IBM Sterling Commerce:Centre Web Administration Tool

User Guide

Documentation Date: 28 February 2013

IBM Sterling Commerce:Centre Web Administration Tool

User Guide

Documentation Date: 28 February 2013

Note
Before using this information and the product it supports, read the information in "Notices" on page 217.

This edition applies to the August 22, 2010 version of IBM Sterling Commerce:Centre (product number xxxx-xxx) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. About Commerce:Centre

About Sterling Commerce:Centre

A complete implementation of IBM® Sterling Commerce:Centre is called a node. A node consists of one or more servers that host the Sterling Commerce:Centre communications components and processing engine.

There are two Sterling Commerce:Centre production nodes:

- Dublin 3 (DUB3)—owned and operated by IBM. DUB3 handles outbound IBM Sterling Web Forms, Managed Services, GIODE, and customer (especially AS2) communications.
- Dublin 4 (DUB4)—owned and operated by IBM. DUB4 handles inbound Sterling Web Forms, ANX interconnects, and interconnects to other VANs.

All nodes are part of the IBM Sterling B2B Collaboration Network and are operated, monitored, and maintained by Customer Delivery Services.

A third node–Dublin alpha (ALF1)–is used for testing. This node is internet-exposed but is used for certifications and testing, such as the Drummond AS2 interoperability tests. It is also used for certificate and PGP key verification.

Overview of Sterling Commerce:Centre Services

Sterling Commerce:Centre works with Sterling Commerce:Network and GIODE to support all of the communications methods, protocols, and services supported by Sterling B2B Collaboration Network.

Sterling Commerce:Centre provides the following services. Additional information about these services can be found in the Sterling B2B Collaboration Network technical overview.

- ANX Service (Interconnects over FTP)
- AS1 Service (over SMTP)
- AS2 Service (over HTTP/HTTPS)
- FTP Service
- Interconnect Service (over FTP)
- U.S. Customs Service
- X.400 COD/COR Service (for WalMart Germany)

Sterling Commerce:Centre Features Available to Distributors

Some Sterling Commerce:Centre features are not available on distributor nodes.

In the WAT, you may be able to view screens on which you cannot make changes. For example, you may be able to view profile information for security levels higher than yours, however, the system does not allow you to submit updates. You may also see information in the online help describing a screen or procedure that you cannot view in the WAT. Still other Sterling Commerce:Centre features are available to you but require the assistance of Customer Support to set up or activate.

For more information, contact Customer Support or your sales representative.

Chapter 2. The WAT Interface

About the WAT

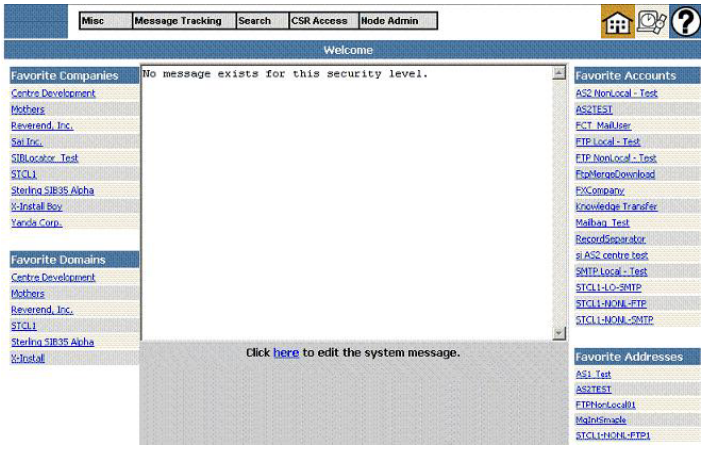
The Web Administration Tool (WAT) for Sterling Commerce:Centre is a browser-based application that runs on each Sterling Commerce:Centre node. The WAT provides an interface for managing accounts and tracking data on a node.

To use the tool, open your Internet browser and identify the private, secure Web site address for your node. Then enter your user ID and password to log on.

The pages of the WAT are displayed in your browser. Use standard browser controls (such as Back and Forward) in combination with the fields, buttons, and links displayed on the pages.

Note: Your login session will expire after 90 minutes of inactivity.

The following example shows the WAT home page.



WAT Icons

In the Web Administration Tool, icons are displayed in the upper-right corner of the browser window.

The following table describes the Web Administration Tool icons.

Icon	Description
	Display the home page for the Web Administration Tool.
	Toggle the display of the current time (as UTC time). UTC (Coordinated Universal Time) is the standard time formerly called Greenwich Mean Time (GMT). UTC is expressed using a 24-hour clock. In the WAT, the UTC value reflects the time on the node (that is, the Windows 2003 server where Sterling Commerce:Centre resides).

Icon	Description
	Open Help for the Web Administration Tool.

WAT Menu Commands

In the Web Administration Tool, the following menus are displayed at the top of the browser window:

Note: The menus and commands you see are determined by your security level.

Miscellaneous Menu

The following table describes the options available from the Miscellaneous menu.

Menu Command	Description
Miscellaneous > Launch Help	Open Help for the Web Administration Tool.
Miscellaneous > Edit Favorites	Change or remove the favorites listed on the home page.
Miscellaneous > Home	Display the home page for the Web Administration Tool.
Miscellaneous > Log Off	Exit the Web Administration Tool.

Message Tracking Menu

The Message Tracking menu allows you to search for messages based on information you know about the message, such as the message ID or subject.

The following table describes the options available from the Message Tracking menu.

Menu Command	Description
Message Tracking > Inbound	Search for an inbound message by time, status, and protocol.
Message Tracking > Outbound	Search for an outbound message by time, status, protocol, and disposition.
Message Tracking > EDI Interchange	Search for messages if you know the EDI ID of the sender, the EDI ID of the receiver, or the time.
Message Tracking > Connect:Mailbox	Search for a message from a Sterling Commerce:Network mailslot if you know the inbound or outbound batch number from Sterling Commerce:Network.
Message Tracking > Message ID	Search for inbound or outbound messages if you know the message ID.
Message Tracking > Transaction ID	Search for inbound or outbound messages if you know the transaction ID.
Message Tracking > MTS ID	Search for inbound and outbound messages if you know the MTS ID.
Message Tracking > Association ID/Type	Search for inbound and outbound messages if you know the association ID.

Menu Command	Description
Message Tracking > Subject	Search for inbound and outbound messages by the subject of the message and by the date and time the message was added to the database.

Search Menu

The Search menu allows you to search for accounts based on what you know about the account, such as the domain or protocol information.

The following table describes the options available from the Search menu.

Menu Command	Description
Search > Company	Search for an account if you know all or part of the company name.
Search > Domain	Search for an account if you know all or part of the domain name or the mailbox name.
Search > Account	Search for an account if you know all or part of the account information.
Search > Address	Search for an address if you know all or part of the address information (such as mailslot ID, name).
Search > Address > SMTP	Search for an account if you know all or part of the SMTP protocol information.
Search > Address > X.400, FTP, AS2, HTTP	Search for an account if you know all or part of the X.400, FTP, AS2, or HTTP protocol information.
Search > Address > Mailslot	Search for an account if you know all or part of the mailslot number.
Search > EDI Info	Search for an account if you know all or part of the EDI ID or all or part of the messaging address (mailbox and mailslot).
Search > App Log – Session ID	Search for all logging events for the Session ID. The search does not use partial substrings, so you must enter the exact Session ID.
Search > App Log – Message ID	Search for all logging events for the Message ID. The search does not use partial substrings, so you must enter the exact Message ID.
Search > Audit Log	Search for audit log entries. This menu option is restricted to users with a Super User or System Administration security level.

CSR Access Menu

The CSR Access menu allows Customer Support personnel to manage accounts and view message statistics.

The following table describes options available from the CSR Access menu.

Menu Command	Description
CSR Access > Mailbox Migration	Migrate EDI IDs from a source mailbox/slot to a destination mailslot. You can migrate all of the IDs in a mailbox/slot or individual IDs. **Note:** This menu option is not available for CSR users. Only users with System Administrator and Super User security levels can use this menu option.
CSR Access > Suspensions	View summary screen of suspended addresses.
CSR Access > Node List	List Sterling Commerce:Centre nodes and their URL addresses. **Note:** The Edit menu option is not available for CSR users and Super Users. Only users with System Administrator security level can edit node details.
CSR Access > Trading Partner ID Management	Set up and maintain cross-references between standard EDI IDs and other identifiers, such as those used in the AS2 hosted customer service.
CSR Access > House Keeping Log	Search for all items in the log for a specified time period.
CSR Access > Certificate Management > CAPI (SMIME)	Display installed security certificates available for AS1 and AS2 accounts. Add and delete certificates. **Note:** This menu option is not available for CSR users. Only users with System Administrator and Super User security levels can use this menu option.
CSR Access > Certificate Management > PGP Key Ring	Display installed PGP keys available for FTP accounts. Add and delete keys. **Note:** This menu option is not available for CSR users. Only users with System Administrator and Super User security levels can use this menu option.
CSR Access > Config Parser Mgmt > Config Parsers	Display a list of available custom parsers. **Note:** CSR users can only view the custom parsers. Only users with System Administrator and Super User security levels can add, edit, and delete parsers.
CSR Access > Config Parser Mgmt > Key Fields	Display a list of fields (including descriptions) that can be configured in a custom parser. **Note:** CSR users can only view the key fields. Only users with System Administrator and Super User security levels can add, edit, and delete key fields.
CSR Access > Node Statistics > Message Turnaround Time	Display the average time between the receipt of an inbound message and the delivery of an outbound message on the node.
CSR Access > Node Statistics > Message Volume	Display statistics about the size and number of messages flowing through the node.
CSR Access > Latest Message Activity	Display detailed information about the messages flowing through the node.
CSR Access > Latest Message Snapshot	Display summary information about the messages flowing through the node.

Node Administration Menu

The Node Administration menu allows OSS to manage account information for the node, such as system profiles and protocol-specific templates.

The following table describes the options available from the Node Administration menu.

Menu Command	Description
Node Administration > System Profiles	Set up and maintain account and address profiles that control the run-time routing and processing of data on the node and on Sterling B2B Collaboration Network. **Note:** This menu option is not available for CSR users. Super Users can use this menu option but cannot edit profiles. Only users with System Administrator security level can edit profiles.
Node Administration > Error Codes	Set up and maintain error codes that can be associated with account and address profiles. **Note:** This menu option is not available for CSR users. Super Users can use this menu option but cannot edit error codes. Only users with System Administrator security level can edit error codes.
Node Administration > Node Address Templates	Set up and maintain protocol-specific templates that can be applied to new addresses. **Note:** This menu option is not available for CSR users. Super Users can use this menu option but cannot edit templates. Only users with System Administrator security level can edit templates.
Node Administration > Message History	Set up, maintain, and view message histories, which track changes in status over the lifetime of a message, including correlating inbound and outbound messages. Data about message histories is stored in the Sterling Commerce:Centre database. **Note:** This menu option is not available for CSR users and Super Users. Only users with System Administrator security level can access this menu option.

WAT User Roles and Security Levels

Sterling Commerce:Centre supports different levels of access to the WAT so users can view information without compromising the security of the system.

The following user roles are provided on the WAT:

- System Administrator
- Super User
- Customer Service Representative (CSR)
- Mail User
- Read Only Access

System Administrator

Users with System Administrator security have the following capabilities and restrictions:

Action	Permissions
Menu access • Miscellaneous • Message Tracking • Search • CSR Access • Node Administration	Can access all menus.
Edit/update options	
Node (view information)	Can view node information.
Company • Search • View information	Can search and view information for all companies.
Domain • Search • View information	Can search and view information for all domains.
Account • Search • View information • Make changes	Can search and view information for all accounts.
Address • Search • View information • Make changes	Can search and view information for all addresses.
EDI information • Search • Make changes	Can search for and make changes to all EDI IDs for all addresses.
Mailbox migration	Can migrate mailboxes for all addresses.
Certificate/key management	Can manage certificates/keys.
Parsers • View • Edit	Can view and edit parsers.
Web password (view)	Can view the Web password for all accounts.
Message management	
Outbound messages • Search/view • Resend • View details and history • Download attachments • Pickup	Can perform all actions on all outbound messages.
Inbound messages • Search/view • Restore/reprocess • View details and history • Change status • Download attachments	Can perform all actions on all inbound messages.

Action	Permissions
Logs • Application logs • Audit logs	Can view all application and audit logs.
WAT management • System message • Node address templates • System profiles • Error codes • Connect:Mailbox status • Housekeeping log • Node statistics	 • Can edit all message levels. • Can view and edit details. • Can view and edit details. • Can view and edit details. • Can update the status. • Can view log. • Can view node statistics.

Super User

Users with Super User security have the following capabilities and restrictions:

Action	Permissions
Menu access • Miscellaneous • Message Tracking • Search • CSR Access • Node Administration	Can access all menus with the following exception: • **Node Administration > Message History**
Edit/update options	
Node (view information)	Can view node information.
Company • Search • View information	Can search and view information for all domains, with the following exception: • Cannot edit templates.
Domain • Search • View information	Can search and view information for all domains, with the following exception: • Cannot edit templates.
Account • Search • View information • Make changes	Can search and view information for all accounts having a security level of Super User or lower. Can only set the security level of an account lower. Can view and edit the status of accounts with a security level of Super User or lower.
Address • Search • View information • Make changes	Can search and view information for all addresses having a security level of Super User or lower. Can only set the security level of an account lower. Can view and edit the status of addresses with a security level of Super User or lower.

Action	Permissions
EDI information • Search • Make changes	Can search for and make changes to all EDI IDs for addresses having a security level of Super User or lower. Can only set the security level of an account lower. Can view and edit the status of addresses with a security level of Super User or lower.
Mailbox migration	Can migrate mailboxes for all addresses.
Certificate/key management	Can manage certificates/keys.
Parsers • View • Edit	Can view and edit parsers.
Web password (view)	Can view the Web password for accounts having a security level lower than Super User.
Message management	
Outbound messages • Search/view • Resend • View details and history • Download attachments • Pickup	Can perform all actions on all outbound messages.
Inbound messages • Search/view • Restore/reprocess • View details and history • Change status • Download attachments	Can perform all actions on all inbound messages.
Logs • Application logs • Audit logs	Can view all application and audit logs.
WAT management • System message • • Node address templates • System profiles • Error codes • Connect:Mailbox status • Housekeeping log • Node statistics	 • Can edit message for Super Users and lower. • Can view details. • Can view and edit details. • Can update the status. • Can update the status. • Can view log. • Can view node statistics.
Other • Add user	Cannot assign the System Administrator security level.

Customer Service Representative (CSR)

Users with CSR security have the following capabilities and restrictions:

Action	Permissions
Menu access • Miscellaneous • Message Tracking • Search • CSR Access • Node Administration	Can access all menus with the following exceptions: • Node Administration • CSR > Mailbox Migration • CSR > Certificate Management > CAPI (SMIME) • CSR > Certificate Management > PGP Key Ring
Edit/update options	
Node (view information)	Can view node information.
Company • Search • View information	Can search and view information for all companies, with the following exception: • Cannot edit templates.
Domain • Search • View information	Can search and view information for all domains, with the following exception: • Cannot edit templates.
Account • Search • View information • Make changes	Can search and view information for all accounts having a security level of CSR or lower. Can only set the security level of an account lower. Cannot edit the status access.
Address • Search • View information • Make changes	Can search and view information for all addresses having a security level of CSR or lower. Can only set the security level of an account lower. Cannot edit the status access.
EDI information • Search • Make changes	Can search for and make changes to all EDI IDs for addresses having a security level of CSR or lower. Can only set the security level of an account lower. Cannot edit the status access.
Mailbox migration	Cannot migrate mailboxes.
Certificate/key management	Cannot perform certificates/key management.
Parsers • View • Edit	• Can view parsers. • Cannot edit parsers.
Web password (view)	Can view the Web password for accounts having a security level lower than CSR.

Action	Permissions
Message management	
Outbound messages • Search/view • Resend • View details and history • Download attachments • Pickup	Can perform all actions on all outbound messages with the following exception: • Cannot resend outbound messages.
Inbound messages • Search/view • Restore/reprocess • View details and history • Change status • Download attachments	Can perform all actions on all inbound messages with the following exception: • Cannot restore/reprocess inbound messages.
Application Logs	Can view all application logs.
WAT management • System message • Node address templates • System profiles • Error codes • Connect:Mailbox status • Housekeeping log • Node statistics	• Can edit message for CSRs and lower. • Cannot view or edit details. • Cannot view or edit details. • Cannot view or edit details. • Cannot update the status. • Can view log. • Can view node statistics.
Other • Add user	Cannot assign the System Administrator and the Super User security levels.

Mail User

Users with Mail User security access a unique interface designed for document tracking by the customer. The user's Inbox refers to messages sent to the user's account from trading partners. The user's Outbox refers to messages sent from the user's account to trading partners.

Users sign on to Document Tracking by entering the user ID and password associated with their account on the node. For more information, see the Help available from the Document Tracking interface.

Users with Mail User security have the following capabilities and restrictions:

Action	Permissions
Menu access • Miscellaneous • Message Tracking • Search • CSR Access • Node Administration	Can access the **Miscellaneous** menu, with the following exception: • Edit Favorites In the **Message Tracking** menu, only the following options are available: • Inbox Message • Outbox Message • Inbox EDI Interchange • Outbox EDI Interchange Cannot access the other menus.
Edit/update options	
Node (view information)	Cannot view node information.
Company • Search • View information	Cannot do company searches or views.
Domain • Search • View information	Cannot do domain searches or views.
Account • Search • View information • Make changes	Cannot do account searches, views, or changes.
Address • Search • View information • Make changes	Can only view information for addresses under the parent account.
EDI information • Search • Make changes	Cannot search or change EDI information.
Mailbox migration	Cannot migrate mailboxes.
Certificate/key management	Cannot perform certificate/key management.
Parsers • View • Edit	Cannot view or edit parsers.
Web password (view)	Cannot view the Web password.
Message management	
Outbound messages • Search/view • Resend • View details and history • Download attachments • Pickup	Can view history and details on outbound messages coming from or going to any address in the same account. Cannot perform any other actions on any outbound messages.

Action	Permissions
Inbound messages • Search/view • Restore/reprocess • View details and history • Change status • Download attachments	Can view history and details on inbound messages coming from any address in the same account. Cannot perform any other actions on any inbound messages.
Logs • Application logs • Audit logs	Cannot view application logs.
WAT management • System message • Node address templates • System profiles • Error codes • Connect:Mailbox status • Housekeeping log • Node statistics	Cannot perform WAT management.

Read Only Access

In addition to the security levels, access to different parts of the WAT can be controlled using fields on a user's Account Details page. These fields are:

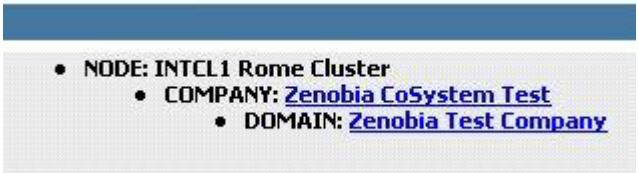
- Read Only
- Prevent Inbound Message Restores
- Prevent Outbound Message Updates
- Prevent Credential List Updates
- Prevent Node Level Updates

Users with Read Only access can still view all of the WAT pages. However, the values defined in these fields control what users can do on the WAT pages by disabling buttons (such as **New**, **Edit**, and **Delete**).

WAT Navigation Links

Using Links on the Hierarchy

As you work with accounts, your browser appends more detailed information to previously displayed information. For example, if you search for an account by company name, you drill down from a list of companies to a list of domains for one company, to a list of accounts for one company-domain entity. Each request displays the new information at the bottom of the page. Meanwhile, the top of the page displays the levels of the hierarchy that precede your current position.



To move to another level, click the appropriate link in the hierarchy. For example, from the hierarchy at the top of Account Details, click the Domain link (**Zenobia Test Company**, in the above example) to display the relevant Domain Details page.

Using Links on the Divider Bar

As you work with accounts, a divider bar separates each portion of the information and includes links for working with the information.

To select an action relevant to information being displayed, click the appropriate link. For example, from the divider bar for Account Details, click **Inbound Messages** to search for any inbound messages for that account.

Alphabetical List of Links on the Divider Bar

Link	Description	Available from
Add Address	Add a new address to the account.	• Account Details
Add Account	Add a new account to the company-domain entity.	• Domain Details
Add Account Profile	Select a profile to apply to an account.	• Account Profiles
Add Address Profile	Select a profile to apply to an address.	• Address Profiles
Add Association ID Type	Add an association ID and type to the node.	• Association ID Types
Add EDI IDs	Add new EDI IDs to an address.	• Address Details
Add Profile Description	Add an account or address profile.	• Profile List
Add to Favorites	Add the current company, domain, account, or address to the favorites listed on the home page.	• Company Details • Domain Details • Account Details • Address Details
Edit Details	Maintain account or address information.	• Account Details • Address Details
Edit Profile Descriptions	Maintain account and address profiles that control data processing.	• Profile List • Profile Details
Edit Status	For System Administrators and Super Users only—Update the status of an account or address. System Administrators can edit the status of any account, address, or EDI information. Super Users can only edit the status of accounts, address, and EDI information with the same or lower security level.	• Account Details • Address Details
Edit Templates	Maintain templates for protocol settings.	• Company Details • Domain Details

Link	Description	Available from
Exclude a Company	Not supported in this release. Specify a company whose accounts are excluded from a distributor's management.	• Companies Excluded List
Inbound Messages	Search for inbound messages sent to a company, domain, account, or address.	• Company Details • Domain Details • Account Details • Address Details
List Nodes	List nodes.	• Edit a Node Listing
List Profile Descriptions	List account and address profiles set up on the node.	• Add Profile • Profile Details
Mailbox Migration	Move EDI IDs associated with a source mailbox or mailslot and attach them to a destination mailslot.	• Address Details
Manage Profiles	Select a profile to apply to an account or address.	• Account Details • Address Details
Outbound Messages	Search for outbound messages sent from a company, domain, account, or address.	• Company Details • Domain Details • Account Details • Address Details
View Details	Drill down for more company, domain, account, or address information.	• Company Details • Domain Details • Account Details • Address Details

Adding Favorites to the Home Page

You can use the home page of the Web Administration Tool to organize and save links to the company, domain, account, or address information that you access frequently. After you set up a favorite, you can click the link on the home page to display the information rather than searching for it each time.

About this task

To add links to frequently accessed information, complete the following steps:

Procedure

1. Open the WAT on the node you want.
2. Display the Company Details, Domain Details, Account Details, or Address Details page that you want.
3. On the divider bar, click **Add to Favorites**.

   A link to the page you chose is added to the home page. You may need to refresh your browser to see the change.

Editing or Removing Favorites on the Home Page

You can modify your home page by editing or removing favorites.

About this task

To edit or remove links from your home page, complete the following steps:

Procedure

1. Open the WAT on the node you want.
2. Select **Miscellaneous > Edit Favorites**.

   A list displays, which is divided into company links, domain links, account links, and address links.
3. Do one of the following:
   - To delete a link, select the check box to the left of the entry and click **Delete**.
   - To edit the displayed name of a link, type your changes. Then select the check box to the left of the entry and click **Update**.
   - While you work, you can click **Check All** (to select all check boxes), **Clear All** (to clear all check boxes), or **Reset** (to undo any changes and restore settings to their original values).
4. Select **Miscellaneous > Home**.

   The home page displays. You may need to refresh your browser to see the change.

Writing a System Message

You can write a message to be displayed on the home page of the Web Administration Tool. You can write one message that everyone reads, or you can write different messages for users with different security levels.

Procedure

1. Open the WAT on the node you want.
2. In the instructions at the bottom of the current message, click **here**.
3. You are prompted to identify the security level of the user whose message you are editing. Then click **Next**.
4. In the Message box, type the text of the message. Then select one or more check boxes to indicate the security level of the users who should see the message.

   If you need, click **Clear** (to remove the message text and clear all check boxes) or click **Reset** (to redisplay the message text and the check box settings that were displayed originally).
5. When you finish, click **Update**.

   Note: If you do not have the option to modify the system message, then you have Read Only access to the WAT.

   The new message replaces any previous message for the indicated security levels.

Chapter 3. Onboarding and Setup

Sterling Commerce:Centre Mailboxes and Account Hierarchy

Each Sterling Commerce:Centre node organizes customer information into an account hierarchy that organizes account information, controls the routing of messages to mailboxes, and controls the access of users to account and tracking information. Onboarding and Customer Support use the WAT to set up customer accounts within the account hierarchy on a node.

Sterling Commerce:Centre Mailboxes

A mailbox is subdivided into one or more mailslots. The number of mailboxes and mailslots depends on the customer's needs. Customers access their data in a mailslot by supplying an ID and password. The mailslot allows a customer to send, store, and receive data. Customers can send data in any format, including EDI files, text files, application files, flat files, and XML files.

Sterling Commerce:Centre Account Hierarchy

Each node maintains a separate account hierarchy, which is described in the following table.

Account Hierarchy	Description
1. Node	On each node, global settings can be specified for all companies with mailboxes on the node. Each node can have different global settings.
2. Company	On each node, company entities exist at the top of a hierarchy. Company information is entered into back-end systems, where it corresponds to a customer record in Vantive, and is replicated to a node.
3. Domain (Mailbox)	Each company can have one or more domains beneath it. Domain information is entered into back-end systems, where it corresponds to a mailbox in the billing system and is replicated to a node. Mailbox names use five alphanumeric characters.
4. Account (User or Customer)	Each domain can have one or more accounts beneath it. Onboarding and Customer Support use the WAT to enter account information. Account information includes contact information (name, address, phone number) and a user ID and password (used to log on to the WAT). The security level assigned to the user ID controls whether the user has access to account information and message tracking for this account only or for higher levels in the hierarchy, such as all accounts for a company.
5. Address (Mailslot)	Each account can have one or more messaging addresses beneath it. Onboarding and Customer Support use the WAT to enter address information, which specifies a mailslot where information is stored. When a new address is added, the WAT assigns the next available mailslot name. Mailslot names are three-character suffixes appended to the mailbox name. The WAT pulls the next available mailslot name from a pool, starting with 001–009, followed by 00A. Address information also specifies a messaging protocol used to communicate with the node. The address can be set up to store information that the customer picks up or to send the information to the customer automatically.

Account Hierarchy	Description
6. EDI IDs	Each address can be associated with many EDI ID and qualifier pairs. EDI IDs are required if the account sends or receives information formatted in one of the EDI standards. However, if the account does not exchange information formatted in an EDI standard, an EDI ID is not required.

Implementation Overview

Review all of the topics in this section before performing any of the onboarding and setup procedures.

Note: Your user account must be set up to allow you to edit account details. If your user account is set as Read Only, then the **Add**, **Edit**, and **Delete** functions will not be available to you.

The following table describes the general process for implementing a new customer:

Step	Group	Task
1	Sales	Uses the Vantive ComTract system to submit the order, which includes entering customer information, creating a company ID, and attaching a Network Services agreement.
2	Contracts	Reviews and approves the agreement.
3	Finance and Administration	Uses the Global Billing System (GBS) to pull customer information from Vantive to set up a billing account. GBS assigns a new mailbox ID to the customer.
4	Onboarding	Creates a new service order in Vantive and the following sections for more information.
5	Onboarding	Creates new mailslots on Sterling Commerce:Network or on a particular node based on the customer's protocol and processing requirements.
6	Onboarding and Communications	If necessary, submits a request to the Communications group to set up communications on the server. When setup is complete, Onboarding Services e-mails the mailslot information to the customer.
7	Onboarding	Works with the customer to exchange test data (inbound and outbound connectivity).
8	Onboarding	Communicates with the customer and with Finance and Administration that the customer is ready to exchange production data.

Customer Requirements

Before you can add an account, you must obtain information from your customer about the type of account and protocol that is required.

Consider these factors:

- What security level does the user need? Most users are assigned the Mail User security level. Does the user need to be able to make update, such as restoring inbound messages, or should the user have Read Only access?

- Will the user pick up data from the mailbox or will data be sent directly to an external address? This decision affects the Local Message Store setting.
- What is the error mailbox for this account? On the Dublin 3 node, the error mailbox is SA900.
- Does the user need an EDI ID? If so, the EDI ID must be unique to that trading partner on Sterling B2B Collaboration Network. Additionally, the EDI ID must be unique to one address on the node. Sterling Commerce:Centre checks that any EDI IDs you enter are unique on the node and converts all EDI IDs and qualifiers to uppercase.
- Does the user need or already have a Sterling Commerce:Network mailslot? If a Sterling Commerce:Network mailslot is needed, Sterling Commerce:Centre can create one when an address is added to the node. This decision affects the SuperTracs setting. If a Sterling Commerce:Network mailbox already exists, Sterling Commerce:Centre can couple (or decouple) a Sterling Commerce:Network mailslot and a node address.

Company and Domain Information

In Sterling Commerce:Centre, all account information is organized in a hierarchy under the company-domain to which it is associated.

Company information (such as the company name) and domain information (such as the five-character mailbox ID) are entered into Vantive and replicated to a node. If a domain name is not entered by Vantive, the company name will be used as the domain name by default.

When that process is complete, users on a node can add one or more accounts beneath a company-domain. The hierarchy controls the routing of messages to mailslots and the access of users to account and tracking information.

Note: If you are a distributor running a Sterling Commerce:Centre node and you have additions or corrections to company or domain information, contact Customer Support.

About Adding Accounts, Addresses (Mailslots), and EDI IDs

When you add a new account to a company-domain, you set up one address and up to five EDI IDs. Afterward, you can edit the account to set up additional addresses and EDI IDs. Each address is associated with a unique mailslot and supports one protocol.

Each EDI ID and qualifier pair is unique to a trading partner on Sterling B2B Collaboration Network. On the node, each EDI ID is uniquely assigned to one address. However, an EDI ID may exist on both the node and Sterling Commerce:Network, where it can be associated with more than one Sterling Commerce:Network mailslot. If the address is coupled with a Sterling Commerce:Network mailslot, the new EDI IDs can be added to Sterling Commerce:Network mailslot.

Note: Nothing is added to the Sterling Commerce:Centre database until you complete the last step and click Finish.

Account and Address Profiles

The following profiles are added by default to new accounts:

- Defer Message Routing
- Defer Parsing
- Route by Mailslot Lookup

Password Restrictions

Several passwords will be automatically generated as you are adding accounts and addresses. The IIBS password can only be changed but after the initial setup is complete.

You can change the passwords during the setup process, but they must adhere to the following restrictions:

- Be at least 10 characters long.
- Include at least one letter.
- Include at least one number.
- Include at least one special character. Only the following special characters are allowed:

  ```
  ( ) , . ! - _ '
  ```

Note: The IIBS and mailslot passwords may be the same, but they must be different from the Web password. If you use the same password for all three (IIBS, mailslot, and Web), a warning message is displayed forcing you to create a different password.⌂If you use different passwords for the IIBS and mailslot, a message is displayed stating that they are different.

Adding Accounts

Account setups vary with the protocols being used and the services being purchased.

About this task

The steps below outline the general process for adding an account with one address (mailslot).

Procedure

1. Open the WAT on the node you want.
2. Display Domain Details for the company-domain to which you will add the account. On the divider bar, click **Add Account**.

   The Account Information page displays.
3. Type the account information as described in the Account Details Page topic.
   - The required fields are marked with asterisks.
   - Be sure to specify the protocol needed for the first address. For more information, refer to the topic corresponding to the protocol of the address you are adding.
   - If you need, click **Clear** (to clear all fields) or **Reset** (to restore all fields to their original values).
4. When you finish, click **Next**.

   The Address Information page displays.

5. Type the address information and provide other settings. Be sure to consider these fields:
   - On SuperTracs – Specify a SuperTracs region to indicate that a Sterling Commerce:Network mailslot is added for the address. Or select **No** to indicate that the address should not be added to Sterling Commerce:Network.

     Note: A SuperTracs value will be set by default for the node.
   - Local Message Store – Indicate whether the user picks up data from the mailbox or whether data is sent directly to an external address.
   - Customer – Indicate whether the address is for a Sterling B2B Collaboration Network customer or a non-customer trading partner.
   - Protocol details – The bottom of the page varies with the protocol type.
6. When you finish, click **Next**.

   The EDI Information page displays.
7. If necessary, type an EDI ID and qualifier. You can specify up to five EDI ID/qualifier pairs to be associated with the address. (Later, you can edit the address to add more EDI IDs, if needed.) Click **Next**.

   If you add a Sterling Commerce:Network mailslot for this address, you must enter at least one unique EDI ID and qualifier. The EDI IDs that you enter are added to the address on the node and to the mailslot on Sterling Commerce:Network.
8. Review the information you entered. If you need to change information, use the back arrow in your browser to display the previous page.
9. When you are satisfied, click **Finish**.

   The Account Details page displays.

Results

When processing is complete, the Status field changes to Active. This process takes more time if an associated Sterling Commerce:Network mailslot is also created.

Adding Addresses

Address setups vary with the protocol being used and the service being purchased.

About this task

The steps below outline the general process for adding an address (mailslot) to an account.

Procedure

1. Open the WAT on the node you want.
2. Display Account Details for the account you want. On the divider bar, click **Add Address**.
3. Select the type of protocol. Click **Next**.

   The Address Information page displays. The bottom portion varies with the protocol you selected.
4. Type the address information.
   - The required fields are marked with asterisks.
   - If you need, you can click **Clear** (to clear all fields) or **Reset** (to restore all fields to their original values).

5. Provide other settings. Be sure to consider these fields:
   - On SuperTracs – Specify a SuperTracs region to indicate that a Sterling Commerce:Network mailslot is added for the address. Or select **No** to indicate that the address is not added to Sterling Commerce:Network. If you are adding an associate mailbox, select a SuperTracs region.

     Note: A SuperTracs value will be set by default for the node.
   - Use Mailbag – If you are adding an associate mailbox, select Yes.
   - Mailslot – If you are adding an associate mailbox, type the mailslot name. Otherwise view the default.
   - Local Message Store – Indicate whether the user picks up data from the mailbox or whether data is sent directly to an external address.
   - Customer – Indicate whether the address is for a Sterling B2B Collaboration Network customer or a non-customer trading partner.
   - Associate Mailbox – Indicate whether a mailbox is an associate mailbox.
   - Protocol details – The bottom of the page varies with the protocol type.
6. When you finish, click **Next**.

   The EDI Information page displays.
7. If necessary, type an EDI ID and qualifier. You can specify up to five EDI ID/qualifier pairs to be associated with the address. (Later, you can edit the address to add more EDI IDs.) Click **Next**.

   If you add a Sterling Commerce:Network mailslot for this address, you must enter at least one unique EDI ID and qualifier. The EDI IDs that you enter are added to the address on the node and to the mailslot on Sterling Commerce:Network.
8. Review the information you entered. If you need to change information, use the back arrow in your browser to display the previous page.
9. When you are satisfied, click **Finish**.

   The Account Details page displays.

Results

When processing is complete, the Status field changes to Active. This process takes more time if an associated Sterling Commerce:Network mailslot is also created.

Adding EDI IDs to Addresses

Each EDI ID and qualifier pair is unique to a trading partner on Sterling B2B Collaboration Network. On the node, each EDI ID is uniquely assigned to one address.

About this task

The steps below outline the general process for adding an EDI ID to one address (mailslot).

Procedure

1. Open the WAT on the node you want.
2. Display Address Details for the address you want. On the divider bar, click **Add EDI IDs**.

   The EDI Information page displays.
3. Type the EDI ID and qualifier pairs to be associated with this address.

4. If the address is not coupled with a Sterling Commerce:Network mailslot, **On CNet** is **No** and cannot be changed.

   If the address is coupled with a Sterling Commerce:Network mailslot, set the **On CNet** field. Select **Yes** to add the EDI ID to the node and to the Sterling Commerce:Network mailslot. Select **No** to add the EDI ID to the node only.

   Note: If the address you are adding this EDI ID to is coupled to Sterling Commerce:Network, you do not have to set the **On CNet** field to **Yes**. However, it is recommended that all EDI IDs for addresses coupled to Sterling Commerce:Network have the **On CNet** field set to **Yes**.
5. Review the information you entered. If you need, click **Clear** (to clear all fields) or **Reset** (to restore all fields to their original values).
6. When you are done, click **Finish**.

   The EDI IDs are added to the node first and then to any coupled Sterling Commerce:Network mailslot.

About Setting up Non-customer Trading Partners on ANX

The ANX network uses FTP protocol. Implementation personnel set up an FTP address on any node for a company that receives data through ANX. Typically, this company is not a Sterling B2B Collaboration Network customer but the trading partner of a customer. For example, Ford Motor Company and Chrysler are non-customer trading partners on ANX.

Additionally, each non-customer trading partner on ANX has special requirements for sending or receiving FTP data. Consequently, each ANX trading partner's account on the node is associated with one or more account or address profiles that meet the unique requirements of that FTP system.

ANX Non-customer Trading Partners	**Setups on the Dublin 4 Node**
Ford Motor Company	Company/Domain: • Sterling B2B Collaboration Network ANX non-customers Account: • Ford ANX – Production Account profile: • EDI File Prefix Address profile: • FTP Client Listen Passively

ANX Non-customer Trading Partners	Setups on the Dublin 4 Node
Chrysler	Company/Domain: • Sterling B2B Collaboration Network ANX non-customers Account: • Chrysler EBMX Account profiles: • Route by Mailslot Lookup • Defer Message Routing • Defer Parsing Address profiles: • Chrysler FTP Client • Chrysler FTP Client Site Command • Chrysler FTP Client Receiver File Type Combination • Chrysler FTP Client Sender Password Combination • FTP Server Allow Upload to Commit

Due to a program with suppliers that requires trading of XML documents, Chrysler Mexico has special setup needs. Specific FTP Site commands will be used for routing by Chrysler EBMX on all documents received by suppliers. XML documents coming into Sterling B2B Collaboration Network from Chrysler EBMX must also come in through a unique Chrysler mailslot to use a BEDI screen for data routing.

For more information about setting up Chrysler Mexico suppliers using XML documents, refer to the "Special Setup Requirements for Chrysler XML" documents (inbound/outbound).

Setting up an AS1 Account

An AS1 account needs to be set up on Sterling Commerce:Centre for any company that uses AS1 for EDI data. Typically, this company is not a Sterling B2B Collaboration Network customer but the trading partner of a customer.

About this task

Both the trading partner account and the certificate that supports SMIME cryptography reside on Sterling Commerce:Centre.

Before you can add an AS1 account, you must add the one or two certificates sent by the AS1 user. If the certificate is a trusted certificate, add it. If the certificate is not trusted, contact Level 3 or Open Systems to add it to Sterling Commerce:Centre. You can use the WAT to add trusted certificates only.

Note: If performance is slow while you are adding accounts/addresses, there could be too many certificates and the expired certificates may need to be deleted. Contact L3 for assistance.

To set up an AS1 account, you must complete the following tasks:

Procedure

1. Obtain the following information from the trading partner.
   - Digital certificates – Obtain the digital certificate of the trading partner. The certificate is a file containing the public key and the private key and is often forwarded through the Sterling B2B Collaboration Network customer. AS1 users may send one or two certificates, depending on whether they use separate keys for encryption and for signing. Also, send an e-mail containing the Sterling B2B Collaboration Network digital certificate to the AS1 user. This certificate contains the public key for the Sterling Commerce:Centre AS1 system. Users install the certificate on their AS1 systems.
   - Security option information – Obtain information from the AS1 user about how receipts are handled, whether separate keys are used for signing and encryption, and what the algorithms are for signing and for encryption.
   - EDI ID and qualifier – Create the EDI ID and qualifier included by the trading partner in AS1 data.
   - SMTP address information – Obtain the external SMTP address used to receive outbound messages from Sterling Commerce:Centre. (AS1 accounts cannot pick up data stored on Sterling Commerce:Centre.) Additionally, AS1 addresses require Extended SMTP and SMIME information.
2. Log in to the WAT on the appropriate node.
3. Select **CSR Access > Certificate Management > CAPI**.
4. In the drop-down list, select the certificate store. For example, choose **MY**. Click **Next**.
5. In the list, verify that the certificate you want is *not* included. Click **New**. The Upload and Verify page displays.
6. Click **Browse** to locate the certificate.
7. Select the certificate and click **Upload Certificate**. The file is analyzed and a list of certificates contained within the file is displayed.
8. Select one or more check boxes for the certificates you want. Click **Add Certificates**. The certificates you indicated are installed and listed on the Installed Certificates page.
9. Use the WAT to add the account. Be sure to add the account under the appropriate company-domain. In addition to the usual account and address information, include the following specifications:
   - Protocol Type – SMTP
   - Security Level – Mail User
   - Local Message Store – No
   - On SuperTracs – To couple this address to Sterling Commerce:Network, select a SuperTracs region from the drop-down menu. Otherwise, select No.
   - Extended SMTP Information – Secure Message Protocol is SMIME. This setting populates the other fields for Extended SMTP Information. Be sure to check that Payload Type correctly specifies the AS1 user's preference.
   - SMIME Information – Use the security options chosen by the AS1 user for SMIME Information, including identifying the certificates you installed.
   - EDI ID and Qualifier – EDI ID and qualifier supplied by the AS1 user

Setting up an AS2 Account

An AS2 account needs to be set up on Sterling Commerce:Centre for any company that uses AS2 for EDI data.

About this task

Note: Managed Services offers an AS2 hosted customer service that supports the use of multiple certificates. For AS2 hosted customer accounts, you set up AS2 accounts as described in this section. Additionally, you set up correlations between traditional EDI IDs and AS2 identifiers.

Before you can add an AS2 account, you must add the AS2 user's digital certificates. If the certificate is a trusted certificate, add it. If the certificate is not trusted, contact Level 3 or Open Systems to add it. You can use the WAT to add trusted certificates only.

Note: If performance is slow while you are adding accounts/addresses, there could be too many certificates and the expired certificates may need to be deleted. Contact L3 for assistance.

To set up an AS2 account, you must complete the following tasks:

Procedure

1. Obtain the following information from the AS2 user.
   - Digital certificates –Obtain the digital certificate of the AS2 user. The certificate is a file containing the public and private keys. If the AS2 user is not a customer, the EDI trading partner may forward the certificate to Customer Support. AS2 users may send one or two certificates, depending on whether they use separate keys for encryption and for signing. Also, send an e-mail containing the Sterling B2B Collaboration Network self-signed X.509 digital certificate to the AS2 user. This certificate contains the public key for the Sterling Commerce:Centre AS2 system. Users install the certificate on their AS2 systems.
   - Security option information – Obtain information from the AS2 user about how receipts are handled, whether separate keys are used for signing and encryption, and what the algorithms are for signing and for encryption.
   - EDI ID and qualifier – Generally, set up one EDI ID/qualifier for testing and another for production.
   - AS2 address information, including server information, IP address, and parameters – Obtain information about the AS2 user's system so it can receive outbound messages from Sterling Commerce:Centre. AS2 users do not pick up data stored on Sterling Commerce:Centre. Additionally, AS2 addresses require SMIME information that identifies the digital certificates stored on Sterling Commerce:Centre.
2. Log in to the WAT on the appropriate node.
3. Select **CSR Access > Certificate Management > CAPI**.
4. In the drop-down list, select the certificate store. For example, select **MY**. Click **Next**.
5. In the list, verify that the certificate you want is *not* included. Click **New**. The Upload and Verify page is displayed.
6. Click **Browse** to locate the certificate.
7. Select the certificate and click **Upload Certificate**. The file is analyzed and a list of certificates contained within the file is displayed.
8. Select one or more check boxes for the certificates you want. Click **Add Certificates**. The certificates you selected are installed and listed on the Installed Certificates page.

9. Use the WAT to add the AS2 account. Be sure to add the account under the appropriate company domain. In addition to the usual account and address information, include the following specifications:
   - Protocol Type – AS2
   - Security Level – Mail User
   - Local Message Store – No
   - On SuperTracs – To couple this address to Sterling Commerce:Network, select a SuperTracs region from the drop-down menu. Otherwise, select No.
   - AS2 Protocol Information – Information about the AS2 user's system is required for the following fields:
     - Identifier
     - Web Server
     - Port
     - Receipt Delivery Mode (synchronous or asynchronous)
     - Remote Path and Parameters
   - SMIME Information – Use the options to identify the certificates you installed on Sterling Commerce:Centre.
   - EDI ID and Qualifier – EDI ID and qualifier used by the AS2 user. Generally, use one EDI ID and qualifier for testing and another for production.
10. Ask AS2 users to send a test purchase order or invoice to their address on Sterling Commerce:Centre. The test should be addressed to the VAN Administration test ID.

    The Sterling Commerce:Centre AS2 system returns an MDN to the user. VAN Administration confirms that the MDN is received.

    VAN Administration generates a functional acknowledgment (997) for the inbound test document and sends it to the AS2 user.

    The user's AS2 system returns an MDN to Sterling Commerce:Centre. VAN Administration confirms that the MDN is received.

Setting up an FTP Account

An FTP account needs to be set up on Sterling Commerce:Centre for any company that uses FTP for EDI data.

About this task

To set up an FTP account, you must complete the following tasks:

Procedure

1. Obtain the following information from the FTP user.
   - For event-driven delivery – Obtain the IP address of the user's FTP server, a user ID and password to access their FTP server, and a directory where they want files delivered.
   - For pull delivery – Share the IP address of our FTP server, a user ID and password to access our FTP server, and the path where they will retrieve their files. Details about FTP communication is available to customers on the information center.
   - EDI IDs and qualifiers – Generally, set up one EDI ID for testing and another for production.

- For PGP users (optional) – Obtain or create the customer's key file containing the public PGP key. For managed PGP service, obtain or create the customer's key file containing the private PGP key and obtain or create the password to access the private key.

  If the FTP user is not a customer, the trading partner may forward the keys to Customer Support.

2. Use the WAT to add the FTP account. Be sure to add the account under the appropriate company-domain. In addition to the usual account and address information, include the following specifications:
   - Protocol Type – FTP
   - Security Level – Mail User (or higher, as appropriate)
   - Local Message Store:
     - **Yes**, if the customer will pull their data.
     - **No**, if the customer will have their data pushed to them.
   - On SuperTracs – To couple this address to Sterling Commerce:Network, select a SuperTracs region from the drop-down menu. Otherwise, select No.
   - FTP Protocol Information – Information about the FTP user's system is required for the following fields:
     - IIBS FTP ID and a unique password
     - Remote IP address/host name (if Local Message Store is **No**)
     - Remote FTP ID and password (if Local Message Store is **No**)
     - Remote path (if Local Message Store is **No**)
   - PGP Information – Include PGP information: **Yes** if the customer will use PGP encryption.⌂If **No**, the following fields are inactive:
     - PGP Exchange Key User ID
     - Inbound signature required
     - Sign outbound
     - Encrypt outbound
     - Have private key (for hosted customers)
     - Password (for hosted customers)

What to do next

If the customer is using PGP, continue with the PGP tasks.

Setting up PGP on FTP Accounts

The following tasks are required only if you are adding PGP encryption for this FTP account. You must have completed Setting up FTP Accounts before starting these tasks.

- "Adding the PGP Key"
- "Adding Engine Bypass for PGP Encryption and Decryption" on page 31
- "Enabling Expired PGP Key Notification" on page 32
- "About Verifying PGP Keys" on page 33

Adding the PGP Key

Customer keys should *not* be loaded into production unless their compatibility has been verified, as described in the procedures below. PGP keys created by tools that

are not compatible with the PGP e-Business Server Version 7.0.1 (which is used by Sterling Commerce:Centre) can cause serious problems to Sterling Commerce:Centre.

Before you begin

Note: Only the following ciphers are supported:

- RSA 1024/2048
- DH/DSS 1024/2048/3072

About this task

Complete the following steps to create a PGP key for a customer:

Procedure

1. On the WAT, select **CSR Access > Certificate Mgmt > PGP Key Ring**.
2. At the bottom of the PGP Key Ring screen, click **Create**.
3. In the Add PGP Key screen, complete the fields and click **Create**.

Results

Note: If you are *manually* adding a PGP key, go to the PGP Key Ring page and click **Refresh**. This is in place of bouncing GMH.

What to do next

Verifying Customer and Trading Partner Keys

Before loading PGP keys to the production nodes, you must verify that the PGP are compatible with Sterling Commerce:Centre.

Once the PGP key has been verified to be compatible with Sterling Commerce:Centre, follow the Load the PGP Key to the Node procedure to load the key on a production node.

Verifying Hosted Customer Keys

For some hosted customers, Sterling Commerce:Centre will generate the customer PGP key. In that case, verification is not needed because there is no potential incompatibility.

Adding Engine Bypass for PGP Encryption and Decryption

For customers using PGP over FTP, you must add the Engine Bypass profile to their PGP address.

About this task

Complete the following steps to add Engine Bypass for PGP encryption and decryption

Procedure

1. On the WAT, open the customer's PGP address details page.
2. In the Address Profiles section, click **Add Address Profile**.

3. On the Select Address Profile page, select **Engine Bypass** from the drop-down list and click **Next**.
4. On the Engine Bypass Address Profile page, do the following:
   a. Select **Enabled** from the Status drop-down list.
   b. To fully ensure that the Engine path cannot be exercised, check Force Bypass.

      Note: The Force Bypass option is for the File Transfer Service path between Sterling Commerce:Centre and GIODE only and should not be used for other data paths (including Sterling Commerce:Network traffic).
   c. Enter values for the **Recipient Mailslots** and **Display Names**. The following bypass entries are examples:
      - Sterling – Uses the mailslot of the node PGP address. Data going to the `Sterling\commit` folder is sent to the engine for normal EDI processing. The inbound message should be encrypted with the public key of the node.
      - HC01 – Represents a hosted customer. This address can trade with more than one hosted customer by creating a bypass entry for each. The mailslot refers to an address that is configured with a PGP key that includes a private key. Data going to the `HC01\commit` folder is decrypted with that private key and sent directly to that FTP address without going through the engine. If the Hosted Customer's account includes the Defer Message Routing account profile, the message is instead routed to Sterling Commerce:Network. The inbound message is encrypted with the hosted customer's public key.
      - TP01 – Represents another trading partner address. This address can trade with more than one trading partner by creating a bypass entry for each. The mailslot refers to an address that is either non-PGP or is configured with a PGP key that does not include a private key. Data going to the `TP01\commit` folder is decrypted with the private key for the node and sent directly to the TP01 address without going through the engine for EDI processing. The inbound message is encrypted with the public key of the node.
   d. Click **Add**.

Enabling Expired PGP Key Notification

You may also want to turn on notification for expired PGP keys. When this profile is enabled, the customer will be notified when their PGP key is expiring and has expired. Notifications are sent 60, 30, 21, 14, and 7 days before expiration. A message is then sent daily until the PGP key is replaced.

Before you begin

Note: The Expired PGP Key Notify profile should be added to a different address for the customer than their PGP address. When the PGP key expires, Sterling Commerce:Centre will not be able to notify the customer from the PGP address using the expired key.

About this task

Complete the following steps to enable Expired PGP Key notification.

Procedure

1. On the WAT, open the customer's address details page.
2. In the Address Profiles section, click **Add Address Profile**.
3. On the Select Address Profile page, select **Expired PGP Key Notify** from the drop-down list and click **Next**.
4. On the PGP Key Expiration Notification page, do the following:
   a. Select the PGP key from the Installed PGP Keys section.
   b. Select **Enabled** from the Status drop-down list.
   c. Optionally, enter a comment in the Comments/Reason field.
   d. Click **Add**.

About Verifying PGP Keys

All PGP keys need to be verified on the ALF1 test node before they can be loaded to a production node.

The following are the IP addresses for the ALF1 servers:

- APP1: 10.35.76.118
- PRT1: 10.35.76.24
- WEB1: 10.35.76.23

The following are the accounts and addresses available on ALF1 for verifying PGP keys:

- Node_PGP
  - ALF1_PGP
  - DUB3_PGP
  - DUB4_PGP
- PGP Verification
  - Local FTP Address 001
  - testing company name_00x—This is the format for test addresses where “testing company name” is the name of the company whose PGP key are you are testing, and 00x is incremented by 1 for each setup when customers have similar names.

PGP Key Verification Procedure Overview

The PGP key verification procedure includes the following tasks:

1. Preparing for PGP Key Verification
2. Before You Begin PGP Key Verification
3. Load the PGP Key to the Node
4. Set up the Test Addresses on ALF1
5. Send PGP Encrypted Test Files
6. Clean up after PGP Testing

Preparing for PGP Key Verification

About this task

Complete the following steps before testing the PGP key:

Procedure

1. Make sure that the Sterling Commerce:Centre PGP keys have been loaded on the production and test (ALF1) nodes.
2. Make sure that private/public key pairs have been generated for test trading partners. (Use the command line interface of the PGP e-Business Server on the APP server of the test node.)
3. Make sure an FTP test address has been added on the production nodes (referred to in the following procedures as FTPTEST). This address will be used to send test files to and receive test files from customers.
4. For each customer and trading partner, do the following:
   - For trading partners, add the trading partner's public key to the test node. Also, do one of the following:
     - If the trading partner is sending PGP to Sterling B2B Collaboration Network, send the Sterling Commerce:Centre public key to the trading partner.
     - If the trading partner is sending PGP to a customer, send the customer's public key to the trading partner.
   - For customers, add the customer's private key and password to the test node.

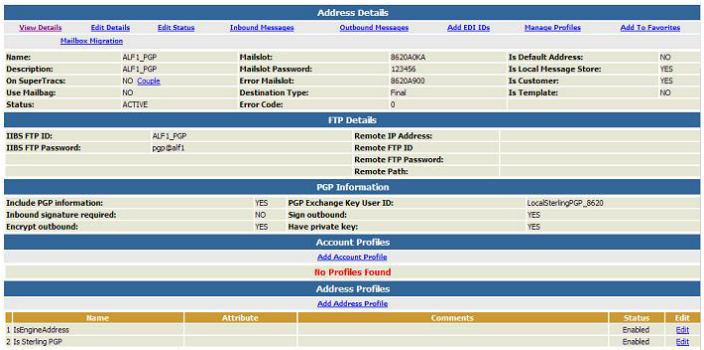
Before You Begin PGP Key Verification

About this task

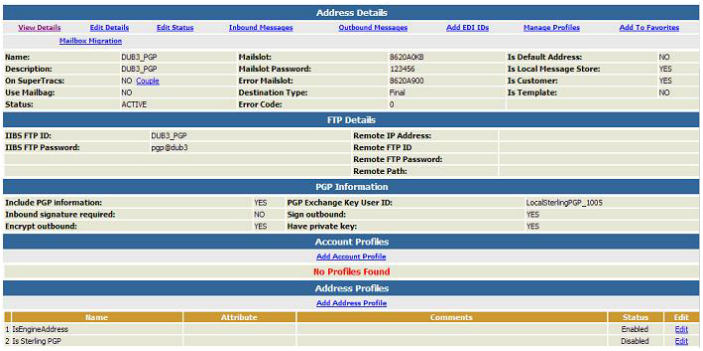
You must complete the following steps before you begin the PGP key verification process.

Procedure

1. Send an e-mail to Sterling Commerce:Centre interested parties and the Certification Center to let them know that you will be testing on ALF1.
2. Verify that APP1, PRT1, and WEB1 are all running the correct services.
3. Verify that the Event Viewers for each server do not show any significant issues.
4. Log on to WEB1 using the ALF1 WAT interface.
5. Search for Node_PGP account.
6. Check each address under Node_PGP to verify that only ALF1_PGP has the IsEngineAddress and IsSterlingPGP profiles **Enabled**.



7. Verify that the DUB3_PGP and DUB4_PGP addresses have the IsSterlingPGP profile **Disabled**.



Loading the PGP Key to the Node

About this task

Complete the following steps to load the PGP key to the node.

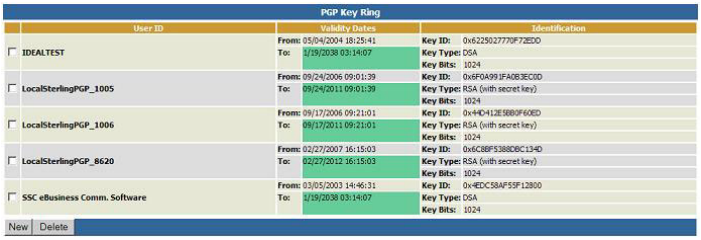
Procedure

1. Select **CSR Access > Certificate Management > PGP Key Ring**.
2. In the list, verify that the key provided by OnBoarding/L1 is *not* included. Click **New**.

   The Upload and Verify page is displayed.
3. Click **Browse** to locate the PGP key.
4. Select the key and click **Upload PGP Key**.

   The file is analyzed and a list of keys contained within the file is displayed.
5. Verify that the Key Type and Key Bits for the new key are supported by Sterling Commerce:Centre.
6. Click **Add PGP Key**.

   The key you added is installed and listed on the Installed Keys page.



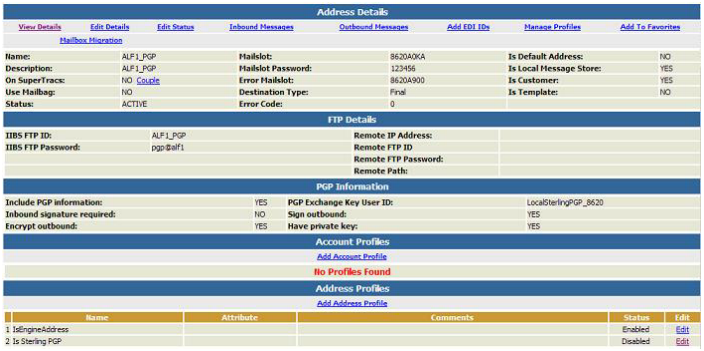
Setting up the Test Addresses on ALF1

About this task

Complete the following steps to set up the test addresses on ALF1.

Procedure

1. Locate the ALF1_PGP address on the Node_PGP account.
2. Disable the IsSterlingPGP profile for that address.



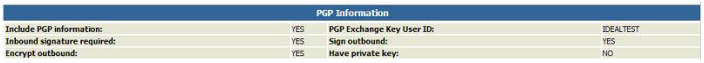
3. Enable the IsSterlingPGP profile on either the DUB3_PGP or DUB4_PGP address. (This will depend on the production node on which the customer's mailbox is setup.)

4. Locate the PGP Verification account.

   The first address for this account is named Local FTP Address 001. The mailslot associated with this address is 8620A0KI.

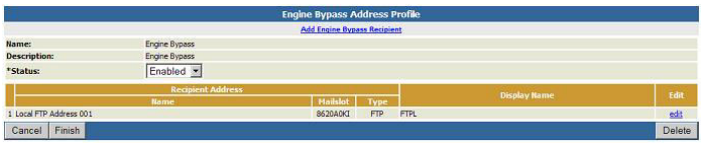
5. Add a new FTP address to this account using naming convention “testing company name_00x” (where x will be incremented by one with each new setup).

6. Set up the PGP Information section with the configuration shown below. Choose the corresponding PGP Exchange Key User ID that was uploaded in “Loading the PGP Key to the Node” on page 35.

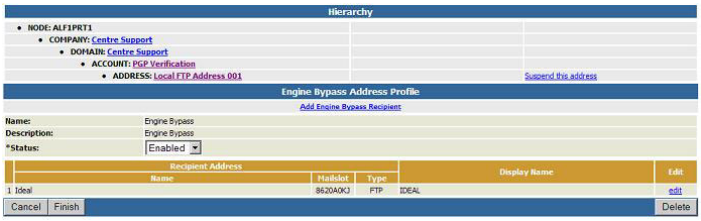


7. Make a note of the new mailslot created. It will be needed in step 9.

8. On this newly created FTP mailslot, add the engine bypass profile as shown below.



9. Go to the Local FTP Address 001 address and configure the Engine Bypass profile. Use the mailslot of the FTP test account created in step 7. Enter a display name that will be used during an FTP session.



Sending PGP Encrypted Test Files

To thoroughly test the key, ask the customer to send test messages and to both encrypt and sign them. This should be done even if the customer does not intend to do this in production.

About this task

Complete the following steps to send PGP encrypted test files.

Procedure

1. Using the encrypted test file sent from Level 1/OnBoarding, open an FTP session to the FTP address that was created for the test customer using IP address 209.95.228.82.
2. Put the test file into the FTPL directory and move it ("rename" it) to the commit directory.
3. Once the FTP session is successful, the file can be traced as an inbound message through the customer test account and as an outbound message in mailslot 8620A0KI.

   The outbound file should be properly decrypted. This decrypted file can be obtained using FTP or picked up through Sterling Commerce:Centre.
4. Using any test data (for example, created in Notepad), open a second FTP session. Log in to mailslot 8620A0KI and put the test data into the directory on the Engine Bypass profile. Ensure that the rename command is completed.
5. Trace the data inbound on address 8620A0KI and outbound on the customer test account. Pick up the outbound file using an FTP "get" session. The file will be encrypted. Send the file to Level 1/OnBoarding, who will send the file back to the test customer.

Clean up after PGP Testing

About this task

Complete the following steps after testing.

Procedure

1. Search for the Node_PGP account. Check each address to verify that only ALF1_PGP has the IsEngineAddress and IsSterlingPGP profiles **Enabled**. The DUB3_PGP and DUB4_PGP addresses should have the IsSterlingPGP profile **Disabled**.
2. Verify that APP1, PRT1, and WEB1 are all running the correct services.
3. Verify that the Event Viewers for each server do not show any significant issues.
4. Send an e-mail Sterling Commerce:Centre interested parties and the Certification Center to notify them that the test on ALF1 is complete.

Potential PGP Issues/Errors

If a file cannot be decrypted, the inbound message will most likely fail with numerous errors on the APP server, in particular. The simplest explanation could be that the customer sent only an encrypted file for testing. The PGP key testing procedure calls for a file that is encrypted and signed.

To confirm this, change the Inbound signature required flag from **YES** to **NO**.

Repeat the FTP test.

If Sterling Commerce:Centre decrypts the customer-provided test file with the Inbound signature required flag set to NO, ask L1/OnBoarding to contact the customer and request a test file that is encrypted and signed. Repeat the test once the new file is received.

If the file still fails, it indicates the potential for more serious problems. Create a ticket and escalate it to L3 Sterling Commerce:Centre.

About Interconnects over FTP

Before Customer Support Representatives (CSRs) can add non-customer IDs to an interconnect, users with a System Administrator security level must set up an account for the VAN on any node.

The VAN setup includes creating a domain (mailbox) for the VAN and creating templates and profiles for the new domain. These setups establish default values that are used by every non-customer trading partner address associated with the VAN.

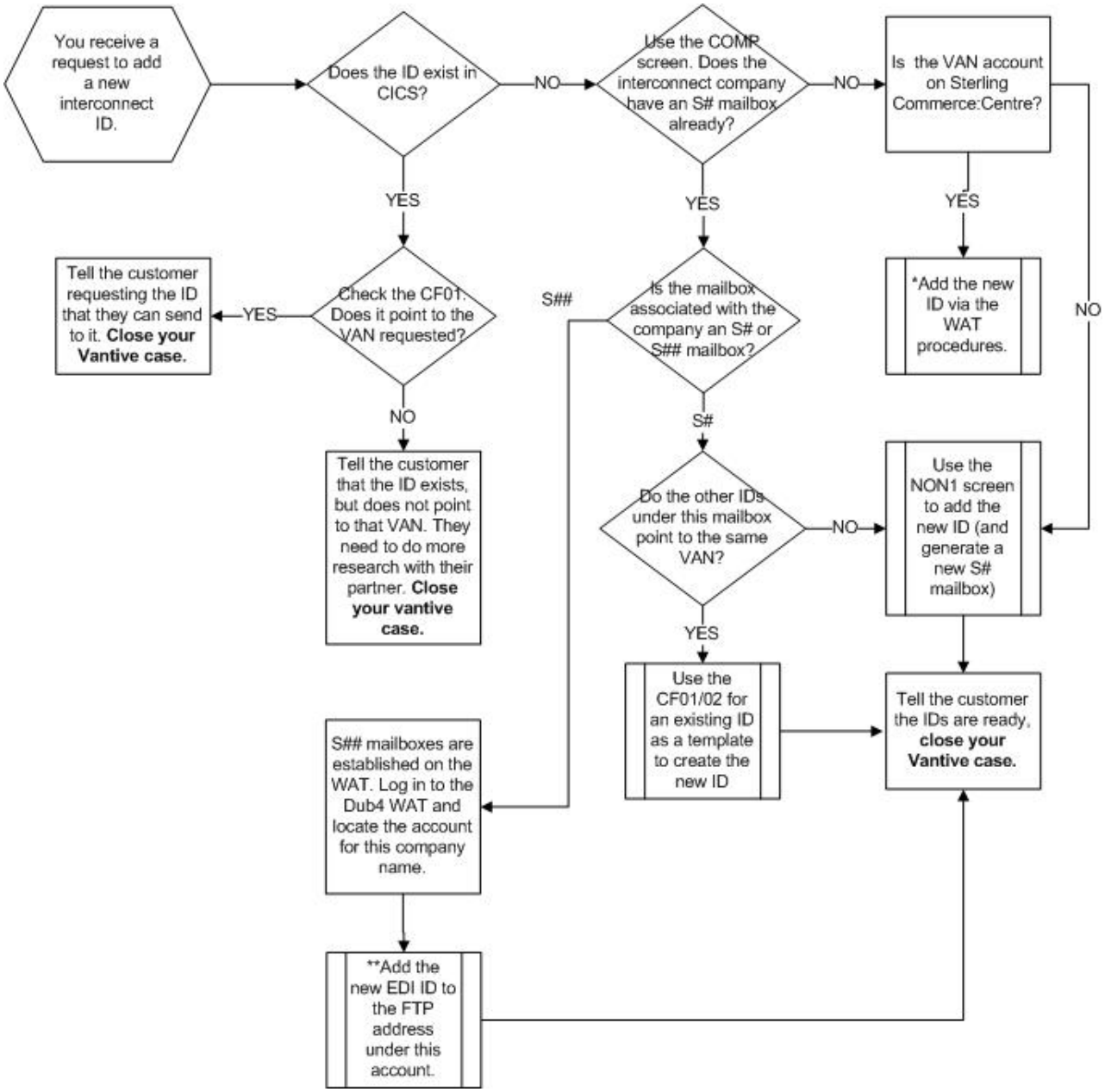
VAN	Interconnect ID on Sterling Commerce:Network for the FTP path	Setups on the Dublin 4 node
EasyLink (AT&T)	MBGMSFTP	Mailbox: S##EL Domain template: Adding an account to the EasyLink domain activates the template, which supplies FTP settings for connecting to EasyLink. Profiles: The EasyLink template enables account and address profiles that supply settings required by the EasyLink FTP system and control the processing of interconnect data on Sterling B2B Collaboration Network. Account profiles: • FastPath (Defer Message Routing) • RouteByMailslotLookup • Defer Parsing Address profiles: None
GXS (General Electric)	MBGEFTP	Mailbox: S##GE Domain template: Adding an account to the GXS domain activates a template, which supplies FTP settings for connecting to GXS. Profiles: The GXS template enables account and address profiles that supply settings required by the GXS FTP system and control the processing of interconnect data on Sterling B2B Collaboration Network. Account profiles: • FastPath (Defer Message Routing) • EDI File Prefix • Defer Parsing Address profiles: • FTP Client Listen Passively • Outbound Message Retry Interval
Kleinschmidt	MBKLEFTP	Mailbox: S##KL Domain template: Adding an account to the Kleinschmidt domain activates a template, which supplies FTP settings for connecting to Kleinschmidt. Profiles: The Kleinschmidt template enables account and address profiles that supply settings required by the Kleinschmidt FTP system and control the processing of interconnect data on Sterling B2B Collaboration Network. Account profiles: • FastPath (Defer Message Routing) • EDI File Prefix • Defer Parsing Address profiles: None

VAN	Interconnect ID on Sterling Commerce:Network for the FTP path	Setups on the Dublin 4 node
Peregrine (Harbinger)	MBHARFTP	Mailbox: S##PG Domain template: Adding an account to the Peregrine domain activates a template, which supplies FTP settings for connecting to Peregrine. Profiles: The Peregrine template enables account and address profiles. These profiles supply settings required by the Peregrine FTP system and control the processing of interconnect data on Sterling B2B Collaboration Network. Account profiles: • FastPath (Defer Message Routing) • RouteByMailslotLookup • Defer Parsing Address profiles: None
Transettlements	MBTRAFTP	Mailbox: S##TS Domain template: Adding an account to the Transettlements domain activates a template, which supplies FTP settings for connecting to Transettlements. Profiles: The Transettlements template enables account and address profiles that supply settings required by the Transettlements FTP system and control the processing of interconnect data on Sterling B2B Collaboration Network. Account profiles: • FastPath (Defer Message Routing) • RouteByMailslotLookup • Defer Parsing Address profiles: None

Note: Refer to the following job aids for additional information:

- Adding a New Interconnect ID
- Adding a New EDI ID for an Existing S## Mailbox

Use the following diagram to determine what steps need to be performed to add an interconnect ID.



Adding Non-customer Account Information and IDs

About this task

Complete the following steps to add account information and IDs for non-customer.

Procedure

1. On Sterling Commerce:Network, check CICS® for the interconnect ID you want to add. If it exists, verify that the ID and the associated VAN are correct.
   - If the ID exists, inform the customer that data can be sent to that ID.
   - If the ID does not exist, go to Step 2.

2. Log in to the WAT on the appropriate node.
3. Select **Search > Company** to search for the VAN you want.
4. On the divider bar, click **Add Account**.
5. Type the account information and click **Next**.
   - Customer name – Company name of the non-customer trading partner
   - Phone – Phone number for the non-customer trading partner
   - Web password – Any 6 characters

     Note: Any mailslot or IIBS password associated with this account must be unique. If you create or edit a mailslot or IIBS configuration under this account using the same password, a Warning message will display forcing you to create a different password.
   - Security level – Mail User
   - Protocol – FTP

   The Address Information page displays.
6. Type the address information. Some settings may be entered automatically because of the template.
   - Be sure that On SuperTracs is not **No**. (A SuperTracs region must be selected.)
   - Be sure that Use Mailbag is **Yes**.
   - Be sure that Destination Type is **Interconnect**.
7. The FTP protocol information is entered automatically because of the template associated with the VAN's domain. Do not change any values. Click **Next**.

   The EDI Information page displays.
8. Type the ID and qualifier for the non-customer trading partner. You can specify up to five pairs to be associated with the address. (If necessary, you can later edit the address to add more EDI IDs.) Click **Next**.
9. Review the information you entered. To change information, use the back arrow in your browser to display the previous page.
10. When you are satisfied, click **Finish**.

    The Account List page redisplays. The new account has a status of **Add Pending**, which indicates that the account is being replicated to Sterling Commerce:Network.
11. Wait a minute or two, then refresh your browser window. The Status field changes to **Active**.
12. Return to CICS to verify that the account is replicated correctly on Sterling Commerce:Network. Use the MB01, CF01, and CF02 screens to check for the new mailslot (address) and non-customer ID.
    - If you find the mailslot and ID in CICS, go to step 13.
    - If the status in step 10 is Active but you cannot find the mailslot or ID in CICS, contact Level 2 for assistance.
13. Tell the customer that data can be sent to the new non-customer ID.

Adding Non-customer IDs to an Existing S## Account (Mailbox)

You can add another non-customer ID for a trading partner that has an existing mailslot (address) on the node.

About this task

Complete the following steps to add a non-customer ID to an existing S## mailbox.

Procedure

1. Log in to the WAT on the Dublin 4 node.
2. Select **Search > EDI Info**.
3. In the Mailslot field, type the S## mailbox number and click **Search**.

   A list of the mailslots (addresses) in the S## mailbox displays.
4. Click the mailslot you want. (The same mailslot may appear on more than one line. Click one of them.)

   Address Details for the non-customer display, including a list of EDI IDs associated with this address.
5. On the divider bar, click **Add EDI IDs**.

   The EDI Information page displays.
6. Type the EDI ID and qualifier and click **Finish**.
7. Wait a minute or two. Return to CICS and check for the new ID on the CF01 and CF02 screens. This step verifies that the information is replicated to Sterling Commerce:Network.
   - If you find the ID in CICS, go to step 8.
   - If you do *not* find the ID in CICS after 30 minutes, contact Level 2 for assistance.
8. Tell the customer that data can be sent to the new non-customer ID.

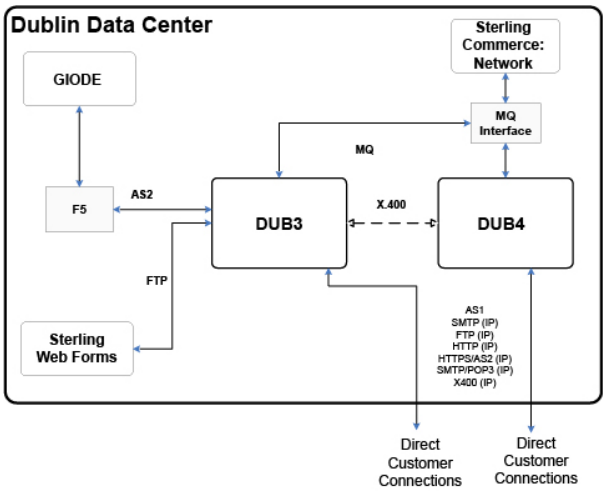
Chapter 4. Supporting Sterling Commerce:Centre

Sterling Commerce:Centre Data Flows

Sterling Commerce:Centre supports several different protocols, each using a different data flow.

The Dublin Data Center houses both Dub3 and Dub4.

The following diagram shows a high-level data flow



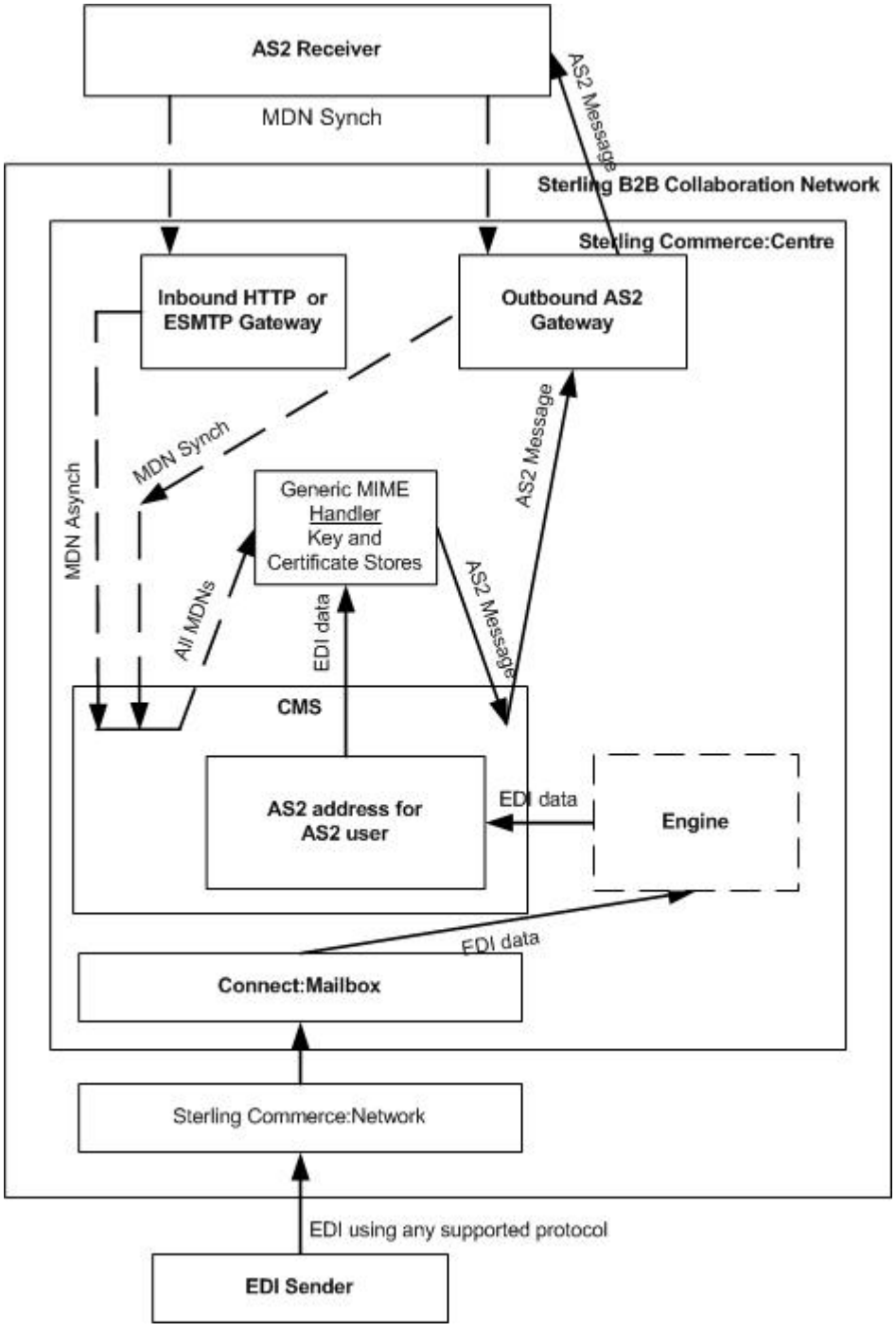
Direct customer connections are established using the following protocols: ANX, AS1, AS2, FTP, HTTP, HTTPS, SMTP, and X.400.

AS2 Data Flows

The AS2 data flows, both inbound and outbound, require Message Disposition Notifications (MDNs).

EDI Sender to AS2 Inbound

The following diagram shows the EDI sender to AS2 receiver data flow.

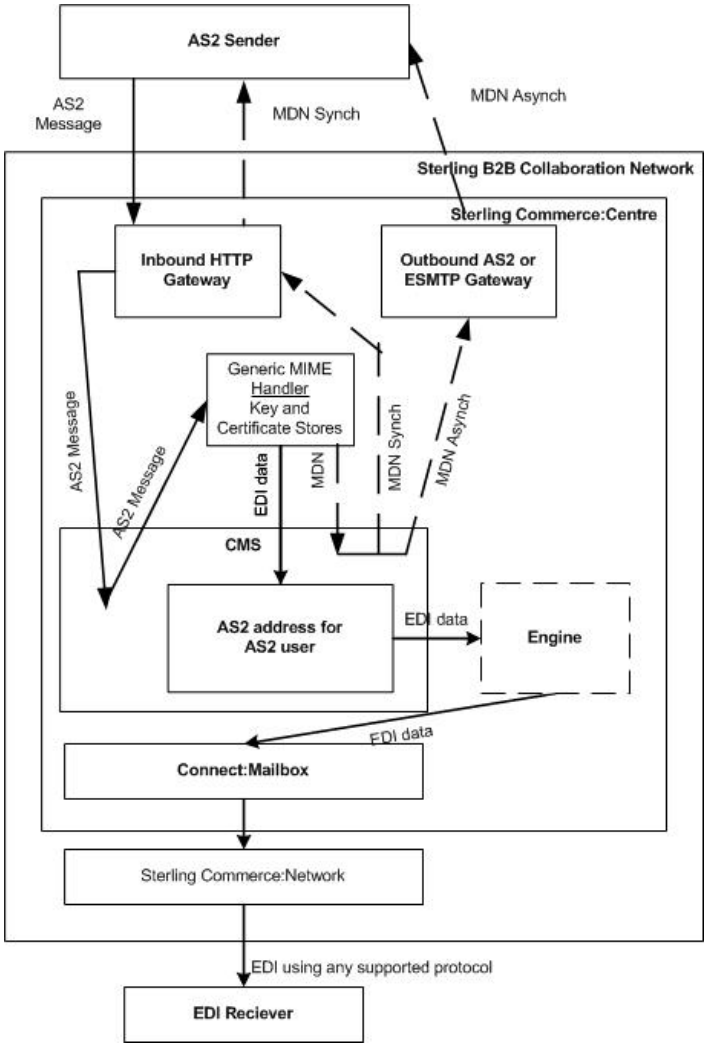


EDI Sender to AS2 Receiver	Tracking Point
The sender sends standard EDI data to a Sterling Commerce:Network mailbox using any supported protocol. Sterling Commerce:Network parses the data and uses the EDI ID of the receiver to route the message to Sterling Commerce:Centre.	AUDI and other standard CICS tracking screens

EDI Sender to AS2 Receiver	Tracking Point
Sterling Commerce:Centre routes the message to the receiver's AS2 address.	Inbound message through Connect:Mailbox to the AS2 address of the receiver
Sterling Commerce:Centre encrypts and signs the data and delivers it to the AS2 receiver over HTTP or HTTPS.	The transaction ID links the original inbound message with the outbound message going to the receiver.
The AS2 receiver receives the data and returns an MDN to Sterling Commerce:Centre. Synchronous MDNs are returned in the same session to the same outbound AS2 gateway (for HTTP). Asynchronous MDNs are returned in another session either by the inbound HTTP gateway (for AS2) or by the inbound ESMTP gateway (for e-mail).	The MTS ID links the outbound message with the inbound MDNs.

AS2 Outbound to EDI Receiver

The following diagram shows the AS2 sender to EDI receiver data flow.

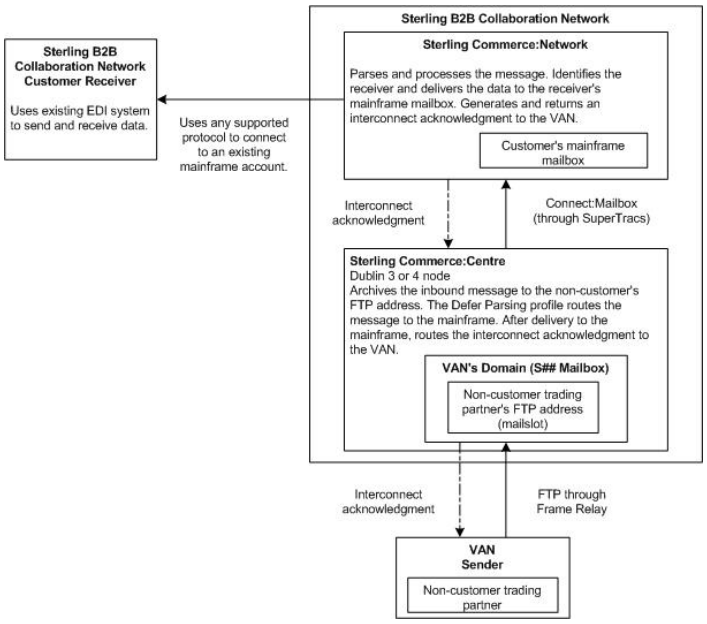


AS2 Sender to EDI Receiver	Tracking Point
The sender sends AS2 data to an AS2 address on Sterling Commerce:Centre. Transmissions are sent over HTTP or HTTPS.	HTTPS protocol connector on Sterling Commerce:Centre
Inbound message to the AS2 address for the sender.	Sterling Commerce:Centre performs security processing (such as authentication and decryption) and returns an MDN to the AS2 sender. Synchronous MDNs are returned in the same session by the same inbound HTTP gateway. Asynchronous MDNs are returned in another session either by the outbound AS2 gateway (for HTTP) or by the outbound ESMTP gateway (for e-mail).
The MTS ID links the original inbound message and the outbound MDNs.	
The decrypted and unpackaged message is routed to the Engine, which parses the message and identifies the EDI ID of the receiver. The receiver has a Sterling Commerce:Network mailbox.	The transaction ID links the original inbound message going to the Engine with the outbound message going to Sterling Commerce:Network through Connect:Mailbox.
Sterling Commerce:Network receives the inbound EDI data, parses it, and delivers it to the receiver.	AUDI and other standard CICS tracking screens.

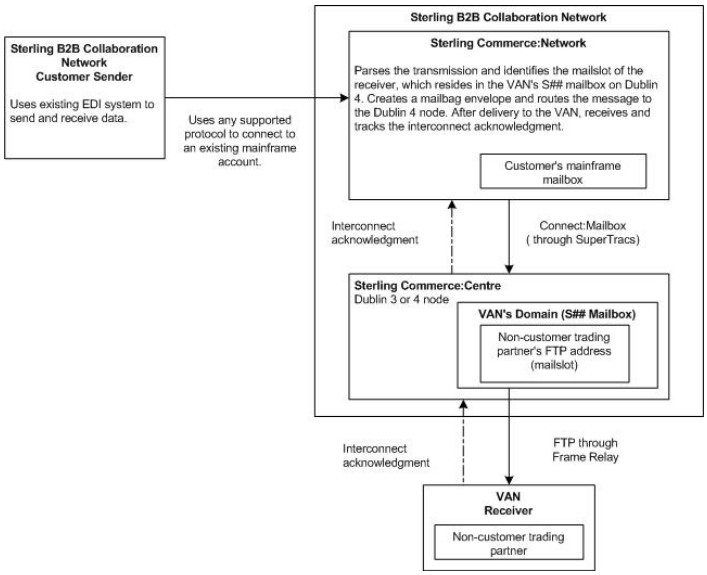
Interconnect Data Flows

Interconnect data is sent over FTP.

Inbound from VAN over FTP Interconnect



Outbound to VAN over FTP Interconnect



PGP over FTP Data Flows

Customers who require additional security for their FTP data can use Pretty Good Privacy (PGP) over FTP. The PGP over FTP feature is set up at the mailslot level.

PGP uses both public-key and private-key cryptography and includes a system that connects the public key to a user's identity. The message recipient must have previously generated a linked-key pair, which includes a public key and a private key.

The sender uses the recipient's public key to encrypt a session key, which is then used to encrypt the text of the message. The message recipient decrypts the message using the session key, which was included in the message in encrypted form and is decrypted using the recipient's private key.

A similar strategy is used to detect whether a message has been altered since it was completed and whether it was sent by the company claiming to be the sender. The sender uses PGP to add to the message a signature that is created using their private key.

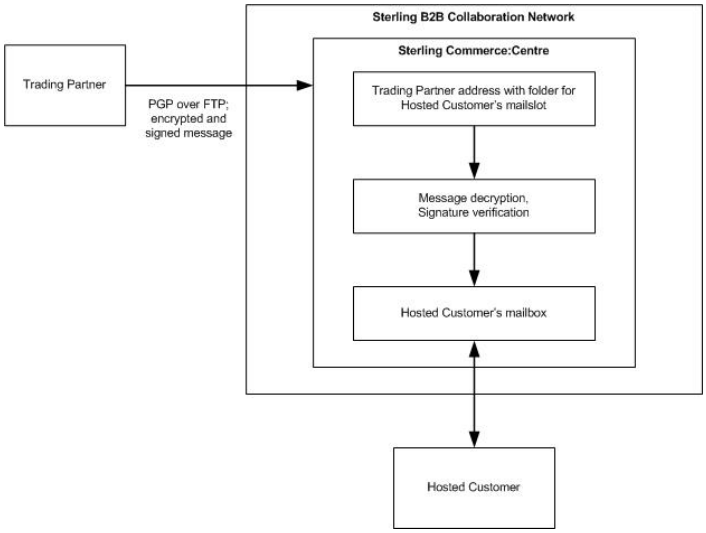
Sterling Commerce:Centre performs the following actions:

- Performs PGP decryption and digital signature verification as messages enter the node.
- Performs PGP encryption and digital signature generation as messages leave the node.
- Holds the public PGP keys of customers. Optionally, holds the private keys of customers.

Data Flow: Trading Partner to Hosted Customer

The trading partner's Sterling Commerce:Centre address has a folder for the hosted customer's mailslot. If using PGP encryption, the trading partner has their Sterling Commerce:Centre FTP address configured for PGP encryption with the Engine Bypass profile.

The following diagram shows the Trading Partner to Hosted Customer data flow:

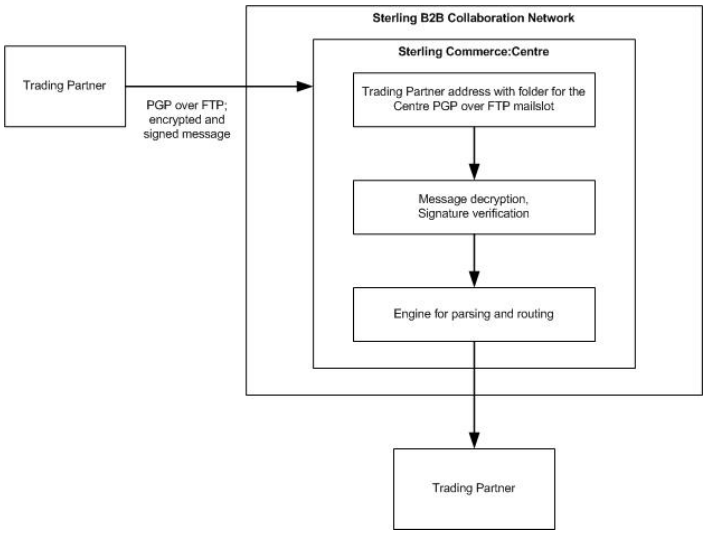


1. If using PGP encryption, trading partners encrypts the message with the customer's public key and, possibly, sign it with their own private key.
2. They log in to their Sterling Commerce:Centre account and place the message in the appropriate hosted customer folder. After upload is successful, they copy the message into the hosted customer's commit folder.
3. If using PGP encryption, Sterling Commerce:Centre decrypts the message using the hosted customer's private key and verifies the signature using the trading partner's public key.
4. Sterling Commerce:Centre then routes the plain text data to the hosted customer's mailslot.
5. The message is delivered.

Data Flow: Trading Partner to Trading Partner

The trading partners have their Sterling Commerce:Centre PGP address configured with the Engine Bypass profile. This address has a folder for the Sterling Commerce:Centre mailslot. This address is configured with the IsSterlingPGP profile.

The following diagram shows the Trading Partner to Trading Partner data flow:



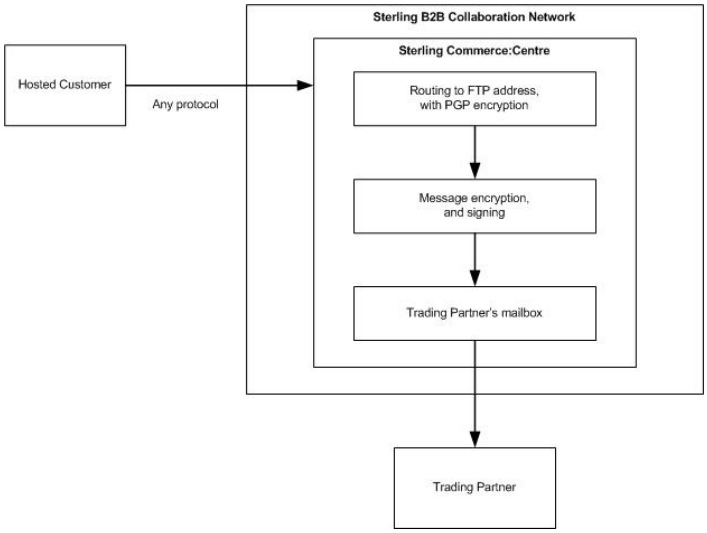
1. The trading partners encrypt the message with the Sterling Commerce:Centre public key and, possibly, sign it with their private key.
2. They log in to their Sterling Commerce:Centre account and place the message in the appropriate Sterling\commit folder.
3. Sterling Commerce:Centre decrypts the message using the private key for the Sterling Commerce:Centre node and verifies the signature using the trading partner's public key.
4. The plain text data is routed to the Engine where it is parsed and then routed appropriately.

Data Flow: Hosted Customer to Trading Partner

Hosted customers have a Sterling Commerce:Centre address configured as PGP with a private key. Their data can come in as non-PGP, probably from Sterling Commerce:Network. In this case, inbound processing is normal. To be able to handle messages coming back from the trading partner, the hosted customer address will also have to have the Defer Routing profile enabled.

Hosted customers may choose to send a message into Sterling Commerce:Centre using a PGP address. In which case, they will use the Trading Partner to Trading Partner method described above. It is during outbound processing that the hosted customer-specific actions take place. Processing is no different if the Hosted Customer is sending to another Hosted Customer.

The following diagram shows the Hosted Customer to Trading Partner data flow:



About Deleting Accounts, Addresses, and EDI IDs

You can delete an account, an address, or an EDI ID. Deleting an account removes all addresses and EDI IDs beneath it in the account hierarchy. Deleting an address removes the mailslot and any EDI IDs attached to it. In addition, messages and EDI interchange information in the Sterling Commerce:Centre database are also deleted. Consequently, no EDI interchange information, no inbound messages, and no outbound messages are displayed for a deleted address.

Deleting an Account or an Address Immediately

Your user account must be set up to allow you to edit account details. If your user account is set as Read Only, then the Add, Edit, and Delete buttons will not be available to you.

About this task

Complete the following steps to delete an account or address.

Procedure

1. Open the WAT on the node you want.
2. Display the Account Details or Address Details, depending on which level you want to remove.
3. On the divider bar, click **Edit**.
4. Verify that the account or address is the one you want. On the bottom-right, click **Delete**.
5. Click **OK** when you are prompted to confirm the deletion. The account or address is removed.

   If an address is coupled with a Sterling Commerce:Network mailslot, the Sterling Commerce:Network mailslot is removed first and then the node address is removed. When processing is complete, the details for the remaining parent level are displayed, either Domain Details or Account Details.

   When the last address is deleted, the account is deleted.

Deleting an EDI ID from an Address Immediately

Your user account must be set up to allow you to edit account details. If your user account is set as Read Only, then the Add, Edit, and Delete buttons will not be available to you.

About this task

Complete the following steps to delete an EDI ID from an address.

Procedure

1. Open the WAT on the node you want.
2. Display the Address Details for the EDI ID you want.
3. In the list of EDI IDs, locate the EDI ID you want and click **Edit** to the right of the entry.
4. Verify that the EDI ID is the one you want. On the bottom-right, click **Delete**.
5. Click **OK** when you are prompted to confirm the deletion. The EDI ID is removed and Address Details redisplays. If the EDI ID is coupled with an EDI ID in a Sterling Commerce:Network mailslot, it is removed first from the Sterling Commerce:Network mailslot and then from the address on the node.

About Updating Accounts, Addresses, and EDI IDs

You can perform the procedures described in the following topics for accounts, addresses, and EDI IDs.

Note: Your user account must be set up to allow you to edit account details. If your user account is set as Read Only, then the **Add**, **Edit**, and **Delete** buttons will not be available to you.

To list accounts, addresses, or EDI IDs, open the WAT on the node and do one of the following:

- To list all accounts in a company-domain, display the Domain Details. On the divider bar, click **View Details**.

- To filter accounts by their status, display the Domain Details. On the divider bar, click **View Details**. Then select the account status you want and click **Filter**.
- To list all addresses for an account, display the Account Details. On the divider bar, click **View Details**.
- To list all EDI IDs for an address, display the Address Details.

Updating Account Information

Updating account information affects all associated addresses and EDI IDs. If items exist on Sterling Commerce:Network, changes are replicated to Sterling Commerce:Network.

Before you begin

Note: Be aware of the following limitations:

- You cannot use this procedure to update the Status field.
- You cannot update an account if any of its addresses or EDI IDs have a status of Add Pending, Update Pending, Delete Pending, Couple Pending, Decouple Pending, Migration Pending, or Delete Succeeded.

About this task

Complete the following steps to update account information.

Procedure

1. Open the WAT on the node you want.
2. Display the Account Details.
3. On the divider bar, click **Edit Details**.
4. Enter the changes and click **Update**.

   If the changes are being replicated to Sterling Commerce:Network, the status of all associated addresses and EDI IDs changes to Update Pending. If the status becomes Update Failed, the changes remain on the node but have not been replicated to Sterling Commerce:Network. In this case, contact Level 2 to resolve the problem.

Updating Address Information

Updating address information affects all associated EDI IDs. If items exist on Sterling Commerce:Network, changes are replicated to Sterling Commerce:Network.

Before you begin

Note: Be aware of the following limitations:

- You cannot use this procedure to update the Status field.
- You cannot update an address if its status or the status of an EDI ID is Add Pending, Update Pending, Delete Pending, Couple Pending, Decouple Pending, Migration Pending, or Delete Succeeded.
- You cannot change the Mailslot value. Doing so may disrupt billing records. Instead, add a new address, migrate the EDI IDs to the new address, and then delete the old address.
- Generally, do not edit the On SuperTracs setting. Instead, redisplay Address Details and use Couple or Decouple. (Only update the On SuperTracs setting if the node and Sterling Commerce:Network are not synchronized.)

About this task

Complete the following steps to update address information.

Procedure

1. Open the WAT on the node you want.
2. Display the Address Details.
3. On the divider bar, click **Edit Details**.
4. Enter the changes and click **Update**.

   If the changes are being replicated to Sterling Commerce:Network, the status of all associated EDI IDs changes to Update Pending. If the status becomes Update Failed, the changes remain on the node but have not been replicated to Sterling Commerce:Network. In this case, contact Level 2 to resolve the problem.

Updating an EDI ID

If an EDI ID exists on Sterling Commerce:Network, changes are replicated to Sterling Commerce:Network.

Before you begin

Note: Be aware of the following limitations:

- You cannot use this procedure to update the Status field.
- You cannot update an EDI ID if its status is Add Pending, Update Pending, Delete Pending, Couple Pending, Decouple Pending, Migration Pending, or Delete Succeeded.
- You cannot change the EDI ID or qualifier. Instead, add a new EDI ID and qualifier before deleting the old one.
- Generally, do not change the On CNet setting for an EDI ID. Instead, use Couple or Decouple. (Only update the On CNet setting if the node and Sterling Commerce:Network are known to be out of synchronization.)

About this task

Complete the following steps to update an EDI ID.

Procedure

1. Open the WAT on the node you want.
2. Display the Address Details.
3. In the list of EDI IDs, locate the EDI ID you want and click **Edit** to the right of the entry.
4. Enter the changes and click **Update**.

   If the changes are being replicated to Sterling Commerce:Network, the status changes to Update Pending. If the status becomes Update Failed, the changes remain on the node but have not been replicated to Sterling Commerce:Network. In this case, contact Level 2 to resolve the problem.

Updating the Status of an Account, Address, or EDI ID

Only users with System Administrator or Super User security level can update the status of an account, address, or EDI ID. Changes to the status of an item affect the information on the node *only* and do not replicate to Sterling Commerce:Network.

About this task

Complete the following steps to update the status of an account, address, or EDI ID.

Procedure

1. Open the WAT on the node you want.
2. Choose the level of your change:
   - Updating the status of an account affects all associated addresses and EDI IDs. Display Account Details. On the divider bar, click **Edit Status**.
   - Updating the status of an address affects all associated EDI IDs. Display Address Details. On the divider bar, click **Edit Status**.
   - To update the status of an EDI ID, display Address Details. Locate the EDI ID you want in the EDI Information at the bottom of the page. In the **Status** column, click **Edit**.
3. Change the status to **Active**, **Inactive**, or **Delayed Delete**. No other status should be assigned manually.

   Note: Changing the status of the address to Inactive disables the address and blocks inbound traffic.
4. Click **Update**.

Suspending an Address

Only users with a System Administrator security level can suspend an address.

About this task

Complete the following steps to update the status of an account, address, or EDI ID.

Procedure

1. Open the WAT on the node you want.
2. Navigate to the account.
3. At the address level in the hierarchy portion of the screen, click **Suspend this address**.
4. On the Suspend Account Profile, select a status of **Enabled** to enable the suspension.

   Note: Disable ends the suspension and re-activates the address.
5. Type a **Reason/Comment** for the suspension.

   Note: This is a required field.
6. Type an **Expiration Date/Time**.

   The dates/times listed on the right are a cheat sheet that allow you to quickly copy/paste your selection.
7. Click **Finish**.

Results

As the expiration time for the suspension nears, if the customer's problem has not been resolved, you may need to change the expiration date/time. From the Account Details, click **Edit/Resume** and update the Expiration Date/Time.

When the customer's problem has been resolved, you need to disable the suspension to re-activate the address. From the Account Details, click **Edit/Resume** and change the status to **Disabled**.

About Coupling and Decoupling Addresses and EDI IDs

To route data from Sterling Commerce:Network to the node, you must set up an address (mailslot) and its EDI IDs on the node and on Sterling Commerce:Network. Internally, Sterling Commerce:Network flags the mailslot as one that is owned by the node. This ownership flag allows Sterling Commerce:Network to route data to the node.

Coupling and decoupling refers to the connection between an address or EDI ID on the node and its associated Sterling Commerce:Network mailslot or EDI ID. When you add an address to the node, you indicate whether a Sterling Commerce:Network mailslot is added at the same time. If an address is coupled with a Sterling Commerce:Network mailslot, you can indicate whether its EDI IDs are also added to the Sterling Commerce:Network mailslot. Later, you can reverse these initial decisions by coupling or decoupling the address or the EDI IDs.

- When you couple an address or EDI ID, you take an item that exists on the node and add it to Sterling Commerce:Network.
- When you decouple an address or EDI ID, you delete the item from Sterling Commerce:Network but leave it on the node.

Internally, coupling and decoupling changes the value of the On SuperTracs setting, a process that creates or removes the associated Sterling Commerce:Network item.

Coupling or Decoupling an Address

About this task

Complete the following steps to couple or decouple an address.

Procedure

1. Open the WAT on the node you want.
2. Display the Address Details for the address you want.
3. To the right of the On SuperTracs field, click **Couple** or **Decouple**.

   To Couple, select a SuperTracs region from the drop-down menu.

   A dialog box displays information about your choice.
4. To continue, click **Here** at the top of the dialog box.

   You are prompted that the process has started.
5. Click **Here** at the bottom of the prompt.

   The Address Details are redisplayed.

   - If you are coupling an address, the status of the address changes to Couple Pending, indicating that the Sterling Commerce:Network mailslot is being added. If the addition fails, the status indicates Couple Failed and the On SuperTracs setting remains No. If the addition succeeds, the status indicates Active and the On SuperTracs setting changes to the region you selected.
   - If you are decoupling an address, the status of the address changes to Decouple Pending, indicating that the Sterling Commerce:Network mailslot is being removed. If the deletion fails, the status indicates Decouple Failed

and the On SuperTracs setting retains its value. If the deletion succeeds, the status indicates Active and the On SuperTracs setting changes to No.

Coupling or Decoupling an EDI ID

To couple or decouple an EDI ID, the address must already be coupled with a Sterling Commerce:Network mailslot. (The On SuperTracs setting for the address is a SuperTracs region.)

About this task

Complete the following steps to couple or decouple an address.

Procedure

1. Open the WAT on the node you want.
2. Display the Address Details for the EDI ID you want.
3. In the EDI IDs section, locate the EDI ID that you want.
4. In the On CNet column, click **Couple** or **Decouple**.
   A dialog box displays information about your choice.
5. To continue, click **Here** at the top of the dialog box.
   A prompt indicates that the process has started.
6. Click **Here** at the bottom of the prompt.
   The Address Details are redisplayed.
   - If you are coupling an EDI ID, the status of the EDI changes to Couple Pending, indicating that the EDI ID is being added to the Sterling Commerce:Network mailslot associated with the current address. If the addition fails, the status indicates Couple Failed and the On CNet setting remains No. If the addition succeeds, the status indicates Active and the On CNet setting changes to Yes.
   - If you are decoupling an EDI ID, the status of the EDI changes to Decouple Pending, indicating that the EDI ID is being removed from the Sterling Commerce:Network mailslot associated with the current address. If the deletion fails, the status indicates Decouple Failed and the On CNet setting remains Yes. If the deletion succeeds, the status indicates Active and the On CNet setting changes to No.

About Migrating EDI IDs

You can migrate all or individual EDI IDs in one mailslot to another mailslot. If the migration is not successful, error codes are displayed on Account, Address, and EDI Information pages.

The following types of migrations are allowed:

- Sterling Commerce:Network to a Sterling Commerce:Centre node
- Sterling Commerce:Centre to Sterling Commerce:Centre on the same node
- Sterling Commerce:Centre to Sterling Commerce:Centre on different nodes

Limitations

Be aware of the following limitations:

- Migrations must be enabled on the node. This is configurable in SCConfigurationParams.

- The source and target mailslots must be different. If you migrate all mailslots in a mailbox, the destination mailslot must reside in a different mailbox.
- If the destination is on Sterling Commerce:Centre, the destination mailslot must exist and have a status of Active.
- If migrating from Sterling Commerce:Centre to Sterling Commerce:Network or from Sterling Commerce:Centre to Sterling Commerce:Centre on the same node, the source mailslot must exist and have a status of Active.
- If the source is on Sterling Commerce:Centre:
  - For mailslot migration, the mailslot must have at least one EDI ID/qualifier pair.
  - For EDI migration, the specified EDI ID/qualifier pair must exist.
- If migrating from Sterling Commerce:Centre to Sterling Commerce:Centre on the same node, both source and destination must have the same value for the On SuperTracs flag.
- If migrating from Sterling Commerce:Centre to Sterling Commerce:Centre on different nodes, both source and destination must not have the On SuperTracs flag set to No.
- If migrating from Sterling Commerce:Network to Sterling Commerce:Centre, the destination mailslot must not have the On SuperTracs flag set to No.

Migration Strategy

Before you begin, you should determine your migration strategy. Consider the following factors:

Migration Goal	Prerequisite Specifications	Processing Description
Migrate EDI IDs from a source mailbox on Sterling Commerce:Network to a target address (mailslot) on the node.	The source mailbox and its mailslots reside on Sterling Commerce:Network. The target address on the node is coupled with a Sterling Commerce:Network mailslot (On SuperTracs is set to a SuperTracs region).	The EDI IDs are migrated on Sterling Commerce:Network first. During this process, the node displays a Migration Pending status. If Sterling Commerce:Network migration fails, the process stops and the node displays a Migration Failed status. If Sterling Commerce:Network migration is successful, the EDI IDs are migrated to the target address on the node. The source mailbox on Sterling Commerce:Network is deleted. A message on Sterling Commerce:Network indicates that the target mailslot is owned by the node.
Migrate EDI IDs from a source mailslot on the node to a target address (mailslot) on Sterling Commerce:Network.	The source mailslot resides on the node. The target mailslot resides on Sterling Commerce:Network.	The EDI IDs are migrated to Sterling Commerce:Network. During this process, the node displays a Migration Pending status. If Sterling Commerce:Network migration fails, the process stops and the node displays a Migration Failed status.
Migrate EDI IDs from a source mailslot on one node to a target address on the same node.	The source account and the target address reside on the same node. Both source and destination mailslots must have the same value for the On SuperTracs flag.	The EDI IDs are migrated from the source account to the target address on the same node. The source EDI IDs are then deleted.

Migration Goal	Prerequisite Specifications	Processing Description
Migrate EDI IDs from a source mailslot on one node to a target address on different nodes.	The source address and the target address reside on different nodes. The On SuperTracs flag must *not* be set to No for both source and destination mailslots.	The EDI IDs are migrated from the source address on one node to the target address on other node. The source EDI IDs are then deleted.

Migrating EDI IDs

Before you begin

You must know the names of the source and target mailslots.

About this task

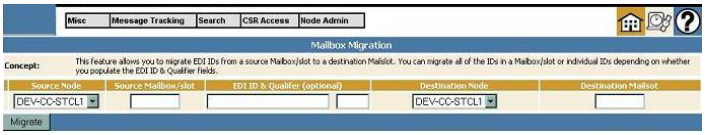
Complete the following steps to migrate an EDI ID.

Procedure

1. Open the WAT on the node you want.
2. Select **CSR Access > Mailbox Migration**.

   Alternatively, navigate to the destination address and click **Mailbox Migration**.

   The Mailbox Migration screen is displayed:



3. Select the Source Node from the drop-down list.
4. Enter the accounts to be migrated:
   - To migrate all EDI IDs in a mailbox, type the five-character mailbox name followed by an asterisk (*) in the Source Mailbox/slot field.
   - To migrate the EDI IDs in a single mailslot, type the address name in the Source Mailbox/slot field. If the source is on Sterling Commerce:Centre, the address name is eight characters long. If the source in on Sterling Commerce:Network, the address name is between six and eight characters long.
   - To migrate an individual EDI ID, type the mailbox name or mailslot address name in the Source Mailbox/slot field and type the EDI ID in the EDI ID & Qualifier fields.
5. Select the Destination Node from the drop-down list, if it is not already selected.
6. Enter the Destination Mailslot. If you are performing this procedure from the destination address, this field is automatically populated.
7. Click **Migrate**.

   The EDI IDs are migrated.

Trading Partner IDs

Some services or trading partners require two systems of identifiers.

Traditional EDI IDs are used to identify a trading partner in traditional EDI data, and another identifier is used to identify the same trading partner in other data or for other purposes.

You can use the WAT interface to search for and set up a cross-reference between two identifiers.

Searching for a Cross Reference

About this task

Complete the following steps to search for a cross reference.

Procedure

1. Open the WAT on the node you want.
2. Select **CSR Access > Trading Partner ID Mgmt**.
3. Click **Search Cross Reference**.
4. Complete at least one of the following fields and click **Search**.
   - EDI ID – Identifier for the trading partner that is used in EDI data.
   - EDI ID Qualifier – Qualifier associated with the EDI ID in EDI data.
   - Trading Partner ID – Identifier for the trading partner that is used in other data or for other purposes.
   - Cross Reference Type:

     AS2 Hosted Customer – This identifier is used in the Identifier field on the AS2 Address page and associates the customer with the correct certificates.
   - Items per Page – Number of records you want to see in one page of the browser when the results are displayed.

Adding a Cross Reference

About this task

Complete the following steps to add a cross reference.

Procedure

1. Open the WAT on the node you want.
2. On the CSR menu, select **Trading Partner ID Mgmt.**
3. Click **Add Cross Reference**.
4. Complete the following information and click **Add**.
   - EDI ID – Identifier for the trading partner that is used in EDI data.
   - EDI ID Qualifier – Qualifier associated with the EDI ID in EDI data.
   - Trading Partner ID – Identifier for the trading partner that is used in other data or for another purpose.
   - Cross Reference Type:
     - AS2 Hosted Customer – This identifier is used in the Identifier field on the AS2 Address page and associates the customer with the correct certificates.
     - EBMX Member ID – This identifier is used in the site command to the Chrysler FTP server.

MSMQ Message Monitoring

MSMQ message monitoring is performed using the MQ View Web site, which is accessible from Production Citrix:

- Dub3 — ccdub3mqview.comm2.sci.local:54323
- Dub4 — ccdub4mqview.comm2.sci.local:54323

This Web site allows you to view MSMQ and IBM MQ messages. In addition, you can resurrect messages on the MSMQ Deadletter queues.

Chapter 5. Searching for Accounts, Addresses, and Messages

Searches

Your security level controls what types of searches you can perform, the range of information included in the search, and the results of your searches.

Where you begin your search also affects the range of information included in the search. For example, if you search for inbound messages from the Message Tracking menu, you search for all inbound messages for all accounts that you can access on the entire node. If you drill down to one account and begin your search from the Inbound link on the divider bar, you limit your search to the inbound messages for the selected account. Similarly, if you search for inbound messages from the Company Details page, only messages for the selected company are included in the search.

Required Fields

When you enter criteria on a search page, an asterisk (*) indicates that a field is required. You must enter information in that field to conduct the search.

Using Wildcard Characters and Substrings

A wildcard character is one that represents any other character. Searches support two wildcard characters:

- Use the percent sign (%) to search for a string of characters. Any number of any type of character will be a match.
- Use the underscore (_) to match a single character. One character of any type in that position will be a match.

You can also enter the initial portion (or substring) of what you want to find. For example, you can enter **s** to search for all company names beginning with **s**. You can enter initial substrings when you search for accounts by company name, by EDI information, and by address protocol. When you track messages, you can enter initial substrings when you search by EDI interchange. However, you must enter complete information when you search for messages by IDs, such as message ID or transaction ID.

Note: To search the application logs, you must use the exact Message ID or Session ID. You cannot use wildcard characters.

Combination Values

In general, choices in the WAT that are in all capital letters are combinations of other values (for example, ALL).

Search Criteria

You can search for *accounts* if you know any of the following:

- Company name
- Domain name
- Account name, phone, or other information

- EDI ID
- Mailbox
- Mailslot
- Protocol information

You can search the *application logs* by Message ID or by Session ID.

You can search for entries in the *housekeeping log*.

You can search for *inbound* and *outbound messages* if you know any of the following:

- Message ID
- Transaction ID
- EDI interchange information
- Sterling Commerce:Network batch number
- MTS ID
- Association ID and type
- Subject

Viewing Search Results

When your search results are displayed, the status bar indicates how many items were returned. Use the scrolling buttons to move through the results.

Button	Description
	Move to the first page of results.
	Move to the previous page of results.
	Move to the previous result.
	Move to the next result.
	Move to the next page of results.
	Move to the last page of results.

Searching for Accounts by Account Information

Searching by account information displays a list of accounts that match your criteria. From the list, you can drill down to account and address details.

About this task

Complete the following steps to search for accounts by account number.

Procedure

1. Open the WAT on the node you want.
2. Select **Search > Account**.
3. Type the following information and click **Search**.
   - Name – Name of the account, usually the name of a contact at the company.
   - Status – Status of the account. See Account and Address Status Codes.
   - C:Network Error Code – Code generated when the EDI ID is migrated from one mailslot address to another mailslot address. See Error Codes in Account, Address, and EDI Information.
   - Telephone number and address, including the country

   Note: To specify the number of records you want to see in one page of the browser when the results are displayed, use the Items Per Page option.

Searching for Accounts by Company

Searching by company name displays a list of companies that match your criteria. From the list, you can drill down to domain, account, and address details. However, company searches are not the most efficient because there may be differences between what you search for and how company information is entered in back-end systems.

About this task

Complete the following steps to search for accounts by company.

Procedure

1. Open the WAT on the node you want.
2. Select **Search > Company**.
3. Type at least the beginning of the company name and click **Search**.

   Note: To specify the number of records you want to see in one page of the browser when the results are displayed, use the Items Per Page option.

Searching for Accounts by Domain or Mailbox

Searching by domain name displays a list of domains and mailbox names that match your criteria. From the list, you can drill down to account and address details.

About this task

Complete the following steps to search for accounts by domain or mailbox.

Procedure

1. Open the WAT on the node you want.
2. Select **Search > Domain**.
3. Type the following information and click **Search**.
   - Domain Name – One or more letters or numbers that begin the name you want to find.

- Mailbox – Five-character identifier for the mailbox where messages are sent. The complete mailing ID uses eight characters: the first five characters identify the mailbox and the last three characters identify the mailslot.

Note: To specify the number of records you want to see in one page of the browser when the results are displayed, use the Items Per Page option.

Searching for Addresses by EDI ID or Mailslot

Searching by EDI information displays a list of addresses that match your criteria. From the list, you can drill down to details about one address.

About this task

Complete the following steps to search for accounts by account number.

Procedure

1. Open the WAT on the node you want.
2. Select **Search > EDI Information**.
3. Type the following information and click **Search**.
   - Mailslot – Three-character identifier for the sub-area within a mailbox where messages are sent. The complete mailing ID uses eight characters: the first five characters identify the mailbox and the last three characters identify the mailslot.
   - EDI IDEDI Qualifier – An identifier and qualifier pair used within EDI transmissions that identifies a business to its trading partners. The ID/qualifier pair must be unique on Sterling B2B Collaboration Network and remains the same whether it corresponds to the sender or the receiver of a transmission. A business chooses its ID/qualifier pair and shares it with its trading partners.

Note: To specify the number of records you want to see in one page of the browser when the results are displayed, use the Items Per Page option.

Searching for Addresses by General Address Information

Searching for addresses by general address information displays a list of addresses that match your criteria. Use this search option to find an address by mailslot if it does not have an EDI ID associated with it. From the list, you can drill down to details about one address.

About this task

Complete the following steps to search for accounts by general address information.

Procedure

1. Open the WAT on the node you want.
2. Select **Search > Address**.
3. Type or select the following information and click **Search**.
   - Mailslot – Three-character identifier for the sub-area within a mailbox where messages are sent. The complete mailing ID uses eight characters: the first five characters identify the mailbox and the last three characters identify the mailslot.

- Is Local Message Store – Indicator of whether the address was added to the local message store.
- Name – Name of the address.
- On SuperTracs – Indicator of which SuperTrac is used if the address was added to Sterling Commerce:Network.
- C:Network Error Code – Code generated when the EDI ID is migrated from one mailslot address to another mailslot address.
- Status – The status of the address.

Note: To specify the number of records you want to see in one page of the browser when the results are displayed, use the Items Per Page option.

Searching for Addresses that are Suspended

Searching for addresses that are suspended displays a list of suspended addresses. Addresses in yellow are within 30 minutes of the suspension expiration date and time. Addresses in red have expired.

About this task

Complete the following steps to search for suspended addresses.

Procedure

1. Open the WAT on the node you want.
2. Select **CSR Access > Suspension**.

Searching for Addresses by AS2 Protocol

Searching for addresses by AS2 protocol information displays a list of addresses that match your criteria. From the list, you can drill down to details about one address.

About this task

Complete the following steps to search for AS2 addresses.

Procedure

1. Open the WAT on the node you want.
2. Select **Search > Address > AS2** .
3. Type the following information and click **Search**.
   - AS2 Identifier – Unique identifier for the user on the user's AS2 system.
   - Local HTTP User ID – User ID set up on the node to authenticate inbound messages. The user ID is assigned by Customer Support and communicated to the user. By default, the value is the name of the address (mailslot).
   - Remote Web Server – Name of the user's Web server.
   - Remote HTTP User ID – User ID set up on the user's AS2 system to authenticate outbound messages. The user ID is assigned by the user and communicated to Customer Support.

   Note: To specify the number of records you want to see in one page of the browser when the results are displayed, use the Items Per Page option.

Searching for Addresses by FTP Protocol

Searching for addresses by FTP protocol information displays a list of addresses that match your criteria. From the list, you can drill down to details about one address.

About this task

Complete the following steps to search for an FTP address.

Procedure

1. Open the WAT on the node you want.
2. Select **Search > Address > FTP** .
3. Type the following information, and click **Search**.
   - IIBS FTP ID – Applies only if data is stored on the node and picked up by the user. User ID for accessing the FTP server on the node.
   - Remote IP Address – Applies only if data is sent to the user automatically. Internet address or host name of the FTP server receiving outbound data from the node.
   - Remote FTP ID – Applies only if data is sent to the user automatically. User ID used by the node to log on to the FTP server that receives the outbound data.

   Note: To specify the number of records you want to see in one page of the browser when the results are displayed, use the Items Per Page option.

Searching for Addresses by HTTP Protocol

Searching for addresses by HTTP protocol information displays a list of addresses that match your criteria. From the list, you can drill down to details about one address.

About this task

Complete the following steps to search for HTTP addresses.

Procedure

1. Open the WAT on the node you want.
2. Select **Search > Address > HTTP**.
3. Type the following information, and click **Search**.
   - Local HTTP User ID – User ID set up on the node to authenticate inbound messages. The user ID is assigned by Customer Support and communicated to the user. By default, the value is the name of the address (mailslot).
   - Remote HTTP User ID – User ID set up on the user's HTTP system to authenticate outbound messages. The user ID is assigned by the user and communicated to Customer Support.
   - Remote Web Server – Name of the user's Web server.

   Note: To specify the number of records you want to see in one page of the browser when the results are displayed, use the Items Per Page option.

Searching for Addresses by Mailslot

Searching for addresses by mailslot number displays a list of addresses that match your criteria. From the list, you can drill down to details about one address.

About this task

Complete the following steps to search for accounts by account number.

Procedure

1. Open the WAT on the node you want.
2. Select **Search > Address > Mailslot**.
3. Type or select the following information and click Search.
   - Mailslot – Three-character identifier for the sub-area within a mailbox where messages are sent. The complete mailing ID uses eight characters: the first five characters identify the mailbox and the last three characters identify the mailslot.
   - Is Local Message Store – Indicator of whether the address was added to the local message store.
   - Name – Name of the address.
   - On CNet – Indicator of whether the address was added to Sterling Commerce:Network.
   - C:Network Error Code – Code generated when the EDI ID is migrated from one mailslot address to another mailslot address.
   - Status – Status of the account.

   Note: To specify the number of records you want to see in one page of the browser when the results are displayed, use the Items Per Page option.

Searching for Addresses by SMTP or AS1 Protocol

Searching for addresses by SMTP or AS1 protocol information displays a list of addresses that match your criteria. From the list, you can drill down to details about one address.

About this task

Complete the following steps to search for SMTP and AS1 addresses.

Procedure

1. Open the WAT on the node you want.
2. Select **Search > Address > SMTP**.
3. Type the following information, and click Search.
   - User IDDomain – User ID and complete Internet domain name. Many Internet domain names begin with a company name as the first element in the domain name: myuserID@Acme.xxx.yyyyyyy.com

     If data is stored on the node and picked up by the user, a unique user ID and Internet domain name corresponding to the POP3 ID (mailbox) on the node.

     If data is sent to the user automatically, a user ID and complete Internet domain name of an existing SMTP e-mail address that resides on an ISP outside of Sterling B2B Collaboration Network.

- POP3 ID – Applies only if data is stored on the node and picked up by the user. Name of the POP3 mailbox on the node where messages are picked up.

Note: To specify the number of records you want to see in one page of the browser when the results are displayed, use the Items Per Page option.

Searching for Addresses by X.400 Protocol

Searching for addresses by X.400 protocol information displays a list of addresses that match your criteria. From the list, you can drill down to details about one address.

About this task

Complete the following steps to search for X.400 addresses.

Procedure

1. Open the WAT on the node you want.
2. Select **Search > Address > X.400**.
3. Type the following information, and click **Search**.
   - Given Name - First name of the user accessing the X.400 connection to the node.
   - Surname – Last name of the user accessing the X.400 connection to the node.
   - PRMD – Private management domain. A private organization (such as a company) that subscribes to the administrative management domain (such as IBM or a distributor). Each PRMD is responsible for its own directories.
   - ADMD – Administrative management domain. The provider of e-mail messaging using X.400 protocol (such as IBM or a distributor).
   - Country – Country where the ADMD (e-mail provider) resides.

   Note: To specify the number of records you want to see in one page of the browser when the results are displayed, use the Items Per Page option.

Searching Application Logs by Message ID

You can search the application logs by message ID.

About this task

Complete the following steps to search for a message ID in the application logs.

Procedure

1. Open the WAT on the node you want.
2. Select **Search > App Log - Message ID**.
3. Type the exact Message ID, and click **Search**.

   Note: You can also access the message ID logs from the Inbound and Outbound Message Details pages by clicking **View Application Logs** next to the message ID.

Searching Application Logs by Session ID

You can search the application logs by session ID.

About this task

Complete the following steps to search for a session ID in the application logs.

Procedure

1. Open the WAT on the node you want.
2. Select **Search > App Log - Session ID**.
3. Type the exact Session ID, and click **Search**.

   You can also access the session ID logs from the Log Message ID Search results page by clicking the session ID number.

   Note: The session IDs you can use for searching come from the application logs or from an alert. These are not the same as the session IDs shown on the Message Detail page.

Searching the Audit Log

You can search the audit log for changes.

About this task

Complete the following steps to search the audit logs.

Procedure

1. Open the WAT on the node you want.
2. Select **Search > Audit Logs**.
3. Enter the following information and click **Search**.

   Note: To specify the number of records you want to see in one page of the browser when the results are displayed, use the Items Per Page option.

   Start Date/Time, End Date/Time

   Date and time range to search for housekeeping log entries. If you do not change this field, the default is the last two hours.

   Date format: MM/DD/YY

   Time format: HH:MM:SS

   Time zone: UTC

   Operation

   - **All** — Include all operations.
   - **Add** — Include only Add operations.
   - **Update** — Include only Update operations.
   - **Delete** — Include only Delete operations.
   - **Restore** — Include only Inbound Message Restore operations.
   - **Pickup** — Include only Outbound Message Pickup operations.
   - **Add certificate** — Include only Security Certificate or PGP Key Add operations.
   - **Delete certificate** — Include only Security Certificate or PGP Key Delete operations.

   Change area

- **All** — Include all areas.
- **EDI** — Include only changes to EDI identifiers.
- **Address** — Include only changes made at the address level.
- **Customer** — Include only changes made at the customer level.
- **Node** — Include only changes made at the node level.

User Name (exact)

Type the WAT login ID of the user whose changes you want to see.

Pre-change text (contains)

Type the text contained in the record before it was changed.

Post-change text (contains)

Type the text contained in the record after it was changed.

Any OID or text (contains)

Type the User OID, Owner OID, Foreign Key, or other text either before or after it was changed.

4. To search for users logging in to the WAT, make the following selections:
   - In the **Operation** field, select **All**.
   - In the **Pre-change** field, enter **SCSecureAccess**.
   - In the **User Name** field, enter the WAT login ID.

Results

The search results include the following:

- Add operations are in green.
- Update and Restore operations are in yellow.
- Delete operations are in red.
- The user name is a link to the Account Search screen with the Web User ID pre-filled.

Searching Housekeeping Logs

You can search the housekeeping logs by session ID.

About this task

Complete the following steps to search the housekeeping logs.

Procedure

1. Open the WAT on the node you want.
2. Select **CSR Access > House Keeping Logs**.
3. Type the date and time range and click **Search**.
   The default is the last two hours.
   Date format: MM/DD/YY
   Time format: HH:MM:SS
   Time zone: UTC

   Note: To specify the number of records you want to see in one page of the browser when the results are displayed, use the Items Per Page option.

Searching for Inbound Messages

Searching for inbound messages displays a list of messages that match your criteria. From the list, you can drill down to more details.

About this task

Complete the following steps to search inbound messages.

Procedure

1. Open the WAT on the node you want.
2. Choose the level of your search:
   - To search for all messages coming into the node, select **Message Tracking > Inbound**.
   - To search for messages inbound to all addresses within a company, domain, or account, display the page you want and click **Inbound** on the divider bar.
   - To search for messages inbound to one address, display Address Details and click **Inbound** on the divider bar.
   - To search for messages inbound from/to Inactive addresses, select Disabled for the Delivery status.
3. Type the following information and click **Search**.

   Note: To specify the number of records you want to see in one page of the browser when the results are displayed, use the Items Per Page option.

   Search Area

   Range of information being searched, such as the name of the node, company, domain, account, or address.

   Start Date/Time, End Date/Time

   Date and time range to search for messages. If you do not change this field, the default is the last two hours.

   Date format: MM/DD/YY

   Time format: HH:MM:SS

   Time zone: UTC

   Include Reply Messages

   Indicates whether you want to include reply messages in the search. Inbound reply messages indicate that the trading partner's system received a message from the node.

   - **Yes**. Include reply messages in the search.
   - **No**. Omit reply messages from the search.

   Delivery Status

   Status of the inbound messages to be retrieved. See Inbound Message Status.

   - **ALL**. Search for all inbound messages regardless of delivery status.

   Note: This is not a real inbound message status. It provides a convenient way to search for all messages regardless of status.

   Protocol

Protocol of the messages being retrieved. To include messages with any protocol type, select **ALL**.

View PGP Messages Only

Indicates whether you want to view only FTP (PGP) messages, regardless of what Protocol you have selected.

- **Yes**. Include *only* FTP (PGP) messages in the search.
- **No**. Do no include *only* FTP (PGP) messages in the search. FTP (PGP) messages may still be displayed along with the other messages. (Selecting **No** does not exclude FTP (PGP) messages from the search.)

View Dropped Messages Only

Applies only to node-level searches from the Message Tracking menu. Dropped messages are inbound messages that are delivered successfully to the node but have no associated outbound messages. Consequently, only messages with a Complete status are searched. Messages with Failed, Restored, or Failed and Reviewed status are ignored.

- **Yes**. Include only inbound messages with no associated outbound messages. All protocols are searched. In the resulting list, the ICN does not link to additional information and clicking the transaction ID indicates that no outbound messages exist.
- **No**. Include inbound messages whether or not associated outbound messages exist. In the resulting list, you must click the transaction ID to see whether any associated outbound messages exist.

Searching for Outbound Messages

Searching for outbound messages displays a list of messages that match your criteria. From the list, you can drill down to more details.

About this task

Complete the following steps to search outbound messages.

Procedure

1. Open the WAT on the node you want.
2. Choose the level of your search:
   - To search for all messages sent out from the node, select **Message Tracking > Outbound**.
   - To search for messages outbound from all addresses within a company, domain, or account, display the page you want and click **Outbound** on the divider bar.
   - To search for messages outbound from one address, display Address Details and click **Outbound** on the divider bar.
3. Type the following information, and click **Search**.

   Note: To specify the number of records you want to see in one page of the browser when the results are displayed, use the Items Per Page option.

   Search Area

   Range of information being searched, such as the name of the node, company, domain, account, or address.

Start Date/Time, End Date/Time

Date and time range to search for messages. If you do not change this field, the default is the last two hours.

Date format: MM/DD/YY

Time format: HH:MM:SS

Time zone: UTC

Include Reply Messages

Indicator of whether you want to include reply messages in the search. Outbound reply messages indicate that the node received a trading partner's message.

- **Yes**. Include reply messages in the search.
- **No**. Omit reply messages from the search.

Delivery Status

Status of the outbound messages to be retrieved. See Outbound Message Status.

- **NOT DELIVERED**. Search for all messages except those with a Delivered status.

Note: This is not a real outbound message status. It provides a convenient way to search for all messages that are not Delivered.

Message Disposition

Status of an outbound message delivered to a mailslot to be picked up by the user.

- **Read**. The receiver has opened the message.
- **Unread**. The receiver has not opened the message.
- **Deleted**. The receiver has deleted the message.

Protocol

Protocol of the messages being retrieved. Select **ALL** to include all protocols, or select a single protocol.

Message Store Type

Indicates whether you want to view messages destined only to local Message Store customers, only non-local Message Store customers, or both.

- **LOCAL**.
- **LOCAL & NON-LOCAL**. The default.
- **NON-LOCAL**.

View PGP Messages Only

Indicates whether you want to view only FTP (PGP) messages, regardless of what Protocol you have selected.

- **Yes**. Include *only* FTP (PGP) messages in the search.
- **No**. Do no include *only* FTP (PGP) messages in the search. FTP (PGP) messages may still be displayed along with the other messages. (Selecting **No** does not exclude FTP (PGP) messages from the search.)

Searching for Messages by EDI Interchange

Searching by EDI interchange lists all interchanges that match your criteria. From the list, you can drill down to more details.

About this task

Complete the following steps to search for messages by EDI interchange.

Procedure

1. Open the WAT on the node you want.
2. Select **Message Tracking > EDI Interchange**.
3. Type the following information, and click **Search**.

   Note: To specify the number of records you want to see in one page of the browser when the results are displayed, use the Items Per Page option.

   Sender ID

   EDI ID of the sender of the transmission. An EDI ID is a unique communications ID on Sterling B2B Collaboration Network that identifies a business to its trading partners.

   Receiver ID

   EDI ID of the receiver of the transmission. An EDI ID is a unique communications ID on Sterling B2B Collaboration Network that identifies a business to its trading partners.

   Start Date/Time, End Date/Time

   Date and time range to search for messages. If you do not change this field, the default is the last two hours.

   Date format: MM/DD/YY

   Time format: HH:MM:SS

   Time zone: UTC

Searching for Messages from Sterling Commerce:Network

Searching by Sterling Commerce:Network batch number displays one inbound or one outbound message associated with the batch number. From the message, you can drill down to more details.

Procedure

1. Open the WAT on the node you want.
2. From the **Message Tracking** menu, select **Connect:Mailbox**.
3. Type the Extract Batch Number and click **Search**.

   Batch number of the message that was sent to or received from Sterling Commerce:Network. The batch number is assigned by Connect:Mailbox. A message inbound to the node receives an outbound batch number on Sterling Commerce:Network. A message outbound from the node receives an inbound batch number on Sterling Commerce:Network.

Searching for Messages by Message ID

Searching by message ID displays one inbound or outbound message that matches the ID. From the message, you can drill down to more details.

About this task

Complete the following steps to search for messages by message ID.

Procedure

1. Open the WAT on the node you want.
2. Select **Message Tracking > Message ID**.
3. Type the following information and click **Search**.
   - Message ID – Unique 24-digit number assigned by Sterling Commerce:Centre to each inbound and each outbound message.
   - Search Area – Search all messages either inbound to the node or outbound from the node.

Searching for Messages by Transaction ID

Searching by transaction ID lists all inbound and outbound messages associated with the ID. From the lists, you can drill down to more details.

About this task

Complete the following steps to search for messages by transaction ID.

Procedure

1. Open the WAT on the node you want.
2. Select **Message Tracking > Transaction ID**.
3. Type the Transaction ID and click **Search**.

   Unique 24-digit number that is assigned by Sterling Commerce:Centre to link inbound messages to one or more associated outbound messages, regardless of how many EDI interchanges are involved.

Searching for Messages by MTS ID

Searching by MTS ID lists all inbound or outbound messages associated with the ID. From the lists, you can drill down to more details.

About this task

Complete the following steps to search for messages by MTS ID.

Procedure

1. Open the WAT on the node you want.
2. Select **Message Tracking > MTS ID**.
3. Type the following information and click **Search**.
   - MTS ID (Message Transport System ID) – Unique ID assigned by a protocol or messaging system outside of Sterling B2B Collaboration Network and used to correlate and track messages across systems. Sterling Commerce:Centre preserves this external ID as the MTS ID. Not all protocols

or protocol implementations support this field. Outside of Sterling B2B Collaboration Network, this ID may be referred to as the message ID or the message-ID.

- Search Area – Search all messages either inbound to the node or outbound from the node.

Searching for Messages by Association ID and Type

Searching by association ID or type lists all inbound and outbound messages associated with the ID or type. From the lists, you can drill down to more details.

About this task

Complete the following steps to search for messages by association ID and type.

Procedure

1. Open the WAT on the node you want.
2. Select **Message Tracking > Association ID/Type**.
3. Type the following information and click **Search**.
   - Association ID – Unique ID that is used to track and correlate messages across systems.
   - Association Type – Category assigned by the node to an association ID that identifies the external system that sends or receives the message.

Searching for Messages by Subject

Searching by subject lists all messages whose subject lines match your criteria. From the list, you can drill down to more details.

Procedure

1. Open the WAT on the node you want.
2. From the **Message Tracking** menu, select **Subject**.
3. Type the following information, and click **Search**.

   Note: To specify the number of records you want to see in one page of the browser when the results are displayed, use the Items Per Page option.

   Search Area

   - **Inbound**. Search all messages inbound to the node.
   - **Outbound**. Search all messages outbound from the node.

   Search Type

   - **Exact Match**. Find messages with subject lines that exactly match the text you enter
   - **Begins With**. Find messages with subject lines that begin with the text you enter.
   - **Ends With**. Find messages with subject lines that end with the text you enter.
   - **Contains (Exact Substring)**. Find messages with subject lines that contain the text you enter, regardless of where the text appears in the subject line.

- **Contains Any (OR)**. Find messages with subject lines that contain one or more of the elements you enter. Separate each element with a space. You can enter elements in any order.
- **Contains All (AND)**. Find messages with subject lines that contain all of the elements you enter. Separate each element with a space. You can enter elements in any order.

Subject

All or part of the text in the subject line of the message. You can use wildcards and substrings.

Data from Sterling Commerce:Network. If the message is inbound to the node from Sterling Commerce:Network, enter the inbound batch number from CICS as the subject of the message.

Start Date/Time, End Date/Time

Date and time range to search for messages. If you do not change this field, the default is the last two hours.

Date format: MM/DD/YY

Time format: HH:MM:SS

Time zone: UTC

Chapter 6. Tracking Messages

Working with Messages

You have a number of ways to track inbound messages (sent *to* accounts on the node) and outbound messages (sent *from* accounts on the node).

- **By sender or by receiver**. You can track messages based on who sent an inbound message or who receives an outbound message. When you search for messages, you can filter by UTC date and time, delivery status, and protocol. To search for all messages inbound to or outbound from the node, use the Message Tracking menu. To limit your search to messages to or from one company, domain, account, or address, display the details page you want and click Inbound or Outbound on the divider bar.
- **By message ID**. Each inbound message and each outbound message is assigned a unique 24-digit number. Use the Message Tracking menu to search by message ID.
- **By transaction ID (or tracking ID)**. A transaction ID is assigned to link inbound messages to one or more associated outbound messages. Each transaction ID is a unique 24-digit number that can be tracked. Use the Message Tracking menu to search by transaction ID.
- **By Interchange Control Number (ICN)**. If a message contains EDI data, an ICN is assigned to each interchange (that is, to each exchange between the EDI ID of the sender and the EDI ID of the receiver). Thus, each inbound message that contains EDI data may have one or more ICNs, but each outbound message is associated with only one ICN. Use the Message Tracking menu to search by EDI interchange number.
- **By batch number from** Sterling Commerce:Network. If a message comes to the node from a Sterling Commerce:Network mailslot, you can track the message using the outbound batch number from Sterling Commerce:Network. Use the Message Tracking menu to search by batch number.
- **By Message Transport System ID (MTS ID)**. Some protocols or messaging systems assign a message ID that is used to correlate and track the message across systems. The node preserves this external ID as the MTS ID. Use the Message Tracking menu to search by MTS ID.
- **By association ID**. Messages exchanged between the node and some external systems may be assigned an association ID used to correlate messages between the two systems. Use the Message Tracking menu to search by association ID.
- **By subject**. You can find inbound or outbound messages based on the subject line. Use the Message Tracking menu to search by subject.

Inbound Messages from Senders to Accounts on the Node

When you search for inbound messages, you display a list of all messages that meet your criteria. The list includes information about the message submission time, status, protocol, and message ID. Some of the displayed information links to other details.

- The divider bar has a button for restoring inbound messages. There is an additional button for Queued Reprocess. Your user account must be set up to allow you to restore inbound messages. If it is not, then the **Reprocess** and **Queued Reprocess** buttons will not be available to you.

- The message ID links to information on the Inbound Message Details page. In turn, some of the information on Inbound Message Details links to other details:
  - The originator address links to details about the sender's address.
  - The transaction ID links to a list of associated outbound messages.
  - The list of attachments links to a display of the data in an attachment.
  - If the message was restored, the MTS ID links the original message and any restored message.
- The transaction ID links to a list of the outbound messages associated with the inbound message.

Outbound Messages from Accounts on the Node to Receivers

When you search for outbound messages, you display a list of all messages that meet your criteria. The list includes information about the message delivery and pickup time, status, protocol, and message ID. Some of the displayed information links to more details.

- The divider bar has buttons for resending outbound messages and for marking outbound messages as being picked up. The **Resend** button is not available for all users.
- The message ID links to information on the Outbound Message Details page. In turn, some of the information displayed on Outbound Message Details links to other details:
  - The recipient address links to details about the receiver's address.
  - The transaction ID links to a list of associated inbound and outbound messages.
  - If the message contained EDI data, information about each interchange and attachment is listed.
  - Interchange information links to details about the EDI document.
  - The list of attachments links to a display of the data in an attachment.
- The transaction ID links to a list of the relevant inbound message and any other outbound messages associated with the inbound message.
- If the outbound message contains EDI data, the ICN links to more details about the interchange and the EDI document.

Tracking Inbound Messages

The procedure to track inbound messages differs depending on the protocol of the message.

Before you begin

For interconnect data that has been sent to Sterling B2B Collaboration Network from another VAN, first use CICS and check the standard search screens. If you cannot find the data in CICS, continue with this procedure.

About this task

Complete the following steps to track inbound messages.

Procedure

1. Obtain the company name of the sender.

   For AS1, this is usually a large hub such as Lowes or Symantex.

For ANX, also obtain the sender ID, receiver ID, or control number used in the data. If you do not know this information, you can search by date and time:

- If you know the date and time when the node received the data from ANX, select **Message Tracking > Inbound**. The protocol is FTP.
- If you know the date and time when the node routed the data to Sterling Commerce:Network, select **Message Tracking > Outbound**. The protocol is Connect:Mailbox.

2. Log on to the WAT on the appropriate node.
3. For ANX, select **Message Tracking > EDI Interchange** and continue with step 6.
4. For AS1, AS2, FTP, and Interconnects, drill down to the account:
   a. Select **Search > Company**.
   b. Type the sender's name and click **Search**. A list of company names displays.
   c. In the list, click the name of the company that is receiving the data. A list of domains (mailboxes) for the company displays.
   d. Click the domain (mailbox) that received the inbound data. A list of accounts in the domain displays.
5. On the divider bar, click **Inbound Messages**.

   The search window displays.
6. Complete the fields and click **Search**.

   For AS1, select **SMTP** as the protocol.

   For Interconnects, select **FTP** as the protocol and be sure to complete the Start and End Date/Time fields.

   A list of messages matching your criteria displays.
7. Locate the message you want and click **Trans ID**.

   The inbound message you selected displays, as well as a list of related outbound messages, including:

   - The MDN sent by Sterling Commerce:Centre to the sender acknowledging the original message.
   - The outbound message sent to Sterling Commerce:Network for delivery to the EDI user's Sterling Commerce:Network mailbox. This message is sent through Connect:Mailbox.

Tracking ANX Messages

For ANX messages, the inbound message uses FTP and the outbound message uses Connect:Mailbox (SuperTracs region).

Verify that the status of the outbound message is Delivered.

- If the status is Delivered, the data was received by the node and routed to Sterling Commerce:Network. Use CICS to continue tracking this data on Sterling Commerce:Network.
- If another status is displayed, escalate this issue. The data was received by the node but was not routed to Sterling Commerce:Network.

Tracking Interconnect Messages

For Interconnects, examine the list for the message you want.

If you cannot find the message you want after examining likely candidates, tell the customer that we have not received the interchange from the other VAN. The customer should contact the trading partner to resolve the issue. Close the WAT and complete your Vantive case.

Use the following strategies to determine whether a message is the one you want.

Strategy	Details
Examine the date and time of the message.	Use the Inbound Messages page.
Verify that a message was received on the node and routed to Sterling Commerce:Network.	1. In the list of inbound messages, click **Trans ID** for the message. The Transaction Details page displays. 2. Check for the following values, which indicate that the message was correctly received by the node and routed to Sterling Commerce:Network: • Inbound protocol = FTP • Outbound protocol = Connect:Mailbox • Inbound status = Complete • Outbound status = Delivered If these values are different, the message may be processing on the node. Contact VAN Administration for help. Inform the customer that we are researching the problem.
Examine the EDI data to verify that a message contains the interchange you want.	1. In the list of inbound messages, click **Trans ID** for the message. The Transaction Details page displays. 2. On Transaction Details, click **Msg ID** for the outbound data. The list of attachments displays. 3. Click the number of the attachment. The EDI data is displayed. 4. Examine the IH header and record the mailbag control number. 5. In CICS, search for the data. • Search for the mailslot on the MAIL and SuperTracs Inbound screens. • Search for the mailbag control number on the MBAS and MBAG screens. If these screens indicate that the mailbag was not acknowledged, contact VAN Administration. • If an acknowledgment was sent, use the AUDI screen to view the inbound batch and locate the interchange.

About Reprocessing Inbound Messages

During reprocessing, the node locates the archived copy of the original inbound message and creates a new inbound message that is processed and delivered as if it were the original message.

Note: Only users with System Administrator and Super User security levels can reprocess inbound messages.

Be aware that reprocessing involves the following constraints:

- An inbound message can be reprocessed only if its delivery status is Complete. For AS2 messages, the node must have returned a synchronous MDN acknowledging the successful delivery.
- An inbound message can be reprocessed only once. To reprocess the same inbound message a second time, you can use the second instance of the message (the one generated by the first reprocessing).
- When an inbound message is reprocessed, the status of the original inbound message changes to Reprocessed.
- The reprocessed inbound message is processed by the node as if it were the original message. The entire message is reprocessed, including all EDI interchanges in the message.
- The reprocessed inbound message has a new message ID and a new transaction ID.
- The reprocessed inbound message retains the same MTS ID as the original message. Consequently, you can find both the original inbound message and the reprocessed inbound message by searching for the MTS ID or by displaying Message Details and clicking the link on the MTS ID.
- If you reprocess an inbound message from Sterling Commerce:Network, you must work with the inbound message on the node and the outbound batch on Sterling Commerce:Network.
- Inbound messages from another node or from the internet that are batched (there are multiple interchanges per file) will hit Sterling Commerce:Network again, and *each* interchange will be delivered again. Be sure to check that this is what you want to do.
- Your user account must be set up to allow you to restore inbound messages. If it is not, then the **Reprocess** and **Queued Reprocess** buttons will not be available to you.

Reprocessing an Inbound Message—Immediate Reprocessing

Select messages to be immediately reprocessed.

About this task

Complete the following steps to reprocess an inbound message immediately.

Procedure

1. Log on to the WAT on the node you want.
2. Do one of the following:
   - Display the Message Details for the inbound message.
   - Search for the inbound message. A list of one or more inbound messages matching your criteria is displayed. In the list, select the check box to the left of each message you want to reprocess.
3. Click **Reprocess**.

   A list confirming the messages you selected is displayed.
4. In the list, locate the inbound messages and verify that the status is Confirmation Required. Select the check box to the left of each message you want reprocessed.
5. When you finish, click **Confirm Reprocess**.
   - If the inbound message contained only one interchange, the node reprocesses the message. The status changes to Complete or Failed.

- If the inbound message contained no interchanges or contained multiple interchanges, the status changes to Reconfirm Required and includes a reason for the reconfirmation. Continue with step 6.

6. Select the check box to the left of each message you want reprocessed and click **Reconfirm Reprocess**.

   The node reprocesses the message. The status changes to Successful or Failed.

Reprocessing an Inbound Message—Queued Reprocessing

Select messages to be queued for reprocessing. The Retry Monitor will scan for this status and then call CMS to reprocess the message. CMS will then change the status to Reprocessed.

About this task

Complete the following steps to add inbound messages to the reprocessing queue.

Procedure

1. Log on to the WAT on the node you want.
2. Do one of the following:
   - Display the Message Details for the inbound message.
   - Search for the inbound message. A list of one or more inbound messages matching your criteria is displayed. In the list, select the check box to the left of each message you want to reprocess.
3. Click **Queued Reprocess**.

   A list confirming the messages you selected is displayed.
4. In the list, locate the inbound messages and verify that the status is Confirmation Required. Select the check box to the left of each message you want reprocessed.
5. When you finish, click **Confirm Reprocess**.

Reprocessing an Inbound Message from Sterling Commerce:Network

To reprocess an inbound message from Sterling Commerce:Network, first work on the node to change the status of the original inbound message. Then work in Doc Tracking (or CICS) to resend the message to the node.

About this task

Complete the following steps to reprocess an inbound message from Sterling Commerce:Network.

Procedure

1. Log on to the WAT on the appropriate node.
2. Search for the inbound message you want to reprocess.

   A list of one or more inbound messages matching your criteria is displayed.
3. In the list, locate the inbound message and click the message ID.

   The Inbound Message Details screen is displayed.
4. Look for the Connect:Mailbox section and make a note of the mailslot number and the outbound batch number from Sterling Commerce:Network.
5. Opposite the Status field, click **Change**.

The Status field changes from Extracted to Restore.

6. Open CICS.
7. Access the Sterling Commerce:Network mailslot and restore the outbound batch you noted.

   Sterling Commerce:Network resends the outbound batch, and the node re-extracts and reprocesses the data.

Changing the Status of Failed Inbound Messages

Periodically, you should search the node for messages that have not been received successfully. After reviewing the message and addressing the problem, you can change the status of the message so that it is omitted from subsequent searches and from any reports generated by the Customer Support monitoring tools.

Before you begin

Check with Level 2 Customer Support before you perform this task.

About this task

Complete the following steps to change the status of a failed inbound message.

Procedure

1. Log on to the WAT on the appropriate node.
2. Search for failed inbound messages. Use the Status field to identify messages that have failed.

   A list of any inbound messages matching your criteria is displayed.
3. In the list, locate the inbound message and click the message ID to display Inbound Message Details.
4. In the Status field, click **Change Status to Reviewed**.

   The status of the message is changed to Failed and Reviewed.

Tracking Outbound Messages

The procedure to track outbound messages may differ depending on the protocol of the message.

Before you begin

If you are tracking data that has been sent from a Sterling B2B Collaboration Network customer with a Sterling Commerce:Network mailbox, the first tracking point is Sterling Commerce:Network, which receives the inbound data and routes it to the appropriate node.

About this task

Complete the following steps to track outbound messages.

Procedure

1. Open the MAIL screen in CICS and locate the sender's (or the ANX) mailbox.
2. In the mailbox, locate the interchange you want. Place your cursor on the batch number and press **PF9**.

   The AUDI screen displays.

3. On the AUDI screen, highlight the batch number and click **Copy** (on the toolbar).
4. Log on to the WAT on the appropriate node.
5. Select **Message Tracking > Connect:Mailbox**.
6. Change the batch type to **Extract**, paste the batch number you copied in step 3and click **Search**.

   The inbound batch is displayed as well as the inbound message ID.
7. Click on the message ID. The Inbound Message Details are displayed.
8. Click **View Transaction**.
9. Verify that the status of the outbound message is Delivered.
   - If the status is Delivered, the node sent the data successfully.
   - If another status is displayed, escalate this issue. The data was received by the node but was not routed successfully.

Tracking Outbound Interconnect Data

When Sterling B2B Collaboration Network sends outbound interconnect data to another VAN, the receiving VAN returns an interconnect acknowledgment.

About this task

On Sterling B2B Collaboration Network, the acknowledgment is received by Dub4, routed to Sterling Commerce:Network, and indicated on the MBAS and MBAG screens in CICS. If the MBAS and MBAG screens indicate that no acknowledgment was returned to Sterling B2B Collaboration Network, follow these steps:

Procedure

1. Use the standard CICS screens to obtain details about this interconnect:
   - The name of the VAN
   - The mailbag control number
   - The batch number on the AUDI screen
2. In CICS, use the MBAS and MBAG screens to verify that an interconnect acknowledgment was received for the outbound interconnect data.
   - If the mailbag was acknowledged, tell the customer that the other VAN accepted delivery of the data. Give the customer the mailbag control number and tell the customer to contact the other VAN. Your task is complete and you can close your Vantive case.
   - If the mailbag was not acknowledged, continue with step 3.
3. Log on to the WAT on the appropriate node.
4. Select the VAN under Favorite Domains.

   The Domain Details page displays.
5. On the divider bar, click **Outbound Messages**.

   The search page for outbound messages displays.
6. Enter the time range in which the data was sent to the VAN, select **FTP** as the protocol, and click **Search**.

   A list of outbound messages for this domain that match your search criteria display. The subject column identifies the batch number from the AUDI screen in CICS.
7. Examine the message.

- If the status is Delivered, the message was sent successfully over FTP to the other VAN. However, an acknowledgment was not received. Contact VAN Administration for help.
- If the status is not Delivered, the message was not sent successfully to the other VAN. Contact VAN Administration for help.

Resending Outbound Messages

The ability to resend outbound messages is not available to all users. Your user account must be set up to allow you to update outbound messages. If it is not, then the Resend and Pickup buttons will not be available to you.

Before you begin

When outbound messages are resent, one of the following happens:

- If outbound messages are sent automatically to the receiver, the node resends the original outbound message.
- If outbound messages are delivered to the receiver's address for pick-up, the node changes the status of the original outbound message so that it is available for pick-up again.

Procedure

1. Log on to the WAT on the appropriate node.
2. Do one of the following:
   - Display Message Details for the outbound message.
   - Search for the outbound message. A list of one or more outbound messages matching your criteria is displayed. In the list, select the check box to the left of each message you want to resend.
3. Click **Resend**.

   A list confirming the messages you selected is displayed.
4. In the list, locate the outbound messages and verify that the status is Confirmation Required. Select the check box to the left of each message you want to resend.
5. When you finish, click **Confirm Resend**.
   - If the outbound message contained only one interchange – For receivers with a local message store, the node resends the message to the receiver and the status changes to Delivered or Failed.

     For receivers with a non-local message store, the message is marked as Retry Requested. The Retry Monitor Service (during its next run) will process the message and attempt to deliver it.
   - If the outbound message contained no interchanges or contained multiple interchanges – The status changes to Reconfirm Required and includes a reason for the reconfirmation. Continue with step 5.
6. Select the check box to the left of each message you want and click **Reconfirm Resend**.

   The node resends the message. The status changes to Successful or Failed.

About Picking up Outbound Messages

If an outbound message has been sent from an account on the node, you can mark it as being picked up.

You can pick up a message by knowing either the outbound message or the inbound message associated with the outbound message you want to pick up.

Note: Your user account must be set up to allow you to update outbound messages. If it is not, then the Resend and Pickup buttons will not be available to you.

Picking up a Message If You Know the Outbound Message

About this task

Complete the following steps to pick up a message if you know the outbound message.

Procedure

1. Log on to the WAT on the appropriate node.
2. Search for the outbound message.

   A list of outbound messages matching your criteria is displayed.
3. In the list, locate the outbound message and select the check box to the left of the entry. You can select one or more outbound messages to be picked up.
4. When you finish, click **Pickup** on the divider bar for Outbound Messages.

   When a non-local message is manually picked up, the Pickup Date/Time is updated on the Message Details page, but the message status will still be Unread. This helps to differentiate between messages that are manually picked up and messages that are successfully delivered during regular processing.

Picking up a Message If You Know the Inbound Message

About this task

Complete the following steps to pick up a message if you know the inbound message.

Procedure

1. Log on to the WAT on the appropriate node.
2. Search for the inbound message that is associated with the outbound message.

   A list of inbound messages matching your criteria is displayed.
3. Click the transaction ID listed in the table for the inbound message.

   A list of outbound messages associated with the inbound message is displayed.
4. In the list, locate the outbound message and select the check box to the left of the entry. You can select one or more outbound messages to be picked up.
5. When you finish, click **Pickup** on the divider bar for Outbound Messages.

Attachments

If an inbound or outbound message contains an attachment, you can identify the type and size of each attachment and view any text-based data, such as EDI data.

Any user who can view an attachment can download the attachment. (Mail users cannot download attachments.)

- Attachments that are not text-based are not displayed coherently.
- You can view only the first 10,000 bytes of data.

- Data that is viewed or downloaded is a copy of the data that is archived on the node when an inbound message is received or an outbound message is sent.

Listing Attachments and Viewing Data

About this task

Complete the following steps to list attachments and view the data.

Procedure

1. Log on to the WAT on the appropriate node.
2. Search for the inbound or outbound message.

   A list of one or more messages matching your criteria is displayed.
3. In the list, locate the message and click the message ID.

   Message details are displayed, including a list of attachments with types and sizes indicated.
4. In the list, locate the attachment and click the number to the left of the entry.

   The data in the attachment displays.

Downloading Attachments

Any user who can view an attachment can download the attachment. (Mail users cannot download attachments.)

About this task

Complete the following steps to download an attachment.

Procedure

1. Log on to the WAT on the appropriate node.
2. Search for the inbound or outbound message.

   A list of messages matching your criteria is displayed.
3. In the list, locate the message and click the message ID.

   Message details are displayed, including a list of attachments with types and sizes indicated.
4. In the list, locate the attachment and click **Download** to the right of the entry.
5. You are prompted to save or open the file.
   - To open the file, click **Open**. The file is downloaded to a temporary file and then opened. You may be prompted to identify which application to use, such as Notepad.
   - To save the file, click **Save** and identify the destination directory where you want the file saved.

Chapter 7. Working with Templates and Profiles

Templates

Templates establish default values for addresses on a node. Templates can supply protocol settings and account or address profiles.

Node Templates

Users with a System Administrator security level can set up node-level templates for each protocol type. Templates establish default values for protocol-related portions of an address and for profiles attached to the account or address. When addresses are added, the relevant template supplies default values for many fields required by the protocol and enables any associated profile. Of course, these default values can be overridden if they are not applicable to a particular address.

Company or Domain Templates

If a group of new addresses deviates from a node template for a given protocol, system administrators can edit a node template and override it at the company or domain level to which the addresses are added. Using templates reduces the information that must be entered when new addresses are added and helps eliminate errors.

Profiles

A profile is a setting that links to code within the Sterling Commerce:Centre database and controls the run-time routing and processing of data.

Profiles are specific to each node. Some profiles are supplied when Sterling Commerce:Centre is installed, but others are unique to one node. A profile can apply to the sender, to the receiver, or to both trading partners. Some profiles are enabled by default on new accounts.

Defining a profile includes the following characteristics:

- An account profile controls the run-time routing and processing of data for all addresses in the account. Internally, an account profile is used by the Sterling Commerce:Centre Engine.
- An address profile controls the run-time routing and processing of data for one address. Internally, an address profile is used by a Sterling Commerce:Centre protocol connector.
- A multiple-level profile can be one of several account profiles or address profiles enabled for the account or address.
- A single-level profile must be the only account profile or the only address profile enabled for the account or address.
- The priority assigned to an account profile determines whether it should be executed before other profiles. The highest priority is 0 (zero). Most account profiles use the default priority of 1. Higher numbers indicate a lower priority.

After coding is added to the database, users with a System Administrator security level set up and administer profiles. Afterward, users with lower security levels can enable or disable profiles for particular accounts or addresses.

Note: Your user account must be set up to allow you to edit account details. If your user account is set as Read Only, then you will not be able to add, enable, disable, or delete profiles from accounts or addresses.

Listing Profiles for an Account or Address

You can list the profiles that are enabled or disabled for an account or an address.

About this task

Complete the following steps to list profiles for an account or address.

Procedure

1. Open the WAT on the node you want.
2. Display the Account Details or Address Details, depending on which type of profile you want.
3. On the divider bar, click **Manage Profiles**.

   A list displays, summarizing any profiles that are associated with the account or the address and indicating whether the profile is enabled or disabled.

Listing Accounts or Addresses for a Profile

About this task

Complete the following steps to list the accounts or addresses for a profile.

Procedure

1. Open the WAT on the node you want.
2. Select **Node Admin > System Profiles**.
3. Select the profile you want.
4. On the divider bar, next to Profile used by, click **All**, **Enabled**, or **Disabled**.

   A list of accounts or addresses that use this profile is displayed.

Enabling a Profile for an Account or Address

About this task

Complete the following steps to enable a profile for an account or address.

Procedure

1. Open the WAT on the node you want.
2. Display the Account Details or Address Details, depending on which type of profile you want.
3. On the divider bar, click **Manage Profiles**.

   A list displays, summarizing any profiles associated with the account or the address.
4. On the divider bar, click **Add Account Profile** or **Add Address Profile** (depending on which page you displayed).
5. In the drop-down box, select the profile you want and click **Next**.
6. Verify that the name and description of the profile are correct. In the Status box, select **Enable**.
7. If necessary, complete any other information required by the profile you selected.

8. Click **Finish**.

   The list of profiles redisplays, indicating that the profile you selected is enabled.

Disabling a Profile for an Account or Address

About this task

Complete the following steps to disable a profile for an account or address.

Procedure

1. Open the WAT on the node you want.
2. Display Account Details or Address Details, depending on which type of profile you want.
3. On the divider bar, click **Manage Profiles**.

   A list displays, summarizing any profiles associated with the account or the address.
4. In the list, locate the profile you want and click **Edit** to the right of the entry.
5. Verify that the name and description of the profile are correct. In the Status box, select **Disable**.
6. Click **Update**.

   The list of profiles redisplays, indicating that the profile you selected is disabled.

Deleting Profiles

A profile controls the run-time routing and processing of data for all addresses in an account or for one address. You can delete a profile for an account or an address. However, the profile still exists on the node and can be associated with other accounts or addresses.

About this task

Complete the following steps to delete a profile.

Procedure

1. Open the WAT on the node you want.
2. Display Account Details or Address Details, depending on which type of profile you want.
3. On the divider bar, click **Manage Profiles**.

   A list displays, summarizing any profiles associated with the account or the address.
4. In the list, locate the profile you want and click **Edit** to the right of the entry.
5. Verify that the name and description of the profile are correct. Click **Delete**.

   The list of profiles redisplays and no longer includes the profile you removed.

Supplied Profiles on Sterling Commerce:Centre

The following list includes profiles that exist on Sterling Commerce:Centre nodes. Profiles are listed as long as the code remains in the database. Profiles that remain in the database and that should not be used are marked as obsolete.

The following table lists all of the supplied profiles in alphabetical order.

Profile	Description
"400 Level Response is Retriable" on page 98	Outbound HTTP and AS2 messages receiving a 400-level error response are marked Retry Requested instead of Undeliverable.
"Allow Email Through Centre" on page 98	Protects customers from spam e-mail messages from the Internet.
"Bad MDN Affect Delivery Status" on page 98	Allows problem MDNs (such as bad Message Integrity Check—MIC—or not signed as requested) to affect the status of the outbound message.
"Billing Address" on page 99	Specifies the address where billing files are sent.
"Chrysler FTP Client" on page 99	Supplies settings required by the Chrysler FTP system.
"Chrysler FTP Client Site Command" on page 99	Specifies the direct site command to use for outbound messages to Chrysler.
"Chrysler FTP Client Receiver File Type Combination" on page 99	Specifies the receiver and file type for a sender/document pair.
"Chrysler FTP Client Sender Password Combination" on page 101	Specifies the sender and password for the SITE command, given a particular sender EDI ID.
"Chunked Transfer Limit" on page 101	Controls when HTTP and AS2 messages are sent using chunked transfer encoding.
"Clorox ICN Rather than IB Batch" on page 102	For outbound messages to Clorox, set the subject to a format that includes the ICN.
"CNet Binary Mode" on page 102	Specifies that binary data loaded to Sterling Commerce:Network should not be converted (ASCII to EBCDIC).
"Connection Close" on page 102	Specifies whether or not to add a "Connection:close" header line to outbound HTTP and AS2 messages.
"Custom Parser" on page 103	Specifies that a defined parser configuration should be used.
"Customer File Name" on page 103	Specifies that the customer-supplied file name is to be used for outbound messages.
"Defer Message Routing" on page 104	Defers message routing to Sterling Commerce:Network.
Defer Parsing	Defers message parsing to Sterling Commerce:Network.
Down	Automatic profile applied by the Retry Monitor when it detects that a recipient is not accepting messages.
Down Control	Prevents the Retry Monitor from applying the automatic Down profile to an address or to all addresses in an account.
"EBMX Member ID XRef" on page 106	Performs EDI ID to EBMX Member ID cross-reference (for Chrysler SITE command).
"EDI File Prefix" on page 106	Adds an attribute value prefix to outbound EDI files.
"Engine Bypass" on page 107	Bypasses the Engine.
"Engine Originator Address Override" on page 107	Overrides the Engine originator address.
"Error Notification Service" on page 108	Specifies that Error Notification Service should be used.
"Expired Certificate Notify" on page 109	Specifies the recipients who are notified about certificate expiration.
"Expired PGP Key Notify" on page 109	Specifies the recipients who are notified about PGP Key expiration.
"Force SMTP Base64" on page 109	Provides the ability to send reports encoded with Base64 to customers.
"FTP Client File Extension" on page 109	On a nonlocal FTP address, adds an extension to the remote file that is used when sending files.
"FTP Client File Name" on page 110	Specifies a static remote FTP file name to use during each upload.
"FTP Client Listen Passively" on page 110	Specifies that the server should be passive; issues only a PORT command.

Profile	Description
“FTP Client Rename Directory” on page 111	Moves a file to a different directory after a successful file transfer.
“FTP Download Merge” on page 111	Concatenates all available messages during a GET.
“FTP Outbound Command” on page 112	Specifies the command to be executed during an outbound FTP session.
“FTP Outbound Filename” on page 113	Specifies the outbound message file name.
“FTP Server Allow Upload to Commit” on page 114	Allows upload to commit.
“Hide Duplicate Files” on page 114	In the FTP local messages store, prevents duplicate files from displaying.
“HTTP Connection Limits” on page 114	Sets the send timeout, the receive timeout, and the maximum number of simultaneous HTTP connections to the remote server.
“IA5 Text” on page 115	Allows an X.400 address to receive data formatted in the IA5 text standard.
“Is Engine Address” on page 115	Looks for an address OID.
“IsSterlingPGP” on page 116	Identifies the address for the Sterling Commerce:Centre private PGP key.
“Maximum Outbound Protocol Connections” on page 116	Sets the maximum connections per customer for a throttled outbound gateway.
“MDN Affect Delivery Status” on page 116	Allows an MDN to affect the status of an outbound message.
“MDN-caused Failed Delivery Status” on page 117	Causes the delivery status to change to Failed upon receipt of a failed MDN.
“MDN-caused Success Delivery Status” on page 117	Causes the delivery status to change to Success upon receipt of a success MDN.
“Metadata Provider” on page 117	Selects the metadata provider that will build the metadata for the destination system.
“MIME Custom Attachment” on page 117	Customize the MIME encoding options for message attachments.
“Outbound Message Retry Interval” on page 118	Overrides the outbound message retry for a specific address.
“Report” on page 118	Generates a report for the account.
“Report File Prefix” on page 119	Adds an attribute value prefix to outbound reports.
“Report Generator Originator” on page 119	Specifies the originator address used for reports.
“Respond with XHTML” on page 120	Return XHTML compatible responses to HTTP posts.
“Route By Mailslot Lookup” on page 120	Routes an inbound message from Sterling Commerce:Network by looking up the receiver's address based on the mailslot supplied by Sterling Commerce:Network.
“Strip CRLF” on page 121	Removes carriage returns and line feeds from inbound messages.
“Suspend Account” on page 121	Suspends non-local outbound protocols for a customer who is down.
“Unwrap Header/Trailer” on page 122	Specifies that Sterling B2B Collaboration Network proprietary headers and trailers should be unwrapped from the message.
“Validate Delivery Status Transitions” on page 122	Ensures that changes to the delivery status of a message are reasonable.
“X400 COD/COR” on page 122	Returns a COD and COR reply message to the node.
“X400 COD Delayed Arrival” on page 123	Allows more time for an X.400 COD to arrive.
“X400 COR Delayed Arrival” on page 123	Allows more time for an X.400 COR to arrive.
“X400 Engine Override Address” on page 124	Allows delivery of outbound messages to appear as if they are from the Dublin 4 Engine.

400 Level Response is Retriable

Outbound HTTP and AS2 messages receiving a 400-level error response are marked Retry Requested instead of Undeliverable.

Field	Description
Name	400 Level Response is Retriable
Description	Messages receiving a 400-level error response are marked Retry Requested.
Type	Address
Level	Single
Attributes	None

Allow Email Through Centre

Protects customers from spam e-mail messages from the Internet.

Field	Description
Name	Allow Email Through Centre
Description	Protects customers from spam e-mail messages from the Internet.
Type	Address
Level	Single
Attributes	None

Bad MDN Affect Delivery Status

Allows MDNs with problems (such as bad MIC or not signed as requested) to affect the status of the outbound message.

Field	Description
Name	Bad MDN Affect Delivery Status
Description	Allows MDNs with problems (such as bad MIC or not signed as requested) to affect the status of the outbound message.
Type	Account
Level	Single
Attributes	When you enable this profile, supply one of the following attributes: • y – Interpret the MDN regardless of its problems. • n – Ignore MDN with bad MIC or other problems.

Billing Address

Enabled for one address on the node. Identifies the address on the node where billing files are sent.

Field	Description
Name	Billing Address
Description	Sends billing files to this address.
Type	Address
Level	Single
Attributes	None

Chrysler FTP Client

Enabled for the Chrysler FTP address only. For outbound messages, supplies settings required by the Chrysler FTP system.

Field	Description
Name	Chrysler FTP Client
Description	Enables logic for outbound FTP sessions to Chrysler.
Type	Address
Level	Single
Attributes	None

Chrysler FTP Client Site Command

Enabled for the Chrysler FTP address only. For outbound messages, specifies the direct site command required by the Chrysler FTP system.

Field	Description
Name	Chrysler FTP Client Site Command
Description	Enables logic for outbound FTP sessions to Chrysler.
Type	Address
Level	Multiple
Attributes	None

Chrysler FTP Client Receiver File Type Combination

Enabled for the Chrysler FTP address only. For outbound messages, specifies the receiver ID and file type used on the Chrysler FTP system. This information varies with the sender and the type of EDI document being sent. The node sends an outbound message to a directory at Chrysler through active mode FTP. After the data is transferred, the node issues the SITE command with parameters specified by this profile.

Field	Description
Name	Chrysler FTP Client Receiver File Type Combination

Field	Description
Description	Specifies a sender-document type and the corresponding receiver-file type that is required by the Chrysler FTP system.
Type	Address
Level	Multiple
Attributes	When you enable this profile, supply the following attributes: • EDI Document Type – Number identifying the type of EDI document being sent or ALL. • Sender EDI ID – The EDI ID of the sender or ALL. • Receiver EDI ID - The ID of the receiver on the Chrysler FTP system. • File Type – The file type of the receiver on the Chrysler FTP system.

Usage Notes

Chrysler has specified the following attributes for most senders using 210, 214, and 856 documents.

EDI Document Type	Sender EDI ID	Receiver EDI ID	File Type	Description
ALL	ALL	LOOPTEST	LOOPBACK	Use for a loop-back test to verify FTP compatibility. Enable these attributes only when no other data is being transferred to Chrysler.
210	ALL	AUDIT	DCX210	Use for 210 documents from most senders to Chrysler.
214	ALL	STARS	EDIX12	Use for 214 documents from most senders to Chrysler.
856	ALL	CHASE	EDIX12	Use for 856 documents from most senders to Chrysler.
ALL	ALL	EDI	EDIX12	Use for EDI documents other than 210, 214, and 856 from most senders to Chrysler.

Additionally, there are unique attributes for testing the FTP system when Federal Express is the sender to Chrysler.

EDI Document Type	Sender EDI ID	Receiver EDI ID	File Type	Description
210	FEDEX001	TEST	DCX210	Use for 210 documents from Federal Express to Chrysler. Testing phase only.
214	FEDEX001	EDI	EDIX12	Use for 214 documents from Federal Express to Chrysler. Testing phase only.

Chrysler FTP Client Sender Password Combination

Enabled for the Chrysler FTP address only. For outbound messages, specifies the sender's EDI ID and a password required by the Chrysler FTP system. The node sends outbound data to a directory at Chrysler through active mode FTP. After the data is transferred, the node issues the SITE command with parameters specified by this profile.

Field	Description
Name	Chrysler FTP Client Sender Password Combination
Description	Specifies the sender EDI ID and password required by the SITE command.
Type	Address
Level	Multiple
Attributes	When you enable this profile, supply the following attributes: <Sender EDI ID or ALL>;<Sender Password> • Sender EDI ID – The EDI ID of the sender or ALL. • Sender Password – The password for the sender on the Chrysler FTP system.

Usage Notes

Chrysler has specified the following attributes for most senders. Additionally, there are unique attributes for testing the FTP system when Federal Express is the sender to Chrysler.

Sender EDI ID	Sender Password	Description
ALL	STE35A	Use for most senders to Chrysler.
FEDEX001	foo	Use when Federal Express is the sender to Chrysler.

Chunked Transfer Limit

Controls when HTTP and AS2 messages are sent using chunked transfer encoding. Messages larger than the specified limit (in bytes) are chunked.

Field	Description
Name	Chunked Transfer Limit
Description	Controls when HTTP and AS2 messages are sent using chunked transfer encoding. Messages larger than the specified limit (in bytes) are chunked.
Type	Account and address
Level	Single
Attributes	When you enable this profile, you must specify a file size limit (in bytes) at which messages are chunked. • non-zero – Messages larger than this value (in bytes) are chunked. • 0 – Do not chunk.

Clorox ICN Rather than IB Batch

For outbound messages to Clorox, set the subject to a format that includes the ICN.

Field	Description
Name	Clorox ICN Rather than IB Batch
Description	For outbound messages to Clorox, set the subject to a format that includes the ICN.
Type	Account
Level	Single
Attributes	None

CNet Binary Mode

Data loaded to Sterling Commerce:Network normally is converted from ASCII to EBCDIC. This may not be wanted for binary data (such as zip files or MS Word documents). This profile is added to the originator address of the data so the binary data will bypass the ASCII-to-EBCDIC conversion.

Field	Description
Name	CNet Binary Mode Profile
Description	Do not convert binary data loaded to Sterling Commerce:Network.
Type	Address
Level	Single
Attributes	When you enable this profile, supply one of the following attributes: • EDI ID – This can be a dummy EDI ID. • Address – The default address.

Connection Close

Specifies whether or not to add a “Connection:close” header line to outbound HTTP and AS2 messages. This profile can be added at both the account and address levels. The account profile can override the node setting, and the address profile can override the node and account settings.

Field	Description
Name	Connection Close
Description	Specifies whether or not to add a “Connection:close” header line to outbound HTTP and AS2 messages.
Type	Account and address
Level	Single
Attributes	When you enable this profile, supply one of the following attributes: • y – Add the header line. • n – Do not add the header line. Default value.

Custom Parser

Identifies the account for which predefined parsing configurations are applied.

Field	Description
Name	Custom Parser
Description	Identifies the account for which predefined parsing configurations are applied.
Type	Account
Level	Single
Attributes	None

Customer File Name

For outbound messages, specifies that a file name is to be used.

Field	Description
Name	Customer File Name
Description	Specifies that the customer-supplied file name is to be used for outbound messages.
Type	Account and address
Level	Multiple
Attributes	When you enable this profile, supply a template string that uses the following attributes as necessary: <%x>, where x is one of the following: • %D – Date in YYYYMMDD format. • %d – Short date in YYMMDD format. • %U – U.S. date in MMDDYYYY format. • %u – Short U.S. date in MMDDYY format. • %T – Time in HHMMSS format. • %O – Outbound message ID. • %F – Original filename. • %N – File in session number. • %A – Attachment number. • %C – Outbound filename. • %M – MTS ID. • %R – Raw filename. • %I – Original MTS ID. • %L – Message customer filename. • %l – (Lowercase L) Attachment customer filename. • %X – Unique 24-digit number.

The following contains examples of the template string and the resulting file name.

Template String	Resulting File Name
%M	MTS ID of the message
EDI-%A.%N	EDI-2.3

Template String	Resulting File Name
%O.%D	335905678634281305701696.20091101

Characters defined after % are case sensitive. File names cannot contain any of the following characters:

\ / : * ? " < > |

Note: For FTP Local message store addresses:

⌂When adding the Customer Filename profile with the %D, %d, %u, or %u attributes (*not* in conjunction with other attributes), you should also enable the Hide Duplicate Files profile. Adding this profile will prevent FTP local messages from being duplicated when the customer is retrieving their messages. When the user is ready to retrieve their messages, only one message will be available in their receive folder at a time and they have to log off and log back in to retrieve every subsequent message.

Defer Message Routing

Also called the FastPath profile. Enabled for the receiver's account. Sends messages to Sterling Commerce:Network to be routed.

By default, the node routes messages. If this profile is enabled for an account, messages for all addresses in the account are sent to Sterling Commerce:Network for routing. Most commonly, this profile is enabled for the FTP address of a receiver.

Field	Description
Name	Defer Message Routing
Description	Defers message routing to Sterling Commerce:Network.
Type	Account
Level	Single
Priority	Number from 0 to *n* that indicates the order in which account profiles are processed. The lower the number, the higher the priority. • 0 – The highest priority. • 1 – The default priority.
Attributes	None

Defer Parsing

Routes messages to Sterling Commerce:Network regardless of the EDI ID of the receiver.

By default, the node parses all inbound messages that contain EDI data and sends each resulting EDI interchange as a separate outbound message to the mailslot associated with the receiver's EDI ID. If Defer Parsing is enabled for an account, inbound messages for all addresses in the account are parsed on the node to record and store EDI interchange information in the database. Then, all EDI interchanges are sent in a single outbound message to Sterling Commerce:Network. Sterling

Commerce:Network completes processing and delivers the EDI interchanges to the mailslots associated with each receiver's EDI ID. This functionality allows the node to capture and track EDI interchange information without breaking the message into multiple interchanges.

This parameter affects the Transmission Confirmation and Transmission Error reports generated for EDI information. If Defer Parsing is disabled, EDI data is parsed and all resulting interchanges are delivered by the node. Consequently, a Transmission Confirmation or Transmission Error report is generated for each EDI interchange that is delivered by the node. If Defer Parsing is enabled, EDI data is captured on the node but sent to Sterling Commerce:Network for complete processing and delivery. Consequently, one Transmission Confirmation or one Transmission Error report is generated for all EDI interchanges contained in the message that the node sent to Sterling Commerce:Network.

Field	Description
Name	Defer Parsing
Description	Defers message parsing to Sterling Commerce:Network.
Type	Account
Level	Single
Priority	Number from 0 to *n* that indicates the order in which account profiles are processed. The lower the number, the higher the priority. • 0 – The highest priority. • 1 – The default priority.
Attributes	When you enable this profile, supply the following attributes: • None • NO_EDI_TRACKING – In this case, inbound messages for all addresses in the account are routed to Sterling Commerce:Network without being parsed on the node for EDI interchange information. One inbound message to the node results in one outbound message to Sterling Commerce:Network, but no EDI interchange information is saved on the node from the inbound message. Enter the following text string as an attribute: NO_EDI_TRACKING

Down

Automatic profile applied by the Retry Monitor when it detects that a recipient is not accepting messages.

Field	Description
Name	Down
Description	Automatic profile applied by the Retry Monitor when it detects that a recipient is not accepting messages.
Type	Address
Level	Single
Attributes	None

Down Control

Prevents the Retry Monitor from applying the automatic Down profile to an address or to all addresses in an account.

Field	Description
Name	Down Control
Description	Prevents the Retry Monitor from applying the automatic Down profile to an address or to all addresses in an account.
Type	Address and account
Level	Single
Attributes	When you enable this profile, supply the following attribute: • 0 – Down processing is permitted. • 1 – Down processing is not permitted.

EBMX Member ID XRef

Perform EDI ID to EBMX Member ID cross-reference to use for Chrysler SITE command.

Field	Description
Name	EBMX Member ID XRef
Description	Perform EDI ID to EBMX Member ID cross-reference to use for Chrysler SITE command.
Type	Address
Level	Single
Attributes	None

EDI File Prefix

For outbound messages, attaches a prefix to the file name of the attachment. You can also replace the file name of the attachment with a name that you specify.

Field	Description
Name	EDI File Prefix
Description	Prefixes outbound EDI files with the attribute value.
Type	Account
Level	Single
Priority	Number from 0 to *n* that indicates the order in which profiles are processed. The lower the number, the higher the priority. • 0 – The highest priority. • 1 – The default priority.
Attributes	When you enable this profile, supply the following attribute: • Prefix – Text to be used as the prefix. To replace the file name of the attachment, type an exclamation mark (!) as the first character of the name you want to use.

Engine Bypass

Enabled for the sender's account for AS2 and FTP addresses. Routes inbound messages to a specified address instead of to the Engine on the node.

By default, data received by the node is parsed by the Engine so it can be delivered to the receiver. If the Engine does not support a particular standard, you can use this profile to route data to an address and bypass the Engine.

Field	Description
Name	Engine Bypass
Description	Routes data to the specified address and bypasses the Engine on the node.
Status	In the drop-down box, select Enabled to configure.
Force Bypass	Check this option to fully ensure that the Engine path absolutely cannot be exercised.
Type	Address
Level	Multiple
Attributes	When you enable this profile, supply the following attributes: • Recipient Mailslot – Address on the node that receives data from the specified Display Name. • Display Name – Unique string. See Usage Notes.

Usage Notes

You can specify one or more pairs of values. For example, specify Recipient Mailslot 1 and Display Name 1 as one pair. Specify Recipient Mailslot 2 and Display Name 2 as another pair.

Protocol Type	Recipient Mailslot	Display Name
AS2	Address that receives data from the specified Display Name	Alphanumeric string. The Display Name is case sensitive and needs to be unique among all Engine Bypass definitions for the recipient. It must match the value passed with the sc-recipient parameter in the URL.
FTP	Address that receives data from the folder specified in Display Name	Name of the directory on the FTP server for the node. Data found in this directory is delivered to the address specified in Recipient Mailslot. Entering this value creates the FTP directory on the FTP server for the node. An FTP directory name is case sensitive and must be unique on the node.

Engine Originator Address Override

Enabled for SMTP addresses only. For outbound messages, overrides the default address used as the origination address of the message.

By default, the origination address of outbound messages is the Engine address of the node. Some customers have back-end systems that check for a particular origination address. If accounts are moved from one node to another, the origination address for outbound messages changes and would require customers to modify their back-end systems. To avoid this problem, enable this profile and specify the old Engine address to be used in outbound messages.

This profile is useful when you are migrating accounts between nodes. For example, you might move accounts from the Dublin 4 node to the Dublin 3 node. In this case, enable this profile for the customer's new account on the Dublin 3 node and specify the Engine address of the Dublin 4 node.

Field	Description
Name	Engine Originator Address Override
Description	Overrides the Engine address of the node with the specified address.
Type	Address
Level	Single
Priority	Number from 0 to *n* that indicates the order in which profiles are processed. The lower the number, the higher the priority. • 0 – The highest priority. • 1 – The default priority.
Attributes	When you enable this profile, supply the following attribute: • SMTP address – Text string to be used as the origination address in outbound messages from this account. If this profile is used when an account is being migrated between nodes, this value is the SMTP Engine address of the original (source) node.

Error Notification Service

Monitors messages from an address for errors. When a message in the address is assigned an error status, this profile detects the error and generates a report. The error report is sent to an address that is identified in the error code set up by the System Administrator.

Field	Description
Name	Error Notification Service
Description	Error notification
Type	Address
Level	Single
Attributes	When you enable this profile, supply the following attributes: • Add – Select the check box to associate this error code with the address. • Code/Description – Name and description of an error code set up by the System Administrator. The code name links to details about the error code.

Expired Certificate Notify

Identifies addresses where notification of expiring and expired certificates are sent.

Field	Description
Name	Expired Certificate Notify
Description	Sends notification of expiring and expired certificates to this address.
Type	Address
Level	Single
Attributes	None

Expired PGP Key Notify

Identifies addresses where notification of expiring and expired PGP keys are sent.

Field	Description
Name	Expired PGP Key Notify
Description	Sends notification of expiring and expired PGP keys to this address.
Type	Address
Level	Single
Attributes	None

Force SMTP Base64

Enabled for SMTP addresses that need to encode outbound messages with Base64. This profile is useful for delivering reports to customers.

By default, reports use ASCII format. Enabling this profile for an address causes outbound reports to be encrypted with Base64.

Field	Description
Name	Force SMTP Base64
Description	Uses Base64 to encode outbound SMTP messages.
Type	Address
Level	Single
Attributes	None

FTP Client File Extension

For outbound FTP messages, attaches a file extension to the name of the file being transferred.

Field	Description
Name	FTP Client File Extension
Description	Attaches a file extension to use when uploading files from this address to remote FTP servers.

Field	Description
Type	Address
Level	Single
Attributes	When you enable this profile, supply the following attribute: • Extension – Text to be used as the file extension. Do not include the period that is used between the file name and the extension.

FTP Client File Name

For outbound FTP messages, specifies the name of the file being transferred.

Field	Description
Name	FTP Client File Name
Description	Specifies the file name to use when uploading files from this address to remote FTP servers. Note that all outbound files use the same name.
Type	Address
Level	Single
Attributes	When you enable this profile, supply the following attribute: • File name – Text to be used as the name of the file.

FTP Client Listen Passively

Enabled for FTP addresses only. Causes the node to issue the PORT command, which requests that the remote FTP server employ active mode FTP while the node listens passively on the IP address and port number specified in the command.

By default, the node connects to a remote FTP server and issues the PASV command initially. The PASV command requests that the remote FTP server listen passively. If the remote FTP server rejects the PASV command, the node retries by issuing the PORT command. This profile causes the node to issue the PORT command initially.

Field	Description
Name	FTP Client Listen Passively
Description	Do not request server to be passive (issue PORT command only)
Type	Address
Level	Single
Attributes	When you enable this profile, supply the following attributes: <PORT parameters> Enter the PORT command with appropriate parameters. Contact Level 2 Customer Support.

FTP Client Rename Directory

Enabled for FTP addresses only. For outbound messages, specifies the directory on the customer's FTP system to which files are committed.

Field	Description
Name	FTP Client Rename Directory
Description	Moves the file to a different directory after a successful file transfer.
Type	Address
Level	Single
Attributes	When you enable this profile, supply the following attribute: • Directory – The complete path and directory name of the directory on the customer's FTP system to which the file is committed. Customers supply this value based on the requirements of their FTP system.

FTP Download Merge

For outbound FTP messages, indicates that all messages being sent to the same receiver are merged into one outbound file. Applies only to FTP addresses for which data is picked up by the receiver. Does not apply to event-driven FTP addresses that deliver data automatically to receivers.

By default, when FTP users pick up data from an address, each file is sent individually unless the user issues the SITE command during the session to request that the available files be merged into one file. To change the default behavior so that the user always picks up a single merged file, enable the FTP Download Merge profile for the address.

- You can enable this profile for an address that receives data or for an address that receives network reports. However, do not enable this profile for an address that receives both data and reports. Doing so would create a file that mixes data and report information.
- Outbound messages are concatenated in the same order as they are listed on the FTP server.
- When the merged file begins to transfer, the delivery status of each message within the merged file changes to Transferring. If any file fails, the Transferring status remains in effect for too long. This condition generates alerts to Production Control. Production Control or Level 2 Customer Support must intervene manually to correct the problem and resend the files.
- Each message within the merged file receives a delivery status of Delivered and a pick-up time only if all files in the merged file are delivered successfully. The pick-up time posted for all messages reflects the time of the last file sent.
- After the entire merged file is transferred, all messages within the file are removed from the FTP server.
- The FTP server on a particular node may be configured with file size and time limits. Once an outbound file reaches the maximum size or exceeds the time limit for transferring, the FTP server does not add any more files to the merged file.

Field	Description
Name	FTP Download Merge

Field	Description
Description	Causes all available files to be concatenated when the receiver issues the RETR command to receive files.
Type	Address
Level	Single
Attributes	None

FTP Outbound Command

For outbound non-local FTP messages, specifies the commands some customer addresses require to correctly receive and process data.

Field	Description
Name	FTP Outbound Command
Description	Enables customers to customize commands to use when processing their data.
Type	Address
Level	Multiple
Attributes	When you enable this profile, supply the following attributes: • Category – When a command can be sent, including before and after messages are transferred and before and after a message is sent. • Sequence – Order that commands in the same category are executed. • Error – Whether processing should continue if an error is returned. • Command – Any valid FTP server command. (See details below.)

The FTP command string must adhere to the following template:

```
Category,sequence,error,command
```

To use the FTP outbound command profile, the address profile should contain an FTP command string that specifies the following:

- **Category** indicates when the command should be sent. Valid values are:
  - A: Per session, after logon and before message attachments are transferred
  - B: Per attachment, before the attachment is sent
  - C: Per attachment, after the attachment is sent
  - D: Per session, after message attachments are transferred and before logoff

  Note: Each session delivers only one message. Currently, outbound messages contain only one attachment.
- **Sequence** indicates when the command should be sent in relation to other commands in that category. For example, a command with a sequence value of 23 should be sent before a command with a sequence value of 67. Valid values are 1 through 99.
- **Error** indicates whether processing should continue if an error is returned. Valid values are:

– **Y**: Yes
– **N**: No

- **Command** indicates the valid FTP server command that should be issued.

Example

```
C,4,Y,BINARY
```

In this example, the BINARY command is sent after each message in the session is sent. The command is sent after category C commands with sequence numbers 1, 2, and 3. Return codes from the remote FTP server are ignored. Processing continues with any category D commands that are defined.

FTP Outbound Filename

For outbound nonlocal FTP messages, allows customers to specify a file name that is more meaningful to them than the file name Sterling Commerce:Centre assigns. For example, some customers might want the date and time included in the file name.

Field	Description
Name	FTP Outbound Filename
Description	Enables customers to specify a file name for their outbound FTP messages.
Type	Address
Level	Single
Attributes	When you enable this profile, supply a template string that uses the following attributes as necessary: <%x>, where x is one of the following: • D – Date, in YYYYMMDD format • d – Short date, in YYMMDD format • T – Time, in HHMMSS format • O – Outbound message ID • F – Original file name • N – File in session number • A – Attachment number • O – Outbound file name • M – MTS ID • U – Long U.S. date, in MMDDYYYY format. • u – Short U.S. date, in MMDDYY format.

The following table contains examples of the template string and the resulting file name.

Template String	Resulting File Name
%M	MTS ID of the message
EDI-%A.%N	EDI-2.3
%O.%D	335905678634281305701696.20091101

Characters defined after % are case sensitive. File names cannot contain any of the following characters:

\ / : * ? " < > |

FTP Server Allow Upload to Commit

Enabled for FTP addresses only. For inbound messages, allows a remote FTP server to place a file directly in the `/send/commit` directory on the FTP server for the node.

By default, the node renames an inbound FTP file and then places it in the `/send/commit` directory.

Field	Description
Name	FTP Server Allow Upload to Commit
Description	Overrides the node configuration to allow an FTP user to upload directly to the `/send/commit` directory.
Type	Address
Level	Single
Attributes	None

Hide Duplicate Files

In the FTP local messages store, prevents duplicate files from displaying.

Field	Description
Name	Hide Duplicate Files
Description	In the FTP local messages store, prevents duplicate files from displaying.
Type	Account
Level	Single
Attributes	When you enable this profile, specify one of the following attributes: • N – Prevent duplicate filenames from displaying by generating unique names. • Y – Prevent duplicate filenames from displaying by hiding the messages.

HTTP Connection Limits

For HTTP/S addresses (including AS2), overrides the default values for time-outs and the maximum number of simultaneous HTTP connections.

By default, the HTTP/S server on a node sets default values for time-outs on outbound messages (send time-outs), time-outs on inbound messages (receive time-outs), and number of simultaneous HTTP connections to a single address. Enable this profile to override these default values for an address.

Field	Description
Name	HTTP Connection Limits

Field	Description
Description	Sets the send time-out, receive time-out, and maximum number of simultaneous HTTP connections to the remote server.
Type	Address
Level	Single
Attributes	When you enable this profile, supply the following attributes: <Send>,<Receive>,<Connections> Be sure to enter the parameters in order, separated by commas, and omitting spaces. • Send – The number of milliseconds to use as the time-out for outbound messages from this address. • Receive – The number of milliseconds to use as the time-out for inbound messages to this address. • Connections – The maximum number of simultaneous connections to this address.

IA5 Text

Enabled for X.400 addresses only. Allows an X.400 address to receive data formatted in the IA5 text standard.

Field	Description
Name	IA5 Text
Description	Delivers data in the IA5 text standard.
Type	Address
Level	Single
Attributes	None

Is Engine Address

Identifies an address as an Engine address.

By default, Engine addresses are defined for the node in the registry. One address is defined for each protocol type. Enable this profile to define additional addresses as Engine addresses. For example, SMTP protocol allows senders to address messages to the Engine. This profile allows more than one SMTP address to be used as an Engine address.

Field	Description
Name	Is Engine Address
Description	Allows multiple SMTP addresses for the Engine.
Type	Address
Level	Single
Attributes	None

IsSterlingPGP

Identifies an address as holding the PGP definition with the Sterling Commerce:Centre private PGP key.

Field	Description
Name	IsSterlingPGP
Description	Identifies an address as holding the PGP definition with the Sterling Commerce:Centre private PGP key.
Type	Address
Level	Single
Attributes	None

Maximum Outbound Protocol Connections

Defines the maximum connections allowed per customer for a throttled outbound protocol gateway.

Field	Description
Name	Maximum Outbound Protocol Connections
Description	Defines the maximum connections allowed per customer for a throttled outbound protocol gateway.
Type	Address
Level	Single
Attributes	When you enable this profile, supply the following attribute: • Limit – The maximum number of simultaneous connections for the customer.

MDN Affect Delivery Status

Allows MDNs to affect the status of the outbound message.

Field	Description
Name	MDN Affect Delivery Status
Description	Allows MDNs to affect the status of the outbound message.
Type	Account
Level	Single
Attributes	When you enable this profile, supply one of the following attributes: • y – Received MDN can change the delivery status of a message. • n – Received MDN has no effect on the delivery status of a message.

MDN-caused Failed Delivery Status

Enable the Failed Delivery status when receiving failed MDN.

Field	Description
Name	MDN-caused Failed Delivery Status
Description	Enable the Failed Delivery status when receiving failed MDN.
Type	Account
Level	Single
Attributes	When you enable this profile, supply one of the following attributes: • 0 – Failed. • 7 – Undeliverable (best choice).

MDN-caused Success Delivery Status

Enable the Success Delivery status when receiving success MDN.

Field	Description
Name	MDN-caused Success Delivery Status
Description	Enable the Success Delivery status when receiving success MDN.
Type	Account
Level	Single
Attributes	When you enable this profile, supply the following attribute: • 1 – Delivered (most likely).

Metadata Provider

Selects the metadata provider that will build the metadata for the destination system.

Field	Description
Name	Metadata Provider
Description	The metadata provider that builds the metadata for the destination system.
Type	Address
Level	Single
Attributes	One of the following attributes: • Centre - basic • GIODE - Nike

MIME Custom Attachment

Customize the MIME encoding options for message attachments.

Field	Description
Name	MIME Custom Attachment

Field	Description
Description	Customize the MIME encoding options for message attachments.
Type	Address
Level	Single
Attributes	None

Outbound Message Retry Interval

Overrides the default retry interval for outbound messages.

By default, outbound messages from an address that are not delivered successfully are resent at an interval specified by the appropriate protocol connector. Enabling this profile for an address causes unsuccessful outbound messages to be resent after the number of seconds you specify.

Note: Because the Retry Monitor runs every 60 seconds, you should set this profile to a value greater than 60 seconds.

Field	Description
Name	Outbound Message Retry Interval
Description	Outbound Message Retry Interval (seconds)
Type	Address
Level	Single
Attributes	Consult Level 3 (Sterling Commerce:Centre development) before enabling this profile. When you enable this profile, supply the following attribute: • Seconds – The number of seconds to wait between attempts to send an outbound message.

Report

Generates a report for the account.

Field	Description
Name	Report
Description	Generates a report for the activity in the account.
Type	Account
Level	Multiple
Priority	Number from 0 to *n* that indicates the order in which account profiles are processed. The lower the number, the higher the priority. • 0 – The highest priority. • 1 – The default priority.

Field	Description
Attributes	When you enable this profile, supply the following attributes: • Report Type – Type of report to be generated: Processing report (020 report), Processing Error Report (030 report), or Daily Activity report (070 report). • Report Format – Format to be used for the report: Text format, Text format with page breaks, or Data format (ASCII code). • Address – The address on the node to which the report is sent.

Report File Prefix

Also called the File Prefix profile. For outbound messages, attaches a prefix to the file name of the attachment. Reports are sent as attachments to outbound messages. You can also replace the name of the attachment with a name that you specify.

Field	Description
Name	Report File Prefix
Description	Prefixes outbound report files with the attribute value.
Type	Account
Level	Single
Priority	Number from 0 to *n* that indicates the order in which account profiles are processed. The lower the number, the higher the priority. • 0 – The highest priority. • 1 – The default priority.
Attributes	When you enable this profile, supply the following attribute: • Prefix – Text to be used as the prefix. To replace the file name of the attachment, type an exclamation mark (!) as the first character of the name you want to use.

Report Generator Originator

Enabled for one address on the node. For outbound messages containing reports, identifies the associated address as the origination address used in the message. Reports are produced by the report generator and sent as attachments to outbound messages.

By default, the origination address used for outbound report messages is ReportGenerator@CommerceCentre. If this profile is enabled for an address, the report generator uses that address as the origination address in outbound report messages.

Field	Description
Name	Report Generator Originator
Description	Identifies the associated address as the origination address used in the message.
Type	Address

Field	Description
Level	Single
Attributes	None

Respond with XHTML

Causes synchronous, non-MDN responses to HTTP POST operations to use a self-closing, XHTML-compliant break tag "<br/>" instead of the usual HTML compliant break tag "<br>". The customer's credentials, which accompany the inbound data, must be successfully authenticated before the profile is applied.

Field	Description
Name	Respond With XHTML
Description	Return XHTML compatible responses to HTTP posts.
Type	Address
Level	Single
Priority	None
Attributes	None

Route By Mailslot Lookup

Routes an inbound message from Sterling Commerce:Network by looking up the receiver's address based on the mailslot supplied by Sterling Commerce:Network. Otherwise, messages from Sterling Commerce:Network are parsed by the node and routed to the address associated with the receiver's EDI ID.

If this profile is enabled for an address, you can track messages to and from the address by searching for inbound and outbound messages. You cannot track messages by searching for EDI interchange information because the node does not parse messages.

Field	Description
Name	Route By Mailslot Lookup
Description	Inbound messages from Sterling Commerce:Network to this account are not parsed. Instead, they are routed to the mailslot address that is supplied by Sterling Commerce:Network.
Type	Account
Level	Single
Priority	Number from 0 to *n* that indicates the order in which account profiles are processed. The lower the number, the higher the priority. • 0 – The highest priority. • 1 – The default priority. If the Strip CRLF profile is enabled for this account, set the priority of the Route by Mailslot Lookup profile to 1 (the second highest priority). All other enabled account profiles can be set to 2.
Attributes	None

Strip CRLF

Removes carriage returns and line feeds from inbound messages. Generally, these inbound messages are routed to Sterling Commerce:Network, which cannot process these characters. When you can enable this profile for an account, you must contact Sterling Commerce:Centre development to set the attributes and the priority level in the database.

Field	Description
Name	Strip CRLF
Description	Removes carriage returns and line feeds from inbound messages.
Type	Account
Level	Single
Priority	Number from 0 to *n* that indicates the order in which account profiles are processed. The lower the number, the higher the priority. • 0 – The highest priority. • 1 – The default priority. When you enable this profile, set the priority to 0 (the highest priority) so that this profile is executed before any other profile associated with the account.
Attributes	When you enable this profile, Sterling Commerce:Centre Level 3 development must set one of the following attributes in the database: • 1 – Remove carriage returns. • 2 – Remove line feeds. • 3 – Remove either carriage returns or line feeds. • 4 – Remove only pairs of carriage returns or line feeds. • 5 – Suppress stripping of CRLF characters when loading data to Sterling Commerce:Network.

Suspend Account

Suspend non-local outbound protocol traffic to a customer who is down.

Field	Description
Name	Suspend Account
Description	Suspend non-local outbound traffic to a customer who is down.
Type	Address
Level	Single
Attributes	When you enable this profile, supply the following attributes: • Reasons – The reason for suspending the address. • Expire – Date and time when the suspension expires and traffic resumes

Unwrap Header/Trailer

Identifies the accounts for which Sterling B2B Collaboration Network proprietary headers and trailers are unwrapped from messages.

Field	Description
Name	Unwrap Header/Trailer
Description	Messages to this account have the Sterling B2B Collaboration Network proprietary headers and trailers removed.
Type	Account
Level	Single
Attributes	When you enable this profile, supply the following attributes: • Priority – A lower number (integer) denotes a higher priority. • Document Type – The type of document that the Sterling B2B Collaboration Network proprietary Header/Trailer should be removed from (for example, XF9).

Validate Delivery Status Transitions

Ensure that changes to the message Delivery Status are reasonable.

Field	Description
Name	Validate Delivery Status Transitions
Description	Ensure that changes to the message Delivery Status are reasonable.
Type	Account
Level	Single
Attributes	When you enable this profile, supply one of the following attributes: • y – Validate all Delivery Status transitions. • n – Do not perform extra checks.

X400 COD/COR

Applies only to outbound messages from X.400 addresses. If this profile is enabled for an X.400 address, each outbound message from the address requests that the receiver return a reply message to the node. The reply message can be a confirmation of delivery (COD), a confirmation of receipt (COR), or both a COD and COR.

Field	Description
Name	X400 COD/COR
Description	Returns a COD, COR, or both, to the node.
Type	Address
Level	Single

Field	Description
Attributes	When you enable this profile, supply one of the following attributes: • 1 – Return a COD to the address on the node. • 2 – Return a COR to the address on the node. • 3 – Return both a COD and a COR to the address on the node.

X400 COD Delayed Arrival

Applies only to X.400 addresses that use the X400 COD/COR profile to request a COD (confirmation of delivery) from the receiver.

If an address sends an outbound X.400 message that requests a COD reply message, the node Retry Monitor checks for the COD to arrive. If the COD does not arrive within the default time specified, the Retry Monitor sends an alert. Use this profile to instruct the Retry Monitor to wait longer for CODs that acknowledge outbound messages from this address.

Field	Description
Name	X400 COD Delayed Arrival
Description	Allows more time for X400 COD to arrive.
Type	Address
Level	Single
Attributes	When you enable this profile, supply the following attribute: • Seconds – The number of seconds to wait for the COD to arrive on the node before sending an alert.

X400 COR Delayed Arrival

Applies only to X.400 addresses that use the X400 COD/COR profile to request a COR (confirmation of receipt) from the receiver.

If an address sends an outbound X.400 message that requests a COR reply message, the node Retry Monitor checks for the COR to arrive. If the COR does not arrive within the default time specified, the Retry Monitor sends an alert. Use this profile to instruct the Retry Monitor to wait longer for CORs that acknowledge outbound messages from this address.

Field	Description
Name	X400 COR Delayed Arrival
Description	Allows more time for X400 COR to arrive.
Type	Address
Level	Single
Attributes	When you enable this profile, supply the following attribute: • Seconds – The number of seconds to wait for the COR to arrive on the node before sending an alert.

X400 Engine Override Address

Applies only to X.400 addresses. For outbound messages, overrides the default address used as the originator of the message.

By default, the originator of outbound messages is the Engine address of the node. Some customers have back-end systems that check for a particular originator. If accounts are moved from one node to another, the originator for outbound messages changes and would require customers to modify their back-end systems. To avoid this problem, enable this profile and specify the old Engine address to be used in outbound messages.

This profile is useful when you are migrating accounts between nodes. For example, you might move accounts from the Dublin 4 node to the Dublin 3 node. In this case, enable this profile for the customer's new account on the Dublin 3 node and specify the Engine address of the Dublin 4 node.

Field	**Description**
Name	X400 Engine Override Address
Description	Overrides the default address used as the message originator.
Type	Address
Level	Single
Attributes	When you enable this profile, supply the following attribute: • dcedub15 – The MTA folder name on Dublin 4 to be used for accounts migrated from Dublin 4 to Dublin 3. The attribute is a text string to be used as the originator in outbound messages from this address. If this profile is used for an address being migrated between nodes, this value is the name of the MTA folder used to process outbound messages on the original (source) node.

Chapter 8. Administering Nodes

Accessing Other Nodes

You can access other nodes if you know the URL address and have a valid user ID and password for the node you want.

Before you begin

Note: Your user account must be set up to allow you to make node level updates. If your user account is set as Read Only, then you will not be able to make any updates to the node.

About this task

Complete the following steps to log on to other nodes.

Procedure

1. Open the WAT on the node you want.
2. Select **CSR Access > Node List**.
   A list of nodes displays.
3. Locate the node you want. Click the name of the node.
   The logon page for the node displays.
4. Type a valid user ID and password and click **Logon**.

Editing a Node Address

Before you begin

Note: Only users with System Administrator security level can edit node details.

About this task

Complete the following steps to edit a node address.

Procedure

1. Open the WAT on the node you want.
2. Select **CSR Access > Node List**.
   A list of nodes displays.
3. Locate the node you want. To the right of the entry, click **Edit**.
4. Type changes to the node name or to the URL address and click **Update**.

Viewing Message Turnaround Time

You can display the average turnaround time for messages on a node. Turnaround time is the average time between the receipt of an inbound message and the delivery of an associated outbound message for the node, regardless of the protocol used or the processing required. You can compute the turnaround time by hour or by day for a particular time period. You can display results in a table or a graph.

About this task

Note: Duplicate messages are not included in message turnaround time statistics.

Complete the following steps to compute the message turnaround time.

Procedure

1. Open the WAT on the node you want.
2. Select **CSR Access > Node Statistics > Message Turnaround Time**.
3. Specify the following information and click **Search**.
   - Start Date/Time, End Date/Time – Date and time range for which statistics are computed. Inbound messages received and the associated outbound messages sent within this range are selected for computation. The default is the last 24 hours. You can request data for the last 35 days.

     Date format: MM/DD/YY

     Time format: HH:MM:SS

     Time zone: UTC
   - Low watermark, High watermark (seconds) – Indicate a range of processing times (in seconds) to be displayed in color. Messages with turnaround times falling within the high and low watermarks are displayed in yellow. Messages with turnaround times greater than the high watermark are displayed in red.
   - Group By – Indicate whether results are grouped by hour or by day.
     - Hour – Compute average turnaround time for each hour within the date-and-time range.
     - Day – Compute average turnaround time for each day within the date-and-time range.

Results

By default, statistics about message turnaround time are displayed in a table. To draw a graph, use the Graph Options—the X-axis and Y-axis drop-down fields and the **Draw Graph** button.

- Date/Time – Day or day and hour for which turnaround time is computed.
- Msgs Processed – Total number of inbound messages processed during the indicated time period.
- Average Processing Time (HH:MM:SS.sss) – Average time from when an inbound message is processed in Sterling Commerce:Centre.
- Msgs Delivered – Total number of outbound messages delivered during the indicated time period.
- Average Turnaround Time (HH:MM:SS.sss) – Average time from when an inbound message is received and an associated outbound message is delivered.

Viewing Message Volume Statistics

You can display statistics about the total number and the total size of messages flowing through the node. You can compute statistics for all messages and all protocols, or you can filter by inbound or outbound message type and by protocol. You can display results in a table or a graph.

Computing Message Volume Statistics

To compute the message volume statistics, complete the following steps:

Procedure

1. Open the WAT on the node you want.
2. From the **CSR Access** menu, point to **Node Statistics**, and select **Message Volume**.
3. Specify the following information and click **Search**.

Start Date/Time, End Date/Time

Date and time range for which statistics are computed. Messages processed by the node within this range are selected for computation. The default is the last 24 hours. You can request data for the last 35 days.

Date format: MM/DD/YY

Time format: HH:MM:SS

Time zone: UTC

Group By

Indicate whether results are grouped by hour or by day.

- **Hour** – Compute totals and display results for each hour in the designated date-and-time range.
- **Day** – Compute totals and display results for each day in the designated date-and-time range.

Select By

Indicate which messages are selected.

- **Inbound** – Compute totals and display result columns for inbound message count and size.
- **Outbound** – Compute totals and display result columns for outbound message count and size.
- **Total** – Compute the sum of inbound and outbound messages. Display result columns for total message count and size.
- **Inbound and Outbound** – Compute separate totals for inbound and for outbound messages. Display result columns for inbound message count and size and for outbound message count and size.
- **Inbound, Outbound, and Total** – Compute separate and combined totals for inbound and outbound messages. Display result columns for inbound message count and size, for outbound message count and size, and for total message count and size.

Connection Type

Protocol for which statistics are computed. Only messages using this protocol are selected for computation.

- **All Separated** – Compute statistics for all protocol types. Display results as a sum of all protocol types and (if the results are expanded) as a sum for each protocol type.
- **All Combined** – Compute statistics for all protocol types. Display results as a sum of all protocol types.
- **No Connection**.

- **AS2, Connect:Mailbox, From Engine, FTP, HTTP, Internal, MQ, SMTP** – Compute statistics for messages using one of these protocols. Display results as a sum for this protocol type. Connect:Mailbox and MQ identify messages received from or sent to Sterling Commerce:Network. From Engine and Internal identify messages exchanged between internal systems on the node.

Results

By default, statistics about message volume are displayed in a table. The number of columns depends on the criteria you entered for computing the statistics. In each column, the figure displayed is a sum of the messages in that category. To draw a graph, use the Graph Options — the X-axis and Y-axis drop-down fields and the **Draw Graph** button.

The first two columns display the time period and the protocol type you selected. Click the boxes in the left column to expand or collapse the view. If the Connection Type is All-Separated, expanding the view displays each total broken down by protocol type.

	Date/Time	Connection Type
⊞	03/02/2001 15:00	All
⊟	03/02/2001 19:00	All
		SMTP
		FTP
		Internal

The Inbound Message Count and Size columns are displayed only if you included inbound messages. Inbound message count is the total number of inbound messages received by the node for the time period and protocol type indicated. Inbound message size is the total cumulative size for all inbound messages.

Inbound Msg Count	Inbound Msg Size
27	3445496
7	136997
4	136997
0	0

The Outbound Message Count and Size columns are displayed only if you selected outbound messages. Outbound message count is the total number of outbound messages sent by the node for the time period and protocol type indicated. Outbound message size is the total cumulative size for all outbound messages.

Outbound Msg Count	Outbound Msg Size
27	3445496
7	203586
6	203586
1	0

The Total Message Count and Size columns are displayed only if you selected totals. Total message count is the number of inbound and outbound messages

handled by the node for the time period and protocol type indicated. Total message size is the total cumulative size for all inbound and outbound messages.

Total Msg Count	Total Msg Size
54	6890992
14	340583
10	340583
1	0
3	0

When you view statistics about message volume or message turnaround time, you can display the results in a graph. After a graph is displayed, you can make adjustments, including changing the type of graph, the colors, and the symbols. You can print the graph, and you can paste the data used to construct the graph into other programs.

Drawing and Printing the Graph

About this task

Complete the following steps to draw a graph of the results.

Procedure

1. Open the WAT on the node you want.
2. Select **CSR Access > Node Statistics** and select either **Message Volume** or **Message Turnaround Time**.
3. Specify the information you want to graph and click **Search**.

   By default, results are displayed in a table.
4. In the X-Axis box, select the criterion you want to use for the horizontal axis.
5. In the Y-Axis box, select the criterion you want to use for the vertical axis.
6. Click **Draw Graph**.

   The default graph is displayed in a separate browser window. If necessary, the color legend appears in the upper right.
7. After the graph is displayed, right-click in the graph window and select **Print**.

Adjusting the Graph

After the graph is displayed, use the graph controls at the top of the graph window to make adjustments.

Data Series

Graph type and color used for each coordinate pair of data. For example, message volume statistics can have 1 – 3 coordinate pairs depending on the combination of inbound, outbound, or total messages selected.

- **Graph Type** – Scatter plot, line, area, or column. Scatter plot graphs can use diamonds, rectangles, triangles, or asterisks as symbols. Line and area graphs can use continuous or discrete lines. Column graphs are bar graphs.
- **Color 1** – Principal color used for the data.
- **Color 2** – Outlines color 1.

Zoom

- **Zoom In** – Enlarge the graph.
- **Zoom Out** – Decrease the size of the graph.
- **Fit Window** – Size the graph to fit the window.

Grid Lines

Turn grid lines on and off.

Show Data

Display the data used to construct the graph.

Copy and Paste Graph Data into Another Program

After the graph is displayed, you can display the data used to construct the graph and paste it into another program. Graph data is displayed as comma-delimited text with one coordinate pair per line.

About this task

Complete the following steps to copy and paste the graph data into another program.

Procedure

1. Draw a graph.
2. In the graph window, click **Show Data**.

   Graph data displays in a text box below the graph.
3. To copy the data, select the data in the text box and press **CTRL+C**.
4. Open the external program you want to use. Press **CTRL+V** to paste the data.

   Some programs may require you to paste the data into a text file (such as Notepad) and then import it into the program you want to use.

Viewing the Latest Message Activity

You can display information about messages flowing through the node at any time.

About this task

Complete the following steps to view the latest message activity.

Procedure

1. Open the WAT on the node you want.
2. Select **CSR Access > Node Statistics > Latest Message Activity**.
3. Specify the following information and click **Search**.
   - Start Date/Time, End Date/Time – Date and time range for which statistics are computed. Inbound messages received and the associated outbound messages sent within this range are selected for computation. The default is the last 24 hours. You can request data for the last 35 days.

     Date format: MM/DD/YY

     Time format: HH:MM:SS

     Time zone: UTC
   - Include Reply Messages – Indicate whether results should also include the reply messages (Yes/No).

Results

The results include information about the messages flowing through the node at the specified time and are displayed in a table that is split into the following areas:

- Outbound Messages Non-local Message Store
- Outbound Messages Local Message Store
- Inbound Messages

These areas in the table have the following columns:

- Connection Type – The protocol or connection the message is using.
- Delivery Time – For outbound messages, the time the message was delivered.
- Add Date/Time – For inbound message, the time the message was sent to the node.
- Recipient/Originator Address –

  For outbound messages, the address of the recipient.

  For inbound messages, the address of the originator of the message.
- Outbound/Inbound Message ID

Viewing the Latest Message Snapshot

You can display a summary about the messages flowing through the node at any time.

About this task

To display this information, complete the following steps:

Procedure

1. Open the WAT on the node you want.
2. Select **CSR Access > Node Statistics > Latest Message Snapshot**.
3. Specify the date range and click **Search**.

   Inbound messages received and the associated outbound messages sent within this range are selected for computation. The default is the last 24 hours. You can request data for the last 35 days.

   Date format: MM/DD/YY

   Time format: HH:MM:SS

   Time zone: UTC

Results

The results are split into outbound and inbound messages. For outbound messages, the message count for each delivery status is displayed. For inbound messages, the message count for each processing status is displayed.

Setting up Node Templates

Before you begin

Users with a System Administrator security level can administer the templates for the protocol types used on a node. (See “WAT User Roles and Security Levels” on page 7 for more information.)

About this task

Complete the following steps to set up a node template.

Procedure

1. Open the WAT on the node you want.
2. Select **Node Administration > Node Address Templates**.

   The Node Details page displays, including a list of any address templates that already exist on the node.
3. In the Add New Template section at the bottom of the page, select the type of protocol you want to use and click **Next**.

   The Address Information page displays.
4. Complete the address information, using the following guidelines. If needed, you can click **Clear** (to clear all fields) or **Reset** (to restore all fields to their original values).
   - In the Name and Description fields, it is helpful to include terms like *template* and terms that identify the associated protocol.
   - You cannot change the Mailslot field, which automatically displays *Template*. When a new address uses the template, this value is replaced with an actual messaging address.
   - You cannot change the Password field, which automatically displays *Password*. When a new address uses the template, this value is replaced with an actual password.
5. When you finish, click **Add**.

Adjusting Node Templates

About this task

Complete the following steps to edit a node template.

Procedure

1. Open the WAT on the node you want.
2. Select **Node Administration > Node Address Templates**.

   The Node Details page displays, including a list of any address templates that already exist on the node.
3. Locate the template you want. To the right of the entry, click **Edit**.

   The Address Information page displays, including a protocol section.
4. Change any of the displayed address or protocol information. If needed, you can click **Clear** (to clear all fields) or **Reset** (to restore all fields to their original values).
5. When you finish, click **Update**.

Editing Templates for a Company or Domain

If a group of new addresses deviates from a node template for an addressing protocol, you can edit the template at the company level or at the domain level to which the addresses are added.

About this task

Complete the following steps to edit a template for a company or domain.

Procedure

1. Open the WAT on the node you want.
2. Display the Company Details or Domain Details for the group of addresses being added.
3. On the divider bar, click **Edit Templates**.
4. In the Add New Template section at the bottom of the page, select the type of protocol you want and click **Next**.

   The Address Information page displays.
5. Complete the address information, using the following guidelines. If needed, you can click **Clear** (to clear all fields) or click **Reset** (to restore all fields to their original values).
   - In the Name and Description fields, it is helpful to include terms like *template* and terms that identify the associated protocol.
   - You cannot change the Mailslot field, which automatically displays *Template*. When a new address uses the template, this value is replaced with an actual messaging address.
   - You cannot change the Password field, which automatically displays *Password*. When a new address uses the template, this value is replaced with an actual password.
6. When you finish, click **Add**.

Administering Profiles for the Node

After coding is set up on the node, users with a System Administrator security level can set up, edit, and remove account and address profiles that are associated with the coding. When other users manage profiles for an account or an address, they work only with the account profiles or the address profiles that the System Administrator has set up.

About this task

Complete the following steps to administer profiles for the node.

Procedure

1. Open the WAT on the node you want.
2. Select **Node Administration > System Profiles**.

   The Profile List displays, which includes all account and address profiles that are defined on the node. The Profile List populates the drop-down lists available when users select an account profile or an address profile.
3. Do one of the following:
   - To view details about a profile, locate the profile in the list and click the name.
   - To edit a profile, locate the profile in the list and click **Edit** to the right of the entry.

     The Profile page displays.

     Make the changes you want and click **Update**.
   - To add a profile, click **Add Profile Description** on the divider bar.

     The Profile page displays.

     Complete the information. Be sure to specify the action ID, the type of profile (account or address), the level (single or multiple), and any other information relevant to the underlying code.

- To remove a profile, locate the profile in the list and click **Edit** to the right of the entry.

  The Profile page displays.

  Click **Delete**.

  The profile is removed from the Profile List and is no longer available on the node.

Administering Types for Association IDs

Association IDs are used to track and correlate messages across systems. The ID itself is either assigned by an external system and maintained within Sterling Commerce:Centre or assigned by Sterling Commerce:Centre and maintained in an external system.

Before you begin

Users with a System Administrator security level can set up or edit the type and description labels that appear on message tracking pages to identify messages from particular systems.

About this task

Support for an external system must be added to the Sterling Commerce:Centre database so the appropriate IDs are either maintained or generated for messages passing to that system. At that time, a type (or category label) is set up that will be displayed on message tracking pages with the ID. The type (and its description) identify the external system that sends or receives the message.

Complete the following steps to administer types for association IDs.

Procedure

1. Open the WAT on the node you want.
2. Select **Node Administration > Association ID Type**.

   A list displays, which includes all types and descriptions that are defined on the node.
3. Do one of the following:
   - To view details about a type, locate the type in the list and click the name.
   - To edit a type or its description, locate the type in the list and click the name.

     On the Details page, click **Edit Details**.

     On the Modify page, make the changes you want and click **Update**.
   - To add a type and its description, click **Add Association ID Type**.

     On the Add page, type the text you want to use for the type and the description.

     Click **Finish**.

Distributor Nodes

Distributor nodes are installations of Sterling Commerce:Centre that are outside of the United States. The node in Mexico is owned and operated by a third party. Traffic from former distributor nodes may continue to enter Sterling B2B Collaboration Network even though the business relationship with the distributor has changed.

Distributors perform some customer support and system maintenance for their nodes, such as handling Level 1 customer problems, running backups, and maintaining hardware. However, distributor nodes are installed, upgraded, and monitored by Sterling B2B Collaboration Network operations and technical personnel.

Implementation

When Sterling Commerce:Centre is installed on a distributor node, the Sterling B2B Collaboration Network implementation team establishes a URL address for the node and uses an initial user ID (with the System Administrator security level) to finish implementation. Afterward, the implementation team establishes the first user ID for the distributor to use. Typically, this user ID is assigned the Super User security level and is used to set up accounts and register other user IDs for the distributor node.

Setting Up the Account Hierarchy

Distributors need to structure the account hierarchy in a way that suits their business needs and contract specifications. Company and domain information is entered in the back-end systems and replicated to the distributor node. Included in the domain information is a unique mailbox that is tied to the back-end billing system. Distributors need to work with IBM to determine how to structure their account hierarchy so that billing concerns and data-entry concerns are addressed.

A distributor's contract with IBM specifies how billing is handled. The following scenarios illustrate the ramifications of different account structures.

- Scenario 1. Create an account hierarchy under a single company-domain that corresponds to the distributor. After, set up accounts on the node for the distributor's customers. This scenario ties billing to a single mailbox associated with the distributor and eliminates the need to contact IBM when company or domain information must be entered or changed.
- Scenario 2. Create an account hierarchy under a single company that corresponds to the distributor but includes domains associated with each of the distributor's customers. This scenario ties billing to mailboxes associated with the distributor's customers, but it requires the distributor to contact IBM when domain information must be entered or changed.
- Scenario 3. Create an account hierarchy that includes multiple companies with one or more domains beneath each one. This scenario ties billing to mailboxes associated with each of the distributor's customers but requires the distributor to contact IBM when company or domain information must be entered or changed.

Functionality on Distributor Nodes

Some services offered by Sterling B2B Collaboration Network are not available on distributor nodes.

- Interconnects to other VANs over FTP
- U.S. Customs Gateway service

Chapter 9. Reference: Billing, Status, and Error Codes

Billing Codes

Codes are displayed in the Billing Flag field on the Message Detail page for inbound or outbound messages.

The node assigns one or more billing codes to an inbound or outbound message. Billing codes are processed by GBS.

The following list describes the billing codes:

- Consider Primary – The billing server should consider this message as the primary message.
- Consider Secondary – The billing server should consider this message as the secondary message.
- Connect Record Generated – The message is billed based on the protocol connector.
- Data Record Generated – The message is billed based on the actual data.
- Report Record Generated – The message is billed as a report.
- Reply Record Generated – The message is billed as a reply.
- Translate Record Generated – The message is billed as a translation.
- No Address To Bill – Warning message. The message cannot be billed because it is not associated with an address on the node.
- No Data Record Generated – The message is not billed for the actual data. The node is configured so that no bill is generated for the message based on the actual data of the message.
- No Connect Record Generated – The message is not billed for the protocol connector. The node is configured so that no bill is generated for the message based on the protocol connector.
- No Outgoing Record Generated – The message is not billed by the node because another system has already billed for it. Examples of such messages include the following:
  - Inbound messages from Sterling Commerce:Network
  - Outbound messages to Sterling Commerce:Network
  - Inbound messages from other nodes
  - Outbound messages routed to Sterling Commerce:Network through the Defer Routing profile

Account and Address Status Codes

Status codes are assigned by the node and are displayed in the Status field on Account, Address, and EDI Information pages.

Status code	Description	Display Color
Active 2	The account, address, or EDI ID is active and can send and receive messages. This status is set automatically when an account, address, or EDI ID is added successfully to the node and (if necessary) to Sterling Commerce:Network. If an address or EDI ID is coupled with a Sterling Commerce:Network item, the item is added to the node first and then added to Sterling Commerce:Network asynchronously.	Green
Add Failed 11	The account, address, or EDI ID was not added, usually because a coupled Sterling Commerce:Network item could not be added. A coupled item is added to the node first and then added to Sterling Commerce:Network asynchronously. If the Sterling Commerce:Network addition is unsuccessful, the status becomes Add Failed and the addition stops. The item is not added to Sterling Commerce:Network or to the node.	Red
Add Pending 1	The account, address, or EDI ID is being added to the node and coupled with a Sterling Commerce:Network mailslot or EDI ID. A coupled item is added to the node first and then added to Sterling Commerce:Network asynchronously. This status indicates that the asynchronous process on Sterling Commerce:Network is not finished.	Yellow
Couple Failed 13	The address or EDI ID was not added to Sterling Commerce:Network. The On SuperTracs setting for the item remains No.	Red
Couple Pending 9	An address is being coupled with a Sterling Commerce:Network mailslot or an EDI ID is being coupled with a Sterling Commerce:Network EDI ID. The asynchronous process of adding the item to Sterling Commerce:Network is not finished.	Yellow
Decouple Failed 14	The address or EDI ID was not removed from Sterling Commerce:Network. The On SuperTracs setting was not changed to No.	Red
Decouple Pending 10	An address is being decoupled from a Sterling Commerce:Network mailslot or an EDI ID is being decoupled from a Sterling Commerce:Network EDI ID. The asynchronous process of removing the item from Sterling Commerce:Network is not finished.	Yellow
	The account, address, or EDI ID is marked for deletion by the housekeeping process.	Red
Delete Failed 7	The account, address, or EDI ID could not be removed, usually because a coupled Sterling Commerce:Network item could not be removed successfully. A coupled item is removed first from Sterling Commerce:Network through an asynchronous process and then from the node. If the Sterling Commerce:Network deletion is unsuccessful, the status becomes Delete Failed and the process stops. The item remains on Sterling Commerce:Network and on the node.	Red
Delete Pending 5	The account, address, or EDI ID is being deleted from the node. A coupled item is removed first from Sterling Commerce:Network through an asynchronous process and then from the node. The asynchronous process on Sterling Commerce:Network is not finished.	Yellow

Status code	Description	Display Color
Delete Succeeded 6	The account, address, or EDI ID is removed from the node and (if necessary) from Sterling Commerce:Network. If an address or EDI ID is coupled with a Sterling Commerce:Network item, the item is removed on Sterling Commerce:Network first and then removed from the node. Deletions follow the account hierarchy, so that deleting an account removes all associated addresses and EDI IDs. Deleting an address removes all associated EDI IDs.	Red
Inactive 3	The account, address, or EDI ID is inactive on the node and cannot be used to send or receive messages.	Red
Migration Failed 12	EDI IDs could not be migrated from the source mailbox or mailslot to the target address on the node. If the source is on the node, the target is an address on the node. If the source is on Sterling Commerce:Network, the target is an address on the node that is coupled with a Sterling Commerce:Network target. An error code indicates the problem.	Red
Migration Pending 8	EDI IDs are being moved from the source mailbox or mailslot to the target address on the node. If the source is on the node, the target is an address on the node. If the source is on Sterling Commerce:Network, the target is an address on the node that is coupled with a Sterling Commerce:Network target. EDI IDs are first moved from the source to the target on Sterling Commerce:Network and then moved to the target on the node. The migration process is not finished.	Yellow
Update Pending 15	Information for an account, address, or EDI ID has been updated on the node and changes are being replicated to Sterling Commerce:Network. Updating account information changes the status of all associated addresses and EDI IDs to Update Pending.	Yellow
Update Failed 16	Information for an account, address, or EDI ID has been updated on the node but has not replicated correctly to Sterling Commerce:Network. The changes remain on the node but have not been made to Sterling Commerce:Network. If an update to account information fails, the status of all associated addresses and EDI IDs changes to Update Failed. Contact Level 2 to resolve the problem on Sterling Commerce:Network.	Red
Unknown 0	The account, address, or EDI ID is missing or corrupt. Usually, this status occurs only during testing.	Red

Error Codes in Account, Address, and EDI Information

Account, Address, or EDI Errors 00 – 09

Error Code	Description and Where Displayed	Cause and Action
00	You are migrating EDI IDs from a source mailslot on Sterling Commerce:Network or on the node to a target address (mailslot) on the node. Error Code field, Account, Address, and EDI Information pages	The migration is successful. All EDI IDs are moved to the target mailslot and removed from the source mailslot. • If the source mailslot resides on Sterling Commerce:Network, the mailslot is removed. • If the source mailslot resides on the node, the EDI IDs are removed but the address still exists.

Error Code	Description and Where Displayed	Cause and Action
01	You are migrating EDI IDs from a source mailslot on Sterling Commerce:Network or on the node to a target address (mailslot) on the node. Error Code field, Account, Address, and EDI Information pages	The source mailbox or mailslot does not exist. Level 1. The messaging address specified for the source mailslot cannot be found. Check the messaging address and retry with a corrected address.
02	You are migrating EDI IDs from a source mailslot on Sterling Commerce:Network or on the node to a target address (mailslot) on the node. Error Code field, Account, Address, and EDI Information pages	The target mailslot does not exist. Level 1. The messaging address specified for the target mailslot cannot be found. Add the address for the target and retry.
03	Mailbox migration. Error Code field, Account, Address, and EDI Information pages	Mailbox to migrate from is part of the same mailbox as the mailslot to migrate to. Applies when EDI IDs are moved to a target mailslot on the node from a source mailslot on Sterling Commerce:Network or on the node. Both the messaging addresses specified for the source and target mailslots exist within the same mailbox. You must specify source and target mailslots that reside in different mailboxes.

Account, Address, or EDI Errors 20 – 29

Error Code	Description and Where Displayed	Cause and Action
20	You are updating EDI information for an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, EDI Information page	The EDI Information cannot be updated on Sterling Commerce:Network because the action code is invalid. Level 1. Contact Production Control, who may contact Level 3 (Sterling Commerce:Centre Development) to resolve the issue.
21	You are adding EDI information to an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, EDI Information page	The EDI information cannot be added to Sterling Commerce:Network because the EDI information is missing from the request. Level 1. Contact Production Control, who may contact Level 3 (Sterling Commerce:Centre Development) to resolve the issue.
22	You are adding EDI information to an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, EDI Information page	The EDI information cannot be added to Sterling Commerce:Network because the mailslot associated with the EDI IDs does not exist on Sterling Commerce:Network. Level 1. First, verify that the mailslot to which you are adding EDI IDs is not set up on Sterling Commerce:Network. Next, display the address on Sterling Commerce:Centre. In the On SuperTracs field, use Couple to add the address to Sterling Commerce:Network. Finally, add the EDI information.

Error Code	Description and Where Displayed	Cause and Action
23	You are adding EDI information to an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, EDI Information page	The EDI information cannot be added to Sterling Commerce:Network because the mailslot associated with the EDI IDs is not flagged as a mailslot owned by Sterling Commerce:Centre. On Sterling Commerce:Network, a code indicates that a mailslot is owned by Sterling Commerce:Centre. Level 1. Verify that the mailslot to which you are adding EDI IDs is owned by Sterling Commerce:Centre. Also verify that Sterling Commerce:Network indicates ownership correctly.
24	You are adding EDI information to an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, EDI Information page	The EDI information cannot be added to Sterling Commerce:Network because the customer flag is invalid. Level 1. Contact Production Control, who may contact Level 3 (Sterling Commerce:Centre Development) to resolve the issue.
25	You are adding EDI information to an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, EDI Information page	The EDI information cannot be added to Sterling Commerce:Network because the EDI ID is already set up on Sterling Commerce:Network. Level 1. Verify that the EDI ID is set up on Sterling Commerce:Network and that it belongs to the appropriate mailslot. If the information on Sterling Commerce:Centre and on Sterling Commerce:Network is the same, display the EDI information on Sterling Commerce:Centre and use the On SuperTracs field to select a SuperTracs region.
26	You are updating EDI information for an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, EDI Information page	The EDI information cannot be updated on Sterling Commerce:Network because the EDI ID is not set up on Sterling Commerce:Network. Level 1. Verify that the EDI ID is not set up on Sterling Commerce:Network. To add the EDI ID to Sterling Commerce:Network, display the EDI information on Sterling Commerce:Centre. Opposite the EDI ID field, use Couple to add the EDI ID to Sterling Commerce:Network.
27	You are updating EDI information for an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, EDI Information page	The EDI information cannot be updated on Sterling Commerce:Network because the EDI ID is not owned by Sterling Commerce:Centre. Level 1. Verify that the EDI ID is owned by Sterling Commerce:Centre. Also verify that Sterling Commerce:Network indicates ownership correctly.
28	You are updating EDI information for an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, EDI Information page	The EDI information cannot be updated on Sterling Commerce:Network because the customer flag is invalid. Level 1. Contact Production Control, who may contact Level 3 (Sterling Commerce:Centre Development) to resolve the issue.

Account, Address, or EDI Errors 30 – 39

Error Code	Description and Where Displayed	Cause and Action
30	You are deleting EDI information from an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, EDI Information page	The EDI information cannot be deleted on Sterling Commerce:Network because the EDI ID is not set up on Sterling Commerce:Network. Level 1. Verify that the EDI ID is not set up on Sterling Commerce:Network. To delete an EDI ID that exists only on Sterling Commerce:Centre, display the EDI information on Sterling Commerce:Centre. Update the On SuperTracs field to No. Then delete the EDI ID.
31	You are deleting EDI information from an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, EDI Information page	The EDI information cannot be deleted on Sterling Commerce:Network because it is not owned by Sterling Commerce:Centre. Level 1. Verify that the EDI ID should be deleted from Sterling Commerce:Network and that Sterling Commerce:Network indicates that the EDI ID is owned by Sterling Commerce:Centre. If the EDI ID should be removed from Sterling Commerce:Centre only, display the EDI information on Sterling Commerce:Centre. Update the On SuperTracs field to No. Then delete the EDI ID.

Account, Address, or EDI Errors 40 – 49

Error Code	Description and Where Displayed	Cause and Action
40	You are updating an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The address information cannot be updated on Sterling Commerce:Network because the action code is invalid. Level 1. Contact Production Control, who may contact Level 3 (Sterling Commerce:Centre Development) to resolve the issue.
41	You are adding an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The address cannot be added to Sterling Commerce:Network because the specified error mailslot is not set up on Sterling Commerce:Network. Level 1. On Sterling Commerce:Centre, verify that the error mailslot is specified correctly. • If the error mailslot is incorrect, edit the address on Sterling Commerce:Centre and re-enter the error mailslot. Then use Couple to add the address to Sterling Commerce:Network. • If the error mailslot is correct, verify that the error mailslot does not exist on Sterling Commerce:Network. If necessary, add the error mailslot to Sterling Commerce:Network. Finally, display the address on Sterling Commerce:Centre and use Couple to link the address to its counterpart on Sterling Commerce:Network.

Error Code	Description and Where Displayed	Cause and Action
42	You are adding an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The address cannot be added to Sterling Commerce:Network because the address (mailslot) template is missing. Level 1. Contact Production Control, who may contact Level 3 (Sterling Commerce:Network Development) to resolve the issue.
43	You are adding an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The address cannot be added to Sterling Commerce:Network because the customer flag is invalid. Level 1. Contact Production Control, who may contact Level 3 (Sterling Commerce:Centre Development) to resolve the issue.
44	You are adding an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The address cannot be added to Sterling Commerce:Network because the interconnect profile (IPRO) was not found on Sterling Commerce:Network during validation. Level 1. Verify that the address requires an interconnect profile on Sterling Commerce:Network and that an interconnect profile does not exist for it. If the IPRO is needed but does not exist on Sterling Commerce:Network, contact Production Control, who may contact Level 3 (Sterling Commerce:Network Development) to resolve the issue.
45	You are adding an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The address cannot be added because the associated Sterling Commerce:Network mailslot is already set up on the CICS MB01 screen. Level 1. In CICS, verify that the MB01 screen for this mailslot includes the same information and belongs to the same customer as the address on the node. If so, display the address on Sterling Commerce:Centre and use the On SuperTracs field to select a SuperTracs region.
46	You are adding an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The address cannot be added because the default Sterling Commerce:Network template does not exist on the CICS MB02 screen. Level 1. Contact Production Control, who may contact Level 3 (Sterling Commerce:Network Development) to resolve the issue.
47	You are adding an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The address cannot be added because the associated Sterling Commerce:Network mailslot is already set up on the CICS MB02 screen. Level 1. In CICS, verify that the MB02 screen for this mailslot includes the same information and belongs to the same customer as the address on the node. Check that all necessary information is completed on the MB02 screen. If so, display the address on Sterling Commerce:Centre and use the On SuperTracs field to select a SuperTracs region.

Error Code	Description and Where Displayed	Cause and Action
48	You are adding an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The address cannot be added because Sterling Commerce:Network already has an MB01-to-MB02 cross-reference for this mailslot. Level 1. Contact Production Control, who may contact Level 3 (Sterling Commerce:Network Development) to resolve the issue.
49	You are adding an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The address cannot be added because there is already a SECURITY setup on Sterling Commerce:Network with the same mailslot. Level 1. Contact Production Control, who may contact Level 3 (Sterling Commerce:Network Development) to resolve the issue.

Account, Address, or EDI Errors 50 – 59

Error Code	Description and Where Displayed	Cause and Action
50	You are adding an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The mailslot cannot be added to Sterling Commerce:Network because the interconnect profile (IPRO) is not set up on Sterling Commerce:Network. Level 1. Verify that the mailslot requires an interconnect profile on Sterling Commerce:Network and that an interconnect profile does not exist for it. If the IPRO is needed but does not exist on Sterling Commerce:Network, contact Production Control, who may contact Level 3 (Sterling Commerce:Network Development) to resolve the issue.
52	You are adding an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The mailslot cannot be added to Sterling Commerce:Network because the error mailslot is not set up on Sterling Commerce:Network. Level 1. On Sterling Commerce:Centre, verify that the error mailslot is specified correctly. If so, add the error mailslot to Sterling Commerce:Network. Then display the address on Sterling Commerce:Centre and use Couple to link the address to its counterpart on Sterling Commerce:Network.
53	You are updating an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The mailslot cannot be updated on Sterling Commerce:Network because it is not set up on Sterling Commerce:Network. Level 1. Verify that the mailslot should exist on Sterling Commerce:Network. If so, display the address on Sterling Commerce:Centre and use Couple to add the address to Sterling Commerce:Network.
54	You are updating an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The mailslot cannot be updated on Sterling Commerce:Network because Sterling Commerce:Centre does not own it. Level 1. Verify that the mailslot should be on Sterling Commerce:Centre. If so, display the mailslot on Sterling Commerce:Network and change the owner flag to Sterling Commerce:Centre. Then, update the address information on Sterling Commerce:Centre.

Error Code	Description and Where Displayed	Cause and Action
55	You are updating an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The mailslot cannot be updated on Sterling Commerce:Network because the customer flag is invalid. Level 1. Contact Production Control, who may contact Level 3 (Sterling Commerce:Centre Development) to resolve the issue.
56	You are updating an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The mailslot cannot be updated on Sterling Commerce:Network because the update of the CICS MB01 screen failed. Level 1. Contact Production Control, who may contact Level 3 (Sterling Commerce:Network Development) to resolve the issue.
57	You are updating an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The mailslot cannot be updated on Sterling Commerce:Network because the CICS MB02 screen is not set up. Level 1. Verify that the mailslot should be set up on Sterling Commerce:Network. If so, correct the CICS MB02 screen on Sterling Commerce:Network. Then display the address on Sterling Commerce:Centre and use Couple to add the mailslot to Sterling Commerce:Network.
58	You are updating an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The mailslot cannot be updated on Sterling Commerce:Network because the update of the CICS MB02 screen failed. Level 1. Contact Production Control, who may contact Level 3 (Sterling Commerce:Network Development) to resolve the issue.
59	You are updating an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The mailslot cannot be updated on Sterling Commerce:Network because the MB01-to-MB02 cross-reference is not set up on Sterling Commerce:Network. Level 1. Contact Production Control, who may contact Level 3 (Sterling Commerce:Network Development) to resolve the issue.

Account, Address, or EDI Errors 60 – 69

Error Code	Description and Where Displayed	Cause and Action
60	You are updating an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The mailslot cannot be updated on Sterling Commerce:Network because the update of the MB01-to-MB02 cross reference failed. Level 1. Contact Production Control, who may contact Level 3 (Sterling Commerce:Network Development) to resolve the issue.
61	You are updating an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The mailslot cannot be updated on Sterling Commerce:Network because the SECURITY setup does not exist on Sterling Commerce:Network. Level 1. Contact Production Control, who may contact Level 3 (Sterling Commerce:Network Development) to resolve the issue.

Error Code	Description and Where Displayed	Cause and Action
62	You are updating an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The mailslot cannot be updated on Sterling Commerce:Network because the update of the SECURITY setup failed. Level 1. Contact Production Control, who may contact Level 3 (Sterling Commerce:Network Development) to resolve the issue.
63	You are deleting an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The mailslot cannot be deleted from Sterling Commerce:Network because it is not set up on Sterling Commerce:Network. Level 1. Verify that the mailslot does not exist on Sterling Commerce:Network. If so, display the address on Sterling Commerce:Centre and change the On SuperTracs field to No. Then delete the address on Sterling Commerce:Centre.
64	You are deleting an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The mailslot cannot be deleted from Sterling Commerce:Network because Sterling Commerce:Centre does not own it. Level 1. Verify that the mailslot should be deleted from Sterling Commerce:Network. If so, change the owner flag on Sterling Commerce:Network so that Sterling Commerce:Centre owns the mailslot. Then, delete the address on Sterling Commerce:Centre.
65	You are deleting an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The mailslot cannot be deleted from Sterling Commerce:Network because the setup on the CICS MB01 screen could not be deleted. Level 1. Contact Production Control, who may contact Level 3 (Sterling Commerce:Network Development) to resolve the issue.
66	You are deleting an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The mailslot cannot be deleted from Sterling Commerce:Network because the setup on the CICS MB02 screen could not be deleted. Level 1. Contact Production Control, who may contact Level 3 (Sterling Commerce:Network Development) to resolve the issue.
67	You are deleting an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The mailslot cannot be deleted from Sterling Commerce:Network because the MB01-to-MB02 cross-reference could not be deleted. Level 1. Contact Production Control, who may contact Level 3 (Sterling Commerce:Network Development) to resolve the issue.
68	You are deleting an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The mailslot cannot be deleted from Sterling Commerce:Network because the interconnect profile (IPRO) was not found. Level 1. Contact Production Control, who may contact Level 3 (Sterling Commerce:Network Development) to resolve the issue.

Error Code	Description and Where Displayed	Cause and Action
69	You are deleting an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The mailslot cannot be deleted from Sterling Commerce:Network because the interconnect profile (IPRO) failed to delete. Level 1. Contact Production Control, who may contact Level 3 (Sterling Commerce:Network Development) to resolve the issue.

Account, Address, or EDI Errors 70 – 79

Error Code	Description and Where Displayed	Cause and Action
70	You are deleting an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Address page	The mailslot cannot be deleted from Sterling Commerce:Network because the SECURITY setup failed to delete. Level 1. Contact Production Control, who may contact Level 3 (Sterling Commerce:Network Development) to resolve the issue.
74	You are adding an address that is coupled with a Sterling Commerce:Network mailslot. Error Code field, Account and Address Information pages	The SuperTracs indicator is invalid or missing. Level 1. Contact OSS, who may contact Level 3 (Sterling Commerce:Centre development) to resolve the issue.

Account, Address, or EDI Errors 80 – 89

Error Code	Description and Where Displayed	Cause and Action
80	You are migrating EDI IDs from source mailslots on Sterling Commerce:Network to the current address (the target) on Sterling Commerce:Centre. The target address is coupled with a Sterling Commerce:Network mailslot. Error Code field, Account, Address, and EDI Information pages.	The mailslots cannot be migrated on Sterling Commerce:Network because the source mailbox is the same as the target mailbox. Level 1. Verify the source and target information. The source mailslot and the target address must reside in different mailboxes.
81	You are migrating EDI IDs from a source mailslot on Sterling Commerce:Network to the current address (the target) on Sterling Commerce:Centre. The target address is coupled with a Sterling Commerce:Network mailslot. Error Code field, Account, Address, and EDI Information pages.	The mailslot cannot be migrated on Sterling Commerce:Network because the source mailslot is the same as the target mailslot. Level 1. Verify the source and target information. The source mailslot must be different from the target address (mailslot).
82	You are migrating EDI IDs from source mailslots on Sterling Commerce:Network to the current address (the target) on Sterling Commerce:Centre. The target address is coupled with a Sterling Commerce:Network mailslot. Error Code field, Account, Address, and EDI Information pages.	The mailslots cannot be migrated on Sterling Commerce:Network because the source mailbox is not set up on Sterling Commerce:Network. Level 1. Verify the source and target information. The source mailslots must reside in a mailbox that exists on Sterling Commerce:Network.

Error Code	Description and Where Displayed	Cause and Action
83	You are migrating EDI IDs from a source mailslot on Sterling Commerce:Network to the current address (the target) on Sterling Commerce:Centre. The target address is coupled with a Sterling Commerce:Network mailslot. Error Code field, Account, Address, and EDI Information pages.	The mailslot cannot be migrated on Sterling Commerce:Network because the source mailslot is not set up on Sterling Commerce:Network. Level 1. Verify the source and target information. The source mailslot must exist on Sterling Commerce:Network.
84	You are migrating EDI IDs from a source mailslot on Sterling Commerce:Network to the current address (the target) on Sterling Commerce:Centre. The target address is coupled with a Sterling Commerce:Network mailslot. Error Code field, Account, Address, and EDI Information pages.	The mailslot cannot be migrated on Sterling Commerce:Network because the source mailslot is not set up on Sterling Commerce:Network. Level 1. Verify the source and target information. The source mailslot must exist on Sterling Commerce:Network.
85	You are migrating EDI IDs from a source mailslot on Sterling Commerce:Network to the current address (the target) on Sterling Commerce:Centre. The target address is coupled with a Sterling Commerce:Network mailslot. Error Code field, Account, Address, and EDI Information pages.	The mailslot cannot be migrated on Sterling Commerce:Network because the target mailslot is not set up on Sterling Commerce:Network. Level 1. Verify the source and target information. If the target address (mailslot) is correct, display the address on Sterling Commerce:Centre. In the On SuperTracs field, use Couple to add an associated Sterling Commerce:Network mailslot. When the status of the address is Active, migrate the EDI IDs to the target.

Account, Address, or EDI Errors 90 – 99

Error Code	Description and Where Displayed	Cause and Action
90	You are migrating EDI IDs from a source mailslot on Sterling Commerce:Network to the current address (the target) on Sterling Commerce:Centre. The target address is coupled with a Sterling Commerce:Network mailslot. Error Code field, Account, Address, and EDI Information pages.	The EDI IDs cannot be migrated as the CF01 information for the EDI ID is not found. Make sure the EDI ID exists on the Network and is associated with the right source mailslot.
91	You are migrating EDI IDs from a source mailslot on Sterling Commerce:Network to the current address (the target) on Sterling Commerce:Centre. The target address is coupled with a Sterling Commerce:Network mailslot. Error Code field, Account, Address, and EDI Information pages.	The EDI IDs cannot be migrated as the MB01 information for the source mailslot is not found on Sterling Commerce:Network. Make sure the source mailslot exists on Sterling Commerce:Network and the EDI ID being migrated is associated with this mailslot.
92	You are migrating EDI IDs from a source mailslot to the current address (the target) on Sterling Commerce:Network. Error Code field, Account, Address, and EDI Information pages.	The EDI IDs cannot be migrated as the MB01 information for the destination mailslot cannot be found on Sterling Commerce:Network. Make sure the destination mailslot exists on Sterling Commerce:Network.

Error Codes in Messages

Errors 0000–9999: Undeliverable Messages

Error Code	Description	Error Type and Where Displayed	Cause and Action
3358	Message undeliverable because recipient is not set up on MTA.		

Errors AS1000–AS1999: AS1, AS2 Messages

Error Code	Description	Error Type and Where Displayed	Cause and Action
AS1001	Decryption failure.	AS1, AS2. Error Code field, Message Detail pages	For inbound messages, the node received AS1 or AS2 data from the trading partner and either could not find the correct encryption key or encountered an error during decryption. For outbound messages, the node received an MDN from the trading partner reporting an unsuccessful decryption of AS1 or AS2 data sent from the node.
AS1002	Authentication failure.	AS1, AS2. Error Code field, Message Detail pages	For inbound messages, the node received AS1 or AS2 data from the trading partner and either could not find the correct signing key or the signature verification failed. For outbound messages, the node received an MDN from the trading partner reporting an authentication failure in AS1 or AS2 data sent by the node.
AS1003	Received Content MIC failure.	AS1, AS2. Error Code field, Message Detail pages	A Message Integrity Check (MIC) fails when the hash values for the digital signature do not match. In this case, the data may be corrupt or altered or the AS1 or AS2 implementation on the two systems may not be compatible. This error can occur in two circumstances: • For inbound messages, the node received AS1 or AS2 data from the trading partner and the hash value in the digital signature did not match the value computed by the node. • For outbound messages, the node received an MDN from the trading partner reporting that the hash value in the digital signature did not match the value computed by the trading partner.
AS1998	Error.	AS1, AS2. Error Code field, Message Detail pages	An error occurred.

Error Code	Description	Error Type and Where Displayed	Cause and Action
AS1999	Internal system error.	AS1, AS2. Error Code field, Message Detail pages	An error occurred within Sterling Commerce:Centre. Check theWindows Event Log on the node.

Errors SC_X400: X.400 Messages

Error Code	Description	Error Type and Where Displayed	Cause and Action
SC_X400_COD_ NOT_ARRIVED	X400 COD has not arrived.	X400. Error Code field, Message Detail pages	
SC_X400_COR_ NOT_ARRIVED	X400 COR has not arrived.	X400. Error Code field, Message Detail pages	

Errors SC00001–SCAS1001: AS1, AS2, Generic MIME Handler

Error Code	Description	Error Type and Where Displayed	Cause and Action
SC00001	Invalid signature on MDN.	AS1 Generic MIME Handler. Error Code field, Message Detail pages	A signed MDN was received for this message, but the signature is invalid. Level 1. Verify that the correct certificate is installed and selected on the node for the trading partner. Level 3. Look at the original outbound message to verify that a signed MDN was requested.
SC00002	Unsigned MDN received when signed MDN requested.	AS1 Generic MIME Handler. Error Code field, Message Detail pages	An unsigned MDN was received, but a signature is required. Level 1. Look at the MDN to see if there is another underlying issue. Contact the trading partner to verify that information is correct on the sender's system. Level 3. Look at the original outbound message to verify that a signed MDN was requested.

Error Code	Description	Error Type and Where Displayed	Cause and Action
SC00003	Synchronous MDN send failed.	AS2 Inbound HTTP Gateway. Error Code field, Message Detail pages	This error occurs when communications are dropped after the node receives the inbound message but before or during the time the node sends the MDN. Normally, this error occurs when local processing time takes longer than the network activity time-out on the trading partner's system or on the node. Level 1. Have the trading partner resend the original message per the AS2 draft. This action should re-send the failed MDN. Check for communications errors and the status of the original message that generated the MDN. Level 2 or 3. Check the Inbound HTTP gateway, the Generic MIME Handler, and the CMS Data Server logs for further details if the problem recurs.
SC00004	MDN not received.	AS2 Retry Monitor. Error Code field, Message Detail pages	An MDN has not been received in response to an outbound AS2 message. MDN should be returned within the time-out interval that is set on the node. MDN time-out periods vary by node. Level 1. Contact the trading partner to determine why an MDN was not sent. Verify that the AS2 address on the node requests an MDN. If the AS2 address is not set up correctly, the MDN may not be requested or received.
SC00005	Invalid Certificate Authority (untrusted root).	AS2 Outbound AS2 Gateway. Error Code field, Message Detail pages	The HTTPS server certificate provided by the trading partner is invalid. If the message that could not be delivered is an MDN, the error is displayed on the original inbound message. Level 2 or 3. Install the server certificate or the Certificate Authority's root as a trusted root on the machine running the Outbound AS2 Gateway.
SC00006	Invalid date or certificate expired.	AS2 Outbound AS2 Gateway. Error Code field, Message Detail pages	The HTTPS server certificate provided by the trading partner is invalid. If the message that could not be delivered is an MDN, the error is noted on the original inbound message. Level 1. Contact the trading partner to update the certificate so that it is valid.

Error Code	Description	Error Type and Where Displayed	Cause and Action
SC00007	Invalid common name (server name) on SSL certificate.	AS2 Outbound AS2 Gateway. Error Code field, Message Detail pages	The HTTPS server certificate provided by the trading partner is invalid. The certificate common name must match the name of the name of the Web server in the Host Name field of the trading partner's AS2 address on the node. If the message that could not be delivered is an MDN, the error is noted on the original inbound message. Level 1. Contact the trading partner to update the certificate so that it is valid. **Note:** Cyclone uses the Contact field of its Company Profile as the certificate common name.
SC00008	Message Undeliverable.	AS2 Outbound AS2 Gateway. Error Code field, Message Detail pages	The message could not be delivered, usually because of a setup problem on the node. Level 1. Check the trading partner's AS2 address on the node and verify that the HTTP parameters are correct.
SC00009	Invalid Receipt Delivery Option.	AS2 Outbound AS2 Gateway. Error Code field, Message Detail pages	An asynchronous MDN was requested, but the Receipt-Delivery-Option string specifying the URL is invalid. Usually, this error is caused by a setup problem on the trading partner's AS2 system. Level 1. Look at the raw message for the Receipt-Delivery-Option header to determine the issue. Contact the trading partner to have them correct the problem.
SC00010	MDN creation failed.	AS2 Generic MIME Handler. Error Code field, Message Detail pages	An MDN could not be created for the message. Level 1. Look at the original outbound message to verify that a signed MDN was requested. Level 3. If a signed MDN was requested correctly, there may have been a setup problem during the installation of Sterling Commerce:Centre. An AS2 System Security ID record must be set up.

Error Code	Description	Error Type and Where Displayed	Cause and Action
SC00011	CMS Archive Failed.	All types CMSObjs. Error Code field, Message Detail pages	Level 2 and 3. Each message entry in the database refers to a segment within a file that contains the actual message. Those files are known collectively as the archive, and are stored in `\Centre\Storage`. This error indicates one of two problems: • For inbound messages, it means that the archive file could not be written. • For outbound messages, it means that the archive files are either missing or corrupted and the message cannot be retrieved. For inbound messages, make sure that the permissions on the Storage folder allow files to be written. For outbound messages, this error usually indicates that some of the archive files have been deleted. They may need to be restored from backup.
SC00012	Duplicate AS2 message received	AS2 Generic MIME Handler, CIMS messages. Error Code field, Message Detail pages	The inbound message requested a synchronous MDN. The original HTTP connection failed after the node received the data but before the MDN was sent. The sender did not receive an MDN and resent the data in accordance with the AS2 standard. This error is also generated for CIMS messages. CIMS has one message and repeatedly resends the data. Level 1. No action is required. The node logs the duplicate message with the same transaction ID as the original message. It does not replicate the data, but returns the identical response (MDN) that it tried for the original message.

Error Code	Description	Error Type and Where Displayed	Cause and Action
SC00013	An AS2 message was received with an unknown sender.	AS2 Generic MIME Handler. Error Code field, Message Detail pages	The AS2 identifier in the message does not match any AS2 address set up on the node. This error can be caused by errors in the AS2 address set up on the node. However, repeated instances of this error could indicate that the node is being spammed. Level 1. Display message details for the failed message. Display attachment 0 and check the AS2-From field in the data. If the message is from a known trading partner, check that the AS2-From field in the data matches the Identifier field in the AS2 address for the trading partner. Correct the problem in the AS2 address or contact the trading partner to correct the problem in the AS2-From field being sent. The trading partner can resend the message. Notify Level 2 and 3 if you suspect that the node is being spammed.
SC00014	HTTP synchronous response not sent.	AS2 Generic MIME Handler. Error Code field, Message Detail pages	
SC00015	Failed to build a MIME message.	AS1, AS2 Generic MIME Handler. Error Code field, Message Detail pages	An internal error occurred. Possible causes include: an installation setup or upgrade error, a transient error (such as the database is down), or a software bug. Level 1. If this is the only outbound message that was affected, attempt to restart the inbound message. Level 2 or 3. Check the Generic MIME Handler log to obtain more error details.
SC00016	AS2 recipient is unknown.	AS1, AS2 Generic MIME Handler. Error Code field, Message Detail pages	
SC00017	Decompression failed on an AS1 or AS2 message.	AS1, AS2 Generic MIME Handler. Error Code field, Message Detail pages	
SC00018	Could not parse an inbound MDN.	AS1, AS2 Generic MIME Handler. Error Code field, Message Detail pages	

Error Code	Description	Error Type and Where Displayed	Cause and Action
SC00019	Disposition type (processed or failed) is missing in an inbound MDN.	AS1, AS2 Generic MIME Handler. Error Code field, Message Detail pages	
SC00020	Received MDN could not be matched with an outbound message.	AS1, AS2 Generic MIME Handler. Error Code field, Message Detail pages	
SC00021	Failed to read HTTP synchronous response.	AS1, AS2 Generic MIME Handler. Error Code field, Message Detail pages	
SCAS1001	AS1 or AS2 MDN not received.	AS1, AS2. Error Code field, Message Detail pages	For inbound messages, the node received an MDN from the trading partner indicating that AS1 or AS2 data was sent to the node, but the node did not return an MDN within the allotted time span. For outbound messages, the node sent AS1 or AS2 data to the trading partner, but the trading partner did not return an MDN within the allotted time span.

Errors SCCP001 – SCE006: Configurable Parser

Error Code	Description	Error Type and Where Displayed	Cause and Action
SCCP001	Config Parser – Failed to read a fixed-length segment. Not enough data in the file.		
SCCP002	Config Parser – COM error while parsing nested segments. Probably a system error.		
SCCP003	Config Parser – Unknown error while parsing nested segments. Probably a system error.		
SCCP004	Config Parser – Error parsing data elements. Not enough data to get to the start of the data element definition.		
SCCP005	Config Parser – Error parsing data elements. Not enough data to read the data element definition.		
SCCP006	Config Parser – Error parsing data elements. Unable to process this field because it should have appeared earlier in the list of data element definitions.		

Error Code	Description	Error Type and Where Displayed	Cause and Action
SCCP007	Config Parser – Parsing fixed-length data element failed; probably not enough data in data file.		
SCCP008	Config Parser – Did not finish reading data element when end of data was reached.		
SCCP009	Config Parser – Local variable in the function has invalid data.		
SCCP010	Config Parser – Local variable in the function has invalid data.		
SCCP011	Config Parser – Failed to parse to the end of the variable-length segment.		
SCCP012	Config Parser – COM error while parsing data elements. Probably a system error.		
SCCP013	Config Parser – Unknown error while parsing data elements. Probably a system error.		
SCCP014	Config Parser – Key field unknown; no match to implement key field action.		
SCCP015	Config Parser – Maximum recursion depth in parser reached. Check for cyclic link in the configuration of the parser. (Max 150 nested segments)		
SCCP016	Config Parser – Failed to determine Aux segment length. Default used (if defined).		
SCCP017	Config Parser – Failed to determine current segment length. Default used (if defined).		
SCCP018	Config Parser – Failed to determine nested segment length. Default used (if defined).		
SCCP019	Config Parser – Failed to determine data element length. Default used (if defined).		
SCE0001	Failed to find a configurable parser object to perform the custom parsing.		
SCE0002	Failed to open the input stream for the parser. Input file may be invalid/ corrupt, deleted, or locked by another process.		
SCE0003	Header tag defined in config parser does not match tag found in data file.		

Error Code	Description	Error Type and Where Displayed	Cause and Action
SCE0004	System Error – Failed to open output stream.		
SCE0005	Parser failed to parse data.		
SCE0006	Parser did not parse any data and stopped to prevent an endless loop while looking for additional interchanges.		

Errors SCMDM: Message Disposition Notifications (MDNs)

Error Code	Description	Error Type and Where Displayed	Cause and Action
SCMDM9541	Message expired.		
SCMDM9670	Message retrieval failed.		
SCMDM9671	MDN not received.		
SCMDM9673	AS2 MDN not received.		

Errors SCPGP: PGP over FTP Messages

Error Code	Description	Error Type and Where Displayed	Cause and Action
SCPGP0001	Unable to perform PGP encryption. Problem with input data or parameter.	FTP Generic MIME Handler. Error Code field, Message Detail pages	Catch-all error code. A problem occurred while trying to perform PGP encryption for an outbound message. Most likely caused by failure of the DCOM or RPC facilities of the operating system or database-related issues. It is likely that widespread errors will be reported by many Sterling Commerce:Centre services. For database and network issues, apply standard clean-up techniques. For Generic MIME Handler problems, examine the application logs of the outbound message.
SCPGP0002	Unable to perform PGP decryption. Problem with input data.	FTP Generic MIME Handler. Error Code field, Message Detail pages	Catch-all error code. A problem occurred while trying to perform PGP decryption for an inbound message. Most likely caused by failure of the DCOM or RPC facilities of the operating system or database-related issues. It is likely that widespread errors will be reported by many Sterling Commerce:Centre services. For database and network issues, apply standard clean-up techniques. For Generic MIME Handler problems, examine the application logs of the inbound message.

Error Code	Description	Error Type and Where Displayed	Cause and Action
SCPGP0003	Problem preparing for PGP decryption.	FTP Generic MIME Handler. Error Code field, Message Detail pages	The PGP decryption process was unable to rename the file holding the encrypted data. Most likely caused by failure of the disk system. It is likely that widespread errors will be reported by many Sterling Commerce:Centre services. For the file system failure, apply standard clean-up techniques. For CMS data server problems, examine the application logs of the inbound message.
SCPGP0004	No attachment data found for PGP decryption. Message summary had no attachments.	FTP Generic MIME Handler. Error Code field, Message Detail pages	The inbound message had no attachment so there was no data available for PGP decryption. Most likely caused by failure of the inbound gateway. For Inbound Gateway or CMS data server problems, examine the application logs of the inbound message.
SCPGP0005	No data found for PGP encryption. Raw data file is missing.	FTP Generic MIME Handler. Error Code field, Message Detail pages	This error is reported by the Router after Generic MIME Handler has indicated success in creating the encrypted data file, but the file does not exist. Most likely caused by a programming error. Contact Level 3.
SCPGP0006	Unable to perform PGP decryption. Could not get PGP configuration information for originator.	FTP Generic MIME Handler. Error Code field, Message Detail pages	An error occurred during PGP decryption while looking in the database for the PGP configuration information for the message originator. Caused by a database problem, network connectivity problem, or a misconfiguration. For database and network issues, apply standard clean-up techniques. The misconfiguration was caused by the address representing the originator having incorrect PGP setup information.
SCPGP0007	Unable to perform PGP decryption. Could not get PGP configuration information for recipient.	FTP Generic MIME Handler. Error Code field, Message Detail pages	An error occurred during PGP decryption while looking in the database for the PGP configuration information for the message recipient. Caused by a database problem, network connectivity problem, or a misconfiguration. For database and network issues, apply standard clean-up techniques. The misconfiguration was caused by the address representing the recipient (probably the PGP address for the node) having incorrect PGP setup information.

Error Code	Description	Error Type and Where Displayed	Cause and Action
SCPGP0008	Unable to perform PGP decryption. Problem with decryption or signature verification.	FTP Generic MIME Handler. Error Code field, Message Detail pages	An error occurred while performing PGP decryption or signature verification. Most likely caused by a misconfiguration of PGP information for the message originator (message not signed or signed with wrong key) or recipient (key not available for decrypting). Verify that the PGP address for the node is configured correctly. Verify that the recipient's PGP information is correct. For Generic MIME Handler problems, examine the application logs of the inbound message.
SCPGP0009	Unable to perform PGP encryption. Problem with input file, missing or empty.	FTP Generic MIME Handler. Error Code field, Message Detail pages	The input file containing the clear text to be encrypted for the outbound message is missing. Indicates a system problem. The Router and Generic MIME Handler should have placed the input data in a known place. Most likely caused by an external process deleting the file before it could be used. Make sure the outbound message was not delivered and that the inbound message did not produce multiple outbound messages. Then, reprocess the inbound message. If the problem persists, contact Level 3.
SCPGP0010	Unable to perform PGP encryption. Could not get PGP configuration information for originator (signer.)	FTP Generic MIME Handler. Error Code field, Message Detail pages	An error occurred during PGP encryption while looking in the database for the PGP configuration information needed to sign an outbound message. Caused by a database problem, network connectivity problem, or a misconfiguration. For database and network issues, apply standard clean-up techniques. The misconfiguration was caused by the originator's address (or the PGP address for the node) having incorrect PGP setup information.
SCPGP0011	Unable to perform PGP encryption. Could not get PGP configuration information for recipient.	FTP Generic MIME Handler. Error Code field, Message Detail pages	An error occurred during PGP encryption while looking in the database for the PGP configuration information for the message recipient. Caused by a database problem, network connectivity problem, or a misconfiguration. For database and network issues, apply standard clean-up techniques. The misconfiguration was caused by the recipient's address having incorrect PGP setup information.

Error Code	Description	Error Type and Where Displayed	Cause and Action
SCPGP0012	Unable to perform PGP encryption. Problem with input data or parameter.	FTP Generic MIME Handler. Error Code field, Message Detail pages	An error occurred while performing PGP encryption. Most likely caused by a misconfiguration of PGP information for the message originator (key not available for signing) or recipient (key not available for encrypting). Verify that the PGP address for the node is configured correctly. Verify that the recipient's PGP information is correct. For Generic MIME Handler problems, examine the application logs of the outbound message.
SCPGP0013	Unable to perform PGP encryption. Problem with input file, missing or empty.	FTP Generic MIME Handler. Error Code field, Message Detail pages	The input file containing the encrypted data of the inbound message is missing. This indicates a system problem. CMS data server should have placed the input data in a known place. Most likely caused by a file system failure or an external process deleting the file before it could be used. Check the application logs to account for a dropped message. The inbound gateway should have returned an error value to the originator so they would know to resend the data. If not, handle the dropped message.

Errors WEDM: Transaction Set

Error Code	Description	Error Type and Where Displayed	Cause and Action
WEDM100	The transaction set that was sent was not mutually agreed.		

Error Codes from the PGP SDK

PGP SDK Errors -10850 to -10899

Error Code	Description		Error Code	Description
-10844	Smart card not found		-10849	Smart card out of memory
-10845	Smart card pin locked		-10850	Smart card error
-10846	Smart card key exists		-10878	LDAP—Bad scope
-10847	Smart card X509 exists		-10879	LDAP—No DN
-10848	Smart card key not found		-10880	LDAP—Not LDAP URL

PGP SDK Errors -10900 to -10949

Error Code	Description		Error Code	Description
-10908	LDAP—Connect error		-10929	LDAP—Busy
-10909	LDAP—Parameter error		-10930	LDAP—Insufficient access
-10910	LDAP—User cancelled		-10931	LDAP—Invalid credentials
-10911	LDAP—Filter error		-10932	LDAP—Inappropriate authorization
-10912	LDAP—Authorization unknown		-10933	LDAP—Alias deref problem
-10913	LDAP—Timeout		-10934	LDAP—Is leaf
-10914	LDAP—Decoding error		-10935	LDAP—Invalid DN syntax
-10915	LDAP—Encoding error		-10936	LDAP—Alias problem
-10916	LDAP—Local error		-10937	LDAP—No such object
-10917	LDAP—Server down		-10938	LDAP—Invalid syntax
-10918	LDAP—Other		-10939	LDAP—Type or value exists
-10919	LDAP—Results too large		-10940	LDAP—Constraint violation
-10920	LDAP—No object class modules		-10941	LDAP—Inappropriate matching
-10921	LDAP—Already exists		-10942	LDAP—Undefined type
-10922	LDAP—Not allowed On RDN®		-10943	LDAP—No such attribute
-10923	LDAP—Not allowed on nonleaf		-10944	LDAP—Partial results
-10924	LDAP—Object class violation		-10945	LDAP—Strong authorization required
-10925	LDAP—Naming violation		-10946	LDAP—Strong authorization not supported
-10926	LDAP—Loop detect		-10947	LDAP—Size limit exceeded
-10927	LDAP—Unwilling to perform		-10948	LDAP—Time limit exceeded
-10928	LDAP—Unavailable		-10949	LDAP—Protocol error

PGP SDK Errors -10950 to -11049

Error Code	Description		Error Code	Description
-10950	LDAP—MIN		-10990	Invalid output format
-10971	PKCS7—Decrypt failure		-10991	Invalid input format
-10972	PKCS7—Encrypt failure		-10992	ASN pack failure
-10973	X509—Certificate parse error		-10993	PKCS7 sign failure
-10974	CRS—Invalid authenticate value		-10994	Missing X509 certificate
-10975	CRS—Invalid attribute value length		-10995	Certificate request—Creation failure
-10976	CRS—Invalid certificate type		-10996	Invalid distinguished name
-10977	CRS—Invalid attribute type		-10997	CMS initialization
-10978	CRS—Invalid character		-10998	Invalid PKCS7 encoding

Error Code	Description		Error Code	Description
-10979	CRS—Missing required attribute		-10999	X509 attribute not supported
-10988	Public key not found		-11049	Sockets—Domain server error
-10989	Invalid certificate extension			

PGP SDK Errors -11050 to -11199

Error Code	Description		Error Code	Description
-11050	Sockets—Host not found		-11093	Sockets—Address family not supported
-11085	Sockets—No static storage		-11094	Sockets—Protocol not supported
-11086	Sockets—Timed out		-11095	Sockets—Operation not supported
-11087	Sockets—Already connected		-11096	Sockets—Not bound
-11088	Sockets—Address not available		-11097	Sockets—Not connected
-11089	Sockets—Listen queue full		-11098	Sockets—In progress
-11090	Sockets—Buffer overflow		-11099	Sockets—Not initialized
-11091	Sockets—Address in use		-11100	Sockets—Network down
-11092	Sockets—Not a socket		-11150	Big number, no inverse

PGP SDK Errors -11200 to -11249

Error Code	Description		Error Code	Description
-11212	SECSH—Received handshake request		-11230	Split—Not enough shares in object
-11213	SECSH—Would block		-11236	X509—Invalid certificate tree
-11214	SECSH—No common cipher		-11237	X509—Invalid certificate format
-11215	SECSH—Key unusable		-11238	X509—Invalid certificate signature
-11216	SECSH—Alert received		-11239	X509—Self-signed certificate
-11217	SECSH—Wrong state		-11240	X509—Needed certificate not available
-11218	SECSH—Version unsupported		-11242	TLS—Received handshake request
-11219	SECSH—Protocol violation		-11243	TLS—Would block
-11220	SECSH—Unexpected close		-11244	TLS—No common cipher
-11225	SKEP—Incorrect version		-11245	TLS—Key unusable
-11226	SKEP—Rejected authentication		-11246	TLS—Alert received
-11227	Split—Identical shares		-11247	TLS—Wrong state
-11228	Split—Different share pool		-11248	TLS—Version unsupported
-11229	Split—Different split keys		-11249	TLS—Protocol violation

PGP SDK Errors -11250 to -11299

Error Code	Description		Error Code	Description
-11250	TLS—Unexpected close		-11289	Server—Timed out

Error Code	Description		Error Code	Description
-11279	Server—Certificate not found		-11290	Server—Unknown response
-11280	Server—No static storage		-11291	Server—Corrupt key block
-11281	Server—Operation requires TLS		-11292	Server—Partial add failure
-11282	Server—Key failed policy		-11293	Server—Not initialized
-11283	Server—Bad keys in search results		-11294	Server—Key already exists
-11284	Server—Partial search results		-11295	Server—Not open
-11285	Server—Search failed		-11296	Server—Open
-11286	Server—Authorization failed		-11297	Server—Request failed
-11287	Server—Authorization required		-11298	Server—Invalid protocol
-11288	Server—Open failed		-11299	Server—Operation not supported

PGP SDK Errors -11300 to -11349

Error Code	Description		Error Code	Description
-11300	Server—In progress		-11330	SIG_LONG
-11311	Deleting derived object		-11335	Unknown padding type
-11312	Key DB mismatch		-11336	Corrupt private key
-11313	Item was deleted		-11337	CRL packet truncated
-11314	Certifying key dead		-11338	Public Key not implemented
-11315	Duplicate user ID		-11339	Public key too large
-11316	Duplicate cert		-11340	Public key too small
-11317	File corrupt		-11341	Key too large
-11318	Invalid property		-11342	Malformed key component
-11319	Item is read only		-11343	RSA public exponent is even
-11320	Out of entropy		-11344	RSA public modulus is even
-11324	Revocation key not found		-11345	Malformed key exponent
-11325	Unknown signature version		-11346	Malformed key modulus
-11326	Extra signature material		-11347	Unknown public key algorithm
-11327	Unknown signature algorithm		-11348	Unknown key version
-11328	Malformed signature integer		-11349	Key packet truncated
-11329	Truncated signature			

PGP SDK Errors -11350 to -11399

Error Code	Description			
-11350	KEY_MIN		-11381	Trouble—Key too big
-11362	Bad compression number		-11382	Trouble—Unexpected trust
-11363	Trouble—CRL too big		-11383	Trouble—Unexpected unknown
-11364	Trouble—Duplicate CRL		-11384	Trouble—Unexpected signature

Error Code	Description			
-11365	Trouble—Importing non-exportable signature		-11385	Trouble—Unexpected name
-11366	Trouble—New secret key		-11386	Trouble—Unexpected subkey
-11367	Trouble—Old secret key		-11387	Trouble—Unknown packet byte
-11368	Trouble—Version bug current		-11388	Trouble—Bad trust
-11369	Trouble—Version bug previous		-11389	Trouble—Signature subkey
-11370	Trouble—Bare key		-11390	Trouble—Key subkey
-11371	Trouble—Duplicate unknown		-11391	Bad packet
-11372	Trouble—Duplicate signature		-11392	ASCII parse incomplete
-11373	Trouble—Duplicate name		-11393	Unknown char map
-11374	Trouble—Duplicate secret key		-11394	Env priority too low
-11375	Trouble—Duplicate key		-11395	Random seed too small
-11376	Trouble—Duplicate key ID		-11396	FIFO read error
-11377	Trouble—Unknown too big		-11397	Wrong scope
-11378	Trouble—Signature too big		-11398	Unbalanced scope
-11379	Trouble—Name too big		-11399	Can't hash
-11380	Trouble—Secret key too big			

PGP SDK Errors -11400 to -11449

Error Code	Description		Error Code	Description
-11400	Invalid commit		-11418	Bad cipher number
-11401	Additional recipient request key not found		-11419	Bad hash number
-11402	Secret key not found		-11420	Out of rings
-11403	Extra date on signature		-11435	Unsupported net tools CA filter
-11404	Signature bits wrong		-11436	Invalid filter parameter
-11405	Bad signature size		-11437	Unknown filter type
-11406	Unknown signature type		-11438	Unsupported HKP filter
-11407	Bad session key algorithm		-11439	Unsupported LDAP filter
-11408	Unknown version		-11440	Inconsistent Filter classes
-11409	Bad session key size		-11442	Deleting self-signature
-11410	Unknown string2key		-11443	Decompression failed
-11411	Can't decrypt		-11444	Bad integrity
-11412	Key is locked		-11445	Self-tests not executed
-11413	Config parse failure—Bad options		-11446	Self-test failed
-11414	Config parse failure—Bad function		-11447	CAPI—Unsupported key
-11415	Config parse failure		-11448	Bad signature
-11416	Size advise failure		-11449	No MAC binary translation available
-11417	Bad key length			

PGP SDK Errors -11450 to -11499

Error Code	Description		Error Code	Description
-11450	Not MAC binary		-11483	Input file
-11451	Minor UnTAR error		-11484	Multiple input options
-11452	UnTAR failed		-11485	No input options
-11453	Compression failed		-11486	Detached signature with encryption
-11460	Incompatible API		-11487	Detached signature without signing key
-11471	Keygen timed out		-11488	Combined conventional and public encryption
-11472	Key unusable for decryption		-11489	Missing passphrase
-11473	Too many ARRKs		-11490	Inconsistent encryption algorithms
-11474	Interrupted		-11491	Output buffer too small
-11475	Skip section		-11492	Key unusable for signature
-11476	Corrupt session key		-11493	Key unusable for encryption
-11477	No decryption key found		-11494	Key invalid
-11478	Detached signature found		-11495	Key disabled
-11479	Missing key DB		-11496	Key expired
-11480	Missing event handler		-11497	Key revoked
-11481	Multiple output options		-11498	Redundant options
-11482	No output options		-11499	Option not found

PGP SDK Errors -11500 to -11949

Error Code	Description		Error Code	Description
-11500	Bad passphrase		-11934	Net LA too many retrievals
-11900	NT Drv Iop—File failed		-11935	Net LA mismatch
-11901	NT Drv Iop—Write failed		-11936	Net LA refused
-11902	NT Drv Iop—Read failed		-11937	No unicode equivalent
-11910	User disabled		-11938	RPC garbled message
-11924	Net LA failed		-11939	RPC failed
-11925	Net LA proxy authorization required		-11940	Win32—Windows operation failed
-11926	LN multiple prod evals		-11941	Win32—Resource operation failed
-11927	LN ver unsupported		-11942	Win32—Registry operation failed
-11928	LA invalid		-11943	Win32—Dll operation failed
-11929	Net LA e-mail failed		-11944	Win32—Communications control operation failed
-11930	Net invalid prod ID		-11945	Win32—COM operation failed
-11931	LN invalid		-11946	NT Drv Object operation failed
-11932	LA corrupt		-11947	NT Drv IOP operation failed
-11933	LN corrupt		-11949	Volume op failed

PGP SDK Errors -11950 to -12050

Error Code	Description		Error Code	Description
-11950	Thread operation failed		-11979	Pref not found
-11951	Sync object operation failed		-11980	Unknown error
-11952	String operation failed		-11981	Bad memory address
-11953	Security operation failed		-11982	Assert failed
-11954	Network operation failed		-11983	Item already exists
-11955	Memory operation failed		-11984	Item not found
-11956	Graphics operation failed		-11985	Lazy programmer
-11959	Disk locked		-11986	Unknown request
-11960	Disk full		-11987	User abort
-11967	Size too large		-11988	End of file
-11968	Buffer too large		-11989	Write failed
-11969	Not connected		-11990	Read failed
-11970	Deadlocked		-11991	File operation failed
-11970	Invalid certificate format		-11992	Illegal file operation
-11971	Already in use		-11994	File locked
-11972	Insufficient privileges		-11995	File permissions
-11973	Resource unavailable		-11996	Can't open file
-11974	Match not found		-11997	File not found
-11975	Feature not available		-11998	Buffer too small
-11976	Corrupt data		-11999	Out of memory
-11977	Improper initialization		-12000	Bad parameters
-11978	End of iteration			

Chapter 10. Reference: Page Descriptions, Protocols, and Message Status

Account Details Page

Displays information about one account.

Name

Name of the account, usually the name of a contact at the company.

Web User ID

User ID for accessing this account through the Web Administration Tool. The user ID for a new account is generated automatically and duplicates the mailslot address. After the account is added, the user ID can be changed.

Web Password

Password for accessing this account through the Web Administration Tool. Use six to ten alphanumeric characters.

Note: This password must be unique. If you use the same password as the WAT account to set up or edit a mailslot, a Warning message is displayed forcing you to create a different password.

Security Level

Level of access assigned to the Web user ID associated with this account.

Read Only

Specifies whether or not the user has access for account/address management. Users with Read Only access can not perform any account or address management.

Protocol

The protocol associated with the first address created for a new account.

Phone

Telephone number of the account.

Note

Comments associated with this account.

Prevent Inbound Message Store

Specifies whether or not the user can restore inbound messages

Prevent Outbound Message Update

Specifies whether or not the user reprocess or pickup outbound messages.

Prevent Credential List Update

Specifies whether or not the user can do certificate management?

Prevent Node Level Updates

Specifies whether or not the user can make updates at the node level, such as edit system profiles or error codes.

Address Line 1, Address Line 2, Address Line 3

Street address for the account mailing address.

P.O. Box

Post office box for the account mailing address.

Mailslot

Mailslot for the account mailing address.

City

City for the account mailing address.

State

State or province for the account mailing address.

Zip

Postal code or ZIP code for the account mailing address.

County

County for the account mailing address.

Country

Country for the account mailing address.

For X.400 addresses, this is the ISO standard (2 letters or 3 numerals).

Status

Refer to Account and Address Status Codes for details.

Addresses divider bar

List of addresses for the account in the account hierarchy.

Account Suspension Search Page

Lists the addresses that have the suspension profile enabled.

Expiration Status

- Select ALL for all addresses with the suspension profile enabled.
- Select Action Required for suspended addresses that are within 30 minutes of expiring or have passed the expiration time.

Include Disabled Profiles

Also display addresses that have been disabled.

1 . . .

Number of the address in the list. The addresses are listed in order by their expiration dates/times.

Status

Profile is enabled or disabled.

Expiration

Date and time the suspension profile expires. Shown in yellow when the expiration time is within 30 minutes of the current time. Shown in red when the expiration time has passed.

Mailslot

Identifier for the sub-area within a mailbox where messages for this address are sent. A complete messaging address uses eight alphanumeric characters: the first five characters identify the mailbox and the last three characters identify the mailslot. For example, mailbox SA123 contains mailslots SA123001, SA123002, and SA123003.

Reason

Reason for the address suspension.

User

Not supported in this release. The user who enabled the suspension profile.

Edit

Available only to users with a System Administrator security level. Edit the expiration date/time or reason for suspension or disable the suspension.

Accounts Page

Lists the accounts in a company-domain entity.

1 . . .

Number of the account in the list.

Name

Name of the account, usually the name of a contact at the company.

Mailbox

Mailbox information for the account. This is a link to the mailbox details.

Phone

Telephone number of the account.

Status

Refer to "Account and Address Status Codes" on page 138 for details.

Error Code

See the error code descriptions for more details.

Address Details Page

Displays information about one address or mailslot.

Name

Name of the messaging address. You can use a template name.

Description

Description of the messaging address.

On SuperTracs

Indicates whether the address is coupled with a Sterling Commerce:Network mailslot.

- **SuperTracs region/Decouple** – A Sterling Commerce:Network mailslot is coupled with the address on the node. When you add an address, the

mailslot information (MB01) and EDI ID information (CF01 and CF02) are added on the Sterling Commerce:Network. To remove the Sterling Commerce:Network mailslot, you can decouple the address.

- **No/Couple** – No Sterling Commerce:Network mailslot is coupled with the address on the node. To add a Sterling Commerce:Network mailslot, you can couple the address. Use this setting if the customer already has a Sterling Commerce:Network mailslot with the same EDI IDs.

  Note: If you are adding an associate mailbox, select a SuperTracs region from the drop-down menu.

Use Mailbag

Indicates whether the address uses a mailbag envelope to enclose data being sent or received.

- **Yes** – The messaging address uses a mailbag envelope. Use Yes only if a Sterling Commerce:Network mailslot is coupled with the address (On SuperTracs not set to No). When the address is replicated to Sterling Commerce:Network, Sterling Commerce:Network uses the CICS IPRO screen to set up mailbagging for the coupled Sterling Commerce:Network mailslot.
- **No** – The messaging address does not use a mailbag envelope.

  Note: If you are adding an associate mailbox, select **Yes**.

Status

Refer to "Account and Address Status Codes" on page 138 for details.

Mailslot

Identifier for the sub-area within a mailbox where messages for this address are sent. When you are adding an address, the mailslot is generated for you. A complete messaging address uses eight alphanumeric characters: the first five characters identify the mailbox and the last three characters identify the mailslot. For example, mailbox SA123 contains mailslots SA123001, SA123002, and SA123003.

Note: If you are adding an associate mailbox, you specify the mailslot.

Mailslot Password

Password for the mailslot (or messaging address).

Note: This password must be unique. If you use the same password as the WAT account to set up or edit a mailslot, a Warning message is displayed forcing you to create a different password.

Error Mailslot

Messaging address where error messages are stored.

Destination Type

Identifies the purpose of the messaging address.

- **Final** – The address is used to route data to a customer, either for pick up or for automatic delivery. Generally, use this setting for customer addresses.
- **Interconnect** – The address is used to route messages to another VAN. Generally, use this setting for interconnect setups for non-customer trading partner addresses.

- **Internal** – The address is used to route messages internally on the node. Generally, this setting is used only by Level 2 or 3.

C:Network Error Code

Refer to the error code topics for more details.

Is Default Address

Applies only if there is more than one address for the account.

- **Yes** – The messaging address is the default address for the account.
- **No** – The messaging address is not the default address for the account.

Local Message Store

Applies to all protocols except AS1.

- **Yes** – Messages for the address are stored on the node and retrieved by the receiver.
- **No** – Messages are sent to the receiver's external address automatically and are not stored on the node.

Customer

Indicates whether the address is for a Sterling B2B Collaboration Network customer or for a non-customer trading partner. This setting is replicated to Sterling Commerce:Network and indicates whether activity to and from this address is billed or not.

- **Yes** – The messaging address is for a customer and its activity is billed.
- **No** – The messaging address is for a trading partner and its activity is not billed. If the address resides in a non-customer mailbox (S## mailbox), No is supplied and cannot be changed.

  Select **No** when setting up an address to be used for internal communication.

Associate Mailbox?

Indicates whether the mailbox is for an interconnect non-customer who is set up as a customer.

Is Template

- **Yes** – The messaging address is an address template.
- **No** – The messaging address is not an address template.

Protocol Details divider bar

Refer to the topics about the different protocol types.

EDI IDs divider bar

List of EDI IDs associated with the address.

Addresses Page

Lists the addresses in an account.

1 . . .

Number of the address in the list.

Name

Name of the messaging address. You can use a template name.

Type

Refer to the topics about the different protocol types.

Description

Description of the messaging address.

Mailslot

Identifier for the mailslot where messages for this address are sent. A complete messaging address uses eight alphanumeric characters: the first five characters identify the mailbox and the last three characters identify the mailslot. For example, mailbox SA123 contains mailslots SA123001, SA123002, and SA123003.

Local MS (Local Message Store)

Applies to all protocols except AS1.

- **Yes** – Messages for the address are stored on the node and retrieved by the receiver.
- **No** – Messages are sent to the receiver's external address automatically and are not stored on the node.

Default

Applies only if there is more than one address for the account.

- **Yes** – The messaging address is the default address for the account.
- **No** – The messaging address is not the default address for the account.

Customer

Indicates whether the address is for a Sterling B2B Collaboration Network customer or for a non-customer trading partner. This setting is replicated to Sterling Commerce:Network and indicates whether activity to and from this address is billed or not.

- **Yes** – The messaging address is for a customer and its activity is billed.
- **No** – The messaging address is for a trading partner and its activity is not billed. If the address resides in a non-customer mailbox (S## mailbox), No is supplied and cannot be changed.

On SuperTracs

- **SuperTracs region/Decouple** – A Sterling Commerce:Network mailslot is coupled with the address on the node. To remove the Sterling Commerce:Network mailslot, you can decouple the address.
- **No/Couple** – No Sterling Commerce:Network mailslot is coupled with the address on the node. To add a Sterling Commerce:Network mailslot, you can couple the address.

Status

Refer to Account and Address Status Codes for details.

C:Network Error Code

Refer to the error code topics for more details.

AS2 Address Page

Displays information for an address that uses AS2 protocol.

Remote Web Server

Name of the user's Web server.

Remote Use Secure Channel

Indicates whether a secure channel is used to send messages.

- **Yes** – Transmissions are sent through HTTPS.
- **No** – Transmissions are sent through HTTP.

Remote Port

Number of the port used to make the HTTP connection to the user's Web server. For an unsecure HTTP connection, the default is 80. For a secure HTTPS connection, the default is 443.

Remote Path and Parameters

Path and parameters identifying the user's Web server. This information identifies a location on the user's system where the node places data.

Remote HTTP User ID

User ID for the user's Web server (if necessary).

Remote HTTP Password

Password for the user's Web server (if necessary).

Identifier

Unique identifier for the user on the user's AS2 system. If an identifier includes a space, double quotation mark, or a back-slash, the special character must be preceded by a back-slash and the entire identifier must be enclosed within double quotation marks.

Examples:

- To use *Sterling Commerce*, type `"Sterling Commerce"`
- To use *Sterling\Commerce*, type `"Sterling\Commerce"`
- To use *Sterling"Commerce*, type `"Sterling\"Commerce"`

If you enter an identifier that does not meet these standards, a message notifies you of the discrepancy. However, a nonstandard identifier will operate correctly as long as the identifier you type is the same as the identifier used in the actual data.

Local HTTP User ID

User ID set up on the node to authenticate inbound messages. The user ID is assigned by Customer Support and communicated to the user. By default, the value is the name of the address (mailslot).

Local HTTP Password

Password used to access the user's address (mailslot) on the node.

Note: This password must be unique. If you use the same password as the WAT account to set up or edit a mailslot, a Warning message is displayed forcing you to create a different password.

Payload Type

Format used for the data payload (the EDI data) of a message.

- If Secure Channel is Yes (HTTPS), select **Signed**.
- If Secure Channel is No (HTTP), select **Signed and Encrypted**.

Signing Algorithm

A cryptographic hash algorithm used to sign data. Select **SHA1**, unless the user requires **MD5**.

Symmetric Algorithm

Algorithm used to encrypt data. Select **3DES 168 CBC**, unless the user requires another algorithm.

Default MIME TypeDefault MIME Subtype

Default MIME type and subtype used for business data in outbound messages sent from this address. Select **Application-EDI X12**.

Receipt Type

Type of acknowledgments to be exchanged. Select **MDN**.

Receipt Signature Type

A cryptographic hash algorithm used to sign receipt acknowledgments. Select **SHA1**.

Receipt Delivery Mode

Method of exchanging reply messages.

- **Synchronous**
- **Asynchronous through HTTP**
- **Asynchronous through HTTPS**
- **Asynchronous through SMTP**

Compression Algorithm

Applies only to AS1 addresses. Algorithm used to compress data before the message is sent.

- **None** – Data is not compressed before sending.
- **ZLIB** – Data is compressed using the ZLIB [RFC 1950] standard algorithm.

SMIME Details divider bar

Certificate information required by an AS2 address. Refer to SMIME Details Page for details.

AS2 Address Search

Displays the results of a search for AS2 addresses.

1 . . .

Number of the address in the list.

AS2 Identifier

Unique identifier for the user on the user's AS2 system.

Local HTTP User ID

User ID set up on the node to authenticate inbound messages. The user ID is assigned by Customer Support and communicated to the user.

Remote Web Server

Name of the user's Web server.

Remote HTTP User ID

User ID for the user's Web server.

Mailslot

Mailslot for this AS2 address. This is a link to the mailslot details.

Association Details Page

Lists the messages that matched a search by association ID.

Association ID Type

Category assigned by the node to an association ID that identifies the external system that sends or receives the message.

Association ID

Unique ID that is used to track and correlate messages across systems.

Outbound Messages divider bar

Lists all outbound messages related to an association ID.

Inbound Messages divider bar

Lists all inbound messages related to an association ID.

Association ID Type Page

Displays the association types and descriptions that are set up on the node.

Association ID Type

Category assigned by the node to an association ID that identifies the external system that sends or receives the message. Association ID types vary by node.

Association ID Type Description

Description of the category.

Association ID Types Supplied on the Dublin 3 Node

XPC_CorrID

Identifies messages routed through the XPC connector to or from sterlingcommerce.net. The association ID is the correlation ID assigned by a MarketSite that is used to track messages into and out of Sterling Commerce:Centre.

Attachment Details Page

Displays information about one attachment.

Number

Number of the attachment in the list, indicating how many attachments are in the message.

Type

Type of attachment – **EDI** indicates that the attachment is formatted according to an EDI standard.

Size

Size of the attachment in bytes.

Customer File Name

Specifies the customer-supplied file name used for outbound messages.

Download

Contents of the attachment, such as EDI data. Data that is not text-based is not displayed coherently. Only the first 10,000 bytes of data are displayed.

Attachments Page

Lists the attachments in a message.

Number

Number of the attachment in the list, indicating how many attachments are in the message.

Type

Type of attachment – **EDI** indicates that the attachment is formatted according to an EDI standard.

Size

Size of the attachment in bytes.

Customer File Name

If present, the name of the customer file in the attachment.

Download

Download the attachment. Available to any user who can view the attachment.

Audit Log Search

Search the audit log for changes.

Start Date/TimeEnd Date/Time

Date and time range to search for housekeeping log entries. If you do not change this field, the default is the last two hours.

Date format: MM/DD/YY

Time format: HH:MM:SS

Time zone: UTC

Items Per Page

Number of entries you want to see on one page of the browser when the results are displayed.

Operation

- **All** – Include all operations.
- **Add** – Include only Add operations.
- **Update** – Include only Update operations.

- **Delete** – Include only Delete operations.
- **Restore** – Include only Inbound Message Restore operations.
- **Pickup** – Include only Outbound Message Pickup operations.
- **Add certificate** – Include only Security Certificate or PGP Key Add operations.
- **Delete certificate** – Include only Security Certificate or PGP Key Delete operations.

Change area

- **All** – Include all areas.
- **EDI** – Include only changes to EDI identifiers.
- **Address** – Include only changes made at the address level.
- **Customer** – Include only changes made at the customer level.
- **Node** – Include only changes made at the node level.

User Name (exact)

Type the WAT login ID of the user whose changes you want to see.

Pre-change text (contains)

Type the text contained in the record before it was changed.

Post-change text (contains)

Type the text contained in the record after it was changed.

Any OID or text (contains)

Type the User OID, Owner OID, Foreign Key, or other text either before or after it was changed.

Certificate Store Page

Lists the installed AS2 (CAPI-SMIME) certificates.

Note: If your user account is set as Read Only, then the New, Delete, and Upload buttons will not be available.

Certificate Stores

Name of the certificate store that is displayed.

On the Choose Certificate Store page, this is a drop-down list.

Common Name

Name of the AS2 certificate.

Validity Dates: From/To

The date range during which the certificate is valid.

Identification

Includes the Serial number, RDN, and Issuer RDN of the certificate.

New

Click to download a certificate.

Delete

Click to delete the selected certificate(s).

Upload Certificate

On the Upload & Verify Certificate page, browse to select a certificate and then click to upload it to the node.

Companies Page

Lists companies that matched search criteria.

1 . . .

Number of the company in the list.

Company Name

Name of the company (which corresponds to a customer in Vantive, a back-end system).

Phone

Telephone number of the company.

Status

Code indicating the status of the company in Vantive, a back-end system.

Company Details Page

Displays information about one company.

Name

Name of the company (which corresponds to a customer in Vantive, a back-end system).

Phone

Telephone number of the company.

Fax

Fax number of the company.

Domains divider bar

List of domains in the account hierarchy for the company.

Connect:Mailbox Details Page

Displays information about the Sterling Commerce:Network mailslot that sent or received messages from the node.

C:N Inbound Batch Number

Applies only to outbound messages from the node to Sterling Commerce:Network. Batch number on Sterling Commerce:Network assigned to a message received from the node.

C:N Outbound Batch Number

Applies only to an inbound message from Sterling Commerce:Network to the node. Batch number on Sterling Commerce:Network assigned to a message sent to the node.

Interchange Number

EDI interchange number associated with the message.

Mailslot

Sterling Commerce:Network mailslot that sent the message to the node or received the message from the node.

Group Number

ID of the group envelope section within the EDI interchange document.

Status

Applies only to inbound messages from Sterling Commerce:Network to the node.

- **Extracted** – The node extracted the outbound batch from Sterling Commerce:Network successfully.
- **Restore** – The node is ready to re-extract the outbound batch when Sterling Commerce:Network restores it.
- **Change** – Change the status from Extracted to Restore.

Domain Details Page

Displays information about one domain.

Name

Name of the domain.

Description

Description of the domain.

Status

Code indicating the status of the mailbox in the back-end billing system.

Mailbox

Identifier for the mailbox that is set up in the back-end billing system and populated to a node. Each company-domain entity has one unique, five-character mailbox ID. Messages are sent to mailslots (messaging addresses) within the mailbox. A complete messaging address uses eight alphanumeric characters. The first five characters identify the mailbox and the last three characters identify the mailslot. For example, mailbox SA123 contains mailslots SA123001, SA123002, and SA123003.

Last Mailslot

Messaging address of the mailslot that was last assigned to an address within the domain. The domain is associated with a mailbox. Accounts within the domain have messaging addresses associated with mailslots in the domain mailbox. A complete messaging address uses eight alphanumeric characters. The first five characters identify the mailbox and the last three characters identify the mailslot.

Next Mailslot

Messaging address of the next mailslot to be assigned to an address within the domain. The domain is associated with a mailbox. Accounts within the domain have messaging addresses associated with mailslots in the domain mailbox. A complete messaging address uses eight alphanumeric characters. The first five characters identify the mailbox and the last three characters identify the mailslot.

Accounts divider bar

List of accounts in the account hierarchy for the domain.

Domains List Page

Lists the domains that match a search for accounts by domain name or by mailbox.

1 . . .

Number of the domain in the list.

Name

Name of the domain.

Description

Description of the domain.

Mailbox

Identifier for the mailbox that is set up in the back-end billing system and populated to a node. Each company-domain entity has one unique, five-character mailbox ID. Messages are sent to mailslots (messaging addresses) within the mailbox. A complete messaging address uses eight alphanumeric characters. The first five characters identify the mailbox and the last three characters identify the mailslot. For example, mailbox SA123 contains mailslots SA123001, SA123002, and SA123003.

Domains Page

Lists the domains in one company.

1 . . .

Number of the domain in the list.

Name

Name of the domain.

Domain Description

Description of the domain.

Mailbox

Identifier for the mailbox that is set up in the back-end billing system and populated to a node. Each company-domain entity has one unique, five-character mailbox ID. Messages are sent to mailslots (messaging addresses) within the mailbox. A complete messaging address uses eight alphanumeric characters. The first five characters identify the mailbox and the last three characters identify the mailslot. For example, mailbox SA123 contains mailslots SA123001, SA123002, and SA123003.

Status

Code indicating the status of the mailbox.

Type

Code indicating the type of mailbox assigned.

Last Mailslot

Messaging address of the mailslot that was last assigned to an address within the domain. The domain is associated with a mailbox. Accounts within the domain have messaging addresses associated with mailslots in

the domain mailbox. A complete messaging address uses eight alphanumeric characters. The first five characters identify the mailbox and the last three characters identify the mailslot.

EDI IDs Page

Lists the EDI IDs associated with an address.

EDI ID EDI Qualifier

An identifier and qualifier pair used within EDI transmissions that identifies a business to its trading partners. The EDI ID and qualifier pair must be unique on the Sterling B2B Collaboration Network and remains the same whether it corresponds to the sender or the receiver of a transmission. A business chooses its EDI ID and qualifier and shares it with its trading partners.

On SuperTracs

If the address is not coupled with a Sterling Commerce:Network mailslot, this value is No and cannot be changed.

If the address is coupled with a Sterling Commerce:Network mailslot, this value can be Yes or No.

- **SuperTracs region/Decouple** – The EDI ID exists in the Sterling Commerce:Network mailslot associated with this address. To remove the EDI ID from the Sterling Commerce:Network mailslot, decouple the ID.
- **No/Couple** – The EDI ID does not exist on the Sterling Commerce:Network mailslot that is coupled with this address. To add the EDI ID to the Sterling Commerce:Network mailslot, couple the ID.

Status

Refer to "Account and Address Status Codes" on page 138 for details.

Error Code

Refer to the error code topics for details.

Edit

Change the EDI ID or qualifier.

EDI Information Page

Lists the addresses that match a search by EDI information.

1 . . .

Number of the address in the list.

Mailslot

Identifier for the sub-area within a mailbox where messages are sent. A complete messaging address uses eight alphanumeric characters: the first five characters identify the mailbox and the last three characters identify the mailslot. For example, mailbox SA123 contains mailslots SA123001, SA123002, and SA123003.

EDI ID EDI Qualifier

An identifier and qualifier pair used within EDI transmissions that identifies a business to its trading partners. The EDI ID and qualifier pair must be unique on the Sterling B2B Collaboration Network and remains

the same whether it corresponds to the sender or the receiver of a transmission. A business chooses its EDI ID and qualifier and shares it with its trading partners.

Status

Refer to "Account and Address Status Codes" on page 138 for detalis.

Error Code

Refer to the error code topics for details.

Expired Certificate Notify Page

The Expired Certificate Notify address profile page allows you to enable notification of expiring and expired AS2 certificates to be sent to the address.

Note: If your user account is set as Read Only, then the **Add** and **Cancel** buttons will not be available.

Name

Expired Certificate Notify

Description

Notify this address when one or more security certificates will be expiring or have expired.

Status

Select whether you want the profile **Enabled** or **Disabled** at this time. You can change the status at any time.

Comments/Reason

Enter a comment or reason, such as why these certificates are being monitored for this address.

(checkbox)

Click in the checkbox to select the certificate for which you want notifications to be sent. You can select multiple certificates to be monitored.

Common Name

Name of the AS2 certificate

Validity Dates

The To/From dates during which the certificate is valid.

- When the expiration date is more than 60 days away, the From box is green.
- When the expiration date is within 60 days, the From box is yellow.
- When the expiration date has passed, the From box is red.

Identification

The serial number, Relatively Distinguished Name (RDN), and issuer RDN of the certificate.

Activity

The date the notification of the expiring/expired certificate was sent and the date the internal Pending state was set.

Cancel

Cancel any changes you have made and return to the Hierarchy page.

Add

Add the profile information to this address. You can add this profile to the address without enabling it.

Expired PGP Key Notify Page

The Expired PGP Key Notify address profile page allows you to enable notification of expiring and expired PGP keys to be sent to the address.

Note: If your user account is set as Read Only, then the **Add** and **Cancel** buttons will not be available.

Name

Expired PGP Key Notify

Description

Notify this address when one or more PGP keys will be expiring or have expired.

Status

Select whether you want the profile **Enabled** or **Disabled** at this time. You can change the status at any time.

Comments/Reason

Enter a comment or reason, such as why these keys are being monitored for this address.

(checkbox)

Click in the checkbox to select the PGP key for which you want notifications to be sent. You can select multiple PGP keys to be monitored.

User ID

Name of the PGP key

Validity Dates

The From/To dates during which the key is valid.

- When the expiration date is more than 60 days away, the To box is green.
- When the expiration date is within 60 days, the To box is yellow.
- When the expiration date has passed, the To box is red.

Identification

The key identification, type of key, and number of bits in the key.

Activity

The date the notification of the expiring/expired key was sent and the date the internal Pending state was set.

Cancel

Cancel any changes you have made and return to the Hierarchy page.

Add

Add the profile information to this address. You can add this profile to the address without enabling it.

FTP Address Page

Displays information for an address that uses FTP protocol.

- If data is stored on the node and picked up by the user, you do not need to supply information about the user's remote FTP server.
- If data is sent to the user automatically, you must supply information about the remote FTP server that receives the data.
- Sterling Commerce:Centre Development provides a form to be completed when an FTP customer is set up. See Development's internal web site.
-

IIBS FTP ID

Generated automatically. Applies only if data is stored on the node and picked up by the user. User ID for accessing the FTP server on the node.

IIBS FTP Password

Applies only if data is stored on the node and picked up by the user. Password for the FTP user ID on the node.

Note: This password cannot match the WAT password. When you create or edit an IIBS FTP password that matches the WAT password, a Warning message is displayed forcing you to create a different password.

Remote IP Address / Host name

Applies only if data is sent to the user automatically. Internet address or host name of the FTP server receiving outbound data from the node.

Remote FTP ID

Applies only if data is sent to the user automatically. User ID used by the node to log on to the FTP server that receives the outbound data.

Remote FTP Password

Applies only if data is sent to the user automatically. Password used by the node to log on to the FTP server that receives the outbound data.

Remote Path

Applies only if data is sent to the user automatically. Relative path on the remote FTP server where the node places outbound messages.

EDI IDs divider bar

List of EDI IDs associated with the address.

PGP Details

Displays PGP information about the selected FTP address.

Include PGP information

Indicates whether this FTP address uses Pretty Good Privacy (PGP) for inbound and outbound messages. If this field is **No**, the remaining fields are inactive.

Inbound signature required

Indicates whether or not the inbound message must be signed by the sender. If this field is **Yes,** and if an inbound message to this address is *not* signed, the message is blocked.

Encrypt outbound

Indicates whether or not outbound messages are encrypted before being sent.

Password (1st copy)

(For add and edit screens only)

Enter the password if Sterling Commerce:Centre has the customer's private PGP key. This is the same password used to add the private key onto the PGP key ring.

PGP Exchange Key User ID

User ID for the PGP key. This information comes from the PGP key ring.

Sign outbound

Indicates whether or not the outbound message will be signed. For customers, the customer's private PGP key is used. Otherwise, the Sterling Commerce:Centre private PGP key is used.

Have private key

For customers, indicates whether or not Sterling Commerce:Centre has the customer's private PGP key.

Password (2nd copy)

(For add and edit screens only)

Re-enter the password (if Sterling Commerce:Centre has the customer's private PGP key). This is the same password used to add the private key onto the PGP key ring.

FTP Address Search

Displays the results of a search for FTP addresses.

1 . . .

Number of the address in the list.

Address Name

Name for this FTP address.

IIBS FTP ID

User ID for accessing the FTP server on the node.

Remote IP

Internet address or host name of the FTP server receiving outbound data from the node.

Remote FTP ID

User ID used by the node to log on to the FTP server that receives the outbound data.

Mailslot

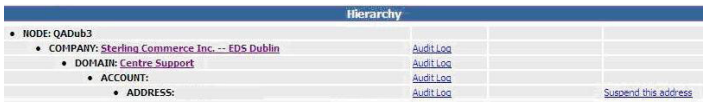
Mailslot for this FTP address. This is a link to the mailslot details.

Hierarchy Page

Displays the levels of the account hierarchy that precede the current company, domain, account, or address information. Click a level of the hierarchy to move to the associated page.

At the address level, users with a System Administration security level can click Suspend this Address to enable the suspension profile for the address.

Users with a Super User or System Administration security level can click the Audit Log link to search for changes in the audit log. The Any OID or text field is filled in with the OID of the corresponding address, account, domain, or company record (depending on which link is clicked).



When an address is suspended, the red SUSPENDED bar is displayed along with a link to edit the suspension profile (for users with a System Administration security level) or to view the suspension profile (for users with a CSR security level).

House Keeping Log Entries Page

Displays the results of a housekeeping log search.

The house keeping function deletes old data. The house keeping log lists what data has been deleted. This log is retained for 35 days.

Added Date/Time

Date and time the record was added to the housekeeping log.

Date format: MM/DD/YYYY

Time format: HH:MM:SS

Time zone: UTC

Table Name of Deleted Record

Name of the table from which the record was deleted

Audit Text

Duration (in milliseconds) of the housekeeping activity

Date and time of the housekeeping activity

Number of records deleted during the housekeeping activity

Note: It is possible that no records were deleted.

HTTP/S Address Page

Displays information for an address that uses HTTP or HTTPS.

Remote Web Server

Name of the user's Web (HTTP) server.

Remote Use Secure Channel

Yes or **No** – Indicates whether the user's HTTP server supports HTTPS. If HTTPS is supported, the node uses HTTPS to send outbound messages to the user.

Remote Port

The TCP/IP port number used to access the user's HTTP server. Typically, port number 80 is used.

Remote Path & Parameters

URL and parameters used to connect to the user's HTTP server.

Remote HTTP User ID

User ID set up on the user's system to authenticate outbound messages. The user ID is assigned by the user and communicated to Customer Support.

Remote HTTP Password

Password set up on the user's system to authenticate outbound messages. The password is assigned by the user and communicated to Customer Support.

Local HTTP User ID

User ID set up on the node to authenticate inbound messages. The user ID is assigned by Customer Support and communicated to the user. By default, the value is the name of the address (mailslot).

Local HTTP Password

Password set up on the node to authenticate inbound messages. The password is assigned by Customer Support and communicated to the user.

Note: This password must be unique. If you use the same password as the WAT account to set up or edit a mailslot, a Warning message is displayed forcing you to create a different password.

HTTP Address Search

Displays the results of a search for HTTP addresses.

1 . . .

Number of the address in the list.

Local HTTP User ID

User ID set up on the node to authenticate inbound messages. The user ID is assigned by Customer Support and communicated to the user.

Remote Web Server

Name of the user's Web server.

Remote HTTP User ID

User ID for the user's Web server.

Mailslot

Mailslot for this HTTP address. This is a link to the mailslot details.

Inbound Message Details Page

Displays information about one inbound message.

Originator Address

Messaging address of the sender (such as an e-mail address). If the sender's address cannot be presented as a string, the mailbox address of the sender is displayed (if available).

Subject

Subject line of the message.

Message Type

Refer to Message Types for details.

Billing Flags

Refer to Billing Codes for details.

Add Date/Time

Date and time the message was saved in the database on the node.

Date format: MM/DD/YY

Time format: HH:MM:SS

Time zone: UTC

Submission Date/Time

Date and time the message was received by the protocol connector on the node.

Date format: MM/DD/YY

Time format: HH:MM:SS

Time zone: UTC

Message ID

Complete 24-digit number that identifies a message.

Select **View Application Logs** to display a list of sessions whose logs for this message can be viewed.

Note: The Message ID Log display does not necessarily list all of the sessions, such as when session logging falls behind due to a heavy traffic load. The actual log files on the server contain all of the information. The session logging function uses those log files to display the information in a more user-friendly format.

Transaction ID

Complete 24-digit number that identifies a transaction. The transaction ID is assigned to link inbound messages to one or more resulting outbound messages, regardless of how many EDI interchanges are encountered.

Select **View Transaction** to display details about the transaction.

Session ID

Identification number of the session

Note: This session ID is not the same as the session ID used in the session log, as described in Message ID above.

MTS ID

ID assigned by a protocol or messaging system outside of Sterling Commerce:Centre and used to correlate and track messages across systems. Not all protocols or protocol implementations support this field. Outside of Sterling Commerce:Centre, this ID may be referred to as the message ID or the message-ID.

Association Type/ID

Refer to Association ID Type Page for details.

Message History

Refer to the topics about message histories.

Metadata

Displays the Metadata Details for the message.

Status

Refer to Inbound Message Status for details.

Protocol

Refer to Protocol Types for details.

Attachment Count

Number of attachments to the message.

Recipient Count

Number of receivers for the message.

Size

Size of the message and attachments in bytes.

COR Requested

Applies only to X.400 messages. Indicates that the X.400 message requests a confirmation of receipt.

- **Yes** – A COR is requested.
- **No** – A COR is not requested.

COD Requested

Applies only to X.400 messages. Indicates that the X.400 message requests a confirmation of delivery.

- **Yes** – A COD is requested.
- **No** – A COD is not requested.

Error Code

Applies to AS1 and AS2 accounts only. The DUNS number or ID of the receiver followed by any error code. See the error code descriptions for more details.

Sample DUNS number without error code: **123456789;**

Sample DUNS number with AS1 error code: **123456789;AS1001**

Notification Status

Indicates the status of processing the data contained in a message, either Waiting, In Process, Sent, Failed, or None.

Customer File Name

If present, the name of the customer file in the attachment.

Connect:Mailbox divider bar

Displayed only if the message came from a Sterling Commerce:Network mailbox.

Attachments divider bar

List of attachments in the message. Refer to Attachment Details Page for details.

Inbound Message Status

The node assigns a status to an inbound message.

Inbound Message Status	Description	Display Color
Complete	The inbound message was delivered to the node and processed successfully.	Green
Disabled	The message is disabled because the address has been set to Inactive. There will be no further processing of the message. The message will not be considered a dropped message.	Gray
Duplicate	A message has the same Message ID as a previous message.	Blue
Failed	The inbound message was not received successfully, either because of a communications problem or because it could not be processed.	Red
Failed and Reviewed	The inbound message failed and was reviewed by Customer Support. Customer Support changed the status to Failed and Reviewed so that the message is omitted from searches for failed messages and from reports generated by Customer Support's monitoring tools.	Orange
In Processing	A large message is taking several minutes to be delivered.	Yellow
Queued Reprocess	Messages that are queued for reprocessing. The Retry Monitor will scan for this status and then call CMS to reprocess the message. CMS will then change the status to Reprocessed.	Yellow
Reprocessed	The inbound message is a copy of an original message that has been resent and reprocessed by the node.	Blue

In addition, you can use the following term when searching for inbound messages. This is not real message status but provides a convenient way for searching.

ALL

Search for all inbound messages regardless of delivery status.

Inbound Messages Page

Lists inbound messages sent to accounts on the node from senders.

Indicates whether the message is included in reprocessing.

Reprocess

Select messages to be immediately reprocessed. Only displayed for users with a security level of CSR and above.

Queued Reprocess

Select messages to be queued for reprocessing. The Retry Monitor will scan for this status and then call CMS to reprocess the message. CMS will then change the status to Reprocessed. Only displayed for users with a security level of CSR and above.

Add Date/Time

Date and time the message was saved in the database on the node.

Date format: MM/DD/YY

Time format: HH:MM:SS

Time zone: UTC

Status

Refer to "Inbound Message Status" on page 190 for details.

Protocol

Refer to "Protocol Types" on page 207 for details.

Message ID

Last portion of the unique 24-digit number that identifies a message.

Transaction ID

Last portion of the unique 24-digit number that identifies a transaction. The transaction ID is assigned to link inbound messages to one or more resulting outbound messages, regardless of how many EDI interchanges are encountered.

Originator Address

Messaging address of the sender (such as an e-mail address). If the sender's address cannot be presented as a string, the mailbox address of the sender is displayed (if available).

Subject

Subject line of the message.

Interchange Details Page

Displays information about one EDI interchange.

ICN

Control number assigned to an EDI interchange by the sender. A single interchange refers to one exchange between a sender-receiver pair. However, the interchange may contain multiple messaging envelopes and multiple EDI documents.

Sender ID

EDI ID and qualifier of the sender.

Format: ID/qualifier

Receiver ID

EDI ID and qualifier of the receiver.

Format: ID/qualifier

Groups divider bar

Lists the group envelope sections within the EDI interchange.

Interchange Groups Page

Displays information about a group envelope section within an EDI interchange.

Group ID

ID of the group envelope section within the EDI interchange document.

Group Control Number

Identifier assigned to the group envelope section within the EDI interchange document.

Document Control Number

Identifier assigned to the EDI document within the group envelope section.

Document Type

Code indicating the type of EDI document.

Segment Count

Number of segments in the EDI document.

Character Count

Number of characters in the EDI document.

Interchanges Page

Lists EDI interchanges in the order they appear in the data.

Status

Status of the interchange on the node.

- **Done** – The interchange is processed.

Transaction ID

Unique 24-digit number that identifies a transaction. The transaction ID is assigned to link inbound messages to one or more resulting outbound messages, regardless of how many EDI interchanges are involved.

Data Type

Code indicating the EDI standard used in the document.

Control Number

Identifier assigned to the group envelope section within the EDI interchange document.

Sender

EDI ID and qualifier of the sender.

Format: EDI ID/qualifier

Receiver

EDI ID and qualifier of the receiver.

Format: EDI ID/qualifier

Envelope Segment Count

Number of segments in the group envelope section.

Document Segment Count

Number of segments in the document.

Log Message ID Search Results Page

Displays a list of sessions for this document. (Click on a session ID to see the application log entries related to this document. For details, see Log Session ID Search Results Page, below.)

The Message ID Log display does not necessarily list all of the sessions, such as when session logging falls behind due to a heavy traffic load. The actual log files on the server contain all of the information. The session logging function uses those log files to display the information in a more user-friendly format.

Timestamp

Date and time the logging session started.

Date format: MM/DD/YY

Time format: HH:MM:SS

Time zone: UTC

Session ID

Unique identification number of the session. Click on the number to display the application log entries for this session.

Application

Name of the application that created the logging session.

Label

Description of the session that this link displays.

Log Session ID Search Results Page

Displays the application log entries related to this document.

The Session ID Log display does not necessarily list all data for the document, such as when session logging falls behind due to a heavy traffic load. The actual log files on the server contain all of the information. The session logging function uses those log files to display the information in a more user-friendly format.

Timestamp

Date and time the logging session started.

Date format: MM/DD/YY

Time format: HH:MM:SS

Time zone: UTC

Severity

Color-coded severity of the event:

- A blue “i” indicates information.
- A green “4” indicates trace info.
- A yellow “!” indicates a warning.
- A red “x” indicates an error.

Event Id

Identification number of the log message. For example, 15428 indicates the start of a session.

Thread Id

Identification number of the application thread that wrote the entry.

Application

Name of the application that created the logging session.

Msg ID

Sterling Commerce:Centre message ID of the message this session belongs to.

Trans ID

Sterling Commerce:Centre transaction ID of the transaction that this session's message belongs to.

Text

Text of the application log entry.

Source

Complete path and name of the log file.

Mailbox Migration Page

Migrate EDI IDs from a source Mailbox/slot to a destination Mailslot.

Source Node

Name of the node that you are migrating the EDI ID from.

Source Mailbox/slot

Mailbox or mailslot that you are migrating.

- To migrate all EDI IDs in a mailbox, type the five-character mailbox name followed by an asterisk (*).
- To migrate the EDI IDs in a single mailslot, type the address name. If the source is on Sterling Commerce:Centre, the address is eight characters. If the source is on Sterling Commerce:Network, the address is between six and eight characters.

- To migrate a single EDI ID, type the mailbox name or mailslot address name and then enter the EDI ID and qualifier.

EDI ID and Qualifier

Name of the EDI ID and qualifier when migrating individual EDI IDs.

Destination Node

Name of the node that you are migrating the EDI ID to.

Destination Mailslot

Mailslot that you are migrating. If you are performing this procedure from the destination address, this field is automatically populated.

Message Types

The node assigns one or more message types to an inbound or outbound message.

Compressed

Message is compressed.

EDI

Message contains data formatted according to an EDI standard.

Encrypted

Message is encrypted.

FastPath

Message is routed to Sterling Commerce:Network as soon as it was received by the node. Refer to "Defer Message Routing" on page 104 and "Defer Parsing" on page 104 for details.

Inbound C:Net

Inbound message to Sterling Commerce:Network (that is, an outbound message from the node).

Inbound Centre

Inbound message to the node.

Inbound PGP

Inbound message to Sterling Commerce:Centre from the customer.

Internodal

Message is inbound from another node.

Local Message Store

Which message store is used, for outbound messages only.

Local & Non-Local Message Store

Which message store is used, for outbound messages only.

Non-Local Message Store

Which message store is used, for outbound messages only.

Outbound C:Net

Outbound message from Sterling Commerce:Network (that is, an inbound messages to the node).

Outbound Centre

Outbound message from the node.

Outbound PGP

Outbound message from Sterling Commerce:Centre to the customer.

Reply, *type*

Message is a reply that is generated automatically by the receiver's system. For inbound messages, a reply indicates that a trading partner's system received a message and sent the reply. For outbound messages, a reply indicates that the node received a trading partner's message and sent the reply. The type of reply can be one of the following:

- **COD**
- **COP**
- **COR**
- **DSN**
- **Inbound notification**
- **Internal notification**
- **MDN**
- **Message failed**
- **Outbound notification**
- **X.400 Delivery Report**

Report

Message is a report.

Signed

Message is signed and requires authentication.

SSL Connection

For HTTP or AS2, message uses HTTPS (SSL).

Transport Already Billed

For MQ, customer has already been billed for this message.

MQ Address Page

Displays information for an address that uses the MQ protocol.

Queue Manager Name

Name of the sending queue manager.

Send Command Queue Name

Name of the queue used for sending commands.

Receive Command Queue Name

Name of the queue used for receiving commands.

Destination Alias

Specified by GIODE as a Sterling Commerce:Centre mailslot, used for engine-bypass.

Send Data Queue Name

Name of the queue used for sending data.

Receive Data Queue Name

Name of the queue used for receiving data.

Node Details Page

Displays information about the current node when you are setting up templates.

Name

Name of the node.

Node ID

ID of the node.

Vantive Node ID

ID of the node in Vantive, a back-end system.

Node/Machine

Server name or ID of the node.

Description

Description of the node.

URL

URL address of the node.

Node Address

IP address of the node.

Cryptography Version

Version of the cryptography used on the node.

Current Node

- **Yes** – The node is the current node.
- **No** – The node is not the current node.

Is Active Trading Node

- **Yes** – The node is active and in production.
- **No** – The node is inactive or in testing.

Cryptography Type

Type of cryptography used on the node.

Node Templates Page

Lists the address templates set up on the node.

Name

Name of the address template. It is helpful to include terms like template and terms that identify the associated protocol.

Type

Protocol type to which the template applies.

Description

Description of the template. It is helpful to include terms like template and terms that identify the associated protocol.

Mailslot

Automatically displays Template. When a new address uses the template, this value is replaced with an actual messaging address.

Local MS, Local Message Store

- **Yes** – Messages for the address are stored on the node and retrieved by the receiver.
- **No** – Messages are sent to the address automatically and are not stored on the node.

Default

Applies only if there is more than one address for the account.

- **Yes** – The messaging address is the default address for the account.
- **No** – The messaging address is not the default address for the account.

Is Template

Yes. The messaging address is an address template.

Status

Status of the account. Refer to Account and Address Status Codes for details.

Error Code

Refer to the error code topics for details.

Edit

Edit the address template. Available only to users with System Administrator security level.

Nodes Page

Lists other nodes that you can access.

Node Name

Name of the node.

Node ID

ID of the node.

Edit

Edit the node name or URL address. Available only to users with System Administrator security level.

Outbound Message Details Page

Displays information about one outbound message.

Recipient Address

Messaging address of the receiver (such as an e-mail address). If the receiver's address cannot be presented as a string, the mailbox address of the receiver is displayed (if available).

Subject

Subject line of the message.

Message Type

Refer to Message Types for details.

Billing Flags

Refer to Billing Codes for details.

Add Date/Time

Date and time the outbound message is saved in the database.

Date format: MM/DD/YY

Time format: HH:MM:SS

Time zone: UTC

Delivery Time

Date and time the message is delivered to the receiver's mailbox on the node or to a destination external to the node.

Date format: MM/DD/YY

Time format: HH:MM:SS

Time zone: UTC

Pickup Date/Time

Date and time the message is picked up by the receiver.

Date format: MM/DD/YY

Time format: HH:MM:SS

Time zone: UTC

Message ID

Complete 24-digit number that identifies a message.

Select **View Application Logs** to display a list of sessions whose logs for this message can be viewed.

Note: The Message ID Log display does not necessarily list all of the sessions, such as when session logging falls behind due to a heavy traffic load. The actual log files on the server contain all of the information. The session logging function uses those log files to display the information in a more user-friendly format.

Transaction ID

Complete 24-digit number that identifies a transaction. The transaction ID is assigned to link inbound messages to one or more resulting outbound messages, regardless of how many EDI interchanges are encountered.

Select **View Transaction** to display details about the transaction.

Session ID

Identification number of the session

Note: This session ID is not the same as the session ID used in the session log, as described in Message ID above.

MTS ID

ID assigned by a protocol or messaging system outside of Sterling Commerce:Centre and used to correlate and track messages across systems. Not all protocols or protocol implementations support this field. Outside of Sterling Commerce:Centre, this ID may be referred to as the message ID or the message-ID.

Association Type/ID

Refer to Association ID Type Page for details.

Message History

Refer to the information about message histories.

Metadata

Displays the Metadata Details for the message.

Customer File Name

If present, the name of the customer file in the attachment.

Status

Refer to Outbound Message Status for details.

Disposition

Status of an outbound message delivered to a mailslot to be picked up by the user.

- **Read**. The receiver has opened the message.
- **Unread**. The receiver has not opened the message.
- **Deleted**. The receiver has deleted the message.

Protocol

Refer to Protocol Types for details.

Size

Size of both the message and attachments in bytes.

COR Requested

Applies only to X.400 messages. Indicates that the X.400 message requests a confirmation of receipt.

- **Yes** – A COR is requested.
- **No** – A COR is not requested.

COD Requested

Applies only to X.400 messages. Indicates that the X.400 message requests a confirmation of delivery.

- **Yes** – A COD is requested.
- **No** – A COD is not requested.

Retry Count

For undelivered messages, the number of attempted deliveries.

Error Code

Applies to AS1, and AS2 accounts only. The DUNS number or ID of the receiver followed by any error code. See the error code descriptions for more details.

Sample DUNS number without error code: **123456789**

Sample DUNS number with AS1 error code: **123456789;AS1001**

Notification Status

Indicates the status of processing the data contained in a message, either Waiting, In Process, Sent, Failed, or None.

Connect:Mailbox divider bar

Displayed only if the message is sent to a Sterling Commerce:Network mailbox.

Interchanges divider bar

EDI interchanges in the message.

Attachments divider bar

List of attachments in the message.

Outbound Message Status

The node assigns a status to an outbound message.

Outbound Message Status	Description	Color
Command in MTA	The command message has been delivered to the command queue. Waiting for the Command Message COA.	Yellow
Command in MTA Too Long	The command message has been in the command queue longer than the allotted time while waiting for the Command Message COA.	Red
Data in MTA	The data message has been delivered to the data queue. Waiting for the Data Message COA.	Yellow
Data in MTA Too Long	The data message has been in the data queue longer than the allotted time while waiting for the Data Message COA.	Red
Delayed Retry Requested	Another delivery of the outbound message has been requested for a later time.	Yellow
Delivered	The outbound message was delivered to the receiver's mailbox on the node or to a destination external to the node.	Green
Delivered Unread	The message was delivered to the next subsystem, but that subsystem has not yet processed the message.	Yellow
Failed and Notified	The outbound message cannot be delivered to the receiver and a notification has been sent to Customer Support.	Red
Incomplete	The outbound message has been created but is not complete.	Red
In Queue	The outbound message is in queue.	Yellow
In Queue Too Long	The outbound message has been in the queue for too long and requires intervention.	Red
In Transfer Agent	The outbound message has successfully made it to the intermediate transfer agent (such as X400 MTA) and is awaiting an acknowledgment message from the transfer agent.	Yellow
Remotely Delivered	The message (command and data) has been completely and successfully delivered to the remote system. Waiting for remote system to process message and send Command Message COD.	Yellow
Remotely Delivered Too Long	The message was successfully delivered to the remote system but was not processed by the remote system within the allotted time while waiting to receive Command Message COD.	Red

Outbound Message Status	Description	Color
Retry Requested	Sterling Commerce:Centre will try again to deliver the outbound message.	Yellow
Retrying	Sterling Commerce:Centre is in the process of re-delivering an outbound message.	Yellow
Still Delivering	The message is still in the Transferring state. The gateway checks the state of the message at configured intervals. This is currently set at three minutes.	Yellow
Suspended	The outbound message cannot be delivered because the customer is down and the address has been Suspended.	Red
Transferring	The outbound message is being transferred.	Yellow
Transferring Too Long	The outbound message has been in the Transferring state for too long and requires intervention.	Red
Undeliverable	The outbound message cannot be delivered to the receiver.	Red

In addition, you can use the following terms when searching for outbound messages. These are not real message states but provide convenient ways for searching.

ALL

Search for all outbound messages regardless of delivery status.

NOT DELIVERED

Search for all outbound messages that are not delivered.

Outbound Messages Page

Lists outbound messages sent from accounts on the node to receivers.

Indicates whether the message is included when messages are resent or marked as picked up.

Add Date/Time

Date and time the outbound message is saved in the database.

Date format: MM/DD/YY

Time format: HH:MM:SS

Time zone: UTC

Status

Refer to "Outbound Message Status" on page 201 for details.

Pickup Date/Time

Date and time the message is picked up by the receiver.

Disposition

Status of an outbound message that was delivered to a mailslot to be picked up by the user.

- **Read** – The receiver has opened the message.
- **Unread** – The receiver has not opened the message.

- **Deleted** – The receiver has deleted the message.

Protocol

Refer to "Protocol Types" on page 207 for details.

Message ID

Last portion of the unique 24-digit number that identifies a message.

Transaction ID

Last portion of the unique 24-digit number that identifies a transaction. The transaction ID is assigned to link inbound messages to one or more resulting outbound messages, regardless of how many EDI interchanges are involved.

Recipient Address

Messaging address of the receiver (such as an e-mail address). If the receiver's address cannot be presented as a string, the mailbox address of the receiver is displayed (if available).

Subject

Subject line of the message.

ICN

Interchange control number assigned to an EDI interchange by the sender. A single interchange refers to one exchange between a sender-receiver pair. However, the interchange may contain multiple messaging envelopes and multiple EDI documents.

Sender ID

EDI ID and qualifier of the sender.

Format: ID/qualifier

Receiver ID

EDI ID and qualifier of the receiver.

Format: ID/qualifier

PGP Key Ring Page

Displays installed PGP keys available for FTP accounts.

Note: If your user account is set as Read Only, then the **New**, **Delete**, and **Create** buttons will not be available.

User ID

Identification of the customer that the PGP key belongs to.

Validity Dates

The From and To dates and times that the PGP key is valid.

Download

Click to download the key.

Identification

Information describing the key, including:

- Key ID

- Key Type
- Key Bits

New

Click to upload a new PGP key.

Delete

Click to delete the selected PGP keys.

Create

Click to create a PGP key.

Refresh

If you manually add a PGP key, click **Refresh** to update the keys. (This is instead of bouncing GMH.)

Upload and Verify Key

Upload a file containing a PGP key.

(blank field)

Enter the name of the file containing the PGP key.

Browse

Click to navigate to the file containing the PGP key.

Upload Key file

Upload the specified file to the node.

Add a Key

Create a PGP key.

Algorithm

Select the algorithm to be used to create a PGP key:

- **RSA (Legacy)**
- **RSA (2 key)**
- **Elgamal (DSA signing)**

Key bits

Select the number of key bits in the PGP key:

- **1024**
- **2048**

Valid days

Enter the number of days until the PGP key expires. Enter **0** for no expiration.

Explanation of key types

Information that explains the Algorithm.

User name

Enter the user's name.

Password

Enter a password for the user. Must be at least six characters.

Re-enter Password

Enter the password again for validation.

Create

Create the PGP key with the information specified.

Cancel

Cancel the PGP key creation and return to the PGP Key Ring page.

File Details

Displays information about the file containing the PGP key.

File name

The name of the file containing the PGP key.

Content Type

Type of file. (Should be plain text.)

Content Length

Size of the file.

Keys in file

Information about the PGP keys contained in the file, including:

- User ID
- Validity Dates
- Identification

  See descriptions of these fields above.

Profile Description Details Page

Displays details about one account or address profile on the node.

Note: If your user account is set as Read Only, then the **Add** and **Edit** buttons will not be available.

Name

Name of the profile.

Description

Description of the profile.

Action ID

ID determined by the code on the current node that is associated with the profile.

Attribute Label, Attribute Description

Applies only if this profile requires attributes. Field label and description used in the WAT to identify the text box in which users enter attributes when they enable this profile.

Date Time Attribute Label, Date Time Attribute Description

Applies only if this profile requires a date-time attribute. Field label and description used in the WAT to identify the text box in which users enter the date-time attribute when they enable this (Suspend) profile.

Boolean Attribute Label, Boolean Attribute Description

Applies only if this profile requires a boolean attribute. Field label and description used in the WAT to identify the text box in which users enter the boolean attribute when they enable this (Unwrap Header/Trailer) profile.

Type

Account – The profile applies to an account and affects the data flow for all addresses in the account.

Address – The profile applies to an address and affects the data flow for the associated address only.

Level

Multiple – This profile can be one of several account profiles or several address profiles enabled for the account or address.

Single – This profile must be the only account profile or the only address profile enabled for the account or address.

Profile Used By: All, Enabled, Disabled

Display a list of the accounts or addresses that use this profile.

List Profile Descriptions

Display a list of all of the system profiles.

Add Profile Description

Add a new profile.

Edit Profile Descriptions

Edit an existing profile.

Profiles Page

Lists all account and address profiles defined on the current node. See information about profiles supplied on the Dublin 3 and Dublin 4 nodes.

Note: If your user account is set as Read Only, then the **Edit** and **Add** buttons will not be available.

Name

Name of the profile.

Description

Description of the profile.

Action ID

ID determined by the code on the current node that is associated with the profile.

Type

Account – The profile applies to an account and affects the data flow for all addresses in the account.

Address – The profile applies to an address and affects the data flow for the associated address only.

Level

Multiple – This profile can be one of several account profiles or several address profiles enabled for the account or address.

Single – This profile must be the only account profile or the only address profile enabled for the account or address.

Edit

Edit the profile.

Add Profile Description

Add a new profile.

Protocol Types

Sterling Commerce:Centre supports several protocol types for account setup and message tracking.

Protocol Type	Description	Use on Sterling Commerce:Centre nodes
AS1	AS1 is an EDI-INT standard. EDI data is secured using SMIME encryption and is transmitted over the Internet in an SMTP data stream. On a node, AS1 addresses are set up as SMTP addresses with Extended SMTP and SMIME information.	Refer to Extended SMTP Details for details.
AS2	AS2 is an EDI-INT standard. EDI data is secured using SMIME encryption and is transmitted over the Internet in an HTTP data stream.	Used for new addresses: Yes Used to search for addresses: Yes Used to search messages: Yes Displayed in message details: Yes
Connect:Mailbox	Connect:Mailbox is the protocol used to exchange messages between the node and a Sterling Commerce:Network mailbox on Sterling Commerce:Network.	Used for new addresses: No Used to search for addresses: No Used to search messages: Yes Displayed in message details: Yes
From Engine	From Engine is a protocol label that identifies messages exchanged between internal systems on the node.	Used for new addresses: No Used to search for addresses: No Used to search messages: Yes Displayed in message details: Yes
FTP	FTP (File Transfer Protocol) is an application protocol that runs over TCP/IP and provides the simplest way to exchange files between computers on the Internet. Both the sender and the receiver require FTP systems.	Used for new addresses: Yes Used to search for addresses: Yes Used to search messages: Yes Displayed in message details: Yes

Protocol Type	Description	Use on Sterling Commerce:Centre nodes
FTP (PGP)	Pretty Good Privacy (PGP) over FTP. FTP (PGP) provides security for FTP transactions.	Used for new addresses: Yes Used to search for addresses: No (Use **FTP** to search for addresses.) Used to search messages: Yes Displayed in message details: Yes
HTTP/HTTPS	HTTP (Hypertext Transfer Protocol) is a protocol that runs over TCP/IP and is used to transmit data over the Internet. By itself, HTTP is not secure. If security is required, HTTPS is used. HTTPS is HTTP combined with SSL (Secure Sockets Layer).	Used for new addresses: Yes Used to search for addresses: Yes Used to search messages: Yes Displayed in message details: Yes
Internal	Internal is a protocol label that identifies messages generated by an internal system on the node. For example, messages containing reports and error notifications use the internal protocol.	Used for new addresses: No Used to search for addresses: No Used to search messages: Yes Displayed in message details: Yes
MQ	MQ is a protocol label that identifies messages exchanged between Sterling Commerce:Centre and Sterling Commerce:Network through the MQ Series Interface.	Used for new addresses: Yes Used to search for addresses: Yes Used to search messages: Yes Displayed in message details: Yes
SMTP	SMTP (Simple Mail Transfer Protocol) is an application protocol that runs over TCP/IP. SMTP is the de facto standard for sending e-mail between servers, usually sending messages from a mail client to a mail server. Typically, users use SMTP for sending e-mail and either POP3 or IMAP for receiving e-mails from their local server. On a node, AS1 addresses use SMTP and require Extended SMTP and SMIME information.	Used for new addresses: Yes Used to search for addresses: Yes Used to search messages: Yes Displayed in message details: Yes
X.400	X.400 is a protocol that runs over TCP/IP and is an ISO and ITU standard for addressing and transporting e-mail messages. Common in Europe and Canada, X.400 is an alternative to the more prevalent e-mail protocol, SMTP.	Used for new addresses: Yes Used to search for addresses: Yes Used to search messages: Yes Displayed in message details: Yes

Queued Reprocess Request Status Page

Displays the status of messages that were queued for reprocessing.

Indicates whether the message is included in reprocessing.

Queued Reprocess Status

Status of the reprocess.

Add Date/Time

Date and time the message was saved in the database on the node.

Date format: MM/DD/YY

Time format: HH:MM:SS

Time zone: UTC

Status

Refer to “Inbound Message Status” on page 190 for details.

Protocol

Refer to “Protocol Types” on page 207 for details.

Message ID

Last portion of the unique 24-digit number that identifies a message.

Transaction ID

Last portion of the unique 24-digit number that identifies a transaction. The transaction ID is assigned to link inbound messages to one or more resulting outbound messages, regardless of how many EDI interchanges are encountered.

Originator Address

Messaging address of the sender (such as an e-mail address). If the sender's address cannot be presented as a string, the mailbox address of the sender is displayed (if available).

Subject

Subject line of the message.

SMIME Details Page

Displays information for X.509 certificates required by an AS1 or AS2 address.

Different Signing and Exchange Certificates

Indicates whether separate certificates are used for encryption and for signing.

- **Yes** – The address uses two certificates, one for encryption and one for signing.
- **No** – The address uses one certificate for both encryption and signing.

Exchange Certificate RDN

Identifies the subject RDN of the encryption certificate.

- If there is one certificate from the trading partner, the subject RDN that is returned when the address's certificate is added using the CSR Access menu.
- If there are two certificates from the trading partner, the subject RDN that is returned when the address's encryption certificate is added using the CSR Access menu.

Signing Certificate RDN

Identifies the subject RDN of the signing certificate.

If there are two certificates from the trading partner, use the subject RDN that is returned when the address's signing certificate is added to the node.

SMTP Address Page

Displays information for an address that uses SMTP protocol, including AS1 addresses.

- If data is stored on the node and picked up by the user, you must enter a new, unique SMTP address. A new POP3 ID is generated automatically, but you must enter a new password for the POP3 ID.
- If data is sent to the user automatically, you must enter an existing SMTP e-mail address that resides on an ISP outside of Sterling B2B Collaboration Network.

SMTP Address

User ID and complete Internet domain name.

- Many Internet domain names begin with a company name as the first element in the domain name (**myuserID@Acme.xx.yyy.com**).
- The first character in the domain name can be a wildcard, the asterisk (*).
- If data is stored on the node and picked up by the user, the address is a unique user ID and Internet domain name corresponding to the POP3 ID (mailbox) on the node.
- If data is sent to the user automatically, the address is a user ID and complete Internet domain name of an existing SMTP e-mail address that resides on an ISP outside of Sterling B2B Collaboration Network.

IIBS POP3 ID

Generated automatically if data is stored on the node and picked up by the user. Name of the POP3 mailbox on the node where messages are picked up.

IIBS POP3 Password

Applies only if data is stored on the node and picked up by the user. Password for the POP3 ID (mailbox).

Note: This password cannot match the WAT password. When you create or edit a mailslot password that matches the WAT password, a Warning message is displayed forcing you to create a different password.

"Extended SMTP Details" Displays information required by an AS1 address.

Secure Message Protocol

None – Use this setting for all SMTP addresses that are not AS1 accounts.

SMIME – Applies to AS1 addresses only. This setting populates the other Extended SMTP fields and requires SMIME information to be specified.

Payload Type

Applies only to AS1 addresses. Format used for the EDI data in messages for this address.

Default MIME Type

Applies only to AS1 addresses. Default MIME type used for non-text data in messages for this address.

Default MIME Sub Type

Applies only to AS1 addresses. Default MIME subtype used for nontext data in messages for this address.

Message Format

Applies only to AS1 addresses. Format used for messages for this address.

Customer Type or Is Hosted Customer

Applies only to AS1 addresses. Trading Partner. The address is for an AS1 trading partner.

Receipt Type

Applies only to AS1 addresses. Type of receipt required in messages for this address.

Receipt Signature Type

Applies only to AS1 addresses. Type of signature required in messages for this address.

Signing Algorithm

Applies only to AS1 addresses. Algorithm used to calculate a hash value that authenticates (or signs) this address as the sender of outbound data. This algorithm is included in an outbound message being encrypted. The address's signing key is used as input to this algorithm, resulting in the hash value which authenticates this address as the sender.

Symmetric Algorithm

Applies only to AS1 addresses. Algorithm used to encrypt outbound data and decrypt inbound data for this address. The address's encryption key is used as input to the algorithm.

Compression Algorithm

Applies only to AS1 addresses. Algorithm used to compress data before the message is sent.

- **None** – Data is not compressed before sending.
- **ZLIB** – Data is compressed using the ZLIB [RFC 1950] standard algorithm.

SMTP Address Search

Displays the results of a search for SMTP addresses.

1 . . .

Number of the address in the list.

User ID

Unique identifier for the user on the user's SMTP system.

Domain

Internet domain name for the user's SMTP

POP3 ID

Name of the POP3 mailbox on the node where messages are picked up.

POP3 Password

Password for the POP3 ID (mailbox).

Mailslot

Mailslot for this SMTP address. This is a link to the mailslot details.

Transaction Details Page

Lists all messages associated with a transaction ID.

Inbound Messages divider bar

Lists all inbound messages associated with a transaction ID.

Outbound Messages divider bar

Lists all outbound messages associated with a transaction ID.

X.400 Address Page

Displays information for an address that uses X.400 protocol.

If data is stored on the node and picked up by the user, you do *not* need to supply information about the user's remote X.400 server.

If data is sent to the user automatically, you *must* supply information about the remote X.400 server that receives the data.

Country

Country where the ADMD (the e-mail provider) resides. This is the ISO standard (2 letters or 3 numerals).

ADMD

Administrative management domain name that is unique within a country. Identifies the provider of e-mail messaging using X.400 protocol (such as IBM or a distributor). Part of the mnemonic ORAddress in X.400 standards.

PRMD

Private management domain name that is unique within a country. Identifies a private organization (such as a company) that subscribes to the administrative management domain (such as IBM or a distributor). Each PRMD is responsible for its own directories. Part of the mnemonic ORAddress in X.400 standards.

Organization

Subcategory of a PRMD that can be used in conjunction with an organization unit (such as a company name). Part of the mnemonic ORAddress in X.400 standards.

Surname

Last name of the user accessing the X.400 connection to the node. Part of the mnemonic ORAddress in X.400 standards.

Given Name

First name of the user accessing the X.400 connection to the node. Part of the mnemonic ORAddress in X.400 standards.

Common Name

Name that identifies the X.400 user if the given name and surname do not clearly identify the user. Part of the mnemonic ORAddress in X.400 standards.

Organization Unit 1Organization Unit 2

Subcategories of the organization (such as a company's region or department). Part of the mnemonic ORAddress in X.400 standards.

DDA Type 1

Domain-defined attribute type, such as whether the value indicated is a payroll number or a billing indicator. You must specify DDA types in order, and each DDA type must have a corresponding DDA value. For example, you cannot specify DDA type 3 without first specifying DDA types 1 and 2. DDA type and value pairs are case sensitive. Part of the mnemonic ORAddress in X.400 standards.

DDA Value 1

Domain-defined attribute value, such as what the payroll amount or billing indicator is. You must specify a DDA value for each corresponding DDA type, and you must specify DDA type and value pairs in order. For example, you cannot specify DDA type and value 3 without first specifying DDA type and values 1 and 2. DDA type and value pairs are case sensitive. Part of the mnemonic ORAddress in X.400 standards.

Comment

Notes related to this address. Not part of the ORAddress in X.400 standards.

Extended X.400 Details

DDA Type 2DDA Type 3DDA Type 4

Domain-defined attribute type, such as whether the value indicated is a payroll number or a billing indicator. You must specify DDA types in order, and each DDA type must have a corresponding DDA value. For example, you cannot specify DDA type 3 without first specifying DDA types 1 and 2. DDA type and value pairs are case sensitive. Part of the mnemonic ORAddress in X.400 standards.

DDA Value 2DDA Value 3DDA Value 4

Domain-defined attribute value, such as what the payroll amount or billing indicator is. You must specify a DDA value for each corresponding DDA type, and you must specify DDA type and value pairs in order. For example, you cannot specify DDA type and value 3 without first specifying DDA type and values 1 and 2. DDA type and value pairs are case sensitive. Part of the mnemonic ORAddress in X.400 standards.

Form

Form name for the address. Not part of the ORAddress in X.400 standards.

Free Form Name

Free-form name for the address. Not part of the ORAddress in X.400 standards.

Gen Qual

Generational qualifier, such as *senior*, *junior*, or *IV*. Part of the mnemonic ORAddress in X.400 standards.

Initials

Initials of the user, up to five characters. Initials must correspond to all names except the surname. For example, Jane Allison Doe specifies *JA* as her initials. Part of the mnemonic ORAddress in X.400 standards.

Label

Label for the address. Not part of the ORAddress in X.400 standards.

Network Address

X.121 address used to address terminals such as Telex, fax, or DDD terminals. Part of the terminal ORAddress in X.400 standards.

Network Num Address

Subset of the network address representing the network address minus the subaddress. Part of the terminal ORAddress in X.400 standards.

Network Sub Address

Subset of the network address that specifies the X.121 provider (such as AT&T or Sprint). Part of the terminal ORAddress in X.400 standards.

Numeric User ID

Numeric string identifying the user's user agent. Applies only to systems requiring numeric schemes, such as Fax-to-X.400. Part of the numeric ORAddress in X.400 standards.

Organization Unit 3Organization Unit 4

Subcategories of the organization (such as a company's region or department). Part of the mnemonic ORAddress in X.400 standards.

PD Country Code

Physical delivery country code identifying the country in which the user receives mail and shipments. This is the ISO standard (2 letters or 3 numerals).

PD Service

Physical delivery service name identifying the carrier who transports mail or other shipments to the user (such as UPS). Part of the postal ORAddress in X.400 standards.

Reply / Request

Reply or request for the address, either Yes or No. Not part of the ORAddress in X.400 standards.

Short Name

Short name for the address. Not part of the ORAddress in X.400 standards.

Telephone

Telephone number for the address. Not part of the ORAddress in X.400 standards.

Terminal ID

ID of the terminal used to verify delivery of the Telex or fax number. Part of the terminal ORAddress in X.400 standards.

Terminal Type

Type of terminal receiving messages, such as Telex, G3 Fax, or IA5 terminals. Part of the terminal ORAddress in X.400 standards.

X.400 Address Search

Displays the results of a search for X.400 addresses.

1 . . .

Number of the address in the list.

Given Name

First name of the user accessing the X.400 connection to the node. Part of the mnemonic ORAddress in X.400 standards.

Surname

Last name of the user accessing the X.400 connection to the node. Part of the mnemonic ORAddress in X.400 standards.

PRMD

Private management domain name that is unique within a country. Identifies a private organization (such as a company) that subscribes to the administrative management domain (such as IBM or a distributor). Each PRMD is responsible for its own directories. Part of the mnemonic ORAddress in X.400 standards.

ADMD

Administrative management domain name that is unique within a country. Identifies the provider of e-mail messaging using X.400 protocol (such as IBM or a distributor). Part of the mnemonic ORAddress in X.400 standards.

Organization

Subcategories of the organization (such as a company's region or department). Part of the mnemonic ORAddress in X.400 standards.

DDA Type

Domain-defined attribute type, such as whether the value indicated is a payroll number or a billing indicator. Part of the mnemonic ORAddress in X.400 standards.

Mailslot

Mailslot for this X.400 address. This is a link to the mailslot details.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

19-21, Nihonbashi-Hakozakicho, Chuo-ku

Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be

incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who want to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

J46A/G4

555 Bailey Avenue

San Jose, CA 95141-1003

U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available. This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are ficticious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Connect Control Center®, Connect:Direct®, Connect:Enterprise, Gentran®, Gentran:Basic®, Gentran:Control®, Gentran:Director®, Gentran:Plus®, Gentran:Realtime®, Gentran:Server®, Gentran:Viewpoint®, Sterling Commerce™, Sterling Information Broker®, and Sterling Integrator® are trademarks or registered trademarks of Sterling Commerce, Inc., an IBM Company.

Other company, product, and service names may be trademarks or service marks of others.

Index

Numerics

A

B

C

D

E

F

G

H

I

R

S

T

U

V

W

X

Product Number: xxxx-xxx

Printed in USA