length	Mandatory/ Conditional	Default Value	Description / Content
-RCVODETT				Command Name
MSGTYPE	X(8)	Mandatory	None	The message type required for extraction. E.g. INVOIC, DELINS, etc. Wildcards of * and ? may be used.
PCFILE	X(255)	Mandatory	None	The output PC filename in the format (drive:)(path)filename(.extension). Only the filename is mandatory.
LOCAL	X(35)	Conditional	None	Use this to restrict the search to a specified local code.

VALORIG	X(1)	Conditional	None	This parameter is valid for this command, but specifying it will have no influence on what happens.
-END		Mandatory		End of Command

Returned

```
-RCVODETT
RETURN CODE nn
I02 MSGTYPE=aaaaaaaa
I08 PCFILE= (drive:)(path)filename(.ext)
I01 LOCAL=aaaa
I56 VALORIG=Y
I99 -END

O47 originating SFID
O09 FTP file name
O30 originating name
O02 msg. type
O48 yy/mm/dd hh:mm:ss virtual-file-name

M98 Request not completed
M99 Request Completed Successfully

E00 Invalid keyword follows
Z99 BAT0006I End of command file reached
```

Example

In the following example, two files containing DELINS messages, and maybe other different types of messages, has been sent to the ODEX system and successfully received. An EERP has been sent back to the sender as confirmation of receipt. We are now in a position to extract the EDI data, and the portion of the command file to do this would look something like this :

```
-RCVODETT
MSGTYPE=DELINS
PCFILE=C:\DELIVINS.EDI
-END
```

No local code was specified so all the completed disk files will be scanned, and not just those from a particular local code. The data will be written to a file called C:\DELIVINS.EDI for later processing. The response file ODEXPC.RSP will look something like this :

```
-RCVODETT
RETURN CODE 00
I02 MSGTYPE=DELINS
I08 PCFILE=C:\DELIVINS.EDI
I99 -END
O47 023987DD1028ED
O09 00000002.CMS
O30 Data Interchange Plc
O02 DELINS
O48 92/07/30 09:39:21 DELIVERY-INST
O47 043987DD1028ED
O09 00000003.CMS
O30 Data Interchange Plc
O02 DELFOR
O48 92/07/31 09:39:21 DELIVERY-INST2
M99 Request Completed Successfully
Z99 BAT0006I End of command file reached
```

In the sample ODEXPC.RSP file shown above, it can be seen that the transaction was successful by the return code on the second line and by the **M99** line next to the end. ODEXBAT would also have exited with the operating system error level set to zero.

Taking the ODEXPC.RSP file line by line, the lines starting with the letter **I** are the command file lines being echoed across to the response file.

Line **O47** gives the SFID code of the originator mailbox.

Line **O09** gives the name of the disk file in which the message was stored in the ODEX system.

This is followed by **O30** which gives the name of the originator mailbox.

The next line in the group is **O02** which gives the message type of the first message in the file.

These are followed by the **O48** line which is the virtual date and time along with the virtual filename of the received file.

As you can see above, the above group of **O** type records are output once for each received file that is extracted (two files so two groups).

Finally **M99** states that the -RCVODETT command has been completed successfully and **Z99** shows that the end of the commands file has been reached.

-REPRCV – Report on Received Files

The purpose of this command is to generate a report, either to a file or to a printer, which shows details of all files that have been received by ODEX (or part received) and their current status on the system. This command can be used to check that a file has been successfully received and whether or not the EERP has been sent back. The parameters on the command allow the user to select a useful range of possible outputs varying from a list of the whole file to a selected single transaction.

It is possible to obtain a complete list of all currently received files (Status = C) to the printer (PRN) by just giving the command and the end statement (-REPRCV and -END) and no parameters at all. To report on a single file, specify either VIRTFILE and VIRTDATE and VIRTTIME or FTPFILE. To report on all files from a particular trading partner, use the local code parameter etc.

A print is generated which is virtually identical in format to the output from the response file as shown in the examples, the only difference being that the line references are omitted on the print output but page headers and dotted lines to divide the entries are included..

Examples of Format/Length column formats:

- X(12) is an alphanumeric field of up to 12 characters.
- 9(5) is a numeric field of maximum length 5 digits.
- 999 is a numeric field of maximum length 3 digits.
- XX is an alphanumeric field of maximum length 2 digits.

Provided

Command	Format/ Length	Mandatory/ Conditional	Default Value	Description / Content
-REPRCV				Command Name
FILETYPE	X	Conditional	C	Type of file to select. **C** = Current files (Not yet EERP'd or extracted). **O** = Old files (both EERP'd and extracted). **B** = Both
LOCAL	X(35)	Conditional	None	Local code to select.
MSGTYPE	X(8)	Conditional	None	Message type to select.
DESTINATION	X(255)	Conditional	PRN	The destination of the output. PRN sends to printer, otherwise use a filename in the format (drive:)(path)filename(.extension).
FTPFILE	X(12)	Conditional	None	The disk file to select.

VIRTFILE	X(26)	Conditional	None	The virtual filename to select.
VIRTDATE	9(6)	Conditional	None	The date of the virtual file to select. In the format YYMMDD.
VIRTTIME	9(6)	Conditional	None	The time of the virtual file to select. In the format HHMMSS.
-END		Mandatory		End of Command

Returned

```
-REPRCV
RETURN CODE nn
I01 LOCAL=aaaa
I02 MSGTYPE=aaaaaaaa
I03 VIRTDATE=yymmdd
I04 VIRTTIME=hhmmss
I05 VIRTFILE=file name
I09 FTPFILE=file name
I16 FILETYPE=t
I70 DESTINATION=dest
I99 -END

E01 Unable to allocate working storage
E01 Unable to open output device /file
E01 Unable to open output device /file
E04 Invalid virtual time
E10 Invalid virtual date
E16 File format not F, T, U or V
E51 Name contains invalid Odette characters
E71 Field size exceeded

R19 Data Interchange UK-TEST (UKTE
R05 Virtual name 92/08/03 17:22:17 TESTDATAFILE
R08 PC name 92/02/17 09:45:08 c:\autoexec.bat
R09 FTP name 92/08/03 17:22:16 00000007.CMS
R02 Message type UNKNOWN
R15 User data
R26 Received 92/08/03 17:22:16
R27 EERP sent 92/08/03 17:21:00
R29 U 00000 0000001 0 Y 000000000 000000000000 40
R18 Current send files = 3
```

Example

The following example will generate a print of all files received from a trading partner with the local code of UKTE, whether old or current (i.e. B for both) writing the output to a file called OUTPUT instead of the printer.

```
REPRCV EXAMPLE
-REPRCV
LOCAL=UKTE
FILETYPE=B
DESTINATION=OUTPUT
-END
```

The response file, ODEXPC.RSP, generated by this command file will echo the output to the OUTPUT file in all except the initial echoing back of the commands and the line reference number on each line. It could look something like the following :

```
REPRCV EXAMPLE
-REPRCV
RETURN CODE 00
I01 LOCAL=UKTE
I16 FILETYPE=B
I70 DESTINATION=OUTPUT
I99 -END
R19 Data Interchange                        UK-TEST                      (UKTE
R05 Virtual name     92/08/03 11:39:22 TEST.EDI
R08 PC name          92/08/05 09:09:56 OUTPUT
R09 FTP name         92/08/03 11:54:32 00000003.CMS
R02 Message type     DELINS Version
R15 User data
R26 Received         92/08/03 11:56:06
R27 EERP sent        92/08/03 11:57:53
R28 Last reason      00 - File successfully processed
R29                   U  00000 0000009   0     Y    000000000 000000008291
98
R19 Data Interchange                        UK-TEST                      (UKTE
R05 Virtual name     92/08/03 11:39:39 TEST.EDI
R08 PC name          92/08/05 09:09:58 OUTPUT
R09 FTP name         92/08/03 11:56:11 00000004.CMS
R02 Message type     DELINS   Version
R15 User data
R26 Received         92/08/03 11:57:45
R27 EERP sent        92/08/03 11:57:50
R28 Last reason      00 - File successfully processed
R29                   U  00000 0000009   0     Y    000000000 000000008291
98
R19 Data Interchange                        UK-TEST                      (UKTE
R05 Virtual name     92/07/31 11:25:13 CONFIG.SYS
R08 PC name          --/--/-- --:--:--
R09 FTP name         92/07/31 11:35:41 00000000.CMS
R02 Message type     UNKNOWN
R15 User data
R26 Received         92/07/31 11:36:04
R27 EERP sent        92/07/31 11:42:39
R28 Last reason      00 - File successfully processed
R29                   U  00000 0000002   0     Y    000000000 000000001695
98
R19 Both current & old received files = 3
M99 Request Completed Successfully
Z99 BAT0006I End of command file reached
```

In the above example, three files have been received from local code UKTE. The first few lines are the echoes of the command file, this is followed by the three file entry groups.

Each file entry starts with an **R19** line giving the trading partner's company name, looked up from the Trading Partner entries, the EDI code of the trading partner, and their local code.

This is followed by an **R05** line showing the date and time of scheduling and the virtual filename.

The **R08** line shows the date and time of creation of the extraction PC filename and the filename itself. If the file has not yet been extracted from ODEX then the date and time will be set to hyphens and the filename will be spaces.

The **R09** line shows the date and time of creation of the disk file and its actual name.

The **R02** line shows the message type contained within the file, in multi-message files this will be the message type of the first message within the file. UNKNOWN indicates that the file contains non-EDI type data.

The **R15** line shows the 8 characters of user data, if they are defined.

Line **R26** shows the date and time the file was received. This will normally be the time of the end of the file receive, when the EFID (End File Identifier) is transmitted, but if transmission is interrupted part way through, this will show that time.

Line **R27** shows the date and time that the EERP (End to End Response) was sent. This will be set to hyphens for the date and time if the EERP has not yet been received.

Line **R28** states the last reason for failure or success. It will normally say 00 - File successfully processed, but in the case of transmission failure it will give the reason code and reason for the last failure.

Line **R29** is a complex line containing the following value in order.

The first value is the file format, F, T, U or V.

The second value is the record length if the file was fixed length records. Otherwise this is set to zeros.

The third value is the size of the file in Kilobytes, rounded to the nearest 1K.

The fourth value is the number of attempts to send this file so far.

The fifth value is an indicator stating whether retries are allowed or not. A value of Y indicates that they are allowed.

The sixth value is the number of records transmitted for files with fixed length records, otherwise it is zero.

The seventh value is the actual file size received, in bytes.

The eighth and last value is the status flag for the file.

Line **R18** states the number of files, of the file type specified, appearing on the report.

This is followed by **M99** and **Z99** indicating a successful report.

-REPSND – Report on Scheduled Files

The purpose of this command is to generate a report, either to a file or to a printer, which shows details of all files that have been scheduled by ODEX for sending and their current status on the system. This command can be used to check that a file has been successfully sent and whether or not the associated EERP has been received. The parameters on the command allow the user to select a useful range of possible outputs varying from a list of the whole file to a selected single transaction.

It is possible to obtain a complete list of all currently scheduled files (Status = C) to the printer (PRN) by just giving the command and the end statement (-REPSND and -END) and no parameters at all. To report on a single file, specify either VIRTFILE and VIRTDATE and VIRTTIME or FTPFILE. To report on all files for a particular trading partner, use the local code parameter etc.

A print is generated which is virtually identical in format to the output from the response file as shown in the examples, the only difference being that the line references are omitted on the print output but page headers and dotted lines to divide the entries are included.

Examples of Format/Length column formats:

- X(12) is an alphanumeric field of up to 12 characters.
- 9(5) is a numeric field of maximum length 5 digits.
- 999 is a numeric field of maximum length 3 digits.
- XX is an alphanumeric field of maximum length 2 digits.

Provided

Command	Format/ Length	Mandatory/Conditional	Default Value	Description / Content
-REPSND				Command Name
FILETYPE	X	Conditional	C	Type of file to select. **C** = Current files (Not yet sent or acknowledged). **O** = Old files (both sent and acknowledged with EERP). **B** = Both.
LOCAL	X(35)	Conditional	None	Local code to select.
MSGTYPE	X(8)	Conditional	None	Message type to select.
DESTINATION	X(30)	Conditional	PRN	The destination of the output. PRN sends to printer, otherwise use a filename in the format (drive:)(path)filename(.extension).

FTPFILE	X(12)	Conditional	None	The disk file to select.
VIRTFILE	X(26)	Conditional	None	The virtual filename to select.
VIRTDATE	9(6)	Conditional	None	The date of the virtual file to select. In the format YYMMDD.
VIRTTIME	9(6)	Conditional	None	The time of the virtual file to select. In the format HHMMSS.
-END		Mandatory		End of Command

Returned

```
-REPSND
RETURN CODE nn
I01 LOCAL=aaaa
I02 MSGTYPE=aaaaaaaa
I03 VIRTDATE=yymmdd
I04 VIRTTIME=hhmmss
I05 VIRTFILE=file name
I09 FTPFILE=file name
I16 FILETYPE=t
I70 DESTINATION=dest
I99 -END

E01 Unable to allocate working storage
E01 Unable to open output device /file
E03 Invalid early date / time
E04 Invalid early date / time
E16 File format not F, T, U or V
E50 Name contains invalid Odette characters
E71 Field size exceeded

R19 Data Interchange                        UK-TEST                      (UKTE
R05 Virtual name     92/08/03 17:22:17 TESTDATAFILE
R08 PC name          92/02/17 09:45:08 c:\autoexec.bat
R09 FTP name         92/08/03 17:22:16 S0000007.ODX
R02 Message type     UNKNOWN
R15 User data
R12 Priority         5
R24 Scheduled at     92/08/03 17:22:16
R10 Send after       92/08/03 17:21:00
R26 Transmitted      --/--/-- --:--:--
R27 EERP received    --/--/-- --:--:--
R29                   U  00000 0000001   0     Y    000000000 000000000000
40
R18 Current send files = 3
```

Example

The following example will generate a print of all files scheduled for transmission to a trading partner with the local code of UKTE, writing the output to a file called OUTPUT instead of the printer.

```
REPSND EXAMPLE
-REPSND
LOCAL=UKTE
DESTINATION=OUTPUT
-END
```

The response file, ODEXPC.RSP , generated by this command file will echo the output to the OUTPUT file in all except the initial echoing back of the commands

and the line reference number on each line. It could look something like the following :

```
REPSND EXAMPLE
-REPSND
RETURN CODE 00
I01 LOCAL=UKTE
I70 DESTINATION=OUTPUT
I99 -END
R19 Data Interchange                        UK-TEST                     (UKTE
R05 Virtual name     92/08/03 16:57:16 TESTOUT.EDI
R08 PC name          92/08/03 16:56:22 u:\testdata\testout.edi
R09 FTP name         92/08/03 16:57:16 00000005.CMS
R02 Message type     DELINS      Version 2           Msgref 2
R15 User data
R12 Priority         5
R24 Scheduled at     92/08/03 16:57:19
R10 Send after       92/08/03 16:56:00
R26 Transmitted      --/--/-- --:--:--
R27 EERP received    --/--/-- --:--:--
R29                   U  00000 0000009   0      Y    000000000 000000000000
40
R19 Data Interchange                        UK-TEST                     (UKTE
R05 Virtual name     92/08/03 16:57:19 TESTOUT.EDI
R08 PC name          92/08/03 16:56:22 u:\testdata\testout.edi
R09 FTP name         92/08/03 16:57:18 00000006.CMS
R02 Message type     DELINS      Version 2           Msgref 2
R15 User data
R12 Priority         5
R24 Scheduled at     92/08/03 16:57:19
R10 Send after       92/08/03 16:56:00
R26 Transmitted      --/--/-- --:--:--
R27 EERP received    --/--/-- --:--:--
R29                   U  00000 0000009   0      Y    000000000 000000000000
40
R19 Data Interchange                        UK-TEST                     (UKTE
R05 Virtual name     92/08/03 17:22:17 TESTDATAFILE
R08 PC name          92/02/17 09:45:08 c:\autoexec.bat
R09 FTP name         92/08/03 17:22:16 00000007.CMS
R02 Message type     UNKNOWN
R15 User data
R12 Priority         5
R24 Scheduled at     92/08/03 17:22:16
R10 Send after       92/08/03 17:21:00
R26 Transmitted      --/--/-- --:--:--
R27 EERP received    --/--/-- --:--:--
R29                   U  00000 0000001   0      Y    000000000 000000000000
40
R18 Current send files = 3
M99 Request Completed Successfully
Z99 BAT0006I End of command file reached
```

In the above example, three files have been scheduled for transmission to UKTE. The first few lines are the echoes of the command file. This is followed by the three file entry groups.

Each file entry starts with an **R19** line giving the trading partner's company name, looked up from the Trading Partner entries, the EDI code of the trading partner, and their local code.

This is followed by an **R05** line showing the date and time of scheduling and the virtual filename.

The **R08** line shows the date and time of creation of the PC filename and the filename itself.

The **R09** line shows the date and time of creation of the disk file and its actual name. This date and time will generally be within seconds of the virtual filename's date and time.

The **R02** line shows the message type contained within the file. In multi-message files this will be the message type of the first message within the file. UNKNOWN indicates that the file contains non-EDI type data.

The **R15** line shows the 8 characters of user data, if they are defined.

Line **R12** shows the priority of the transmission. The lower the number, the higher the priority. This will only be of use in busy systems where many large files are queued for sending.

Line **R24** shows the date and time the file was scheduled. This will be the same as the date and time on line R05.

Line **R10** shows the earliest date and time that the file can be sent. This will default to the date and time of scheduling but may be changed.

Line **R26** shows the date and time that the file was sent. This will normally be the time of the end of the file send, when the EFID (End File Identifier) is transmitted, but if transmission is interrupted part way through, this will show the time of the interruption.

Line **R29** is a complex line containing the following values in order.

The first value is the file format, F, T, U or V.

The second value is the record length if the file was fixed length records. Otherwise this is set to zeros.

The third value is the size of the file in Kilobytes, rounded to the nearest 1K.

The fourth value is the number of attempts to send this file so far. This will normally be zero or one unless problems occur. Zero indicates that transmission has not been attempted yet.

The fifth value is an indicator stating whether retries are allowed or not. A value of Y indicates that they are allowed.

The sixth value is the number of records transmitted for files with fixed length records, otherwise it is zero.

The seventh value is the actual file size transmitted, in bytes.

The eighth and last value is the status flag for the file.

Line **R18** states the number of files, of the file type specified, appearing on the report.

This is followed by **M99** and **Z99** indicating a successful report.

-RUNTASK – Run a task from the Event Scheduler

This command is no longer supported under ODEX Enterprise.

-SNDFILE – Schedule a file to be sent

This command's purpose is to schedule a non-EDI file to be sent to a trading partner. Any file of any type or length or format can be sent using this function (including EDI files if required, although this is not the function for which it was intended).

The data for transmission is taken from the original PC file into the ODEX system where it is stored below the ODEX installation directory in the ..\Data\Comms_Out directory under the control of ODEX itself. Therefore as soon as the file has been scheduled it may be removed from the system if so desired, as ODEX has taken a copy to send.

Note that this command format is very similar to the -SNDODETT command, the only difference being the necessity for a local code. This is because, as the file is not in EDI format, the UNB segment is not present in the file to direct the data to the correct trading partner, thus making it necessary for the command file to provide this information.

Important Note

In the Batch Interface, the PRIORITY parameter values range from 1 to 9, where 9 is the highest priority and 1 is the lowest. This is to ensure compatibility with users who have upgraded from ODEX Professional. This differs from the way Priority fields are handled in the rest of ODEX Enterprise, where 1 is the highest priority.

Please Note - Whilst it is possible to schedule and send files with virtual filenames that include space characters, the OFTP standards state that this is not an accepted practice. It is supported in ODEX by popular request, but you should clear its use with your trading partner because some OFTP software will reject the file.

Examples of Format/Length column formats:

- X(12) is an alphanumeric field of up to 12 characters.
- 9(5) is a numeric field of maximum length 5 digits.
- 999 is a numeric field of maximum length 3 digits.
- XX is an alphanumeric field of maximum length 2 digits.

Provided

Command	Format/ Length	Mandatory/ Conditional	Default Value	Description / Content
-SNDFILE				Command Name
LOCAL	X(35)	Mandatory	None	The local code of the destination trading partner.

OLOCAL	X(35)	Conditional	None	The local code of the originating (internal) mailbox. If this parameter is not specified, then the first mailbox associated with the default internal network (of the same protocol type as the destination trading partner) is used.
PCFILE	X(255)	Mandatory	None	The drive path and filename of the file containing the data to be sent. In the format (DRIVE:)(PATH)Filename(.EXT) where only the filename is mandatory.
VIRTFILE	X(26)	Conditional	Filename part of PCFILE	The EDI Virtual Filename to be given to the transmission. If this is omitted the system will use the PC Filename, excluding the drive, path and extension.
EARLYDATE	9(6)	Conditional	Current Date	This is the earliest date that ODEX may send this file. In the format YYMMDD.
EARLYTIME	9(6)	Conditional	Current Time	This is the earliest time that ODEX may send this file. In the format HHMMSS. It is possible to specify that the file should be scheduled a number of minutes in the future by placing a **+** and the desired value in minutes by which the transmission of the file is to be delayed.
PRIORITY	9	Conditional	5	The priority of the transmission. (Priority **9** will be sent first from the queue)

FORMAT	X	Conditional	U	The format of the transfer. Valid values are **U**, **T, F** or **V**.
RECSIZE	9(5)	Conditional	0	If format is set to **F** for "Fixed" length records, this parameter specifies the record length.
USERDATA	X(8)	Conditional	Spaces	Passed with the file ID, this can be used for any purpose agreed with trading partners.
PAD_SPACES	9(4)	Conditional	-1	This is used to ensure that every line of the PC file is of a set length. Generally used when sending fixed length files. The default value of -1 means that padding should not be used.
-END		Mandatory		End of Command

Returned

```
-SNDFILE
RETURN CODE nn
I01 LOCAL=aaaa
I08 PCFILE= (drive:)(path)filename(.ext)
I05 VIRTFILE=file name
I10 EARLYDATE=yymmdd
I11 EARLYTIME=hhmm
I03 PRIORITY=n
I13 FORMAT=a
I14 RECSIZE=nnnnn
I15 USERDATA=aaaaaaaa
I99 -END

O46 destination EDI code
O45 yy/mm/dd hh:mm:ss size = nnnnnnnnn
O09 FTP file name
O48 yy/mm/dd hh:mm:ss virtual-file-name

E00 Invalid Keyword Follows (this followed by line echoed from file)
E01 Unknown origin/destination
E08 Invalid PC file name
E10 Invalid early date. Use YYMMDD
E10 Invalid early time. Use HHMM
E13 FORMAT=3 value is Not 'F', 'T', 'U', or 'V'
E44 File size is not a multiple of record size
E44 Record size cannot be zero for fixed file format
E71 XXX has no value (where XXX is the parameter name)
E71 XXX value is longer than Y (where X = param name, Y = max length)
E73 XXX=Y value is not numeric (where XXX=Y is the echo of the command file
parameter line, XXX being the numeric parameter name).
E99 Mandatory missing parameter XXX (where XXX is the mandatory param name)

M04 Invalid Length for PAD_SPACES
M98 Request Not Completed
M99 Request Completed Successfully
```

```
Z99 BAT0006I End of command file reached
```

Example

A non-EDI file, C:\DATA\NONEDI.TXT is scheduled to be sent at the earliest opportunity. The file will be sent to a trading partner with the local code of UKTE. The virtual filename that it will be sent under is TEXT-FILE. The parameters in the ODEX batch file required to complete this task are:

```
-SNDFILE
LOCAL=UKTE
PCFILE=C:\DATA\NONEDI.TXT
VIRTFILE=TEXT-FILE
-END
```

The resultant response file would look like this, assuming that no errors were encountered.

```
-SNDFILE
RETURN CODE 00
I01 LOCAL=UKTE
I08 PCFILE=C:\DATA\NONEDI.TXT
I05 VIRTFILE=TEXT-FILE
I99 -END
O46 UK-TEST
O45 23/07/92 18:12:00 SIZE = 000003621
O09 00000023.CMS
O48 92/07/24 14:23:04 TEXT-FILE
M99 Request Completed Successfully
Z99 BAT0006I End of command file reached
```

Taking this example, line by line, the first line is the command used, immediately followed by the return code showing how successful this command was. In this case a return code of 00 indicates to us that the command was completely successful and that no problems were encountered.

The next three lines, starting **I01**, **I08**, **I05** and **I99**, are the rest of the command file echoed across to the response file.

The following **O** type lines are the output of information regarding the sending of the file.

Line **O46** gives the EDI code of the destination. This has been derived from the local code input.

Line **O45** states the date and time of creation of the data file and its size in bytes.

Line **O09** states the name of the operating system file that now holds the data, ready for transmission. This file, the disk file, will remain in the ODEX database until either the EERP is received stating that the file has been successfully received at the remote end (and the retention period has expired), or until it is deleted from the database by user action deleting the scheduled files.

Line **M99** indicates that the command has been completed, and **Z99** indicates that the end of the command file has been reached and there are no more transactions to process.

-SNDODETT – Schedule an EDI file to be sent

This command's purpose is to schedule an EDI formatted file to be sent to a trading partner.

The main difference between this command and the -SNDFILE command is that this command requires no local code to provide information on the destination of the outgoing call, the EDI code being provided by the UNB or routing segment of the message to be sent. Because of this routing, and the fact that a single EDI file can contain many messages (with many UNBs), a single command can generate multiple outgoing messages. This makes the -SNDODETT command very powerful and flexible.

The data for transmission is taken from the original PC file into the ODEX system where it is stored below the ODEX installation directory in the ..\Data\Comms_Out directory under the control of ODEX itself. Therefore as soon as the file has been scheduled it may be removed from the system if so desired, as ODEX has taken a copy to send.

Important Note

In the Batch Interface, the PRIORITY parameter values range from 1 to 9, where 9 is the highest priority and 1 is the lowest. This is to ensure compatibility with users who have upgraded from ODEX Professional. This differs from the way Priority fields are handled in the rest of ODEX Enterprise, where 1 is the highest priority.

Please Note - Whilst it is possible to schedule and send files with virtual filenames that include space characters, the OFTP standards state that this is not an accepted practice. It is supported in ODEX by popular request, but you should clear its use with your trading partner because some OFTP software will reject the file.

Examples of Format/Length column formats:

- X(12) is an alphanumeric field of up to 12 characters.
- 9(5) is a numeric field of maximum length 5 digits.
- 999 is a numeric field of maximum length 3 digits.
- XX is an alphanumeric field of maximum length 2 digits.

Provided

Command	Format/ Length	Mandatory/ Conditional	Default Value	Description / Content
-SNDODETT				Command Name
PCFILE	X(255)	Mandatory	None	The drive path and filename of the file containing the data to be sent. In the format (DRIVE:)(PATH)Filename(.EXT) where only the filename is mandatory.

VIRTFILE	X(26)	Conditional	Filename part of PCFILE	The EDI Virtual Filename to be given to the transmission. If this is omitted, the system will use the PC Filename, excluding the drive, path and extension.
EARLYDATE	9(6)	Conditional	Current Date	This is the earliest date that ODEX may send this file. In the format YYMMDD.
EARLYTIME	9(6)	Conditional	Current Time	This is the earliest time that ODEX may send this file. In the format HHMMSS. It is possible to specify that the file should be scheduled a number of minutes in the future by placing a **+** and the desired value in minutes by which the transmission of the file is to be delayed.
PRIORITY	9	Conditional	5	The priority of the transmission. (Priority **9** will be sent first from the queue)
FORMAT	X	Conditional	U	The format of the transfer. Valid values are **U**, **T, F** or **V**.
RECSIZE	9(5)	Conditional	0	If format is set to **F** for Fixed length records, this parameter specifies the Record length.
USERDATA	X(8)	Conditional	Spaces	The SFID User Data passed with the file ID, this can be used for any purpose agreed with trading partners.
-END		Mandatory		End of Command

Returned

```
-SNDODETT
RETURN CODE nn
I08 PCFILE= (drive:)(path)filename.ext
I05 VIRTFILE=file name
```

```
I10 EARLYDATE=yymmdd
I11 EARLYTIME=hhmm
I03 PRIORITY=n
I13 FORMAT=a
I14 RECSIZE=nnnnn
I15 USERDATA=aaaaaaaa
I99 -END

O45 yy/mm/dd hh:mm:ss size = nnnnnnnnn
O01 destination local code
O46 destination EDI code
O09 FTP Workfile name
O02 msg. type
O48 yy/mm/dd hh:mm:ss virtual-file-name

E00 Invalid Keyword Follows
E05 Invalid virtual file name
E08 Invalid PC filename
E10 Invalid early date / time
E13 File format not F, T, U or V
E14 Invalid record size
E44 File size is not a multiple of record size
E90 No Authority to use this option
E93 User Directory entry not found
E94 Invalid origin for user profile

M02 TEXT record longer than 2048
M04 Not an EDI format input file
M05 Missing 'END' segment
M06 No terminating line feed character
M08 Missing 'END' segment
M09 Invalid EDI file structure
M10 Sub-element table overflow
M11 Element table overflow
M12 Unknown origin code
M13 Unknown destination code
M14 Control file is full
M15 Error creating output file

M99 Request Completed Successfully

Z99 BAT0006I End of command file reached
```

Example

An EDI file, C:\DATA\DELIVINS.EDI is scheduled to be sent at the earliest opportunity. The UNB segment from the EDI file will provide all the required information of where the file is to be sent. The virtual filename that it will be sent under is DELIVERY-INSTRUCTIONS. The parameters in the ODEX batch file required to complete this task are:

```
-SNDODETT
PCFILE=C:\DATA\DELIVINS.EDI
VIRTFILE=DELIVERY-INSTRUCTIONS
-END
```

The resultant response file would look like this, assuming that no errors were encountered.

```
-SNDODETT
RETURN CODE 00
I08 PCFILE=C:\DATA\DELIVINS.EDI
I05 VIRTFILE=DELIVERY-INSTRUCTIONS
I99 -END
O45 23/07/92 16:16:00 SIZE = 000008601
O01 UKTE
O46 UK-TEST
O09 00000017.CMS
```

```
O02 DELINS
O48 92/07/24 14:23:04 DELIVERY-INSTRUCTIONS
M99 Request Completed Successfully
Z99 BAT0006I End of command file reached
```

As can be seen from the example response file, rather more information is presented back than needs to be input in the first place. Taking this example, line by line, the first line is the command used, immediately followed by the return code showing how successful this command was. In this case a return code of 00 indicates to us that the command was completely successful and that no problems were encountered.

The next three lines, starting **I08**, **I05** and **I99**, are the rest of the command file echoed across to the response file.

The following **O** type lines are the output of information regarding the sending of the file.

Line **O45** states the date and time of creation of the EDI data file and its size in bytes.

Line **O01** gives the local code of the file's destination so that we can look it up easily if required.

Line **O46** gives the EDI code of the destination.

Line **O09** states the name of the disk file that now holds the data, ready for transmission. This file will remain in the ODEX database until either the EERP is received stating that the file has been successfully received at the remote end (and the retention period has expired), or until it is deleted from the database by user action deleting the scheduled files.

The next line, **O02**, states that the data that is to be sent is actually DELINS standard information.

The **O48** line gives the date and time that the file was scheduled for sending together with the Virtual filename.

Line **M99** indicates that the command has been completed, and **Z99** indicates that the end of the command file has been reached and there are no more transactions to process.

-STOPSERVER – Stop ODEX

The purpose of this command is to stop ODEX running.

Provided

Command	Format/ Length	Mandatory/ Conditional	Default Value	Description / Content
-STOPSERVER				Command Name

Returned

There are no parameters and no returns from this command.

Example

The following example will stop ODEX running immediately.

```
STOPSERVER EXAMPLE
-STOPSERVER
```

The response file, ODEXPC.RSP , generated by this command file will simply contain the following:

```
Z99 Batch processing stopped.
```

-TRNSLATE – Translate an EDI File

The function of this command is to translate an EDI format file into an in-house format file. This command allows a file to be translated independently of the scheduling and extraction systems of ODEX.

Examples of Format/Length column formats:

- X(12) is an alphanumeric field of up to 12 characters.
- 9(5) is a numeric field of maximum length 5 digits.
- 999 is a numeric field of maximum length 3 digits.
- XX is an alphanumeric field of maximum length 2 digits.

Provided

Command	Format/ Length	Mandatory/ Conditional	Default Value	Description / Content
-TRNSLATE				Command Name
EDI	X(255)	Mandatory	None	The EDI output filename
DEF	X(32)	Conditional	None	The In-house ID identifying the contents of the file to be translated. This should correspond with the name given in the translator index file's HSE statement
IHS	X(255)	Mandatory	None	The name of the in-house format file to be translated.
-END				

Returned

```
-TRNSLATE
RETURN CODE nn
I93 EDI=(drive:)(path)filename(.ext)
I95 DEF=(drive:)(path)filename(.ext)
I94 IHS=(drive:)(path)filename(.ext)
I41 HARDCOPY
I42 TRACE
I43 DISPLAY
I99 -END

E00 XLT0005E *** Invalid Keyword Follows ***
E01 *** NO SET (set-name) ON IDX FILE ***
E02 *** INVALID EDI FILE ***
E97 User requested termination
E99 Missing mandatory parameter (parameter)
E08 Invalid pc filename
E50 XLT0003 No Msg (messagetype) on IDX file
E71 (command) is longer than nn
M01 Number of segments read            = n
M02 Number of in-house records written = n
```

-WRITELOG – Write a line to the ODEX log

The purpose of this command is to write a specific line to the ODEX log.

Provided

Command	Format/ Length	Mandatory/ Conditional	Default Value	Description / Content
-WRITELOG				Command Name
LogLine		Mandatory	None	The text line to be written to the log.

Returned

There are no returns from this command.

Example

The following example will write a line to the log, indicating the failure of another command.

```
WRITELOG EXAMPLE
-WRITELOG USR0000T The file scheduling failed.
```

The response file, ODEXPC.RSP , generated by this command file will simply contain the following:

```
Z99 BAT0006I End of command file reached
```

-DOS – Obey a DOS command

The -DOS script command has been provided in order to allow DOS commands to be executed from within an ODEX batch command file.

The syntax of the command is :

```
-DOS Command Para1 Para2 ..... ParaN
```

where Command is any standard DOS command such as COPY or TYPE and Para1, Para2, etc., are the parameters for the DOS command. Any DOS program can be run with the -DOS command but larger programs may run out of memory as this must be shared with the ODEXBAT system. It is therefore suggested that only simple DOS functions are used.

Example

Let us assume that a Non-EDI file has been received from a trading partner, the file is extracted from ODEX and copied to another directory from where it is copied to the printer. The command file would look like this:

```
-RCVFILE
LOCAL=UKTE
NEW
PCFILE=OUTFILE.TXT
-END
-DOS COPY OUTFILE C:\PRINTS\COPYFILE.TXT
-DOS COPY C:\PRINTS\COPYFILE.TXT PRN
```

The output from this command file to the response file would look like this:

```
-RCVFILE
RETURN CODE 00
I01 LOCAL=UKTE
I10 NEW
I08 PCFILE=OUTFILE.TXT
I99 -END
O47 UK-TEST
O09 00000002.CMS
O02 UNKNOWN
O48 92/07/31 11:26:02 TESTDATAFILE
M99 Request Completed Successfully
-DOS COPY OUTFILE C:\PRINTS\COPYFILE.TXT
-DOS COPY C:\PRINTS\COPYFILE.TXT PRN
Z99 BAT0006I End of command file reached
```

Note how these commands do not line up in the normal manner but just echo to the response file.

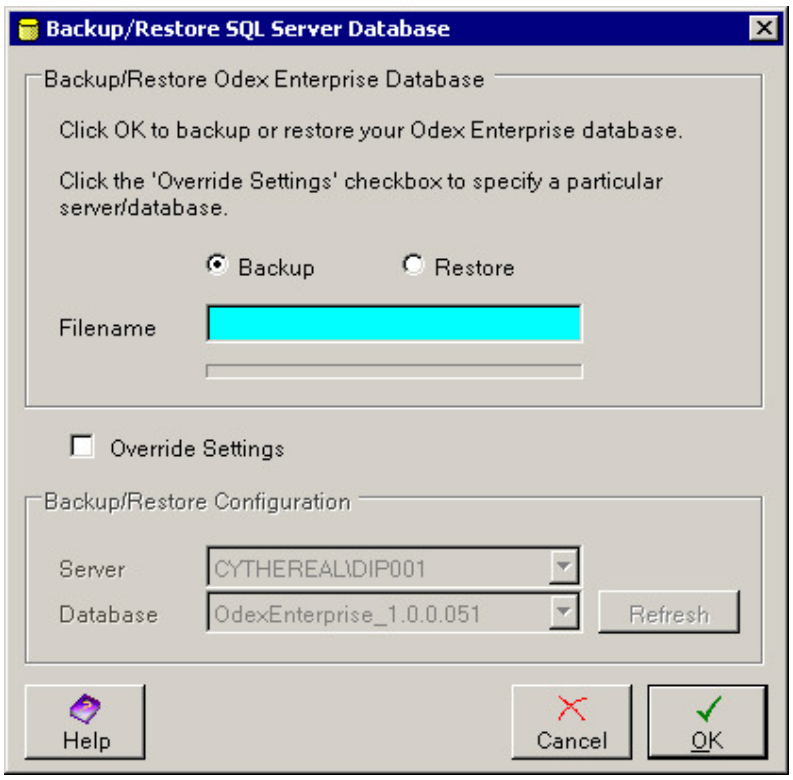
Database Backup and Restore

Introduction

We recommend that you backup the ODEX Enterprise database regularly. This can be achieved quickly and easily from the Start menu. The frequency with which you should perform the backup will depend on your usage of the ODEX software.

Perform a backup or restore

Select **Start >> Programs >> Data Interchange Plc >> ODEX Enterprise >> ODEX Database Backup** to bring up the following dialog.



This dialog is used for both backup and restore operations.

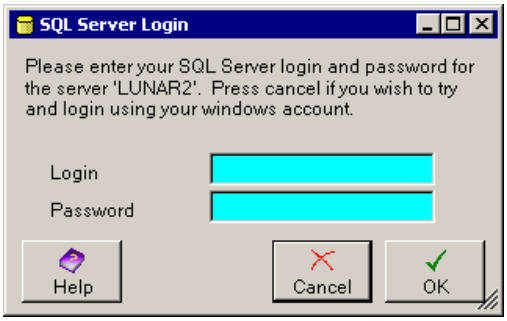
Select the appropriate operation (Backup or Restore) and type in the name of the file that the database is to be backed up to or restored from.

The default server location and database name (shown in the Server and Database fields at the bottom of the dialog) will be used for the operation, unless you select the Override Settings tickbox. This will enable these fields and allow you to change the details using the dropdown arrows.

The **Refresh** button, only available if you have selected the Override Settings tickbox, can be used to reset the Database field to the value it held when you opened the dialog.

Using a non-default server

If you select a Server for which a login and password details are required, you will see a dialog similar to the example below.

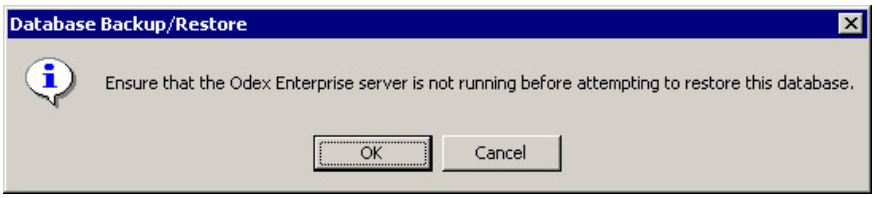


Type your login and password in the appropriate fields and click **OK** to continue. Otherwise click **Cancel** if you wish to try and login using your Windows account.

Performing the operation

Please note that the ODEX Enterprise server may be left running while you perform a backup, but you must close the server before running a restore.

Whenever you attempt to run a restore, you will see the following message box, whether the server is running or not.



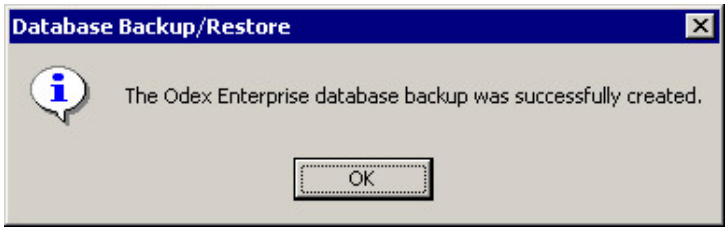
Check in the system tray (usually in the bottom right-hand corner of your screen) for the ODEX server icon. To check for the relevant icon, hold your cursor over the icon and its name will appear. To close the server, right-click on the icon and select Shut Down from the context menu that appears. You can now proceed with the restore.

N.B. Users running ODEX as a system service will need to stop the service in order to run a restore. Please see the section entitled "Running ODEX as a system service" for details of how to do this.

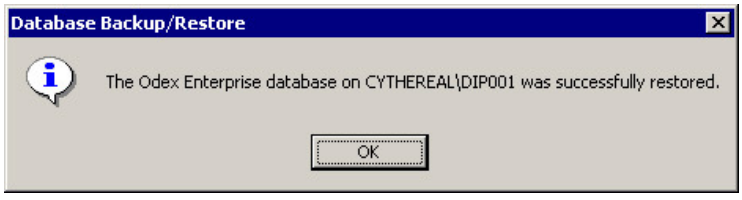
Once the restore is complete, you can start the server (or system service) again.

Whether you perform a backup or a restore, the success of the operation will be indicated to you via a message box, as shown below.

For a backup



or for a restore



Clicking **OK** will close both the message box and the Backup/Restore dialog.

Frequently Asked Questions

How do I add a new trading partner using a direct IP connection?

1. Open the Comms page of the ODEX Administrator.
2. Select the Trading Partners node in the tree view, then click the **New** button on the Trading Partners Actions page.
3. Add the Name and Address details of the Trading Partner on the Overview page.
4. This step is optional, depending on your trading requirements. Open the EDI Codes page and add the EDI code(s) you will use for this Trading Partner, by clicking the **Add** button. Please note that at this stage you will not be able to associate the EDI code with a network.
5. Save these new Trading Partner details.
6. Select the Trading Partner Networks node in the tree view, then click the **New** button on the Trading Partners Networks Actions page and select **New OFTP Network**.
7. On the Overview page, select the new Trading Partner in the Company field, using the dropdown list.
8. Make sure that the Subsystem field contains the value "TCP/IP" and select the appropriate Network connection using the dropdown list.
9. Fill in the remaining mandatory fields on the Overview page.
10. Provide the OFTP passwords if they are required for this Trading Partner, and fill in the description field if you wish to.
11. This step is optional, depending on your trading requirements. Open the Mailboxes page and add a mailbox for this network by clicking the **Add** button.
12. Save the new Trading Partner Network details.
13. Now return to the Trading Partner you just added, if you want to associate the Trading Partner with the new network and, if applicable, with the new mailbox.
14. Select the EDI Codes page of the Trading Partner to be edited, select the EDI Code from the list and click the **Edit** button. Now select the network to be associated with the EDI code. If you have configured a mailbox for this network, this will automatically appear in the Mailbox field when you select the network.
15. Save the EDI Code details, then save the edited Trading Partner details.

How do I add a new trading partner using a local CAPI connection?

1. First you must set up a Local CAPI2 subsystem if you have not already done so. If you have already done so, skip forward to step 7. Open the Comms page of the ODEX Administrator.
2. Select the Subsystems node in the tree view, then click the **New** button on the Subsystems Actions page. Select "Local CAPI2 card subsystem" from the options you are offered.

3. Provide a name for the subsystem on the Overview page, and, if necessary, change any of the values that have been provided as defaults.
4. Save the new subsystem details.
5. You must define at least one listener if you want to receive incoming calls on this subsystem. To do this, double-click on the new subsystem in the tree view, open the Listeners page and click the **Add** button. Provide a name for the listener, and any other information you wish to provide.
6. Save the listener details and the edited subsystem.
7. Open the Comms page of the ODEX Administrator.
8. Select the Trading Partners node in the tree view, then click the **New** button on the Trading Partners Actions page.
9. Add the Name and Address details of the Trading Partner on the Overview page.
10. This step is optional, depending on your trading requirements. Open the EDI Codes page and add the EDI code(s) you will use for this Trading Partner, by clicking the **Add** button. Please note that at this stage you will not be able to associate the EDI code with a network.
11. Save these new Trading Partner details.
12. Select the Trading Partner Networks node in the tree view, then click the **New** button on the Trading Partners Networks Actions page and select **New OFTP Network**.
13. On the Overview page, select the new Trading Partner in the Company field, using the dropdown list.
14. Select your new Local CAPI2 subsystem in the Subsystem field, then type in the ISDN number of this subsystem in the ISDN Number field.
15. Fill in the remaining mandatory fields on the Overview page.
16. Provide the OFTP passwords if they are required for this Trading Partner, and fill in the description field if you wish to.
17. This step is optional, depending on your trading requirements. Open the Mailboxes page and add a mailbox for this network by clicking the **Add** button.
18. Save the new Trading Partner Network details.
19. Now return to the Trading Partner you just added, if you want to associate the Trading Partner with the new network and, if applicable, with the new mailbox.
20. If you previously added an EDI code for this trading partner, select the EDI Code from the list, click the **Edit** button, and select the OFTP network to be associated with this EDI code. Otherwise click the **Add** button, type in the EDI code and select the OFTP network with which this trading partner is to be associated. If you have configured a mailbox for this network, this will automatically appear in the Mailbox field when you select the network.
21. Save the EDI Code details, then save the edited Trading Partner details.

How do I add a new trading partner using an HTTP connection?

1. First you must set up an HTTP subsystem if you have not already done so. If you have already done so, skip forward to step 8.

2. Open the Comms page of the ODEX Administrator. Select the Subsystems node in the tree view, then click the **New** button on the Subsystems Actions page. Select "HTTP subsystem" from the options you are offered.
3. Provide a name for the subsystem on the Overview page by overwriting the words “New Subsystem Entry” in the Name field.
4. You will see that the Local IP address and Port have been provided with default values. These have been obtained from your machine settings, but you may change them if necessary.
5. If you want to use SSL (i.e. add extra security to the HTTP connection using a secure socket layer), select the Use SSL checkbox. This will change the prefix of the URL in the ‘Your URL’ field from http to https. It will also enable the arrow to the right of the ‘Server certificate’ field, which you must use to select a private key certificate for use with this subsystem. Select a certificate (or import or create one) and return to the Overview page.
6. If you need to provide Proxy Server details, open the Advanced page and provide the details there.
7. Save the new subsystem details.
8. Open the Comms page of the ODEX Administrator.
9. Select the Trading Partners node in the tree view, then click the **New** button on the Trading Partners Actions page.
10. Add the Name and Address details of the Trading Partner on the Overview page.
11. This step is optional, depending on your trading requirements. Open the EDI Codes page and add the EDI code(s) you will use for this Trading Partner, by clicking the **Add** button. Please note that at this stage you will not be able to associate the EDI code with a network.
12. Save these new Trading Partner details.
13. Select the Trading Partner Networks node in the tree view, then click the **New** button on the Trading Partners Networks Actions page and select **New AS2 Network**.
14. On the Overview page, select the new Trading Partner in the Company field, using the dropdown list.
15. Select your new AS2 subsystem in the Subsystem field, then type in the URL of the trading partner network in the URL field.
16. Type in the Name and the AS2 identifier for this trading partner network.
17. Select the appropriate Network Connection for this network, and fill in the description field if you wish to.
18. Turn to the Inbound, Outbound and MDN Receipts pages and configure the settings to the requirements of this AS2 network (these requirements will generally be those of your trading partner). Use the Help button on these pages to find out how to configure the settings.
19. Save the new Trading Partner Network details.
20. Now return to the Trading Partner you just added, in order to associate the Trading Partner with the new network.
21. Select the EDI Codes page of the Trading Partner to be edited.

22. If you previously added an EDI code for this trading partner, select the EDI Code from the list, click the **Edit** button, and select the AS2 network to be associated with this EDI code. Otherwise click the **Add** button, type in the EDI code and select the AS2 network with which this trading partner is to be associated.

23. Save the EDI Code details, then save the edited Trading Partner details.

How do I make an automatic call to a trading partner?

You can do this by using a scheduled event.

Please note that a call will be made to your trading partner even if you have no files to send.

1. Decide at what time and at what interval you want to make your call.
2. Check to see whether a schedule already exists for the required time and interval. If it does not, create a new schedule. For full details, please refer to the section entitled "Adding/Editing Schedules".
3. Now set up an event to call a specific network. Make sure you select the new schedule from the 'Event or Schedule' field.
4. Select 'Call Network' from the 'Single Action – Action' field.
5. Double-click on the Network parameter in the Edit Action dialog and then select the appropriate network. Please note that, to call all your partners, you will have to set up an event to call each network individually.

For full details of setting up event actions, please refer to the section entitled "Adding/Editing Event Actions".

How do I test a connection to a trading partner?

1. Open the Comms page of the ODEX Administrator.
2. Select the Trading Partner Networks node in the tree view, then click the **View** button on the Trading Partners Actions page.
3. Select the Trading Partner whose connection you want to test and click the **Edit** button.
4. Open the Status page and click the **Test call** button. This will initiate a call to the Trading Partner without sending him any data. However, if the Trading Partner has any data for you, he will send it.
5. Click the **Refresh** button to see the results of the call. The Files Received field will show you if any files were received from your Trading Partner during the call.

How do I automatically pick up files from a directory and schedule them?

1. Open the Workflow page of the ODEX Administrator.
2. Select the Data Sources node in the tree view, then click the **New** button on the Data Sources Actions page. Select "Directory Data Source" from the options you are offered.
3. Provide a name for this Data Source, and type in the full directory path in the Directory field.
4. Select the appropriate Filename mask using the dropdown list. You may provide a description if you wish.

5. Save the new Directory Data Source.
6. Select the Workflows node in the tree view, then click the **New** button on the Workflows Actions page.
7. Provide a name for this Workflow on the Overview page, then open the Jobs page.
8. Click the **Add** button and select "Schedule" from the list of jobs.
9. Go through the list of parameters for the Schedule job and provide the appropriate value for each one.
10. Save the new Workflow.
11. Select the Channels node in the tree view, then click the **New** button on the Channels Actions page.
12. On the Overview page, provide a name for this Channel.
13. In the Workflow field, select the Workflow you have just created.
14. In the Data Source field, select the Data Source you have just created.
15. If you want to restrict this workflow to process only certain files, you should configure a data definition to ensure that only the correct files will be scheduled. However, this will not be necessary if you place only files that are to be scheduled in the Data Source Directory.
16. In the Error workflow field, select an existing Error Workflow or create a new one. For details of how to create a new one, please refer to the FAQ entitled "How do I create an error workflow?".
17. Save the new Channel.

For further details of how the Workflows section is used, please refer to the section entitled "How to use the Workflow Manager".

How do I automatically copy received files to a directory?

1. First configure a Comms Data Source. This can be as restricted or as open as you like, according to the requirements of your system.
2. If you want to be specific about the type of files you want to receive, or about their origin or destination, configure a Data Definition accordingly.
3. Now configure a Workflow containing the "Copy" job. You may include other jobs too, but the Copy job will perform the extraction for you.
4. Ensure that you provide the appropriate parameter values for the Copy job.
5. Now configure a Channel which contains the appropriate data source, data definition and workflow.

For full details of how to configure all these items, please refer to the section entitled "How to use the Workflow Manager".

How do I create an error workflow?

1. In the Administrator, select the Workflows node in the tree view, then click the **New** button on the Workflows Actions page.
2. Provide a name for this Error Workflow on the Overview page, then open the Jobs page.

3. Click the **Add** button and select whichever jobs you want to be triggered by the error workflow. You can select any job to be included in an error workflow, but probably the most useful will be the Copy, E-mail and Run Application jobs.
4. Go through the list of parameters for each job you have selected and provide the appropriate value for each one.
5. Save the new Workflow. It can now be included as the error workflow for any "normal" workflow.

How do I add a workflow to translate received files, trap translation errors and raise e-mail alerts?

1. Open the Workflow page of the ODEX Administrator.
2. Select the Data Sources node in the tree view, then click the **New** button on the Data Sources Actions page. Select "Comms Data Source" from the options you are offered.
3. Provide a name for this Data Source.
4. Type in a filename mask if required e.g. *.cms (CMS is the file extension used by ODEX to denote any file received or sent via ODEX comms)
5. If you want to restrict this Comms Data Source to the processing of files to or from specific mailboxes, select the specific mailbox in the relevant field.
6. Save the new Data Source.
7. Select the Workflows node in the tree view, then click the **New** button on the Workflows Actions page.
8. Provide a name for this Workflow on the Overview page, then open the Jobs page.
9. Click the **Add** button and select "Translate" from the list of jobs.
10. Go through the list of parameters for the Translate job and provide the appropriate value for each one.
11. To trap translation errors, you need to edit the Return Code Actions for the Translate job. The Return Codes "ERROR" and "All other codes" are set to "Unhandled" by default. These should both be amended in order to trap any non-zero return codes from the Translate job. See steps 12 - 17 for details on how to do this.
12. Highlight the Translate job in the Jobs list on the Jobs page, then select the Return Code Actions page tab at the bottom.
13. Select the "ERROR" return code and click the **Enter** button to see the Edit Return Code dialog.
14. Select "Move to error workflow" in the Action field.
15. Select the appropriate error workflow from the Error workflow field at the bottom of the dialog.
16. Save the changes on this dialog.
17. Repeat steps 12 – 16, but this time select the "All other codes" return code in step 13.
18. To raise e-mail alerts, you need to create an error workflow that will send an e-mail when an error occurs. You have several options as to how you achieve this.

- The error workflow can be selected as the error workflow on the Overview page of the Workflow. For details of how to create an error workflow, please refer to the FAQ entitled "How do I create an error workflow?".
- You can select "Move to error workflow" as the Action to be performed when a non-zero code is returned from a job in the workflow.
- The error workflow can be selected as the error workflow for the channel(s) in which the workflow runs.

19. Save the new Workflow.

How do I add a workflow to construct and schedule files, trap construction errors and raise e-mail alerts?

1. Open the Workflow page of the ODEX Administrator.
2. Select the Data Sources node in the tree view, then click the **New** button on the Data Sources Actions page. Select the appropriate Data Source from the options you are offered.
3. Provide a name for this Data Source.
4. Type in any other details required by the Data Source you have chosen e.g. the directory and filename mask for a Directory Data Source
5. If you want to restrict a Comms Data Source to the processing of files to or from specific mailboxes, select the specific mailbox in the relevant field.
6. Save the new Data Source.
7. Select the Workflows node in the tree view, then click the **New** button on the Workflows Actions page.
8. Provide a name for this Workflow on the Overview page, then open the Jobs page.
9. Click the **Add** button and select "Construct" and "Schedule" from the list of jobs.
10. Go through the list of parameters for the Construct job and provide the appropriate value for each one.
11. To trap construction errors, you need to edit the Return Code Actions for the Construct job. The Return Codes "ERROR" and "All other codes" are set to "Unhandled" by default. These should both be amended in order to trap any non-zero return codes from the Construct job. See steps 12 - 17 for details on how to do this.
12. Highlight the Construct job in the Jobs list on the Jobs page, then select the Return Code Actions page tab at the bottom.
13. Select the "ERROR" return code and click the **Enter** button to see the Edit Return Code dialog.
14. Select "Move to error workflow" in the Action field.
15. Select the appropriate error workflow from the Error workflow field at the bottom of the dialog.
16. Save the changes on this dialog.

17. Repeat steps 12 – 16, but this time select the "All other codes" return code in step 13.
18. To raise e-mail alerts, you need to create an error workflow that will send an e-mail when an error occurs. You have several options as to how you achieve this.
    - The error workflow can be selected as the error workflow on the Overview page of the Workflow. For details of how to create an error workflow, please refer to the FAQ entitled "How do I create an error workflow?".
    - You can select "Move to error workflow" as the Action to be performed when a non-zero code is returned from a job in the workflow.
    - The error workflow can be selected as the error workflow for the channel(s) in which the workflow runs.
19. Save the new Workflow.

How do I unlock an ODEX component?

To unlock a component, select the System page of the ODEX Administrator and select the Licence Codes node in the tree view.

Now please read the section entitled "Components".

How can I fix connection problems?

You will sometimes find that your calls to and from your trading partners and clearing centres fail. Details of failures can be seen in the following places:

- All errors – in the Log section of the Communications Monitor (failures will be displayed in red, with the reason for the failure given in the Message column).
- ISDN errors – in the "Last call details" section of the Connections page of the network view (highlight the relevant connection to see its last call details)
- ESID errors – on the Status page of the network view
- SFNA errors – on the Scheduled Files view after a file has failed

To find out what the error codes mean, please refer to the sections entitled "ESID Error Codes" and "SFNA/EFNA Error Codes".

How do I integrate with SAP?

Integration with SAP is a three-part operation:

- Configure the details of your SAP system in ODEX
- Automate the import of SAP IDocs (into ODEX from SAP) and their construction into EDI files
- Automate the translation of EDI files into IDocs and their export, together with status documents, from ODEX into SAP

N.B. If you have not yet unlocked the SAP and XLATE components of ODEX you should do so now. For details of how to do this, please refer to the FAQ entitled "How do I unlock an ODEX component?".

Configure the details of your SAP system

1. Open the System page of the ODEX Administrator.

2. Select the Back Office Systems node in the tree view, then click the **New** button on the Back Office Systems Actions page. For full details of how to edit this section, please refer to the section entitled "Adding/Editing SAP Back Office Systems".
3. On the Overview page provide a name for the SAP system and a description for it if you wish.
4. On the Integration page fill in all the relevant details of your SAP system.
5. On the Advanced page provide the relevant directory details for exporting files to SAP and check whether the default values on this page are acceptable for your system, changing them if necessary. Likewise, review which status records are required by your system and uncheck any that are not required.
6. Save the details of the new Back Office System.

You have now completed the configuration of your SAP system in ODEX. The next step is to automate the import of SAP IDocs into ODEX .

Automate the import of SAP IDocs into ODEX

1. Open the Workflow page of the ODEX Administrator.
2. Select the Data Sources node in the tree view, then click the **New** button on the Data Sources Actions page. Select 'Directory Data Source' from the options you are offered.
3. Provide a name for the Data Source.
4. Type in the directory and filename mask to be used for the import of SAP IDocs to ODEX. This is the directory where ODEX will look for the IDocs.
5. Save the new Data Source.
6. Select the Data Definitions node in the tree view, then click the **New** button on the Data Definitions Actions page. Select 'Non-EDI Data Definition' from the options you are offered.
7. Provide a name for the Data Definition, select SAP IDoc as the format and provide the type of IDoc in the Type field (e.g. DELINS).
8. Save the new Data Definition.
9. If you have not yet unlocked the SAP and XLATE components of ODEX, please do so now. For details of how to do this, please refer to the FAQ entitled "How do I unlock an ODEX component?".
10. Select the Workflows node in the tree view, then click the **New** button on the Workflows Actions page.
11. Provide a name for this Workflow on the Overview page, then open the Jobs page.
12. Click the **Add** button and select "Construct" and "SAP (Associate)" from the list of jobs. Make sure that "Construct" is above "SAP (Associate)" in the list of Jobs on your return to the Jobs page.
13. Go through the list of parameters for the Construct job and provide the appropriate value for each one. To find out what each parameter is used for, highlight the parameter and read the text that appears in the grey box below it. As a minimum you must provide the In-house Definition. Other blank fields may be left blank if you wish to use the default settings.

14. Go through the list of parameters for the SAP (Associate) job and provide the appropriate value for each one. (Double-click on the SAP System parameter. On the Edit Parameter dialog that appears, select the SAP System that you entered in step 3 in the "Configure the details of your SAP system" section above.)
15. Save the new Workflow.
16. Select the Channels node in the tree view, then click the **New** button on the Channels Actions page.
17. On the Overview page, provide a name for this Channel, then select the Workflow, the Data Source and the Data Definition you have just created, using the dropdown arrow alongside the appropriate fields.
18. In the Error workflow field, select an existing Error Workflow or create a new one. For details of how to create a new one, please refer to the FAQ entitled "How do I create an error workflow?".
19. Save the new Channel.

You have now completed the automation of SAP IDoc import into ODEX. The next step is to automate the export of SAP IDocs and status documents from ODEX into SAP.

Automate the export of SAP IDocs into SAP

1. You should first configure the Workflow section to receive EDI files from your trading partners and translate them into SAP IDoc format.
2. Select the Workflows node in the tree view, then click the **New** button on the Workflows Actions page.
3. Provide a name for this Workflow on the Overview page, then open the Jobs page.
4. Click the **Add** button and select "Translate" and "SAP (Export)" from the list of jobs. Make sure that "Translate" is above "SAP (Export)" in the list of Jobs on your return to the Jobs page.
5. Go through the list of parameters for the Translate job and provide the appropriate value for each one. To find out what each parameter is used for, highlight the parameter and read the text that appears in the grey box below it. Blank fields may be left blank if you wish to use the default settings.
6. Go through the list of parameters for the SAP (Export) job and provide the appropriate value for each one. (Double-click on the SAP System parameter. On the Edit Parameter dialog that appears, select the SAP System that you entered in step 3 in the "Configure the details of your SAP system" section above.)
7. Save the new Workflow.
8. Select the Channels node in the tree view, then click the **New** button on the Channels Actions page.
9. On the Overview page, provide a name for this Channel, then select the Workflow, the Data Source and the Data Definition you have just created, using the dropdown arrow alongside the appropriate fields.
10. In the Error workflow field, select an existing Error Workflow or create a new one. For details of how to create a new one, please refer to the FAQ entitled "How do I create an error workflow?".

11. Save the new Channel.

You have now completed the automation of SAP IDoc export into SAP from ODEX.

How do I use OFTP security?

Review the section entitled “Encryption and Signatures” which explains the basic concepts of security.

You will need your own certificate, containing a private and a public key, and your trading partner's public key certificate.

1. Obtain your certificate from a Trusted Certification Authority or you will be able to create your own self-signed certificate later.
2. To define your certificate to ODEX, open the Comms page of the ODEX Administrator.
3. Select the Internal Networks node in the tree view and click the plus sign against the network you want to use security with.
4. On the internal network’s File Security page, in the Signature section, select radio button “Sign with the same certificate as for decryption”.
5. In the Decryption section, select the radio button “Decrypt with the following certificate” and click the arrow button at the side of the certificate field. The Select Certificate dialog appears. You can use this dialog to select your private key certificate or to create a new one. If you create a new one, remember to export the public key certificate to a file ready to send to your trading partner. See the section entitled “Common Dialogs - Select Certificate”.
6. Save your changes to the internal network.
7. Exchange public key certificates with your trading partner(s). See the section entitled “Certificate Management”.
8. To define your trading partner’s certificate to ODEX, select the Trading Partner or Clearing Centre Networks node in the tree view and click the plus sign against the network you want to use security on.
9. On the external network’s Security page, in the External Network Security section, select radio button “The following certificate will be used for encryption and verification” and click the arrow button at the side of the certificate field. The Select Certificate dialog appears. You can use this dialog to select or import your trading partner’s public key certificate. See the section entitled “Common Dialogs - Select Certificate”.
10. In the Options section, check the tick boxes “Session authentication” and “Request signed acknowledgment”.
11. Save your changes to the external network.

You have now completed the security definitions for this trading partner and when you exchange files, they will be signed and encrypted.

How do I configure ODEX to send ENGDAT folders?

Before you attempt to configure ODEX to use ENGDAT, please ensure that you have entered your ENGDAT licence code in the ODEX Administrator. You will not be able to start the ENGDAT workstation application until you have entered an ENGDAT licence code. Please refer to the section entitled 'Licence Codes' for more information on how to enter a licence code for the ENGDAT component.

You must also up your company, contact and communication details and the corresponding details of your trading partner(s). This will provide ODEX with the company and contact information that is required to generate ENGDAT folders and messages. For details of how to set up your own company details, please refer to the following sections:

Adding/Editing Internal Companies

Adding/Editing an Internal OFTP Network

For details of how to set up your trading partner's details, please refer to the following sections:

Adding/Editing Trading partners

Adding/Editing Networks

You must define an ENGDAT relationship for each trading partner with which you will exchange ENGDAT data. The ENGDAT relationship allows you to specify which version of the ENGDAT message will be used and to which OFTP mailbox the files will be transmitted. For details of how to configure an ENGDAT relationship, please refer to the section entitled 'ENGDAT Relationships'.

For detailed information on creating the ENGDAT folder, please refer to the following sections:

Outbound Folders – Actions (Create folder action)

ENGDAT Folder Editor

You can now create an ENGDAT folder.

1. Start the ENGDAT Workstation application and select the 'Outbound folders' tab.
2. Select **Actions >> Create folder,** right-click on the files list and select '**Create folder**' from the context menu, or click the '**Create folder**' button on the toolbar.
3. You will be presented with a list of ENGDAT relationships. Select a relationship and click 'Create'.
4. Use the ENGDAT Folder Editor to create and save an ENGDAT folder. The folder will be shown in the list of folders on the 'Outbound folders' tab.
5. To schedule the folder, select **Actions >> Schedule folder**

After scheduling the folder, you will notice that the folder status will change to 'Scheduled' and a value will appear in the 'Scheduled Date/Time' column. A call will now automatically be made to your trading partner, provided that your trading partner's network settings allow it and the trading partner's network is not in 'retry' mode.

If the call is made, the ENGDAT folder will commence transmission. The folder status will change to 'Partly sent' until all of the files have been sent. As the files

are being sent, the progress column will show an estimate of how much of the folder has been transmitted. You may also monitor the progress of the folder transmission using the ODEX Communications Monitor.

Once all files in the folder have been sent, the folder status will change to 'Sent'. Once acknowledgements have been received for each file in the folder, the folder status will be changed to 'Sent and Acknowledged'.

How do I configure ODEX to receive ENGDAT folders?

Before you attempt to configure ODEX to use ENGDAT, please ensure that you have entered your ENGDAT licence code. You will not be able to use the Update ENGDAT Folder workflow job until you have entered an ENGDAT licence code in the ODEX Administrator. Please refer to the section entitled 'Licence Codes' for more information on how to enter a licence code for the ENGDAT component.

You must also have your company, contact and communication details and the corresponding details of your trading partner(s) set up. This will provide ODEX with the necessary information to receive ENGDAT folders and to process inbound ENGDAT messages. For details of how to set up your own company details, please refer to the following sections:

Adding/Editing Internal Companies

Adding/Editing an Internal OFTP Network

For details of how to set up your trading partner's details, please refer to the following sections:

Adding/Editing Trading partners

Adding/Editing Networks

Once the company, contact and communication details are configured, you then need to configure an ENGDAT relationship for the trading partner. The ENGDAT relationship indicates the type of ENGDAT message that you expect to receive from your trading partner and which OFTP mailbox the ENGDAT files will be received from. Please refer to the section entitled 'ENGDAT Relationships' for further information on setting up an ENGDAT relationship.

For an overview of Data Sources, Workflow Jobs and Channels, please refer to the section entitled 'Workflows'. More detailed information on Data Sources, Workflow Jobs and Channels can be found in section entitled 'Workflow Manager'.

The following steps outline how to set up a basic workflow that will create ENGDAT folders from received ENGDAT files and extract the files to a specified location. The workflow jobs allow for many more possibilities – for example, you can decompress received ENGDAT files that are compressed and send e-mail alerts when files are received.

1. Open the Workflow page of the ODEX Administrator
2. A Comms Data Source must be used for the received ENGDAT files. Click the 'Data Sources' node in the navigation panel and add a new Comms Data Source for the received ENGDAT files. Alternatively, you may use the 'Received Files Source' that is installed with ODEX.
3. Select the 'Workflow' node in the navigation panel.
4. On the workflow actions page, select 'New' to add a new workflow.

5. On the workflow page, select the ‘Jobs’ tab.
6. Click ‘Add’ and select the ‘Update ENGDAT Folder’ job from the list of jobs.
7. The job will now be added to the workflow with the default parameters. In its current state, the job will process ENGDAT files and add them to folders, but will not do any further processing (e.g. extraction, decompression).
8. If you are going to receive ENGDAT folders that will not contain an ENGDAT message, set the ‘Process ENGDAT Message’ parameter to ‘False’.
9. Set ‘Extract’ to ‘Folder’ or ‘File’. If you select ‘Folder’, each file in the ENGDAT folder will be extracted once the entire folder has been received. If you select ‘File’, each file will be extracted one at a time as they are received.
10. You must now enter a directory and filename for the extracted files. To enter the directory and filename, double-click the ‘Extract filename’ parameter.
11. Enter a directory and filename. You must use placeholders in the directory and/or filename to ensure that each extracted file is given a unique filename. Click **Insert >> ENGDAT >> ENGDAT filename**. This will insert the ENGDAT filename (%EFN%) placeholder. This placeholder corresponds to the filename given to the ENGDAT data file in the ENGDAT message.
12. Enter a name for the workflow and save the workflow
13. Click on the ‘Channels’ node in the navigation panel.
14. Click the ‘New’ button to add a new Channel.
15. On the channel overview page, enter a name for the channel. Select the Comms Data Source and workflow from the drop-down lists.
16. Save the Channel.

Any files that you receive will now be processed as ENGDAT folders and extracted. Once the first file in an ENGDAT folder is received, you will be able to see it on the ‘Inbound folders’ tab of the ENGDAT workstation. Each individual ENGDAT file can be viewed on the ‘Inbound’ tab of the ODEX Workstation.

Appendices

Events

This section has a table for each different event, showing all criteria for that event.

Acknowledgement Received

Description – Fired when an acknowledgement has been received.

Event Criterion	Description
Mailbox	The trading partner or clearing centre mailbox for which this application event is valid, or Any.

Acknowledgement Sent

Description – Fired when an acknowledgement has been sent.

Event Criterion	Description
Mailbox	The trading partner or clearing centre mailbox for which this application event is valid, or Any.

Call Ended

Description – This event is fired when a call ends.

Event Criterion	Description
Network	The trading partner or clearing centre network node for which this application event is valid, or Any.
Call direction	The direction of the call (Incoming, Outgoing, Any)
Protocol	The protocol used for the call (AS2, FTP, OFTP, Any)
Connection Type	The type of connection used for the call (CAPI2, HTTP, TCP, X.25, Any)

Call Failed

Description – This event is fired whenever a call attempt fails.

Event Criterion	Description
Network	The trading partner or clearing centre network node for which this application event is valid, or Any.

Call Retry Limit

Description – Fired when all connections for a call have reached their retry limit

.Event Criterion	Description
Network	The trading partner or clearing centre network node for which this application event is valid, or Any.

Call Started

Description – This event is fired when a call starts.

.Event Criterion	Description
Network	The trading partner or clearing centre network node for which this application event is valid, or Any.

.Event Criterion	Description
Call direction	The direction of the call (Incoming, Outgoing, Any)
Protocol	The protocol used for the call (AS2, FTP, OFTP, Any)
Connection Type	The type of connection used for the call (CAPI2, HTTP, TCP, X.25, Any)

Connection Failed

Description – This event is fired whenever a connection reaches retry limit.

Event Criterion	Description
Network	The trading partner or clearing centre network node for which this application event is valid, or Any.

Database sweep completed

Description – Fired when the database sweep is complete.

Event Criterion	Description
None	

File Not Sent

Description – Fired when a file fails to be sent.

Event Criterion	Description
Mailbox	The trading partner or clearing centre mailbox for which this application event is valid, or Any.

File Received

Description – Fired when a file has been received.

Event Criterion	Description
Mailbox	The trading partner or clearing centre mailbox for which this application event is valid, or Any.

File Retry Limit

Description – Fired when a file reaches its retry limit.

Event Criterion	Description
Mailbox	The trading partner or clearing centre mailbox for which this application event is valid, or Any.

File Sent

Description – Fired when a file has been sent.

Event Criterion	Description
Mailbox	The trading partner or clearing centre mailbox for which this application event is valid, or Any.

General System Error

Description – Fired when an error message is logged.

Event Criterion	Description

Event Criterion	Description
Source	The source ID of the log message for which the event will be raised. Leave blank to fire the event for all errors.

Primary Connection Failed

Description – Fired when the first connection reaches retry limit.

Event Criterion	Description
Network	The trading partner or clearing centre network node for which this application event is valid, or Any.

SAP Export Failed

Description – Fired when a SAP IDoc or Status record update fails.

Event Criterion	Description
SAP System	The SAP system to which updates are to be sent, or Any

Server Started

Description – Fired when the server has started.

Event Criterion	Description
None	

Server Starting

Description – Fired when the server is starting.

Event Criterion	Description
None	

Server Stopped

Description – Fired when the server is stopped.

Event Criterion	Description
None	

Workflow File Hold

Description – Raised when the status of a workflow file changes to **Hold**.

Event Criterion	Description
None	

Workflow File EDI Reject

Description – Raised when a workflow file is rejected through an EDI functional acknowledgement.

Event Criterion	Description
None	

Unexpected Receipt Received

Description – Fired when an acknowledgement is received that cannot be matched to a file (using VFN for OFTP and Message ID for AS2).

Event Criterion	Description
Network	The trading partner or clearing centre network node for which this application event is valid, or Any.
Call direction	The direction of the call (Incoming, Outgoing, Any)
Protocol	The protocol used for the call (AS2, FTP, OFTP, Any)
Connection Type	The type of connection used for the call (CAPI2, HTTP, TCP, X.25, Any)

Unhandled Workflow Error

Description – Fired when an error occurs in the workflow manager and there is no error workflow defined against the workflow or channel.

Event Criterion	Description
None	

Actions

This section has a table for each Action that can be triggered by an event or schedule, showing the parameters that can be used for that action, whether they are mandatory or conditional (M/C) and what their default value is.

Call Network

Description – Calls a network.

Parameter	Description	M/C	Default Value
Network	Specifies the network to attempt to call.	M	None

Check Certificates

Description – checks the validity of all the digital certificates configured for use with ODEX.

Parameter	Description	M/C	Default Value
Error days to expiry	An error will be raised if any certificate is found to be this number of days from expiry or fewer	M	7
Log file	A summary of the results of the action will be written to this file	C	None

Check EDI Acknowledgements

Description – checks the EDI acknowledgement status of workflow files and flags them if the acknowledgements are now overdue.

Parameter	Description	M/C	Default Value
None			

Check Performance Counter

Description – Check the value of a performance counter against a fixed value.

Parameter	Description	M/C	Default Value
Performance counter	The full name of a performance counter that has been defined in the system settings view	M	None
Condition	The condition test to apply when comparing values (less than or greater than)	M	Less than
Value	The fixed value with which the performance counter value should be compared	M	None

The counter full name is given in the form:

```
Category.Instance.SubInstance.Counter
```

For instance, the full name:

```
Comms.Files.Sent.All.ItemsPerMinute
```

Breaks down as follows:

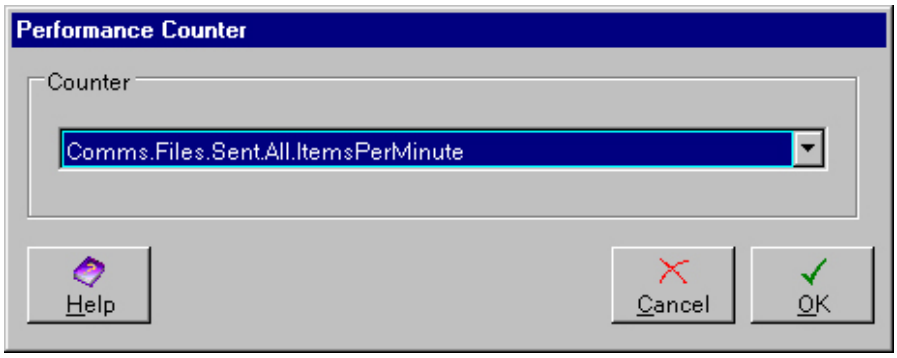
Category – 'Comms'

Instance – 'Files.Sent'

Sub-instance – 'All' (all networks)

Counter (metric) – 'ItemsPerMinute'

The dialog shown below is used to select the performance counter from a drop-down list of those defined in theSystem Settings view.



If the comparison defined in the event action evaluates to **true** then the event action will **fail**, that is, it will complete unsuccessfully. For instance, the event action is configured to check whether the number of files sent per minute is below a fixed value. If the counter value is below the fixed value then the action will fail. This can be used to trigger other event actions if a performance counter value is above or below a threshold. The steps to take are:

- Define an event action triggered by a schedule that specifies how often you want to check the counter value.
- Add an action to check the counter against a fixed value (using the default action mode, which is 'stop-on-success').
- Add a second action, using the Advanced Actions tab, to respond to a failure of the counter check. For instance, send an e-mail or SNMP trap by way of warning.

Poll Message Queue

Description – Polls a message queue and retrieves any messages that exist.

Parameter	Description	M/C	Default Value
MQ Data Source	MQ Workflow Data Source.	M	None

Poll Monitored Directory

Description – Checks a directory to see if any files have arrived.

Parameter	Description	M/C	Default Value
Directory Data Source	The directory data source you wish to poll.	M	None

Run Application

Description – Runs an external application.

Parameter	Description	M/C	Default Value
Application	The full path of the application to run.	M	None
Arguments	Any arguments that need to be passed to the application (separated by spaces).	C	None
Wait for Exit	Should we wait for the application to finish before marking the action as processed?	M	True
Timeout	Specifies the timeout interval to wait for the application to finish executing. -1 specifies 'Wait Forever' and 0 specifies 'Do Not Wait'. Any other value indicates the number of seconds to wait.	M	-1
Delay	The number of seconds to wait after the application has finished, or timed out, before marking the action as processed.	M	0
Working Directory	The working directory that the application uses.	C	None
New Window	Flag specifying whether to start the application in a new window.	M	False

Parameter	Description	M/C	Default Value
Window Style	The style of the window the application uses.	M	Hidden
Success Return Code	The application return code that indicates that it completed successfully.	C	None

Send E-mail

Description – Sends an e-mail to one or more specified addresses.

Parameter	Description	M/C	Default Value
To	The e-mail address(es) of the recipient(s).	M	None
From	The e-mail address of the sender.	C	None
Subject	The subject of the e-mail.	C	None
Body	The body of the e-mail.	C	None
Attachment	The attachment for the email.	C	None

Send SNMP Trap

Description – Send an SNMP trap to a specified IP address.

Parameter	Description	M/C	Default Value
System name	The name of the system that sends the trap (max 50 characters)	M	“ODEX Enterprise”
Destination address	The destination IP address for the trap	M	None
Event code	An event code that will be sent in the trap (max 8 characters – the last character determines the type of trap sent, where ‘I’ = appInfo, ‘W’ = appWarn, ‘E’ = appError)	M	None
Message	The message that will be sent in the trap (max 255 characters). Supports the inclusion of system placeholders in the text	M	None

Windows Application Log

Description – Write a message to the Windows application log.

Parameter	Description	M/C	Default Value
Message Text	Specifies the message to write to the log.	C	None
Message ID	Specifies the ID of the log message.	M	1

Parameter	Description	M/C	Default Value
Log Entry Type	Specifies the type of the message to write.	M	SuccessAudit
Use Local Machine	Specifies whether to write the log message to the local machine's log.	M	True
Remote Machine Name	Specifies the name of the machine to write the log message to, if not using the local machine.	C	None

Write File

Description – Write to a file details of an event.

Parameter	Description	M/C	Default Value
Filename	The full name and path of the file to be written.	M	None
Create	If the file does not exist, should we create it?	M	True
Append	If the file exists, should we append to the end of it?	M	True
Start on new line	Flag indicating whether to start writing to the file on a new line.	M	True
End on new line	Flag indicating whether to end writing to the file with a carriage return.	M	True
Text	The text to be written.	C	None

Write to Message Queue

Description – Writes the given message to an MQ message queue.

Parameter	Description	M/C	Default Value
MQ System	The MQ system you wish to write to.	M	None
Message	The message you wish to write to the MQ message queue.	M	None

Jobs

This section has a table for each Job that can be included in a Workflow, showing the parameters that can be used for that job, whether they are mandatory or conditional (M/C) and what their default value is.

Acknowledge

Description – Schedules an acknowledgement for transmission.

Parameter	Description	M/C	Default Value
EERP User Data	Specifies the acknowledgement's user data.	C	None

Parameter	Description	M/C	Default Value
Processing Successful	Specifies whether processing was successful on the file in which case a positive acknowledgement will be sent, otherwise a negative acknowledgement will be sent	M	True

Analyse

Description – Performs analysis of files to determine content.

Parameter	Description	M/C	Default Value
Validate Interchange	Indicates whether or not the originator and destination EDI codes will be validated against those profiled in the system.	M	True
Force Analysis	Indicates whether or not to force the Analyser to analyse the file even if it has already been done	M	False
Condense Messages	If true, messages of the same type will be saved as a single message with an increased count. However, some message level information, such as Document numbers, may be lost.	M	False

Call Network

Description – Calls a network.

Parameter	Description	M/C	Default Value
Network	Specifies the network to attempt to call.	M	None
Test call	Specifies whether the call attempted should be a test call. This means a communications session where no files are transferred either way.	M	False

Construct

Description – Constructs an EDI file from an in-house file.

Parameter	Description	M/C	Default Value
Index	Specifies the path of the index file.	C	Defaults to the Xlate directory below the ODEX installation directory.

Parameter	Description	M/C	Default Value
Control Blocks Directory	Specifies the directory in which the control blocks files are to be written.	C	Defaults to the Xlate directory below the ODEX installation directory.
Tables Directory	Specifies the directory in which the EDI and In-House definitions are located.	C	Defaults to the Xlate directory below the ODEX installation directory.
In-House Definition	The In-House definition name.	M	None
Keep Log File	Specifies whether to keep the log file created by Xlate.	M	True
Warn For Numerics	Specifies whether a warning should be given when a non-numeric character (such as whitespace) is found in a numeric field.	M	False
Trace	Specifies whether to enable tracing in Xlate.	M	False

Convert File Encoding

Convert File Encoding allows you to convert a file from one format into another format. This may entail changing the encoding of the file e.g. conversion from EBCDIC to ASCII, and it may entail the manipulation of records within the file e.g. addition or removal of record delimiters.

You may need to convert an incoming file from its existing format into a format that can be handled by your in-house system. Likewise you may need to convert files produced by your in-house system from their existing format into one that will be accepted by your trading partner.

There are various file conversion scenarios that can be handled by this job, a selection of which are described in the sub-section below entitled Sample Solutions.

How to use the Convert File Encoding job

First of all you need to understand the requirements of each conversion, by comparing your file formats with those of your trading partner.

Ask yourself the following questions:

- Is an encoding conversion required i.e. will the source file and target file use different encoding?
- If so, can you use a pre-defined code page or do you need to define your own map file?
- Is any file manipulation required e.g. do records have to be fixed length? Do record delimiters need to be inserted or removed?

These questions refer to the basic objectives of a conversion. Your answers determine which parameters to use.

The full list of parameters shown in the Convert File Encoding Job table is not used in every conversion. Although many parameters have default values they will be ignored if your other parameter choices dictate this. For example, if you select anything other than Unicode, BigEndianUnicode or UTF8 in the Target Encoding field, the Target Write Byte Order parameter will be ignored.

The sections below indicate which parameters relate to which functions of the Convert File Encoding Job. Each function is listed, with a description of how each related parameter is used.

A table showing each parameter with its status (mandatory or conditional) and its default value can be seen in the sub-section below entitled Convert File Encoding Summary.

Encoding conversion

If encoding conversion is required and a pre-defined code page exists that will suit your purpose, you should use the Source Encoding and Target Encoding parameters. If no pre-defined code page exists that will suit your purpose, you should use the Map File parameter.

Source Encoding

Select from the drop-down list the encoding which matches your input file. Or, if the file contains EDI data, use the <Auto Detect> option, which means the convert job will try to determine the encoding itself. Alternatively, you may type in a code page id to be used.

Target Encoding

Select from the drop-down list the encoding which matches your output file. Alternatively, you may type in a code page id to be used.

Target Write Byte Order

Set this parameter to True if you have selected Unicode, BigEndianUnicode or UTF8 in the Target Encoding field.

If you set this parameter to True, the conversion job will write a byte order mark in the first few bytes of the target file to indicate how the file is encoded (Unicode, BigEndianUnicode or UTF8).

Map File

Using this parameter requires you to have written your own map file.

Type in this field the full path and filename of the map file to be used for the conversion.

Source Bytes per Character

The value in this field will be ignored unless you have provided a value in the Map File field.

Possible values are 1 and 2.

Source Little Endian

The value in this field will be ignored unless you have provided a value in the Map File field.

This parameter indicates whether the bytes in each input file character are low order first (Little Endian) or high order first (Big Endian).

Big or Little Endian encoding is only applicable to encodings which use 2 bytes per character. On a Windows system, most applications will expect Little Endian encoding. Mainframes will expect Big Endian encoding. Unix systems may use either, depending on their operating system.

Target Bytes per Character

The value in this field will be ignored unless you have provided a value in the Map File field.

Possible values are 1 and 2.

Target Little Endian

The value in this field will be ignored unless you have provided a value in the Map File field.

This parameter indicates whether the bytes in each output file character are low order first (Little Endian) or high order first (Big Endian).

Big or Little Endian encoding is only applicable to encodings which use 2 bytes per character. On a Windows system, most applications will expect Little Endian encoding. Mainframes will expect Big Endian encoding. Unix systems may use either, depending on their operating system.

Map Direction

The value in this field will be ignored unless you have provided a value in the Map File field.

Specifies whether to map from values on the left hand side of the map file to values on the right (Standard) or from the right hand side to the left (Reverse).

File manipulation

There are three basic file types that can be manipulated, differentiated by the type of records they contain:

- Variable length records – Since the records can be any length, they are each terminated with delimiter characters so that their end can be determined by the computer.
- Fixed length records – The length of each record is the same. Therefore no delimiters are required. The file length is an exact multiple of the record length.
- Undefined records – this file type is neither of the above. There are no delimiters, nor are there record boundaries at fixed positions.

*N.B. Please note that if your trading partner requires fixed length records, the records should **not**, as a general rule, be delimited. The Convert File Encoding job takes this into account and will not allow you to set Insert Delimiter to True if Pad or Truncate is set to True.*

Therefore if, for whatever reason, you want to place a delimiter at the end of fixed length records, you will have to run the Convert File Encoding job twice – once to create the fixed length records and once to add the delimiter.

Insert Record Delimiter

Set this parameter to True if you want to insert a record delimiter character at a certain position within each record or, in exceptional cases, at the end of a fixed length record.

If you set this parameter to True, you must also specify the actual delimiter to be used and the position in which to place it, using the Record Delimiter parameter and the Record Length parameter respectively.

Although this parameter can be used to insert a delimiter at the end of a fixed length record, its purpose is mainly to create a file that is more easily readable by a human. For example, a continuous stream of data can be converted into 80-character records that can be viewed easily in a text editor.

Remove Record Delimiter

This parameter can be used alone or in conjunction with the Pad or Truncate Record parameter.

There are three values for this parameter: **No**, **All** and **Based on Record Length**.

This parameter requests the conversion job to remove delimiter characters every so many characters or to remove all occurrences.

If the parameter is set to **No**, no record delimiters will be removed.

Set this parameter to **All** if you want to remove all record delimiters from a file containing variable length records. You must also specify the actual delimiter to be removed, using the Record Delimiter parameter.

If you set this parameter to **Based on Record Length**, you must also specify the actual delimiter to be removed and the position of the delimiter, using the Record Delimiter parameter and the Record Length parameter respectively.

The latter option could be used if you have a file where, for example, a CR/LF character has been inserted every 72 characters and also at the end of each record. You may want to remove all delimiters except those at the end of each record. In this case the Record Length you provide should be 72.

Pad or Truncate Record

Set this parameter to True if you want to create a file containing fixed length records.

If this parameter is set to True, the conversion job will make all records in the target file the same length (i.e. the length you specify in the Record Length parameter).

It will pad short records to the required length with the specified padding character. It will truncate records that are longer than the required length. You should therefore take care when specifying the record length, since data could be lost if the value is less than the longest record in the file.

If this parameter is set to True, you must also specify the actual padding character to be inserted and the record length required, using the Padding Character parameter (or Padding as Numeric parameter) and the Record Length parameter respectively.

Padding Character

Use this parameter to specify the character to be used to pad short records when making fixed length records.

You must set this parameter if you have set the Pad or Truncate parameter to True. Two values are provided in the Edit Parameter dialog, but you may type in your own value if you wish. Alternatively, if you cannot type in your chosen padding character, you may set this parameter to be blank and use the Padding as Numeric parameter instead.

This parameter will only be used if the Pad or Truncate parameter is set to True, and you have supplied a value other than blank.

Padding as Numeric

Use this parameter if the padding character cannot be entered via the keyboard.

Use this parameter to enter its decimal representation instead. For example, letter A in ASCII is 65 in decimal.

This parameter will only be used if the Pad or Truncate parameter is set to True and the Padding Character parameter has been set to be blank.

Record Length

You must set this parameter if you have set the Insert or Pad parameters to True, or have set the Remove Record Delimiter parameter to “Based on record length”.

In conjunction with the Pad or Truncate Record parameter, use this parameter to specify the number of characters (not bytes) in each fixed length record.

In conjunction with the Insert or Remove Record Delimiter parameter, use this parameter to specify after every how many characters the delimiter should be inserted or removed.

This parameter will only be used if the Insert, Remove or Pad parameters are set to True.

Record Delimiter

If you want to manipulate record delimiters, use this parameter to specify the character that marks the end of each record.

Two values are provided in the Edit Parameter dialog, but you may type in your own value if you wish. Alternatively, if you cannot type in your chosen record delimiter, you may set this parameter to be blank and use the Delimiter as Numeric parameter instead.

This parameter will only be used if the Insert Record Delimiter parameter is set to True, or the Remove Record Delimiter parameter is set to All or Based on Record Length, and you have supplied a value other than blank.

Delimiter as Numeric

Use this parameter if the record delimiter character cannot be entered via the keyboard.

Use this parameter to enter its decimal representation instead. For example, the carriage return delimiter is 13 in decimal.

This parameter will only be used if the Record Delimiter parameter has been set to be blank.

Sample Solutions

This section shows, with sample scenarios, how to use the parameters to achieve the appropriate results.

Example 1

Problem

Your in-house system produces ASCII files consisting of a number of variable-length records. Each record is delimited by a CR/LF character. If you were to send such files to your trading partner he would reject them as the wrong format for his system. He wants the file in ASCII format, he wants each record to be 128 bytes long (padded with spaces) and he wants the data without delimiters i.e. in a continuous stream.

In this example, the only requirement is the manipulation of records within the file.

Solution

Source Encoding = ASCII (or <Auto Detect> if the file contains EDI data)

Target Encoding = ASCII

Remove Record Delimiter = All

Pad or Truncate Record = True

Padding Character = Space or Blank

Record Length = 128

Record Delimiter = Carriage return immediately followed by linefeed

All remaining parameters should be left with their default values so that they will be ignored.

Example 2

Problem

Your trading partner sends you files in EBCDIC format that your in-house system would reject. You need to convert the EBCDIC file into ASCII format, which your in-house system will recognise. The in-house systems of both you and your trading partner want the data in fixed length records.

In this example, the only requirement is to convert from one encoding to another.

Solution

Source Encoding = EBCDIC (or <Auto Detect> if the file contains EDI data)

Target Encoding = ASCII

All remaining parameters should be left with their default values so that they will be ignored.

Example 3

Problem

Your in-house system produces all its files in ASCII format, where each record in the file is of variable length and delimited with a CR/LF character. These files have to be converted into EBCDIC for your trading partner. In addition you have to pad each record to 128 characters with spaces before sending him the file, otherwise he will reject it for being in an incorrect format.

In this example, you would need to convert from one encoding to another and manipulate the records within the file.

Solution

Source Encoding = ASCII (or <Auto Detect> if the file contains EDI data)

Target Encoding = EBCDIC

Remove Record Delimiter = All

Pad or Truncate Record = True

Padding Character = Space or Blank

Record Length = 128

Record Delimiter = Carriage return immediately followed by linefeed

All remaining parameters should be left with their default values so that they will be ignored.

Convert File Encoding Summary

Description – Converts the encoding of a file between code pages and allows for conversion from one file format to another. It is not applicable to show whether these parameters are mandatory or conditional.

Parameter	Description	Default Value
Source Encoding	Code page name or code page ID for the input file.	Auto Detect
Target Encoding	Code page name or code page ID for the output file.	ASCII
Target Write Byte Order	In the first few bytes of the target file, write a byte order mark to indicate how the file is encoded (Unicode, BigEndianUnicode or UTF8)	False
Map File	A conversion file to be used instead of code pages to convert all the bytes of the file.	None
Source Bytes per Character	The number of bytes there are for each character in the source file.	1
Source Little Endian	Specifies if the bytes in a character are low order first (Little Endian) or high order first (Big Endian).	True
Target Bytes per Character	The number of bytes there are for each character in the target file.	1
Target Little Endian	Specifies if the bytes in a character are low order first (Little Endian) or high order first (Big Endian).	True
Map Direction	Specifies whether to map from values on the left hand side of the map file to values on the right (Standard) or from the right hand side to the left (Reverse).	Standard

Parameter	Description	Default Value
Insert Record Delimiter	Requests the conversion job to insert a character (see Record Delimiter) every so many characters.	False
Remove Record Delimiter	Requests the conversion job to remove a character (see Record Delimiter) every so many characters (see Record Length) or to remove all occurrences.	No
Pad or Truncate Record	Requests the conversion job to make all records the same length (see Record Length and Padding Character).	False
Padding Character	The character used to pad short records when making all records the same length.	Space or Blank (will be ignored if Pad or Truncate Record is False).
Padding as Numeric	If the pad character cannot be entered via the keyboard, enter its decimal representation instead. For example, letter A in ASCII is 65 in decimal.	0
Record Length	Used by INSERT/REMOVE/PAD as the number of characters (not bytes) in a record.	128
Record Delimiter	Used by INSERT/REMOVE/PAD as the character that marks the end of each record.	Carriage return immediately followed by line feed.
Delimiter as Numeric	If the record delimiter character cannot be entered via the keyboard, enter its decimal representation instead. For example, carriage return is 13 in decimal.	0

Copy

Description – Copies a workflow file to a specified directory.

Please note that, if you leave the Replace and Append parameters set to their default values (both False), the file will not be copied.

Parameter	Description	M/C	Default Value
Output Filename	Specifies the path to export the file to.	M	None
Replace	Specifies whether the output file should be overwritten if it already exists.	M	False

Parameter	Description	M/C	Default Value
Received File	In the case where a workflow file is associated with both received and sent comms files, this specifies whether to use the received or sent file details for creating the output filename.	M	True
Create Directory	Specifies whether to create the necessary directory if it doesn't exist	M	False
Append	Specifies whether data should be appended to the output file if it already exists	M	False

Copy (with Xml)

Description – Copies a workflow file along with a Data Interchange standard XML file.

Please note that, if you leave the Replace and Append parameters set to their default values (both False), the file will not be copied.

Parameter	Description	M/C	Default Value
Output Filename	Specifies the path to export the file to.	M	None
XML Output Filename	Specifies the path to use for the xml file. If this is not set, it will use the Output filename and add the extension '.xml'	C	None
Replace	Specifies whether the output file should be overwritten if it already exists.	M	False
Received File	In the case where a workflow file is associated with both received and sent comms files, this specifies whether to use the received or sent file details for creating the output filename.	M	True
Create Directory	Specifies whether to create the necessary directory if it doesn't exist	M	False

E-mail

Description – Sends an e-mail to one or more specified addresses.

Parameter	Description	M/C	Default Value
To	The e-mail address(es) of the recipient(s).	M	None
From	The e-mail address of the sender.	C	None
Subject	The subject of the e-mail.	C	None

Parameter	Description	M/C	Default Value
Body	The body of the e-mail.	C	None
Attachment	The attachment for the email.	C	None

Extract Data

Description – Extracts and saves data from a file.

Parameter	Description	M/C	Default Value
Retain from	The starting byte position from which data will be extracted (use 1 to extract from the start of the file.	M	1
Retain to	The end byte position up to which data will be extracted (use zero to extract to the end of the file)	M	0

Insert Data

Description – Inserts data from one file into another.

Parameter	Description	M/C	Default Value
Insert at	The byte position at which data will be inserted (use 1 for the start of the file and 0 for the end of the file)	M	0
Insert from	The full path of the file containing the data to be inserted	M	None

Map

Description – Maps a file from one format to another using the Xe mapping engine.

Parameter	Description	M/C	Default Value
In-House Definition	The In-House definition name.	C	None
Data Type	Specifies the data type of the file that will be passed to Xe.	M	Auto Please see notes below this table.
Index	Specifies the path of the index file.	C	Defaults to the Xe directory below the ODEX installation directory.

Parameter	Description	M/C	Default Value
Definitions Directory	The directory of the definition files which Xe will use.	C	Defaults to the Xe directory below the ODEX installation directory.
Keep Log File	Specifies whether to keep the log file created by Xe.	M	True
Log Trace	Specifies whether to enable tracing in Xe log.	M	False
Log EDF	Specifies whether to log the contents of the EDF.	M	False
Log HDF	Specifies whether to log the contents of the HDF.	M	False
Log Index	Specifies whether to log the contents of the Index.	M	False
Log Tables	Specifies whether to log the tables Xe uses to map.	M	False
Log Configuration	Specifies whether to log the Xe mapping configuration.	M	False
Log Xml Schema	Specifies whether to log the Xml schema (if necessary).	M	False
Log Data	Specifies whether to log all the data of a file, e.g. Segment records for EDI files.	M	False
Log Maps	Specifies whether to log each map.	M	False
Log Deep	Specifies whether to log everything at a very low level. This should only be used if there is an error mapping files.	M	False
Stop on error	Specifies whether Xe should stop if a recoverable error occurs during mapping.	M	False
Stop on warning	Specifies whether Xe should stop if a warning occurs during mapping.	M	False
Error config file	Specifies the path of the error configuration file.	C	None
Cache maps	Specifies whether Xe should cache the maps it performs for this file.	M	True

Parameter	Description	M/C	Default Value
Timeout	The maximum time (in seconds) allowed for the map job to complete. After this time the job will be aborted. Use a value of 0 to indicate that no maxiumum time is set.	C	60
Validate content	Indicates whether Xe should validate the content of source and target messages.	C	True
Validate ICR	Indicates whether Xe should attempt to validate interchange control references of source EDI interchanges using streams defined in its index file.	C	False
Instance	ODEX can use up to 10 instances of XE at the time. Specify an instance number (0-9) if you want to allocate this map job to a specific instance	M	0
Instance priority	Changes the priority of the instance of XE used to run this map job. Specify '2' for normal priority, '3' for below normal and '1' for above normal	M	2
Save errors	Indicates whether validation errors that occur in a map should be saved (i) for display in the audit line details dialogs of the workstation, and (ii) so they can be addressed using the %JERR% workflow placeholder	M	Yes

Data Type explanation

If the Data Type default value of Auto is used, the Xe mapping engine will try to detect the type of file automatically, by carrying out the following checks in the following order:

- Checks for known EDI service segments
- Checks for XML
- Checks for an IDoc header record

If the syntax has not been detected by now, and a HSE-ID was specified, the Xe mapping engine will assume the file is flat or CSV. Otherwise, the syntax is unknown and the job will fail.

Notes

The Xe map job returns one of the following codes:

OK – The map completed successfully and an output file was produced.

ERROR – The map failed (the Xe job log should be consulted for more details).

TIMEOUT – The job was not completed before the maximum time allowed and was aborted.

OK-MULTI – The map completed successfully and more than one output file was produced. In this case, a new child workflow file will be produced in respect of each file produced by Xe. The default return code actions are STOP, against the main (parent) workflow file, and CONTINUE against the child files.

NO-DATA – Xe finished processing without error, but no output file was produced. This is most likely to happen when an Xe map is ended using the XE.Exit function with a code indicating that the map is to be skipped.

Print Report

Description – Send a report file created in the Xe mapper to a printer.

Parameter	Description	M/C	Default Value
Printer name	Select the printer to which the report will be rendered	M	None
Paper tray	Specify the source paper tray on the selected printer	M	Automatic

Process AUTACK

Description – Processes received AUTACK messages (responses and detached signatures).

Parameter	Description	M/C	Default Value
Verification certificate	The default certificate used to verify a signature. If not specified then ODEX will try to find the certificate specified in the received EDI data. Can be overridden by a certificate specified against the sender EDI code	C	None
Install certificate	Specifies whether to install certificates received in EDIFACT packages	M	False
Create response	Specifies whether to create an AUTACK response if requested	M	True
Sign response	Specifies at what level the automatically created AUTACK response should be signed (none, interchange or message)	M	None
Signing certificate	The signing certificate to use (for signing AUTACK response)	C	None

Parameter	Description	M/C	Default Value
Signing specification	The signing specification – EANCOM or AECOC (for signing AUTACK response)	M	EANCOM
Hash algorithm	The hash algorithm to use – SHA1 or RIPEMD160 (for signing AUTACK response)	M	SHA1
Padding mechanism	The padding mechanism to use – ISO 97962 or PKCS1 Signature (for signing AUTACK response)	M	ISO 97962
Filter mechanism	The filter mechanism to use – EDA or EDC (for signing AUTACK response)	M	EDC

Return codes

The Process AUTACK job returns one of these codes:

- OK – a detached signature AUTACK was processed successfully.
- OK-AUTACK - a detached signature AUTACK was processed successfully. A response AUTACK was produced in a child workflow file.
- INVALID - a detached signature AUTACK was processed and the signature found to be invalid.
- INVALID-AUTACK - a detached signature AUTACK was processed and the signature found to be invalid. A response AUTACK was produced in a child workflow file.
- RESPONSE-OK – a response AUTACK indicating a valid signature was processed successfully.
- RESPONSE-NEGATIVE – a response AUTACK indicating an invalid signature was processed successfully.
- RESPONSE-INVALID – an invalid response ATUACK was received.
- ERROR – there was an error processing the received AUTACK.

Reformat

Description – Reformat an EDI file.

Parameter	Description	M/C	Default Value
Format	Specifies the format of the reformatted output EDI file.	M	A2 Please see notes below this table.
Record Size	Specifies the record size of the reformatted output EDI file.	M	72

Parameter	Description	M/C	Default Value
Fill Character	Specifies the fill character to pad records in the reformatted output EDI file.	C	Space Will be ignored if Format is not 'F'.
Keep Log File	Specifies whether to keep the log file created by Xlate.	M	True

Format

The following formats are available:

- **A1** – ASCII, format 1. Segments are terminated by C/R L/F to make the file more readable when displayed on a screen.
- **A2** – ASCII, format 2. As A1 above, but in addition C/R L/F are inserted every 'record size' bytes to make it possible to edit the file with a text editor that displays, for example, only the first 72 characters of a line.
- **A3** – ASCII, format 3. C/R L/F are inserted every 'record size' bytes to make the file compatible with COBOL programs that require 'line sequential' input. However, no account of segments is taken.
- **F** – Fixed length records of 'record size' bytes are written padded with 'fill character' where necessary. New messages are begun on 'record size' boundaries.

U – Unstructured, there is no record format. The file is written as a string of bytes. C/R L/F and leading spaces are dropped if the input file is ASCII format.

Run Application

Description – Runs a specified external application.

Parameter	Description	M/C	Default Value
Application	Specifies the name of the application to run.	M	None
Arguments	Specifies any arguments needed by the application.	C	None
Wait for Exit	Specifies whether to wait for the application to exit, before continuing processing. If this is false, the return code from the application cannot be checked and any problems will be ignored.	M	True
Timeout	Specifies the timeout interval to wait for the application to finish executing. -1 specifies 'Wait Forever' and 0 specifies 'Do Not Wait'. Any other value indicates the number of seconds to wait.	M	-1

Parameter	Description	M/C	Default Value
Delay	Specifies the time to wait (in seconds) after the application has completed.	M	0
Synchronised	Synchronous processing ensures that while a file is being processed by an external application, ODEX will not allow another file to enter this job.	M	False
Output Filename	Specifies the name of the file created by the application.	C	None
Output Filemask	Specifies the filemask to use for the file.	C	None
Copy or Move	Specifies whether the files should be copied or moved after the application has executed.	M	Copy
Use Application Return Code	Specifies whether this should return the application's return code.	M	True
Priority	Specifies the priority of the thread that the application runs in.	M	3 N.B. The lower the number, the higher the priority.
Working Directory	Specifies the working directory of the application.	C	None
New Window	Specifies whether the application should be run in a new window.	M	False
Window Style	Specifies the state of the window the application is run in.	M	Hidden
Received	When a workflow file is associated with both received and sent comms files, this specifies which file details to use for creating the output filemask.	M	True

SAP (Associate)

Description – Associates the file with the SAP monitor. This causes status records to be exported to SAP as the file is constructed and transmitted.

Parameter	Description	M/C	Default Value
SAP System	The SAP System that ODEX will send status records to as the file goes through the system.	M	None

Parameter	Description	M/C	Default Value
SR – analysis	If set to true, ODEX will create a status record to send to SAP, after the file has been analysed.	M	True
SR – construction	If set to true, ODEX will create a status record to send to SAP, after the file has been mapped or constructed.	M	True
SR – scheduling	If set to true, ODEX will create a status record to send to SAP, after the file has been scheduled to a trading partner.	M	True
SR – association	If set to true, ODEX will create a status record to send to SAP, after the file has been associated with a SAP system.	M	True
SR – retransmission	If set to true, ODEX will create a status record to send to SAP, after the file has been sent to a trading partner, after at least one failed attempt.	M	True
SR – acknowledgement	If set to true, ODEX will create a status record to send to SAP, after the file has been acknowledged by a trading partner.	M	True
SR – transmission	If set to true, ODEX will create a status record to send to SAP, after the file has been sent to a trading partner.	M	True

SAP (Export)

Description – Queues an IDoc file to be exported to SAP.

Parameter	Description	M/C	Default Value
SAP System	The SAP System that ODEX will export the IDoc to.	M	None

Schedule

Description – Schedules a file for transmission.

Parameter	Description	M/C	Default Value

Parameter	Description	M/C	Default Value
Sender Mailbox	Specifies the sender mailbox from which the file will be scheduled. You may select 'Auto detect' to determine the sender mailbox based on EDI codes in the file. Select 'Use local codes' to specify the mailbox by local code. When this option is selected, you must provide a value for the 'Sender local code' parameter.	M	Auto detected
Receiver Mailbox	Specifies the receiver mailbox to which the file will be scheduled. You may select 'Auto detect' to determine the receiver mailbox based on EDI codes in the file. Select 'Use local codes' to specify the mailbox by local code. When this option is selected, you must provide a value for the 'Receiver local code' parameter.	M	Auto detected
Priority	Specifies the priority to use when scheduling the file.	M	5 N.B. The lower the number, the higher the priority.
Earliest Date/Time	Specifies the earliest time to send the file.	M	Current system time
SFID User Data	Specifies the SFID user data.	C	None
File Type	Specifies the file type.	M	Unformatted
VFN	Specifies the VFN of the file.	C	The original filename of the workflow file.
Description	The description is only used when scheduling a file to a trading partner using a version of OFTP 2 or higher. The description consists of up to 999 characters that are passed with the file identification and may be used for whatever purpose you and the destination agree. If you are in any doubt as to a value to specify, leave this empty.	C	None

Parameter	Description	M/C	Default Value
Validate VFN	If set to false, ODEX will not check that the VFN consists only of valid OFTP characters. Valid chars are: 0 to 9, A to Z, and &() -/.	M	True
Record Length	Specifies the length of records in the file.	M	0 N.B. Should be set to 0 unless records are fixed length.
Pad Fixed	Specifies whether to pad the file to make it the correct size.	M	False
Use Routing Table	Specifies that the routing table will be used to determine the destination and originator mailboxes for the scheduled file. If the 'Use received comms file' parameter is set to true, the routing table will be searched for an entry with source file criteria that matches the received file. If the 'Use received comms file' parameter is set to false, the search will be done using the scheduled file. If a matching routing table entry is found, the destination and originator mailboxes of the scheduled file will be set to the target destination and originator mailboxes of the routing table entry, otherwise the file will be scheduled as normal.	C	False
Use Received File Placeholders	When set to true, placeholder values will be populated with data taken from a received file associated with the workflow file. If set to false, the placeholders will be populated using details of the scheduled file.	C	False
Use Received Comms File	Used when a file is received and the destination mailbox is defined on an external network (the file is being forwarded). This specifies that the destination and originating mailboxes used to schedule the file will be taken from the received file.	C	False

Parameter	Description	M/C	Default Value
Use Mailbox Settings	When set to true, the encoding settings on the receiver mailbox will be used to automatically convert the file encoding, if the receiver mailbox specifies a target encoding or map file. The OFTP file format settings will also be taken from the receiver mailbox. When set to false, the file encoding will not be converted and the OFTP file format will be set to the value in the File Type parameter.	C	True
Expect Functional Acknowledgement	When true and also configured against the receiver EDI code, EDI functional acknowledgements will be expected for the file. The acknowledgement status of the file can be monitored and updated when acknowledgements are received and processed.	C	False
Sender Local Code	If you specify 'Use local codes' for the sender mailbox parameter, you must specify the local code of the sender mailbox. Enter the local code of the sender mailbox from which the file will be scheduled.	C	None
Receiver Local Code	If you specify 'Use local codes' for the receiver mailbox parameter, you must specify the local code of the receiver mailbox. Enter the local code of the receiver mailbox to which the file will be scheduled.	C	None

Schedule ENGDAT file

Description – Schedules an ENGDAT file according to the relationship its ENGDAT folder was created under.

Sign EDI

Description – Applies digital signatures to EDI interchanges and messages.

Parameter	Description	M/C	Default Value

Parameter	Description	M/C	Default Value
Signing certificate	Specifies the default certificate to use for signing. Can be overridden by a certificate specified against the sender EDI code	C	None
Sign on client	Whether to hold the workflow file for signing on the client (ODEX Workstation)	M	False
Sequence on release	When signing on the client, specify whether to release held files in the order they were submitted to the workflow manager	M	True
Sign non-V4	Specifies whether EDI data with syntax versions below 4 can be signed	M	False
Signing method	Specifies the signing method – attached or detached	M	Attached
Sign detached	Specifies whether to sign the detached signature AUTACK	M	False
Detached file	Specifies whether to create a new file for the detached signature AUTACK	M	True
Signing level	Specifies the signing level – message or interchange	M	Message
Signing specification	The signing specification – EANCOM or AECOC	M	EANCOM
Request response	Specifies whether to request an AUTACK response from the recipient	M	False
Package certificate	Specifies whether to include the signing certificate (public key) in an EDIFACT package sent with the data	M	False
Hash algorithm	The hash algorithm to use – SHA1 or RIPEMD160	M	SHA1
Padding mechanism	The padding mechanism to use – ISO 97962 or PKCS1 Signature	M	ISO 97962
Filter mechanism	The filter mechanism to use – EDA or EDC	M	EDC

Return codes

The Sign EDI job returns one of these codes:

- OK – the file was signed successfully.
- OK-AUTACK – the file was signed successfully and a detached signature AUTACK was processed in a child file.
- ERROR – there was an error processing the file.

Split

Description – Splits files into separate interchanges.

This Job has no parameters.

Translate

Description – Translates an EDI message into an in-house file format.

Parameter	Description	M/C	Default Value
Index	Specifies the path of the index file.	C	Defaults to the Xlate directory below the ODEX installation directory.
Control Blocks Directory	Specifies the directory in which the control blocks files are to be written.	C	Defaults to the Xlate directory below the ODEX installation directory.
Tables Directory	Specifies the directory in which the EDI and In-House definitions are located.	C	Defaults to the Xlate directory below the ODEX installation directory.
In-House Definition	The In-House definition name.	C	None
Keep Log File	Specifies whether to keep the log file created by Xlate.	M	True
Warn For Numerics	Specifies whether a warning should be given when a non-numeric character (such as whitespace) is found in a numeric field.	M	False
Trace	Specifies whether to enable tracing in Xlate.	M	False

Update ENGDAT Folder

Description – Processes inbound ENGDAT files. Files can be added to a new or existing ENGDAT folder.

Parameter	Description	M/C	Default Value

Parameter	Description	M/C	Default Value
Match with VFN	When set to true, all files that have a VFN starting with 'ENG' and ending with 6 digits will be treated as ENGDAT files. When set to false, the first three characters of the VFN will be ignored when determining if a file is an ENGDAT file. In both cases the VFN must be 26 characters in length and end with 6 digits for the file to be treated as an ENGDAT file.	C	True
Process ENGDAT message	When this parameter is set to true, the first file in a received ENGDAT folder will be treated as an ENGDAT message. You will then be able to view the message contents in the ENGDAT workstation. Set this parameter to false if you are receiving ENGDAT folders that do not contain ENGDAT messages	C	True
Extract	When set to 'No', files will not automatically be extracted. When set to 'Folder', files will be automatically extracted once the entire ENGDAT folder has been received. When set to 'File', each file will be extracted immediately after receipt of the file	C	No
Extract file name	The directory and filename to which the files will be extracted	C	
Create directory	Specifies whether to create the extract directory if it does not exist	C	True
Extract ENGDAT message	When 'Extract' is set to true and this parameter is set to true, the ENGDAT message file will be extracted along with the other files in the folder. When set to false, the ENGDAT message file will not be extracted	C	False
Decompress zip archive	When set to 'True' ODEX will extract received zip archive files to the extract directory. When set to 'False' ODEX will not attempt to extract files from zip archives	C	False

Parameter	Description	M/C	Default Value
Zip archive filename	When decompressing inbound files, if you wish to copy the zip file, specify a directory and filename for the zip file. Leave this parameter blank if you do not wish to keep a copy of the zip file	C	

Notes

The Update ENGDAT folder job returns one of the following codes:

OK – New folder – The file is the first file in an ENGDAT folder. This means a new folder has been created for the file and the file has been successfully added to the folder.

OK – Folder file – The file is an ENGDAT folder file that has successfully been added to an existing ENGDAT folder.

OK – Folder complete – The file is the last file in an ENGDAT folder to be received. The file has successfully been added to the folder and the folder has now been fully received.

OK – Not folder file – The file is not an ENGDAT file and the file has therefore been ignored. This will occur for any file where the VFN does not indicate that the file is an ENGDAT file.

For ENGDAT folders that contain only a single file, the 'OK – Folder complete' code will be returned once the file is received and processed.

Verify Signed EDI

Description – Verifies digital signatures on EDI interchanges and messages.

Parameter	Description	M/C	Default Value
Verification certificate	The default certificate used to verify a signature. If not specified then ODEX will try to find the certificate specified in the received EDI data. Can be overridden by a certificate specified against the sender EDI code	C	None
Signing method	Attached or detached	M	Attached
Remove security	Strip security service segments from attached security messages	M	False
Install certificate	Specifies whether to install certificates received in EDIFACT packages	M	False

Parameter	Description	M/C	Default Value
Create response	Specifies whether to create an AUTACK response if requested	M	True
Sign response	Specifies at what level the automatically created AUTACK response should be signed (none, interchange or message)	M	None
Signing certificate	The signing certificate to use (for signing AUTACK response)	C	None
Signing specification	The signing specification – EANCOM or AECOC (for signing AUTACK response)	M	EANCOM
Hash algorithm	The hash algorithm to use – SHA1 or RIPEMD160 (for signing AUTACK response)	M	SHA1
Padding mechanism	The padding mechanism to use – ISO 97962 or PKCS1 Signature (for signing AUTACK response)	M	ISO 97962
Filter mechanism	The filter mechanism to use – EDA or EDC (for signing AUTACK response)	M	EDC

Return codes

The Verify Signed EDI job returns one of these codes:

- OK – a signed file was verified successfully.
- OK-AUTACK - a signed file was verified successfully. A response AUTACK was produced in a child workflow file.
- INVALID – a signature was found to be invalid.
- INVALID-AUTACK - a signature was found to be invalid. A response AUTACK was produced in a child workflow file.
- NO-SIGNATURE – an attached signature was expected but not was present.
- ERROR – there was an error verifying the received file.

Wait for Acknowledgement

Description – Pauses execution until the file has been acknowledged.

Parameter	Description	M/C	Default Value

Parameter	Description	M/C	Default Value
Acknowledged Timeout	Specifies the timeout interval (mins) to wait for a sent files acknowledgement to be received. -1 specifies 'Wait Forever' and 0 specifies 'Do Not Wait'.	M	1

Wait for Transmission

Description – Wait for communications event on a file.

Parameter	Description	M/C	Default Value
Sent Timeout	Specifies the timeout interval (mins) to wait for the scheduled file(s) to be sent. -1 specifies 'Wait Forever' and 0 specifies 'Do Not Wait'.	M	1

Windows Application Log

Description – Write a message to the Windows application log.

Parameter	Description	M/C	Default Value
Message Text	Specifies the message to write to the log.	C	None
Message ID	Specifies the ID of the log message.	M	1
Log Entry Type	Specifies the type of the message to write.	M	SuccessAudit
Use Local Machine	Specifies whether to write the log message to the local machine's log.	M	True
Remote Machine Name	Specifies the name of the machine to write the log message to, if not using the local machine	C	None
Received	When a workflow file is associated with both received and sent comms files, this specifies which file details to use for the placeholders in the log message.	M	True

Write To File

Description – Write to a file details of an event.

Parameter	Description	M/C	Default Value
Filename	The full name and path of the file to be written.	M	None
Create	Create the file if it does not exist.	M	True
Append	Append to the file if it already exists.	M	True

Parameter	Description	M/C	Default Value
Start on new line	Start on a new line by adding a CRLF before appending the new text.	M	True
End on new line	End on a new line by adding a CRLF after writing the new text.	M	True
Text	The text to be written.	C	None
Received	When a workflow file is associated with both received and sent comms files, this specifies which file details to use for placeholder replacement in the filename and text.	M	True
Copy to Job Log	As well as writing to the file, copy the new event details to the Job Log. 'Record Audit Trail' on the Channel must be ticked.	M	True

Write to MQ Message Queue

Description – Writes a message and/or file to an MQ message queue.

Parameter	Description	M/C	Default Value
MQSystem	The MQ queue you wish to write to.	M	None
Message	The message you wish to write.	C	None
Received	Specifies whether to use inbound files.	M	False
IncludeFile	Include workflow file in message	M	False

Condition Parameters

Some workflow jobs have a parameter called 'Condition' that allows you to control whether or not they are carried out. The condition parameter consists of an expression that can be used to test the value of one or more placeholders. If the expression evaluates to TRUE then the job is performed. If it evaluates to FALSE then the job is skipped.

The basic form of the conditional expression is:

[placeholder] [operator] [value]

For instance, to test that the workflow file's user data has the value "MAP02", the following conditional expression is used:

%FUD% == "MAP02"

The supported comparison operators are:

==	Equal
!=	Not equal
>	Greater than
<	Less than

>=	Greater or equal
<=	Less or equal

If both values (the value in the expression and the value represented by the placeholder) are numeric the a numeric comparison is carried out. For instance the values “33.0” and “33” are considered equal. Otherwise a string comparison is carried out.

More complex expressions can be built by using the Boolean AND (&&) or OR (||) operators and parentheses to combine expressions. For example:

(%FUD% == “MAP02”) || (%FUD% == “MAP04”)

In which case the job will be performed only if the placeholder has one of the two values specified.

These factors should be borne in mind when writing condition tests:

- If a placeholder cannot be evaluated at the time the condition test is carried out (that is, just before the workflow job is to be performed) then the test will fail and the job will be skipped.
- Parentheses are not required, but are helpful in determining the order of precedence (the order in which each part of the expression is evaluated). If parentheses are not used, the expression is evaluated from left to right.
- Quotes are not always required around the values to be tested. Quotes are required if the value contains any whitespace or any of these characters:

  < > = ! % & | “ ( )
- Be careful to use the equality operator ‘==’ rather than ‘=’, which will result in an error.

Placeholders

This section has a table for each different class of placeholder, showing the placeholder name and a brief description of the information provided by each placeholder.

Communication File Placeholders

In this table, references to Trading Partner should be understood to refer to the communications computer used by the trading partner. References to Trading Partner should be understood to refer equally to Clearing Centres.

Please note that both received and sent communications files are referred to by communication file placeholders. We therefore refer to receiver and sender instead of you and your trading partner, since either of you can be the receiver or the sender.

Placeholder Name	Placeholder Marker	Description
Acknowledged Date/Time	%ADT_dtformat%	The date and time at which the file was acknowledged (with an EERP for an OFTP file, or an MDN for an AS2 file).

Placeholder Name	Placeholder Marker	Description
Acknowledged Session ID	%ASI%	The ID of the communications session in which the acknowledgement was received.
AS2 Message ID	%MSG_ID%	The unique message ID allocated to an AS2 file by ODEX.
File Size	%CFSIZE%	The size of the file in bytes.
File Status	%CFS%	The file status as displayed on the appropriate Workstation View.
OFTP File Format	%FFMT%	The format of the file e.g. Unformatted
OFTP Record Count	%RECCOUNT%	The number of records contained in the file (for fixed format files only).
Received Date/Time	%RDT_ dtformat %	The date and time at which the file was received (incoming files only).
Receiver AS2 Identifier	%AS2_FROM%	The AS2 identifier of the file receiver. If you received the file, the AS2 Identifier is as specified on the Internal Network Overview page. If your trading partner received the file, the AS2 Identifier is as specified on the Trading Partner Network Overview page.
Receiver Mailbox Local Code	%RML%	The Local Code associated with the mailbox that received the file.
Receiver Mailbox Name	%RMC%	The name of the mailbox that received the file.
Receiver Network Local Code	%RNL%	The Local Code associated with the network that received the file.
Receiver Network Name	%RNC%	The name of the network that received the file.
Receiver SFID	%RSFID%	The SFID of the mailbox that received the file.
Receiver SFID User Data	%RSFID_UD%	The SFID User Data of the mailbox that received the file.
Receiver SSID	%RSSID%	The SSID of the network that received the file.

Placeholder Name	Placeholder Marker	Description
Receiver SSID User Data	%RSSID_UD%	The SSID User Data of the network that received the file.
Remote Filename	%RFN%	Only valid for files received from an FTP source, this is the filename without extension of the file put into an incoming FTP server directory or retrieved by the FTP client.
Remote Filename Extension	%RFN_E%	Only valid for files received from an FTP source, this is the filename extension, including dot, of the file put into an incoming FTP server directory or retrieved by the FTP client.
Remote Filename Extension No Dot	%RFN_EX%	Only valid for files received from an FTP source, this is the filename extension, excluding dot, of the file put into an incoming FTP server directory or retrieved by the FTP client.
Remote Filename With Extension	%RFN_W_E%	Only valid for files received from an FTP source, this is the full filename, including extension, of the file put into an incoming FTP server directory or retrieved by the FTP client.
Remote Filepath	%RFP%	Only valid for files received from an FTP source, this is the full filepath, excluding filename, of the file put into an incoming FTP server directory or retrieved by the FTP client.
Remote Full Filepath	%RFP_F%	Only valid for files received from an FTP source, this is the full filepath, including filename, of the file put into an incoming FTP server directory or retrieved by the FTP client.
Scheduled Date/Time	%SDT_dtformat%	The Date and Time at which the file was scheduled (outgoing files only).

Placeholder Name	Placeholder Marker	Description
Sender AS2 Identifier	%AS2_TO%	The AS2 identifier of the file sender. If you sent the file, the AS2 Identifier is as specified on the Internal Network Overview page. If your trading partner sent the file, the AS2 Identifier is as specified on the Trading Partner Network Overview page.
Sender Mailbox Local Code	%SML%	The Local Code associated with the mailbox that sent the file.
Sender Mailbox Name	%SMC%	The Mailbox name of the file sender. If you sent the file, the Sender Mailbox Name is as specified on the Mailboxes page of the Internal Network. If your trading partner sent the file, the Sender Mailbox Name is as specified on the Mailboxes page of the Trading Partner Network.
Sender Network Local Code	%SNL%	The Local Code associated with the network that sent the file.
Sender Network Name	%SNC%	The Network name of the file sender. If you sent the file, the Sender Network Name is as specified on the Overview page of the Internal Network. If your trading partner sent the file, the Sender Network Name is as specified on the Overview page of the Trading Partner Network.
Sender SFID	%SSFID%	The SFID of the file sender. If you sent the file, the SFID is as specified on the Overview page of the Internal Network. If your trading partner sent the file, the SFID is as specified on the Overview page of the Trading Partner Network.

Placeholder Name	Placeholder Marker	Description
Sender SFID User Data	%SSFID_UD%	The SFID User Data of the file sender. If you sent the file, the SFID User Data is as specified on the Mailbox dialog of the Internal Network. If your trading partner sent the file, the SFID User Data is as specified on the Mailbox dialog of the Trading Partner Network.
Sender SSID	%SSSID%	The SSID of the file sender. If you sent the file, the SSID is as specified on the Overview page of the Internal Network. If your trading partner sent the file, the SSID is as specified on the Overview page of the Trading Partner Network.
Sender SSID User Data	%SSSID_UD%	The SSID User Data of the file sender. If you sent the file, the SSID User Data is as specified on the Overview page of the Internal Network. If your trading partner sent the file, the SSID User Data is as specified on the Overview page of the Trading Partner Network.
Sent or Received Session ID	%TSI%	The ID of the communications session in which the file was sent or received.
Transmission Date/Time	%TDT_dtformat%	The Date and Time at which the file is actually sent (outgoing files only).
VFN	%VFN%	The Virtual Filename of the file. This is the name given to the file when it is scheduled.
Virtual Date	%VDATE%	The Virtual Date of the file. This is the date when the file is scheduled.
Virtual Time	%VTIME%	The Virtual Time of the file. This is the time at which the file is scheduled.

Communications Details Placeholders

In this table, references to Trading Partner should be understood to refer to the communications computer used by the trading partner. References to Trading Partner should be understood to refer equally to Clearing Centres.

Placeholder Name	Placeholder Marker	Description
Address	%NCADD%	The address or hostname of your Trading Partner Network, as specified on the Connections Overview page.
Connection Result	%NCR%	Text indicating the result of the attempted connection e.g. “Successful connection”.
Connection Type	%NCT%	The type of connection e.g. TCP/IP. This will equate to a subsystem type.
IP Address	%IPAD%	Only applicable to TCP/IP connections. The IP address of your Trading Partner Network, as specified on the Connections Overview page.
Local ISDN Number	%LOC_ISDN%	Only applicable to CAPI communications. This is your ISDN Number, as specified on the Subsystem – Advanced page.
Network Last Error	%NLE%	If applicable, indicates the last error that occurred while trying to connect to this network.
Number of Attempts	%ATTEMPTS%	Indicates how many times ODEX has tried to connect to this network.
Port Number	%PORT%	The Port Number used by this Trading Partner Network, as specified on the Connections Overview page.

Placeholder Name	Placeholder Marker	Description
Remote ISDN Number	%REM_ISDN%	Only applicable to CAPI communications. This is the ISDN Number of your Trading Partner Network, as specified on the Trading Partner Network Overview page.
SSID	%SSID%	The SSID of your Trading Partner Network, as specified on the Trading Partner Network Overview page.
SSID User Data	%SSID_UD%	The SSID User Data used for this Trading Partner Network, as specified on the Advanced (OFTP) page of the Trading Partner Network.
Subsystem Name	%SUBSYS%	The subsystem used to connect to this Trading Partner Network.
Trading Partner Network Connection Name	%NCC%	The name you have given to the Trading Partner Network Connection, as specified on the Trading Partner Network Connection Overview page.
Trading Partner Network Name	%NWC%	The name you have given to the Trading Partner Network, as specified on the Trading Partner Network Overview page.
Last Error	%LE%	The last error message for this file. If the file has failed, this will give the reason why.

Date/Time Placeholders

Placeholder Name	Placeholder Marker	Description

Placeholder Name	Placeholder Marker	Description
Current Date/Time	%DTM_dtformat %	This placeholder brings up the Date/Time Placeholder dialog, which allows you to select the format in which the current date/time will be displayed. ODEX interprets MM as the month and mm as minutes. You must include separators if you want them.
Current Day	%DTM_dd%	The current day of the month expressed as a number e.g. 12 is the 12th day of the month
Current Hours (12 Hr)	%DTM_hh%	The current hour expressed in terms of a 12-hour clock e.g. 02 is either 2 a.m. or 2 p.m.
Current Hours (24 Hr)	%DTM_HH%	The current hour expressed in terms of a 24-hour clock e.g. 14 is 2 p.m.
Current Minutes	%DTM_mm%	The minutes component of the current time e.g. if the time is 10.30 the Current Minutes will be 30.
Current Month	%DTM_MM%	The current month expressed as a number e.g. 10 is October
Current Seconds	%DTM_ss%	The seconds component of the current time e.g. if the time is 10:30:59 the Current Seconds will be 59.
Current Year	%DTM_yy%	The current year expressed as its last two digits e.g. for 2004, the Current Year will be 04

Log Placeholders

Placeholder Name	Placeholder Marker	Description

Placeholder Name	Placeholder Marker	Description
Date/Time	%LOG-DTM_dtformat%	The date and time at which the error occurred, in the format specified by the date/time placeholder.
ID	%LOG-ID%	The 8-character error message ID.
Level	%LOG-LVL%	The logging level at which this error occurred e.g. General.
Message	%LOG-MSG%	The actual error message
Type	%LOG-TYPE%	Indicates the type of log entry. This can be seen in the System Log Archive by selecting Type from the View button. If the log entry is not associated with a Type, the value that replaces the placeholder will be “None”.
Unique ID	%LOG-UI%	If present, this value may represent a Session ID, a Workflow File ID or a User Name, depending on the context of the log entry.

SAP System Placeholders

Placeholder Name	Placeholder Marker	Description
Back Office System Description	%BOS-DESC%	The description of the SAP system as shown on the Back Office System list page.
Back Office System Name	%BOS-NAME%	The name of the SAP system as shown on the Back Office System list page.
Client	%SS-CLI%	The SAP Client ID as given on the Integration page of the Back Office System.

Placeholder Name	Placeholder Marker	Description
Creation Date/Time	%SU-CREAT-DT_dtformat%	The date and time at which the SAP IDoc file was created, ready for export to the SAP system.
Exported Date/Time	%SU-EXPORT-DT_dtformat%	The date and time at which the SAP IDoc file was exported to the SAP system.
Exported File	%SU-EXP-FILE%	The name of the file exported to the SAP system.
IDoc Directory	%SS-IDOC-DIR%	The directory to which the file is to be exported, as given on the Advanced page of the Back Office System.
IDoc Number	%SU-IDOC-NUM%	The number allocated to the IDoc by the SAP system.
IDoc or Status Record	%SU-IDOC-SR%	An indication of whether the file contained an IDoc or a Status Record.
IDoc Status	%SU-IDOC-STAT%	The Status of the IDoc. Only present if the file is a SAP Status Record. Possible values are: Acknowledged, Analysis, Construction, Retransmission, Scheduled, Submitted and Transmission.
Port	%SS-PORT%	The name of the Port within the SAP system to which the file has been passed, as given on the Integration page of the Back Office System.
SAP ID	%SS-SAP-ID%	The 3-character identifier assigned to your SAP instance, as given on the Integration page of the Back Office System.
Status	%SU-STATUS%	The status of the SAP (Export) operation e.g. Failed.

Placeholder Name	Placeholder Marker	Description
System Number	%SS-SYS-NO%	The SAP system number as given on the Integration page of the Back Office System.
Temporary Disk File	%SU-TEMP-FILE%	The full filepath of the file to be exported, including the filename and extension, where it is held temporarily by ODEX prior to export to the SAP system.
Update Directory	%SS-UPD-DIR%	The Status Records directory, as given on the Integration page of the Back Office System.

User Data Placeholders

User Data can be stored against Companies, Networks, Mailboxes and Data Sources. There can be up to 10 User Data values against each. Therefore, to access different values, an index can be specified. For example, the placeholder for the Destination Networks User Data is - %DEST_NET_USR_DEF%. This will be replaced with the first User Data entry against the destination network. To use other values against this network, an index can be used. For example - %DEST_NET_USR_DEF[7]% will reference the 7th value. Omitting the index or using [1] will use the first value.

Placeholder Name	Placeholder Marker	Description
Destination Company User Data	%DEST_CMP_USR_DEF%	The User Data for the destination company of a file.
Destination Network User Data	%DEST_NET_USR_DEF%	The User Data for the destination network of a file.
Destination Mailbox User Data	%DEST_MBX_USR_DEF%	The User Data for the destination mailbox of a file.
Originator Company User Data	%ORIG_CMP_USR_DEF%	The User Data for the originator company of a file.
Originator Network User Data	%ORIG_NET_USR_DEF%	The User Data for the originator network of a file.
Originator Mailbox User Data	%ORIG_MBX_USR_DEF%	The User Data for the originator mailbox of a file.

Placeholder Name	Placeholder Marker	Description
Data Source User Data	%DATA_SRC_USR_DEF%	The User Data for the Data Source the file entered the system on.

Workflow File Placeholders

Placeholder Name	Placeholder Marker	Description
Channel Name	%CHL%	The name of the channel in which the file was processed, as designated by you on the Channel list page.
Communications File Status	%WFC%	The status of the comms file at the time the placeholder is used. If the file is not a comms file, the value that replaces the placeholder will be “NoCommsFile”.
Destination Trading Partner	%DTP%	Only applicable to files imported via a Comms Data Source. The name of the trading partner to which the file was sent.
File ID	%FID%	The ID of the file, as designated by ODEX. This value is used in the File ID column of the appropriate Workstation View.
File ID (Padded to 8 characters)	%FID8%	This placeholder incorporates the digit 8, whose effect is to pad or truncate the file ID to 8 characters. If truncation occurs, characters from the beginning of the file ID will be truncated. Example of use: “C:\MyDir\%FID8%.edi” The 8 can be replaced by any number from 1 to 99 inclusive.
File Size	%WFSIZE%	The size of the file in bytes.
File Status	%WFS%	The status of the workflow file at the time the placeholder is used.

Placeholder Name	Placeholder Marker	Description
Full Original Filepath	%OFP_F%	The full original filepath of the file, including the filename and extension. If the file was imported via a OFTP Comms Data Source, this will simply be the VFN (including the virtual date and time) without any filepath. If it came from an FTP Source then this will be the RFP_F (See above for definition). If not a comms file, this will be the filepath of the file that was imported via a Command or Directory Data Source.
Full System Filepath	%SFP_F%	The full system filepath of the file, including the filename and extension. The system filepath is where ODEX has placed the file. The format of the filename will be nnnnnnnn.n.ODS where nnnnnnnn is a sequential value generated by ODEX, n is an index value starting with 1 and increasing each time ODEX creates a new version of the file (if applicable) and ODS is the extension.
Import Date/Time	%IDT_dtformat%	The date and time at which the file was imported into ODEX.
Message Type	%MSGTYPE%	Details of the message type, if the file is an EDI file e.g. DELFOR D96A
Original Filename	%OFN%	The original name of the file, without its 3-character extension. For Comms files this will only be applicable for files being sent or received via FTP.

Placeholder Name	Placeholder Marker	Description
Original Filename Extension	%OFN_E%	The 3-character extension of the original filename. For Comms files this will only be applicable for files being sent or received via FTP.
Original Filename with Extension	%OFN_W_E%	The original name of the file, including its 3-character extension. For Comms files this will only be applicable for files being sent or received via FTP.
Original Filepath	%OFP%	The original filepath of the file, without the filename and extension. If the file was imported via an OFTP Comms Data Source, this will simply be the VFN (including the virtual date and time). If imported from a FTP source, this will be the RFN. If not a comms file, this will be the filepath of the file that was imported via a Command or Directory Data Source.
Originator Trading Partner	%OTP%	Only applicable to files imported via a Comms Data Source. The name of the trading partner that sent the file.
Processing End Date/Time	%PED_dtformat%	The date and time at which ODEX finished processing the file, in the format specified by the date/time placeholder. Blank if processing has not yet ended.
Processing Start Date/Time	%PSD_ dtformat %	The date and time at which ODEX started processing the file, in the format specified by the date/time placeholder.

Placeholder Name	Placeholder Marker	Description
System Filename	%SFN%	The system filename of the file, without the extension. The format of the filename will be nnnnnnnn.n where nnnnnnnn is a sequential value generated by ODEX, and n is an index value starting with 1 and increasing each time ODEX creates a new version of the file (if applicable).
System Filename Extension	%SFN_E%	The 3-character extension of the system filename. Always .ODS
System Filename with Extension	%SFN_W_E%	The system name of the file, including its 3-character extension. The format of the filename will be nnnnnnnn.n.ODS where nnnnnnnn is a sequential value generated by ODEX, n is an index value starting with 1 and increasing each time ODEX creates a new version of the file (if applicable) and ODS is the extension.
System Filepath	%SFP%	The system filepath of the file, without the filename and extension. The system filepath is where ODEX has placed the file.
User Data	%FUD%	This is (optional) data attached to the file by the user when the file was submitted to the system e.g. from a Submit dialog.
Job Errors	%JERR%	Errors reported by a job; currently implemented only for map jobs

File Analysis Placeholders

The file analysis placeholders expose details taken from the first interchange and first message in an EDI file. If the file is not EDI, then these values will not be populated.

NOTE: The file must go through an Analyse job in order to obtain these values before they can be used as placeholder parameters.

Placeholder Name	Placeholder Marker	Description
(Interchange) Application Reference	%INT-APRF%	Identification of the application area assigned by the sender, to which the messages in the interchange relate.
(Interchange) From EDI Code	%INT-FEDI%	Name or coded representation of the sender of a data interchange.
(Interchange) From EDI Code Qualifier	%INT-FEDIQ%	Qualifier referring to the source of codes for the identifiers of interchanging partners.
(Interchange) From Routing Address	%INT-FRA%	Address specified by the sender of an interchange to be included by the recipient in the response interchanges to facilitate internal routing.
(Interchange) Interchange Control Reference	%INT-CTRF%	Unique reference assigned by the sender to an interchange.
(Interchange) Length	%INT-LEN%	The number of bytes of data this interchange and all messages within the interchange occupy.
(Interchange) Offset	%INT-OFS%	The number of bytes occupied in the file before this interchange begins.
(Interchange) Security Status	%INT-SECS%	EDI security status relating to the interchange.
(Interchange) Syntax	%INT-STX%	The EDI syntax that has been used in the file (e.g. Edifact, VDA)
(Interchange) Syntax Identifier	%INT-STXID%	Coded identification of the agency controlling a syntax and syntax level used in an interchange.
(Interchange) Syntax Version	%INT-STXVR%	Version number of the syntax identified in the syntax identifier.
(Interchange) Test Indicator	%INT-TEST%	Indication that the interchange is a test.
(Interchange) To EDI Code	%INT-TEDI%	Name or coded representation of the recipient of a data interchange.

Placeholder Name	Placeholder Marker	Description
(Interchange) To EDI Code Qualifier	%INT-TEDIQ%	Qualifier referring to the source of codes for the identifiers of interchanging partners.
(Interchange) To Routing Address	%INT-TRA%	Address specified by the recipient of an interchange to be included by the sender and used by the recipient for routing of received interchanges inside his organisation.
(Interchange) Transmission Date Time	%INT-TRDT%	Local Date and Time when the interchange was prepared.
(Message) Agency	%MSG-AGY%	Code identifying the agency controlling the specification maintenance and publication of the message type.
(Message) Association Name	%MSG-ASS%	Code, assigned by the association responsible for the design and maintenance type concerned, which further identifies the message.
(Message) Common Access Reference	%MSG-CAR%	Reference serving as a key to relate all subsequent transfers of data to the same business case or file.
(Message) Message Count	%MSG-CNT%	The message index within the interchange.
(Message) Message Reference	%MSG-REF%	Unique message reference assigned by the sender.
(Message) Message Version	%MSG-VER%	Version number of a message type.
(Message) Release	%MSG-REL%	Release number within the current message type version number.
(Message) Security Status	%MSG-SEC%	EDI security status relating to the message.
(Message) Type	%MSG-TYP%	Code identifying a type of message and assigned by its controlling agency.

Placeholder Processing Instructions

Placeholders are used to represent properties of entities in ODEX (files, networks, mailboxes, messages, and so forth). When text containing the placeholder is processed, the real value of the property is substituted for the placeholder (the date and time that a message was received, the name of a mailbox, and so forth).

Processing instructions have been included in ODEX to allow you to manipulate the value that is substituted for a placeholder. For instance, if the placeholder %VFN% represents the virtual filename of a message sent by OFTP, then %VFN[$.LEFT(5)]% represents the leftmost 5 characters of the virtual filename.

The processing instruction is contained in square brackets after the main body of the placeholder, but before the closing '%' character.

The character '$' in the instruction represents the original value of the property before manipulation. The character '.' Tells ODEX that a function to manipulate the property value will follow. The functions supported at present are described below.

LEFT(n)

Returns the leftmost *n* characters of the value. For instance, if the virtual filename is "ABCD0001234", then %VFN[$.LEFT(4)]% returns "ABCD".

RIGHT(n)

Returns the rightmost *n* characters of the value. For instance, if the virtual filename is "ABCD0001234", then %VFN[$.RIGHT(4)]% returns "1234".

MID(s,n)

Returns the *n* characters of the value starting from position *s*, where *s* is a zero-based index. For instance, if the virtual filename is "ABCD0001234", then %VFN[$.RIGHT(4,3)]% returns "000".

UPPER()

Returns the value converted to uppercase.

LOWER()

Returns the value converted to lowercase.

PADLEFT(n,"c")

Returns the string padded with *n* instances of the character *c* to the left of the original, where *c* is a single letter, digit or space. For instance, if the virtual filename is "ABCD0001234", then %VFN[$.PADLEFT(5,"0")]% returns "00000ABCD0001234".

PADRIGHT(n,"c")

Returns the string padded with *n* instances of the character *c* to the right of the original, where *c* is a single letter, digit or space. For instance, if the virtual filename is "ABCD0001234", then %VFN[$.PADRIGHT(3,"X")]% returns "ABCD0001234XXX".

Multiple functions may be combined in one placeholder if required, For instance, the placeholder %VFN[$.LEFT(6).LOWER()]% returns the leftmost 6 characters of the virtual filename converted to lowercase.

OFTP Cause and Diagnostic Codes

ESID Error Codes

The ESID (End session ID) error codes are set by the OFTP protocol at session termination.

Code (Decimal)	Problem	Description
00	Normal Session Termination	No problem has occurred.
01	Command not recognised	An exchange buffer was received, containing an invalid OFTP command. The OFTP monitor at the remote does not conform correctly to the OFTP standard. Get your trading partner to correct the problem at their end.
02	Protocol violation	An OFTP command has been received that is invalid at this point in the protocol flow. e.g. an SSID was received inside a file transmission. Get your trading partner to correct the problem at their end.
03	User code not known to system	A Start Session (SSID) command contains an unknown or invalid Identification Code. Make sure you and your partner have the EDI codes of the sender and recipient set up correctly.
04	Invalid password	A Start Session (SSID) command contains an invalid password. Make sure you and your partner have the Send and Receive passwords set up correctly.
05	Local site emergency close down	There is an emergency shutdown in process and sessions are being terminated.
06	Command contained invalid data	An OFTP command contained invalid data, e.g. a field that should contain a 'Y' or 'N' contained something else; or a numeric field contained alphabetic characters.
07	Exchange Buffer size error	An exchange buffer has been received that has an invalid size. If the exchange buffer contains an OFTP data command, then the exchange buffer size exceeds that negotiated at session start-up. If the exchange buffer contains an OFTP command then the size of the exchange buffer is inconsistent with the size of the OFTP command.
08	Resources not available	While processing an OFTP command, resources needed within the computer

Code (Decimal)	Problem	Description
		system could not be made available. e.g. memory allocation for the processing of a received OFTP exchange buffer could not be allocated. This type of problem is machine dependent and can normally be overcome by retrying the communications.
09	Time-out	An OFTP command has not been acknowledged for a significant period of time. Normally this is caused by computer overload at the remote end or an invalid configuration, either locally or remotely.
10	Mode or capabilities	This situation can occur when both OFTPs specify 'incoming only' or both specify 'outgoing only' for the direction of file transfer. Clearly it is not practical to continue in such an event.
11	Invalid challenge	The Authentication Response (AURP) to an Authentication Challenge (AUCH) command was not correctly signed. This is probably because the wrong certificate has been used.
12	Secure authentication required	In the Start Session (SSID) command, the caller has requested authentication but the trading partner does not support it. Agree between yourselves whether authentication is to be used.
99	Unspecified abort code	An error or event occurred for which no specific code is defined.

SFNA/EFNA Error Codes

These codes are set during communications by the OFTP protocol at the start of a file (SFNA = Start File Negative Acknowledgement) and end of a file (EFNA = End File Negative Acknowledgement).

Code (Decimal)	Problem	Description
00	File successfully processed	No problem has occurred.
01	Invalid filename	The virtual filename does not contain valid ODETTE characters. Ensure that only upper case alphabetic characters, numbers 0 to 9 and characters & ()-./ are used.
02	Invalid destination	The destination EDI code (file or message node) is not profiled in the Comms Manager section of the Administrator.
03	Invalid origin	The origin EDI code (file or message node) is not profiled in the Comms Manager section of the Administrator.
04	Storage record format not supported	The storage format for the virtual file cannot be supported by the destination. This would occur if, for example, a Variable length record was sent to a machine that could only handle Fixed length records.
05	Maximum record length not supported	The maximum record length that the destination machine can handle has been exceeded.
06	File size is too large	The file is too large for either the OFTP or the remote site to handle.
10	Invalid record count	The 'Number of records' field, stored on the EFID, does not match the number counted during the transmission.
11	Invalid byte count	The 'Number of bytes' field, stored on the EFID, does not match the number counted during the transmission.
12	Access method failure	The remote site has had a problem storing the virtual file. This is often caused by the receiver running out of disk space.
13	Duplicate file identity	The Virtual filename, Date, and Time should be unique. This message states that a second virtual file has been transmitted with exactly the same name, date and time as an existing file.
14	File direction refused	A sender only cannot receive a file and vice versa.

Code (Decimal)	Problem	Description
15	SFNA : Cipher suite not supported EFNA : Invalid signature	If present in a SFNA, the algorithm used to sign/encrypt the file is not supported. Agree with your trading partner which cipher suite you will use. If present in an EFNA, the signature failed verification. The file has become corrupted.
16	SFNA : Encrypted file not allowed EFNA : Decryption failed	If present in a SFNA, the receiver does not want files to be encrypted. If present in an EFNA, the file could not be decrypted. It has become corrupted.
17	SFNA : Unencrypted file not allowed EFNA : Decompression failed	If present in a SFNA, the receiver requires files to be encrypted. If present in an EFNA, the file could not be decompressed. It has become corrupted.
18	Compression not allowed	The receiver does not support advanced OFTP compression.
99	Unspecified reason code	There has been an error that does not fit into any of the above categories.

ISDN Clearing Cause Codes

These codes appear as a result of an ISDN call clearing.

Code (Hex)	Code (Dec)	Description
00	00	No cause available.
01	01	Unassigned (unallocated) number.
02	02	No route to specified transit network.
03	03	No route to destination.
06	06	Channel unacceptable.
07	07	Call awarded and being delivered in an established channel.
10	16	Normal call clearing.
11	17	User busy.
12	18	No user responding.
13	19	User alerting, no answer.
15	21	Call rejected.
16	22	Number changed.
1A	26	Non-selected user clearing.
1B	27	Destination out of order.
1C	28	Invalid number format.
1D	29	Facility rejected.
1E	30	Response to status enquiry.
1F	31	Normal, unspecified.
22	34	No circuit/channel available.
26	38	Network out of order.
29	41	Temporary failure.
2A	42	Switching equipment failure.
2B	43	Access information discarded.
2C	44	Requested channel not available.
2F	47	Resource unavailable.
31	49	Quality of service unavailable.
32	50	Requested facility not subscribed.
39	57	Bearer capability not authorised.
3A	58	Bearer capability not available.
3F	63	Service or option not available.
41	65	Bearer capability not implemented.

Code (Hex)	Code (Dec)	Description
42	66	Channel type not implemented.
45	69	Channel type not implemented.
46	70	Only restricted digital info capability available.
4F	79	Service or option not implemented.
51	81	Invalid call reference value.
52	82	Identified channel does not exist.
53	83	A suspended call exists, but not this id.
54	84	Call identity in use.
55	85	No call suspended.
56	86	Call with this id has been cleared.
57	87	Incompatible destination.
5B	91	Invalid transit network selection.
5F	95	Invalid message specified.
60	96	Mandatory information element missing.
61	97	Message type non-existent.
62	98	Message not compatible with call state.
63	99	Info element non existent.
64	100	Invalid info element contents.
65	101	Message not compatible with call state.
66	102	Recovery on time expiry.
6F	111	Protocol error, unspecified.
7F	127	Interworking, unspecified.

CAPI Errors

These codes indicate problems in CAPI communications.

Code	Description
0x0001	NCPI not supported by current protocol, NCPI ignored
0x0002	Flags not supported by current protocol, flags ignored
0x0003	Alert already sent by another application
0x1001	Too many applications
0x1002	Logical block size too small, must be at least 128 bytes
0x1003	Buffer exceeds 64 Kbytes
0x1004	Message buffer size too small, must be at least 1024 bytes
0x1005	Max. number of logical connections not supported

Code	Description
0x1006	Reserved
0x1007	The message could not be accepted because of an internal busy condition
0x1008	OS Resource error (e.g. no memory)
0x1009	COMMON-ISDN-API not installed
0x100a	Controller does not support external equipment
0x100b	Controller does only support external equipment
0x1101	Illegal application number
0x1102	Illegal command or subcommand or message length less than 12 octets
0x1103	The message could not be accepted because of a queue full condition
0x1104	Queue is empty
0x1105	Queue overflow, a message was lost
0x1106	Unknown notification parameter
0x1107	The message could not be accepted because of an internal busy condition
0x1108	OS resource error (e.g. no memory)
0x1109	COMMON-ISDN-API not installed
0x110a	Controller does not support external equipment
0x110b	Controller does only support external equipment
0x2001	Message not supported in current state
0x2002	Illegal Controller/PLCI/NCCI
0x2003	Out of PLCI
0x2004	Out of NCCI
0x2005	Out of LISTEN
0x2006	Out of FAX resources (protocol T.30)
0x2007	Illegal Message parameter coding
0x3001	B1 protocol not supported
0x3002	B2 protocol not supported
0x3003	B3 protocol not supported
0x3004	B1 protocol parameter not supported
0x3005	B2 protocol parameter not supported
0x3006	B3 protocol parameter not supported
0x3007	B protocol combination not supported
0x3008	NCPI not supported

Code	Description
0x3009	CIP Value unknown
0x300a	Flags not supported (reserved bits)
0x300b	Facility not supported
0x300c	Data length not supported by current protocol
0x300d	Reset procedure not supported by current protocol
0x3301	Protocol error layer 1 (broken line or B-channel removed by signalling protocol)
0x3302	Protocol error layer 2
0x3303	Protocol error layer 3
0x3304	Another application got that call
0x3311	Connecting not successful (remote station is no FAX G3 machine)
0x3312	Connecting not successful (training error)
0x3313	Disconnected before transfer (remote station does not support transfer mode, e.g. resolution)
0x3314	Disconnected during transfer (remote abort)
0x3315	Disconnected during transfer (remote procedure error, e.g. unsuccessful repetition of T.30 commands)
0x3316	Disconnected during transfer (local tx data underrun)
0x3317	Disconnected during transfer (local rx data overflow)
0x3318	Disconnected during transfer (local abort)
0x3319	Illegal parameter coding (e.g. SFF coding error)
0x3481	Unallocated (unassigned) number
0x3482	No route to specified transit network
0x3483	No route to destination
0x3486	Channel unacceptable
0x3487	Call awarded and being delivered in an established channel
0x3490	Normal call clearing
0x3491	User busy
0x3492	No user responding
0x3493	No answer from user (user alerted)
0x3495	Call rejected
0x3496	Number changed
0x349a	Non-selected user clearing
0x349b	Destination out of order
0x349c	Invalid number format

Code	Description
0x349d	Facility rejected
0x349e	Response to STATUS ENQUIRY
0x349f	Normal, unspecified
0x34a2	No circuit / channel available
0x34a6	Network out of order
0x34a9	Temporary failure
0x34aa	Switching equipment congestion
0x34ab	Access information discarded
0x34ac	Requested circuit / channel not available
0x34af	Resources unavailable, unspecified
0x34b1	Quality of service unavailable
0x34b2	Requested facility not subscribed
0x34b9	Bearer capability not authorized
0x34ba	Bearer capability not presently available
0x34bf	Service or option not available, unspecified
0x34c1	Bearer capability not implemented
0x34c2	Channel type not implemented
0x34c5	Requested facility not implemented
0x34c6	Only restricted digital information bearer capability is available
0x34cf	Service or option not implemented, unspecified
0x34d1	Invalid call reference value
0x34d2	Identified channel does not exist
0x34d3	A suspended call exists, but this call identity does not
0x34d4	Call identity in use
0x34d5	No call suspended
0x34d6	Call having the requested call identity has been cleared
0x34d8	Incompatible destination
0x34db	Invalid transit network selection
0x34df	Invalid message, unspecified
0x34e0	Mandatory information element is missing
0x34e1	Message type non-existent or not implemented
0x34e2	Message not compatible with call state or message type non-existent or not implemented
0x34e3	Information element non-existent or not implemented
0x34e4	Invalid information element contents

Code	Description
0x34e5	Message not compatible with call state
0x34e6	Recovery on timer expiry
0x34ef	Protocol error, unspecified
0x34ff	Interworking, unspecified

X.25 Clearing Cause Codes

These codes appear in the X.25 Clear packet.

Code (Hex)	Code (Dec)	Problem	Description
00	00	DTE Clearing	The remote cleared the session. If the associated diagnostic code is non zero, then the remote is abnormally terminating the session.
01	01	Number busy	All incoming logical channels at the remote are busy. The call should be tried again later.
03	03	Invalid call	Invalid call.
05	05	Number unknown	An NUA has been specified that does not exist.
09	09	Out of order	The equipment at the remote end is not active. Either their computer is powered off or their X.25 link level 2 protocol has not been activated.
0B	11	Access barred	The remote is part of a Closed User Group to which you do not belong.
0D	13	Not obtainable	Not obtainable.
11	17	Remote procedure error	A problem exists between the remote DTE and the network. This is a remote problem and is normally as a result of an invalid remote configuration.
13	19	Local procedure error	A problem exists between the local DTE and the network. This is a local problem and is normally as a result of an invalid local configuration.
15	21	RPOA out of order	Recognised Public Operating Agency.
19	25	Reverse charging not subscribed	Reverse charging not subscribed.
21	33	DTE incompatible	DTE incompatible call.

Code (Hex)	Code (Dec)	Problem	Description
		call	
29	41	Fast select not subscribed	Fast select not subscribed.
39	57	Ship absent	Ship not in port (offshore).

X.25 Diagnostic Codes

These codes appear in the X.25 Clear packet as the X.25 clearing diagnostic.

Code (Hex)	Code (Dec)	Description
00	00	No additional information.
01	01	Invalid P(S).
02	02	Invalid P(R).
10	16	Packet type invalid.
11 12 13 14 15 16 17 18 19 1A 1B 1C 1D	17 18 19 20 21 22 23 24 25 26 27 28 29	Packet type invalid for state R1. Packet type invalid for state R2. Packet type invalid for state R3. Packet type invalid for state P1. Packet type invalid for state P2. Packet type invalid for state P3. Packet type invalid for state P4. Packet type invalid for state P5. Packet type invalid for state P6. Packet type invalid for state P7. Packet type invalid for state D1. Packet type invalid for state D2. Packet type invalid for state D3.
20	32	Packet not allowed.
21 22 23 24 25 26 27 28 29 2A 2B 2C	33 34 35 36 37 38 39 40 41 42 43 44	Unidentifiable packet. Incoming call received on one-way channel. Clear or Call packet received on a PVC. Packet on unassigned logical channel. Reject not subscribed to. Packet received - too short. Packet received - too long. Invalid GFI. Restart packet on LCN zero. Illegal fast select packet. Unauthorised Interrupt CONF packet received. Unauthorised Interrupt packet received.
30	48	Timer expired : on Clear request.
31 32 33 34	49 50 51 52	Timer Expired; Incoming Call. Timer Expired; Clear Indication. Timer Expired; Reset Indication. Timer Expired; Restart Indication.
40	64	Unspecified Call Set-Up Problem.
41 42 43 44	65 66 67 68	Facility code not allowed. Invalid facility parameter. Invalid Called Address. Invalid Calling Address.
70	112	Inter network problem.

Code (Hex)	Code (Dec)	Description
80	128	Reserved for network.
90	144	DTE/DCE congestion.
91	145	Received fast select CLEAR request.
92	146	Line restarting fast select CLEAR request.
93	147	Invalid RESTART conf in state R3.
94	148	Loop trunk lines detected.
95	149	Invalid length trunk restart.
96	150	Call quota distribution clear.
97	151	Reconnect multiple race.
98	152	Reconnect time-out.
9F	159	Network table overflow.
A0	160	Non-zero RESET cause from DTE.
A1	161	Data packet too long.
A2	162	INTERRUPT packet too long.
A2	162	DTE not operational.
A3	163	INT. packet too short, no user data.
A4	164	INT. confirmation packet too long.
A5	165	RR packet too long.
A5	165	RNR packet too long.
A7	167	RESET packet too long.
A8	168	RESET confirmation packet too long.
A9	169	Invalid Q bit in data packet.
AA	170	Packet window range exceeded.
AB	171	Invalid P(S).
AC	172	Invalid P(R)
AF	175	RESET packet to short, no cause.
B0	176	REJECT packet too long.
B2	178	Unsuccessful reconnection resync.
B3	179	Non-reconnect call in state C1.
B4	180	Second ID packet from DTE.
B5	181	Bad data transfer state in reconnect.
B6	182	Packet format invalid.
B7	183	FACILITY byte count too large.
B8	184	Invalid packet detected.
B9	185	FACILITY/UTILITY field byte count > 63.
BA	186	Outgoing calls barred.
BB	187	Incoming calls barred.
BC	188	Clearing of PVC.
BD	189	Called address too long.
BE	190	Called address too short.
BF	191	Calling address too short.
C3	192	User data field too long.
C4	193	No buffer available.
C6	194	FACILITY negotiation invalid.
C7	195	Mandatory utility not input.
C8	196	Buffer not available for TNIC.
C9	197	Overflow of TNIC in buffer.

Code (Hex)	Code (Dec)	Description
CA	198	DTE line congested.
CB	199	Table error in packet procedures.
CC	200	Insert table overflow.
CD	201	Delete table overflow.
D3	211	Invalid event in state D1.
D4	212	Call collision on trunk line.
D5	213	No buffer available in end control block.
D6	214	Call collision on DTE line.
D7	215	DTE restart.
D8	216	Call request to trunk line time-out.
D9	217	Reconnect set-up timed out.
DA	218	Invalid output side state.
DB	219	Error detected in blind packet Q proc.
DC	220	RESET ind. re transmission count
DD	221	expired.
DE	222	Invalid output side state.
DF	223	Blind buffer queue overflow in state D4. Blind buffer queue overflow in state C1.
E0	224	Blind buffer queue overflow in state C2.
E1	225	CLEAR packet byte count invalid.
E2	226	Non-zero CLEAR cause.
E4	228	Call collision.
E5	229	Invalid TP load request call packet.
E7	231	Routing loop detected.
E8	232	PVC call request failure.
E9	233	Reconnect call request failed.
BE	235	No buffer available.
EC	236	Call redirection CLEAR.
ED	237	No path to route call.
EE	238	Call routed to DTE line.
EF	239	Call cannot be re-routed.
F0	240	Address not in routing tables.
F1	241	Routing table change during call routing.
F2	242	No LC available on fake trunk.
F3	243	Remote DTE down on a PVC.
F4	244	Invalid control block event detected.
F5	245	Invalid packet received : state D4.
F6	246	Invalid packet received : state D5.
F7	247	Invalid packet received : state P8.
F8	248	Internal processing failure.
F9	249	Invalid RESTART indication received.
FA	250	Line status change in state R5.
FB	251	Invalid packet received : state R5.
FC	252	Invalid packet received : state R4.
FD	253	Line status change in state R3.
FE	254	Line status change in state R2.
FF	255	Line status change in state R1.

Glossary

Child File

A child file is the result of splitting an EDI file into its component files. A file containing one or more interchanges can be split into several files, each of which contains one of those interchanges. The original file is then deemed to be a parent, and each file it was split into is deemed to be a child of that parent.

Data Source

A data source is the definition of how and where files are imported into ODEX. Files can be imported from a monitored directory, from ODEX comms or from a command. A monitored directory imports files that are placed in it. Comms imports all files received via ODEX comms. A command data source is for files that have been manually imported into ODEX.

EERP

Stands for End-To-End-Response. This is part of the OFTP protocol. It is sent by the recipient of a file to indicate that the file has been received successfully.

Placeholder

Placeholders are typically used when running an application program whose parameter values are not known until the time of execution. The purpose of a placeholder is to mark the position of the value to be inserted. A placeholder takes the form of an acronym preceded and followed by a percentage (%) sign. For example, %SFN% represents System Filename.

URL

URL stands for Uniform Resource Locator. This is the address used to connect with AS2 networks. Some sample URL formats are shown below.

http://0.0.0.0:00/

http://as2.tradingpartner.net:5678/receiver/

or, for a secure connection using SSL,

https://0.0.0.0:00/

https://as2.tradingpartner.net:5678/receiver/

The four parts of the URL are:

the URL 'scheme' (http or https)

the host (or IP address) in the format ://1.2.3.4 or ://as2.tradingpartner.net

the port (optional). If omitted, http URLs default to port 80, and https URLs default to port 443

the resource (optional) to the right of the host (and port, if used). e.g. http://0.0.0.0:00/abc/def Defaults to '/' if no resources are used.

VFN

VFN stands for Virtual Filename. This is the name that is given to a file when it is sent to a trading partner. Together with the Virtual Date and Virtual Time it creates a unique file identifier