

Sterling e-Invoice Gateway

Implementation Guide

Version 1.0

Sterling Standards Library Build 5400

Sterling Commerce
An IBM Company

© Copyright 2009 Sterling Commerce, Inc. All rights reserved.

Contents

Implementing the Sterling e-Invoice Gateway	5
Overview	5
Prerequisite Knowledge	5
Implementation Steps	5
Customer Support	6
Credentials Fulfillment	6
Picking Up Renewed Certificates in Two Years	9
Configuring the Check Expire Service	10
If Your Technical Contact Information Changes	10
If You Lose the Password And/Or Control Code	10
Maintenance Updates	10
Optimize System Performance	11
Installing the e-Invoice Archive Install Script	12
Overview	12
Executing the Archive Install Script on a non-iSeries Operating System	12
Executing the Archive Install Script on an iSeries Operating System	13
Configuring the eInvoice Archive Service	15
Setting Global Configuration Parameters for e-Invoicing	16
Overview	16
Setting Global Parameters	16
Implementing e-Invoice Partner Relationships	19
Overview	19
Before You Begin	19
Setting Up e-Invoicing Trading Profiles	19
Implementing e-Invoice Identity Records	20
Overview	20
Creating an Identity Record for Your Organization	20
Creating an Identity Record for Your Trading Partner	21
Implementing e-Invoice Agreements	23
Overview	23
Creating an e-Invoice Agreement	23
Implementing Envelopes for the Sterling e-Invoice Gateway	26
Overview	26
Setting Global e-Invoicing Envelope Properties	26
Creating a New Envelope	27
Updating Envelope Properties	28
Setting e-Invoice Permissions	29
Overview	29
Creating Permissions for Sterling e-Invoice Gateway Users	30
Creating Groups for Sterling e-Invoice Gateway Users	31

Creating a Password Policy	33
Creating User Accounts with e-Invoicing Permissions	33
Creating Maps for Use with the Sterling e-Invoice Gateway	37
Overview	37
Canonical Invoice Format Components in the Map Editor	38
Creating a Canonical Invoice Format Map	39

Implementing the Sterling e-Invoice Gateway

Overview

The Sterling e-Invoice Gateway enables you to use electronic invoices (e-Invoices) while also maintaining the requisite legal compliance. This enables elimination of paper trails that companies have to maintain for compliance with Value Added Tax (VAT) laws, including complying with all the audit requirements for tax purposes.

The Sterling e-Invoice Gateway uses the e-signature method of compliance, which uses digital signatures to allow the seller to sign an invoice digitally using keys approved by the government of the seller's country. The signature is then verified by the buyer and these signatures can be verified in future tax audits for their authenticity and integrity by re-verifying the signatures on archived invoices. The e-signature method of compliance is the preferred option of the tax authorities because it provides an unequivocal technical guarantee of the authenticity and integrity of the invoice.

Sterling Commerce has partnered with TrustWeaver™ to provide e-signature signing and verification through its on-demand service. All other e-Invoice functionality is created by Sterling Commerce. TrustWeaver offers products and on-demand services that support all of the necessary hardware and certificate authorities.

This documentation describes how to implement the Sterling e-Invoice Gateway.

Prerequisite Knowledge

The following are prerequisites to using the Sterling e-Invoice Gateway:

- ◆ The audience using this software should be familiar with the application, e-Invoicing, TrustWeaver, and Value Added Tax (VAT) compliance regulations.

Note: This documentation is not intended to explain e-Invoicing or how to use TrustWeaver software.

- ◆ You must have purchased an e-Invoicing license for use with the application.

Implementation Steps

To implement the Sterling e-Invoice Gateway, you must complete the following tasks:

1. Prior to using the Sterling e-Invoice Gateway, if you want to use the Integrated Archive you must execute the e-Invoice Archive Install script to create the necessary archive database configurations. This step is not necessary if you will be using an external or custom/trading partner archive. See *Installing the e-Invoice Archive Install Script* on page 12 for more information.
2. Obtain and check in the necessary certificates. See *Credentials Fulfillment* on page 6 for more information.
3. Ensure that you have the correct VAT ID from the Central European Union database (URL: http://ec.europa.eu/taxation_customs/vies/vieshome.do?selectedLanguage=EN). Verifying that you have the VAT ID correct is your legal responsibility. This database does not identify the country but verifies that a European Union VAT ID is a valid code.

4. Configure global e-Invoicing parameters.
5. Assign the appropriate permissions for those users performing e-Invoicing tasks.
6. Verify whether you currently have business processes using the same names as the predefined e-Invoicing business processes and, if so, rename those business processes.
7. Create the necessary maps to translate your invoice format to the canonical format used by the Sterling e-Invoice Gateway.

Note: You may need to keep the canonical maps for archival purposes so that they can be inspected by an auditor.

8. Create an identity for each trading relationship.
9. Create an agreement to describe each relationship between you and your trading partners.
10. Update outbound envelopes or set the size limit for interchanges and transactions in the `customer_overrides.properties` file.
11. Optimize your system performance by completing the steps in *Optimize System Performance* on page 11.

Customer Support

Sterling Commerce fosters long-term business partnerships with its customers. Committed to customer satisfaction and quality support, Sterling Commerce Customer Support has a world-wide staff providing support 24 hours per day, 365 days per year. For assistance with installation, implementation, usage, or for enhancement information, contact Customer Support. Check your maintenance contract for details about the type of support you have purchased for your product.

Note: Customer Support cannot validate or certify VAT compliance or recommend how to maintain compliance. Contact SCI Sales and Professional Services for information on maintaining compliance. Customer Support is a technical resource, not a business resource.

Additionally, the Sterling Commerce Web site (www.sterlingcommerce.com) provides a wealth of information at your fingertips. The site includes information about e-commerce, a solutions database, document tracking tools, an issue tracking system, fix information, product and service documentation, workshop information, contact information, sunset and retirement schedules, and ordering information.

Before contacting Sterling Commerce Customer Support, we recommend that you review the documentation provided with your product. The documentation may help you to identify or resolve the problem you are experiencing. Additionally, we recommend that you review the *Customer Support Reference Guide* (www.sterlingcommerce.com/PDF/CustSuppRefGuide.pdf), which describes the Sterling Commerce Customer Support offerings, best practices, contact information, and contact methods you should use to ensure that Customer Support receives the necessary information to quickly respond and resolve any issues.

Credentials Fulfillment

For the Sterling e-Invoice Gateway, you need to obtain credentials that establish your identity and authorize your install of the application to connect with the TrustWeaver server. Before you obtain a copy of the Sterling e-Invoice Gateway, you must provide an e-mail address and fax number for your technical contact to Sterling Commerce Sales.

Sterling Commerce will provide this contact information to TrustWeaver and TrustWeaver uses this contact information to send you the information you need to obtain credentials. This information will be provided in two parts for security purposes. The first part will be in an e-mail addressed to your technical contact, and the second part will be faxed to you from TrustWeaver. You will need both parts of this information to download the necessary digital certificates from a link that TrustWeaver will provide you in the e-mail they send to you. TrustWeaver will also add the e-mail address you provide to its list of subscribers, so they can notify you of critical product alerts and system status updates. For this reason, we recommend you provide an e-mail alias or group account that can be managed long-term, independent from an e-mail address of an individual employee.

To use these credentials, you must complete these tasks in sequential order:

Step Number	Task	For More Information
1	<p>Provide Sterling Commerce Sales with your contact information. When your order is fulfilled, you will receive an e-mail and a fax from TrustWeaver. The e-mail will include a password and the fax will contain your Control Code.</p> <p>Caution: You must retain this information in a secure place because you will need it when you pick up renewed certificates two years after your initial install.</p>	<p>If you do not receive the e-mail and fax from TrustWeaver, contact your Sterling Commerce account representative.</p> <p>If you are having trouble downloading the necessary certificates after receiving the e-mail and fax from TrustWeaver, open a Support Case with Sterling Commerce Customer Support.</p>
2	<p>Download the CA and PKCS12 digital certificates (for authentication with the TrustWeaver server) from TrustWeaver.</p>	<p>To download the digital certificate, follow the instructions provided in <i>Obtaining Digital Certificates from TrustWeaver</i> on page 7.</p>
3	<p>Check in the CA and PKCS12 certificates to the application.</p>	<p><i>Checking In Digital Certificates</i> on page 8</p>
4	<p>Configure the Check Expire service so you will be warned using your preferred output method at least 14 days prior to when your certificates expire, to avoid the risk of downtime when these certificates expire. We recommend that you use e-mail as the output method for alerts.</p>	<p>See <i>Managing Services and Adapters</i> for more information on configuring the Check Expire service.</p>

Obtaining Digital Certificates from TrustWeaver

To obtain digital certificates from TrustWeaver:

1. Contact TrustWeaver and register for credential download.

You will receive notification from TrustWeaver with a web link to the location from which you can download the certificates. The link will contain an email code, which is half of the certificate password. The other half of the password, the Control Code, will be faxed to you at the fax number you supply during registration.

2. Once you have the link and your Control Code, you use the link to access the TrustWeaver web page from which you can download the CA certificate and the PKCS12 certificate. Download both certificates.
3. Rename the .p12 file that you downloaded from step 2 to use the file extension .pfx.
4. Follow the instructions below to check in the digital certificates.

Checking In Digital Certificates

To check in the CA and PKCS12 digital certificates so your invoices can be securely transported to and from TrustWeaver:

1. Save the certificate to a file on your local computer.
2. In the application, from the **Administration** menu, select **Trading Partner > Digital Certificates > CA**.
3. Next to Check in New Certificate, click **Go!** to check in the CA certificate.
4. **In the Filename** field, type or browse to the file name of the certificate and click **Next**.
5. Verify the name of the certificate you are checking in.

Note: For each certificate in the file you selected, the Certificate Name field contains a suggested name built out of the issuer relative distinguished name (RDN) and serial number of the certificate. Below the name is a summary of the identifying information in the certificate. For convenience, the application records the name of the certificate in its database. You can change the name to fit your file name conventions or to something easier to remember.

6. Next to **Validate When Used**, if you want to validate your certificate using one of the following options, select the appropriate validation options:
 - ◆ **Validity** – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
 - ◆ **Auth Chain** – Constructs a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
 - ◆ **CRL Cache** – Checks the Certificate Revocation List (CRL) in the CRL cache to ensure that the certificate is not revoked or in a held state.

Note: To use the CRL Cache option, you must have the CRL feature enabled and create business processes to download CRLs. The CRL Cache option displays only for certificates issued by a CA and does not display if you use a self-signed certificate.

7. If there is more than one CA certificate in the file you selected, you can check in each certificate by selecting the check box next to it.
8. Click **Finish** to check the CA certificate in to the application.
9. In the application, from the **Administration** menu, select **Trading Partner > Digital Certificates > System**.
10. Next to Check in PKCS12 Certificate, click **Go!** to check in the new PKCS12 certificate.

11. In the Specification page, complete the following fields and click **Next**.

Field	Description
Certificate Name	Type a unique and meaningful name for the PKCS12 certificate. Required
Private Key Password	Type the private key password. This is the password used to encrypt the PKCS12 certificate. Required. Note: The Private Key Password and Key Store Password are the same, and they are the concatenation of the email code and control code from <i>Obtaining Digital Certificates from TrustWeaver</i> on page 7. For example, if your password is xYKt and Control Code is A5hzTXpM, the concatenation of both is xYKtA5hzTXpM. You must retain the password and control code information because you will need it when you pick up renewed certificates two years after your initial install.
Key Store Password	Type the key store password. This is the password for the PKCS12 object. It may be the same as the private key password. Required. Note: The Private Key Password and Key Store Password are the same, and they are the concatenation of the email code and control code from <i>Obtaining Digital Certificates from TrustWeaver</i> on page 7. For example, if your password is xYKt and Control Code is A5hzTXpM, the concatenation of both is xYKtA5hzTXpM. You must retain the password and control code information because you will need it when you pick up renewed certificates two years after your initial install.
Filename (.pfx)	Type the filename of the certificate or click Browse to select the file name of the PKCS12 certificate. Required.

12. Next to **Validate When Used**, if you want to validate your certificate using one of the following options, select the appropriate validation options:

- ◆ Validity – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
- ◆ Auth Chain – Constructs a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.

13. If there is more than one PKCS12 certificate in the file you selected, you can check in each certificate by selecting the check box next to it.

14. Click **Finish** to check the PKCS12 certificate in to the application.

Picking Up Renewed Certificates in Two Years

You can download the CA and PKCS12 digital certificates again at any time if you retain the information provided to you in the e-mail and fax you receive from TrustWeaver.

Additionally, two years after you have downloaded the digital certificates for the first time, you will need to pick up the renewed certificates. TrustWeaver automatically makes these certificates available for you to pick up sixty days prior to the expiration of the certificates, and TrustWeaver will e-mail your registered contact to inform you that the renewed certificates are available for you to pick up.

You need to pick up the renewed certificates from TrustWeaver, and then either you can check in the certificates or SCI Professional Services can assist you with checking in the certificates.

Configuring the Check Expire Service

The application Check Expire service alerts you when certificates are about to expire, or have expired. The Check Expire service runs on a schedule (by default it runs daily at 2:30 AM), and reviews each checked-in certificate to compare its expiration date against the value set in the application (the default is 14 days). Any certificates that have already expired or will expire within the specified number of days are listed on your Admin Console Home page in **System Alerts**, **System Alerts on Dashboard**, and the **Event Viewer** under the **Operator** menu. These alerts remain in the system for 60 days.

Note: You need to configure the Check Expire service so you will be warned using your preferred output method at least 14 days prior to when your certificates expire, to avoid the risk of downtime when these certificates expire. We recommend that you use e-mail as the output method for alerts. See *Managing Services and Adapters* for more information about configuring the Check Expire service.

If Your Technical Contact Information Changes

If your technical contact information changes (specifically, your e-mail address or fax number), open a Support Case requesting a change of record through Support on Demand. Sterling Commerce will verify that you are authorized to obtain credentials.

If You Lose the Password And/Or Control Code

If you ever lose the password and/or control code information sent to you by TrustWeaver, open a Support Case requesting a replacement through Support on Demand. Sterling Commerce will verify that you are authorized to obtain credentials.

Maintenance Updates

If TrustWeaver updates its software, we may need to provide an update to the Sterling e-Invoice Gateway. If an update is necessary, it will be posted on Support on Demand like standard maintenance patches are posted.

To use the Support on Demand Web site (free of charge):

1. Open your Internet browser and go to www.sterlingcommerce.com.
2. Select **Customer Support**.
3. In the Support on Demand box, click **LOGIN**.
4. Type your E-mail address and password.

If you do not have a Support on Demand password, follow the instructions on Support on Demand to request one.

5. Click **Login** and follow the online instructions.

Optimize System Performance

To optimize the performance of the Sterling e-Invoice Gateway, complete the following steps:

1. Choose a single workflow queue to dedicate solely to the TrustWeaverEInvoicing process (for example, queue 5).
2. Stop the application.
3. Modify the tuning properties so that the chosen queue has a minimum and maximum pool size equal to the number of simultaneous connections allowed to TrustWeaver. For example, if you are using queue 5, and are using up to 10 simultaneous connections to TrustWeaver, you need to set the following two properties in the **tuning.properties** property file:

```
NOAPP.MAX_POOL_SIZE_5=10
```

```
NOAPP.MIN_POOL_SIZE_5=10
```

4. After you edit the properties file, run **setupfiles.sh**, and then restart the application.

Installing the e-Invoice Archive Install Script

Overview

Prior to using the Sterling e-Invoice Gateway, you must execute a script to create the necessary archive database configurations.

Note: This script is available when you install the Sterling e-Invoice Gateway.

Note: If the application is installed on the iSeries operating system, then only the native iSeries DB2 database can be used for the integrated archive.

Executing the Archive Install Script on a non-iSeries Operating System

Complete the following instructions to install the e-Invoice Archive Install Script on a UNIX or Windows operating system:

1. Install or upgrade the application by following the application *Installation* documentation.
2. From the **Administration** menu, select **Operations > System > Troubleshooter**.
3. Click **Stop the System**.
The application displays the warning, This will shut down the whole environment and end your session. Do you want to continue?
4. To shut down the application, click **OK**. The application must be shut down because the Archive Install Script will be making modifications to properties files.
5. Change to the **<Application Installation Directory>/bin/** directory.
6. Install the **setupEInvoiceArchive** file using the following commands:
 - ◆ If you are installing on a UNIX operating system, type `setupEInvoiceArchive.sh`
 - ◆ If you are installing on a Windows operating system, type `setupEInvoiceArchive.cmd`
7. *For clustered environments only*, is this the primary node of the cluster? Type **yes** and press **Enter** if you are running on the primary node of the cluster. Otherwise (if you are not running the script on the primary node of a cluster), type **no** and press **Enter**.

Note: The e-Invoice Archive Setup script must be executed on each node of the cluster.

8. Which database do you want to use?

Note: Supported databases are MySQL, Microsoft SQL Server, Oracle and DB2. For a full list of supported database version and supported JDBC drivers, please refer to the application installation requirements documentation. If MySQL is used, the default table type must be **InnoDB**. This can be specified by adding the line **default-storage-engine=innodb** to the **[mysqld]** section of the **my.cnf** configuration file.

- ◆ When you are prompted to enter the database username, type the username for the archive database and press **Enter**.

- ◆ When you are prompted to enter the database password, type the password for the archive database and press **Enter**.
- ◆ When you are prompted to enter the database name, type the database name for the archive database and press **Enter**.

Note: The archive database must be different than the application database or any other archive database. If the application is installed on the iSeries operating system, then only the native iSeries DB2 database can be used for the integrated archive.

- ◆ When you are prompted to enter the database host name, type the host name or IP for the archive database and press **Enter**.
- ◆ When you are prompted to enter the database host port, type the port to use for the archive database and press **Enter**.
- ◆ When you are prompted to enter the full path of the JDBC drivers, type the path for the JDBC driver to use and press **Enter**.

Note: See the application installation requirements documentation for the list of supported driver versions.

- ◆ When you are prompted to enter the version of the JDBC drivers, type the version of the driver being used and press **Enter**.

9. If you are not installing in a clustered environment, you have finished the install procedure. If you are installing in a clustered environment, use the following commands:

Note: The startCluster command must be executed on each node of the cluster.

- ◆ If you are installing in a clustered environment on a UNIX operating system, type
`./startCluster.sh <node_number>`
- ◆ If you are installing in a clustered environment on a Windows operating system, type
`startCluster.cmd <node_number>`

For example, if you are installing on Node 1 on a UNIX operating system, you would type
`./startCluster.sh 1`

10. If you are running the script in a clustered environment, the script asks you if this instance is your primary node. If the instance is not your primary instance, the script will not create new tables in the primary node archive database.

Caution: Once your archive database is installed, under no circumstances should you ever directly delete or update rows in your production integrated archive database.

Executing the Archive Install Script on an iSeries Operating System

Complete the following instructions to install the e-Invoice Archive Install Script on an iSeries operating system:

Note: When you execute the archive install script on an iSeries, the installation log is located at
<Application Installation Directory>/installeinv.log

1. Install or upgrade the application by following the application *Installation* documentation.
2. From the **Administration** menu, select **Operations > System > Troubleshooter**.

3. Click **Stop the System**.

The application displays the warning, This will shut down the whole environment and end your session. Do you want to continue?

4. To shut down the application, click **OK**. The application must be shut down because the Archive Install Script will be making modifications to properties files.
5. Log on to your iSeries using your application user profile.
6. Is there a save file named **EINV** in QGPL on your iSeries?
 - ◆ If yes, clear the save file by typing `CLRSAVF FILE(QGPL/EINV)`.
 - ◆ If no, type `CRTSAVF FILE(QGPL/EINV)` to create a save file on your iSeries.
7. Copy the `einvsavf` file from **<Application Installation Directory>/bin/einvsavf** to the save file created in QGPL by typing: `CPYFRMSTMF FROMSTMF(`<Application Installation Directory>/bin/einvsavf') TOMBR(`/QSYS.LIB/QGPL.LIB/EINV.FILE') MBROPT(*REPLACE) CVTDTA(*NONE)`
8. Type `RSTLIB SAVLIB(EINV) DEV(*SAVF) SAVF(QGPL/EINV)` to restore the installation objects.
9. Type `ADDLIBLE LIB(EINV)` from an iSeries command line to add the installation programs to your library list.
10. Create a collection (library) to hold the e-Invoice archive database. You can use an existing non-application library, provided that it has a system-created journal and journal receiver, or you can create a new collection. To create a new collection, type `STRSQL` from an iSeries command line to bring up an interactive SQL session.
11. Type `create collection libname` and press Enter (where **libname** is the new library that you want to create). This creates the library and system journal and journal receiver.
12. Once created, press **F3** to exit and press **Enter** to exit the session.
13. To run the installation script, type `EINV` and press **Enter** from an iSeries command line.
14. Type the installation directory of your application instance and press **Enter**.
15. You are prompted to enter the connection information for the database you want to use for the e-Invoice archive.

Note: The e-Invoice archive database must be different from your application database. The only supported database for an iSeries installation is iSeries DB2, on the same machine where you are running the application.

- ◆ When you are prompted to enter the database username, type the username for the archive database user and press **Enter**.

Note: This should be the same user that created the collection in step 8, or should be the owner of the library if an existing collection is being used.

- ◆ When you are prompted to enter the database password, type the password for the archive database and press **Enter**.
- ◆ When you are prompted to enter the database name, type the database name for the archive database and press **Enter**.

Note: The archive database must be different than the application database or any other archive database. If the application is installed on the iSeries operating system, then only the native iSeries DB2 database can be used for the integrated archive.

- ◆ When you are prompted to enter the database host name, type the host name or IP for the archive database and press **Enter**.

Caution: Once your archive database is installed, under no circumstances should you ever directly delete or update rows in your production integrated archive database.

Configuring the eInvoice Archive Service

Now you can configure and implement the eInvoice Archive service. The eInvoice Archive service is used to archive e-Invoices. Depending on the type of archive you select, this service either archives the e-Invoices in a canonical format to a database or provides the archive information to an external system through a business process. This service enables you to update the status of an invoice stored in the e-Invoicing archive, during normal processing, after it has already been signed or verified by TrustWeaver. This service also updates the status of an e-Invoice when errors occur during normal processing. See *eInvoice Archive Service* for more details.

Setting Global Configuration Parameters for e-Invoicing

Overview

The Sterling e-Invoice Gateway enables you to set global parameters to limit the maximum number of connections that can be established by the Sterling e-Invoice Gateway with TrustWeaver and the maximum size of invoices that can be sent to the TrustWeaver Server for processing. You need to set these parameters or accept the defaults to ensure that the TrustWeaver Server is not overloaded when you send data for signing or verification.

Setting Global Parameters

To set the global parameters:

1. From the **Administration** menu, select **eInvoicing > Configuration**.
2. Next to **Edit Configuration Parameters**, click **Go!**.
3. Complete the following TrustWeaver Configuration parameters:

Parameter	Definition
TrustWeaver Host	The name of the TrustWeaver Server. Required.
TrustWeaver URI	The name of the TrustWeaver Universal Resource Indicator representing incoming requests. Required.
CA Certificate	The digital security certificate used to provide authentication to TrustWeaver. Required. Note: The client certificate must be valid. A client certificate is only required by the Sign method.
System Certificate	The system certificate contains the private key the SSL server will use to communicate with TrustWeaver. Required. Note: To access information from TrustWeaver Server, you must establish an encrypted channel (SSL) to the server to ensure that only the intended client can read the information sent to and from the server. SSL is also used to authenticate the server, and a client authenticates the server through the SSL server certificate.

4. Click **Next**.

5. Complete the following EInvoice Configuration Parameters or accept the defaults:

Parameter	Definition	Default Value
Maximum Invoice Size (MB)	The Maximum size of the invoice message that can be sent to the TrustWeaver Server. Required. Note: If the size of the SOAP request created by the TrustWeaver Request service (when it retrieves the primary document from process data) is greater than the value specified here, the process is stopped and an error is generated.	4
Maximum Open Connections	The maximum number of open connections that can be made with TrustWeaver Server. This parameter is used to ensure that the TrustWeaver Server is not overloaded with invoice messages. Required. Note: The number of open connections is limited by the Semaphore service.	5
Immediate Retry	Number of retries allowed when a self-correcting, transient error (essentially a hiccup in the processing, which is not expected to be repeated, or not expected to last for long) is returned by the TrustWeaver Server. This parameter specifies the number of times to loop with a small pause between each loop. Required.	3
Delayed Retry	Number of retries allowed when a delaying error (a self-correcting, transient error, but an error that is expected to take some time to resolve) is returned by the TrustWeaver Server. This parameter specifies the number of times to loop with a pause between each loop. Required.	24
Immediate Retry Wait (sec)	Number of seconds to pause before retrying when a self-correcting, transient error occurs. Required.	200
Delayed Retry Wait (min)	Number of minutes to pause before retrying when an error occurs when a handling error occurs (and the error is transient and self-correcting but not immediately fixable). Required. Note: If a TrustWeaver error occurs while processing an invoice, the all the processes involving the buyer and supplier countries for the time period specified in this parameter. For example, if an error occurs while processing an invoice from UK to PL, all processing of invoices to and from UK from and to any other country, and to and from PL and from and to any other country will be paused for this interval.	60
Time to wait for an available connection (sec)	The maximum number of seconds to wait to get a connection with the TrustWeaver Server. Note: This allows for a controllable amount of access as required by the application or resource. This may be useful for performance implications, because of limited resources or any other reason.	300

6. Click **Next**.

7. Click **Finish** to set the global parameters.

Implementing e-Invoice Partner Relationships

Overview

To effectively set up trading partners that implement e-Invoicing, you must configure the Sterling e-Invoice Gateway with specific message data settings for the standard you are using. Additionally, you need to set up an agreement to administer e-Invoice data sent to and received from your partners. This section provides an overview of the steps to set up trading partner information, along with the specific configuration settings that enable you to meet your e-Invoicing data exchange requirements.

Before You Begin

Before you configure an e-Invoicing identity, agreement, and envelopes, and to simplify the tasks you must perform, collect and prepare the following information about your organization and trading partners, which includes:

- ◆ The standard you are using to exchange messages with your trading partners.
- ◆ Trading partner name and address information, including:
 - ◆ DUNS numbers
 - ◆ Contact information, such as addresses, telephone numbers, e-mail addresses
- ◆ Transport information, including:
 - ◆ HTTP URLs
 - ◆ CA certificates for trading partner if using SSL
- ◆ Security information, digital signatures, and encryption and certificates (for example, certificates used to encrypt and decrypt).
- ◆ If you are using digital certificates, check in the appropriate certificate.
- ◆ Your VAT ID or lookup identifier.
- ◆ E-mail address to which error notifications can be sent.
- ◆ Your lookup identifier.

Setting Up e-Invoicing Trading Profiles

When setting up trading profiles for e-Invoicing, you must perform the following tasks:

1. Create an identity record for your organization, indicating your organization as the base identity. Alternatively, you can reuse an existing identity and just edit it to add the necessary VAT IDs.
2. Create an identity record for each of your trading partners. Alternatively, you can reuse an existing identity and just edit it to add the necessary VAT IDs.
3. Create an agreement for each trading partner.
4. Update your existing envelopes or create new envelopes for use with e-Invoices.

Implementing e-Invoice Identity Records

Overview

Every trading partner is represented by at least one record, referred to as an *identity*. An identity record describes the trading partner and contains information referenced when a business process involving the trading partner is executed. A trading partner can have more than one identity to represent the different ways it does business. For example, a company's central office procurement organization might be very different from its manufacturing supplies procurement organization, and in this case you need a separate identity record for each organization within the company.

A base identity is a regular identity that you can use as a starting point to create a new identity. The base identity maintains a link to the identity that inherited its properties. If you modify the base identity, all related identities (that is, ones that inherited the base identity properties) change, as well. When you create an identity record using a base identity, everything in the new identity is the same as in the base identity, except the identity name, description, and other unique parameters, such as unique identification numbers.

Note: If you plan to create many identities using the base identity, do not use the base identity in production. You should record the identities that are related to the base identity.

You must create an identity before you can create a transport, document exchange, delivery channel, packaging, profile, and (when required) a contract. Each of these components references an identity. For the Sterling e-Invoice Gateway, only an identity record is mandatory; the transport, document exchange, delivery channel, packaging, profile, and contract are only necessary if the standard you are using requires them.

Creating an Identity Record for Your Organization

When setting up your trading profile, consider that your organization is the base identity.

To create an identity record:

1. From the **Administration** menu, select **Trading Partners > Advanced > Identities**.
2. Next to Create New Identity, click **Go!** or type an existing identity name into Search by Identity Name and click **Go!**.
3. In the Base Identity page, for Select Base Identity, verify that **No Base Identities Available** is selected, and click **Next**.
4. In the Information page, complete the following fields and click **Next**:

Field	Description
Name	Name of your organization. Required.
Reference URL	Internet address of your organization. Optional.
DUNS	Unique 9-13 character identification number of your organization, as issued by Dun & Bradstreet Corporation. Optional.

Field	Description
Identifier	Primary ID of your organization. Use DUNS number. Required.
Address Line 1	Conventional mailing address of your organization. Required.
Address Line 2	Additional mailing address information of your organization. Optional.
City	City where your organization is located. Required.
State or Province	State or province where your organization is located. Optional.
Zip or Postal Code	ZIP Code or postal code where your organization is located. Optional.
E-mail Address	E-mail address of your organization. Optional.
Telephone Number	Telephone number of your organization. Optional.
Time Zone	Time zone where your organization is located. Optional.
Country	Country where your organization is located. Optional.
Federation Peers	Discovery point URL for the trading partner you want to associate this identity with. Optional.
VAT ID	The VAT transaction tax identifier. Optional. Note: When you add VAT IDs to an identity, an associated permission ID is created, and the user is assigned that permission ID.
Internal Notification E-Mail	The internal e-mail address to which you want error notifications to be sent. Optional.
Lookup ID	The identifier used to look up the e-Invoice agreement. Optional.
Lookup ID Comments	Any comments regarding the identifier used to look up the e-Invoice agreement. Optional.

5. Click **Next** to access the Confirm page.
6. Click **Finish** to add the identity.

Creating an Identity Record for Your Trading Partner

For each trading partner with which you are exchanging e-Invoices, you must create an identity record.

To set up an identity record for your trading partner:

1. From the **Administration** menu, select **Trading Partners > Advanced > Identities**.
2. Next to Create New Identity, click **Go!** or type an existing identity name into Search by Identity Name and click **Go!**.
3. In the Base Identity page, for Select Base Identity, select the name of the identity record that you created for your organization, and click **Next**.

4. In the Information page, complete the following fields and click **Next**:

Field	Description
Name	Name of your trading partner. Required.
Reference URL	Internet address of your trading partner. Optional.
DUNS	Unique 9-13 character identification your trading partner number, as issued by Dun & Bradstreet Corporation. Optional.
Identifier	Primary ID of your trading partner. Use DUNS number. Required.
Address Line 1	Conventional mailing address of your trading partner. Required.
Address Line 2	Additional mailing address information of your trading partner. Optional.
City	City where your trading partner is located. Required.
State or Province	State or province where your trading partner is located. Optional.
Zip or Postal Code	ZIP Code or postal code where your trading partner is located. Optional.
E-mail Address	E-mail address of your trading partner. Optional.
Telephone Number	Telephone number of your trading partner. Optional.
Time Zone	Time zone where your trading partner is located. Optional.
Country	Country where your trading partner is located. Optional.
Federation Peers	Discovery point URL for the trading partner you want to associate this identity with. Optional.
VAT ID	The VAT transaction tax code. Optional. Note: When you add VAT IDs to an identity, an associated permission ID is created, and the user is assigned that permission ID.
Error Notification E-Mail	The e-mail address to which you want error notifications to be sent. Optional.
Lookup ID	The identifier used to look up the e-Invoice agreement. Optional.
Lookup ID Comments	Any comments regarding the identifier used to look up the e-Invoice agreement. Optional.

5. Click **Next** to access the Confirm page.

6. Click **Finish** to add the identity of this trading partner.

You are now ready to create an agreement for this trading partner.

Implementing e-Invoice Agreements

Overview

An agreement is a configurable object that relates two e-Invoice parties (the “supplier” and the “buyer,” and stores their e-Invoice processing options (including any “on behalf” options). It is linked to an Sterling e-Invoice Gateway identity.

Note: The agreement is a relationship object that enables the necessary legal separation of supplier and buyer e-Invoicing steps.

You must create an e-Invoice agreement for each trading partner with whom you will be exchanging e-Invoices.

Creating an e-Invoice Agreement

To create an e-Invoice agreement:

1. From the Administration menu, select **eInvoicing > Agreements**.
2. In the Agreements page, in the **Create** section next to **New Agreement**, click **Go!**.
3. In the New Agreement page, complete the following parameters, as appropriate, and click **Next**.

Field	Description
Name	Unique name of the agreement. Required.
Comments	A brief description of the agreement being created. Required.
Supplier Identity	Identity of the Supplier. Optional. Note: You must have already created this identity in the Sterling e-Invoice Gateway.
Buyer Identity	Identity of the Buyer. Optional. Note: You must have already created this identity in the Sterling e-Invoice Gateway.
Message Type	Type of message. This parameter enables you to specify the type of message exchanged if you have multiple agreements with the same supplier/buyer information but use different message types. Optional.
Supplier Processing Option	Indicates which process option is used by the supplier. Optional. The valid values are: <ul style="list-style-type: none"> ◆ No Processing Note: If you select No Processing for the supplier, this processing option will not be available for the buyer. <ul style="list-style-type: none"> ◆ Sign and Archive (integrated) ◆ Sign and Archive (external) ◆ Sign and Archive (custom)

Field	Description
Business Process for Supplier Custom Archive (if applicable)	Business process to be executed. Optional. Note: This parameter is only valid if you selected Sign and Archive (custom) for Supplier Processing Option .
Buyer Processing Option	Indicates which process option is used by the buyer. Optional. The valid values are: <ul style="list-style-type: none"> ◆ No Processing Note: If you select No Processing for the buyer, this processing option will not be available for the supplier. <ul style="list-style-type: none"> ◆ Verify Signature and Archive (integrated) ◆ Verify Signature and Archive (external) ◆ Verify Signature and Archive (custom)
Business Process for Buyer Custom Archive (if applicable)	Business process to be executed. Optional. Note: This parameter is only valid if you selected Sign and Archive (custom) for Buyer Processing Option .
Business Process for Post-Processing	This is the business process to run after the e-Invoicing business process is executed. Note: For example, if prior to implementing the Sterling e-Invoice Gateway, you would create invoices using one of the enveloping services (X12 Enveloping service, EDIFACT Enveloping service, Generic Envelope service, and so forth) and the invoice envelope definition would contain a business process that would run after the enveloping was finished (to send the invoices to your trading partner). That business process is considered to be your “post-process.” For e-Invoicing, the “post-process” is replaced by the e-Invoicing process. This parameter allows you to specify that the regular post process will be automatically run after the e-Invoicing process.
Document Format	Document format for this agreement. Optional. The valid values are: <ul style="list-style-type: none"> ◆ GENERIC (default) ◆ PDF ◆ XML
Digital Signature Format	The format of the digital signature used. Optional. The valid values are: <ul style="list-style-type: none"> ◆ PKCS7 (default) ◆ SMIME ◆ XMLSIG ◆ XMLCON Note: Use the XMLCON format if you need to produce XML signatures that support a double-signature (for example, signatures for two countries). We recommend you use XMLCON format instead of XMLSIG. The XMLCON signature format is not valid with PDF or GENERIC document formats; it is only valid with XML-formatted documents. <ul style="list-style-type: none"> ◆ PDF

Field	Description
Test / Production Indicator	Whether the e-Invoice process is in test or production mode. Optional. The valid values are: <ul style="list-style-type: none">◆ Test◆ Production (default)
Map for Translation to Canonical Format	The map used to translate the invoice to the canonical format. Optional.
Notify Internal Contact on Supplier-side Error	Whether to notify the internal contact when supplier-side errors occur. Valid values are: Yes (notify - this is the default) and No (do not notify).
Notify Internal Contact on Buyer-side Error	Whether to notify the internal contact when buyer-side errors occur. Valid values are: Yes (notify - this is the default) and No (do not notify).

Implementing Envelopes for the Sterling e-Invoice Gateway

Overview

The documents that you are sending to be signed can be in the format of any of the standards supported in the application (for example, ASC X12, EDIFACT, TRADACOMS, and VDA). You may be sending documents that already exist but will now have the additional step of being signed by TrustWeaver, before sending them on to be processed normally in the application. Or, you may be creating documents to be signed by TrustWeaver. In either case, you will use the same application envelopes as you would if you were not sending documents to TrustWeaver, and you will either update existing envelopes with new e-Invoicing-specific parameters or create envelopes like they normally would for the standard(s) you currently use (with the additional step of setting the size limit required by TrustWeaver).

Note: The only envelopes to which you can add the size limit are outbound envelopes for standards that use interchanges.

Alternatively, you can set the size limit directly by setting properties using the **customer_overrides.properties** file. In the **enveloping.properties** file there is a property for each supported standard, as well as specific properties for each message type (for example, 810 for an ASC X12 invoice) that can override the standard property. If you add properties to the **customer_overrides.properties** file, you are specifying global properties, and then you are able to specify in each envelope whether to use the global properties or to override specific properties.

Setting Global e-Invoicing Envelope Properties

To set global e-Invoicing envelope properties:

1. In the **install_dir/properties** directory, locate (or create, if necessary) the **customer_overrides.properties** file.
2. Open the **customer_overrides.properties** file in a text editor.
3. If desired, add interchange size limit properties, using the following format:

```
enveloping.enveloping.<standard>.MaxInterchangeSize=[size_in_bytes]
```

For example:

```
enveloping.enveloping.X12.MaxInterchangeSize=30
```

4. If desired, add interchange size limit properties for specific message types, using the following format:

```
enveloping.enveloping.<standard>.<transaction set>.MaxInterchangeSize=[size_in_bytes]
```

For example:

```
enveloping.enveloping.X12.810.MaxInterchangeSize=30
```

Note: When you choose to specify a maximum value, the value entered is checked to make sure it is at least a specific number of bytes based on the standard:

EDIFACT: 173

TRADACOMS: 354
 VDA: 456
 X12: 249

These values are based on the header and trailer size (in bytes) for the given standard.

5. Save and close the **customer_overrides.properties** file.
6. Stop and restart the application to use the new values.
7. Test your changes to ensure that the overrides give the desired results. If you have problems, contact Sterling Commerce Customer Support for assistance.

Creating a New Envelope

To create a new envelope:

1. From the **Administration** menu, select **Trading Partner > Document Envelopes > Envelopes**.
2. Under Create, next to New Envelope, click **Go!**
3. On the Envelope Standards page, select one of the following and click **Next**:
 - ◆ ACH
 - ◆ CHIPS
 - ◆ CII
 - ◆ EDIFACT
 - ◆ FEDWIRE
 - ◆ RND
 - ◆ SWIFT
 - ◆ TRADACOMS
 - ◆ VDA
 - ◆ ASC X12

Note: To create an envelope using the ODETTE or AUTACK standard, select EDIFACT.
4. Select the level of envelope you want to create, including whether it is inbound or outbound, and click **Next**.
5. Do one of the following:
 - ◆ To create this envelope from a base envelope, select the Base envelope from the Select Envelope list, and click **Next**.
Note: All the properties are pre-filled but you can update them as needed.
 - ◆ To create a new envelope, select the Not Applicable from the Select Envelope list, and click **Next**.
6. On the Name page, type a unique name for the envelope, and a description or comments, then click **Next**.

7. Complete the properties for the envelope as necessary and click **Next** after each page until you reach the confirm page. Required fields are highlighted in blue.

Note: For standards that use interchanges, you will be able to specify limits for interchange size on the outbound interchange and transaction envelopes. For performance reasons, the size is estimated for some components of the interchange (for example, control numbers) when determining the size. For this reason, the actual enforced size limit is slightly smaller than the value you specify.

If you choose to specify a maximum value, the value you specify is checked to make sure it is a specific number of bytes (based on the header and trailer size for that standard).

8. Click **Finish** to add the envelope.
9. Click **Return** to continue.

Updating Envelope Properties

To update envelope properties if you already created envelopes and just need to specify e-Invoicing information:

1. From the **Administration** menu, select **Trading Partner > Document Envelopes > Envelopes**.
2. Find the envelope using the Search or List function.
3. From the list of envelopes, click **source manager** next to the envelope you want to update.
4. Click **edit** next to the envelope you want to update.
5. Update envelope properties and settings as necessary, clicking **Next** to continue.

Note: For standards that use interchanges, you will be able to specify limits for interchange size on the outbound interchange and transaction envelopes. For performance reasons, the size is estimated for some components of the interchange (for example, control numbers) when determining the size. For this reason, the actual enforced size limit is slightly smaller than the value you specify.

6. Click **Finish** to update the envelope.
7. Click **Return** to continue.

Setting e-Invoice Permissions

Overview

The application requires system passwords for administrative functions and uses role-based security to provide different levels of access to different users within the organization. This role-based security provides access to certain files, business processes, Web templates, services, and product features, according to the permissions associated with the user account.

A user account contains the groups the user belongs to, the permissions associated with each group or user, and the password policy applied to the user. Groups are collections of permissions and other groups that are required by a user for access to different modules. Permissions provide access to the different modules within the application and are the foundation of role-based security. Password policies are sets of security decisions that you make and apply to different user accounts according to security policies in your company.

Each user account is linked to an application user name and password. Each time you log in, the application verifies you as a valid user and grants access to only the areas you are allowed to use according to the permissions assigned to you by the system administrator.

For the Sterling e-Invoice Gateway, permissions ensure the security of your data and provide the legal separation of who can view e-Invoice data. Access to invoices in the archive will be restricted based on permissions. Permissions control which legal entities a user may access and what functions they can perform on the invoices.

Note: A Tax Auditor user is denied access to the non-e-Invoicing operational the application user interface unless you explicitly grant the Tax Auditor user the necessary permissions.

The user group **commandlineuser** is included with the Sterling e-Invoice Gateway. This user group has all the needed permissions to perform import and export operations from the command line. The permissions associated with this user group can also be changed to deny import and export operations from the command line.

The e-Invoicing-specific permissions enable users to:

- ◆ View invoices
- ◆ Revalidate invoices
- ◆ Download invoices
- ◆ Create and edit agreements
- ◆ Perform operations on behalf of all legal entities.
- ◆ Perform operations on behalf of a specific legal entity (requires separate permission to be set up per entity, by the operator of all the entities).

Note: To perform an operation on behalf of a buyer or a supplier, the VAT ID of the buyer or the supplier must be used to create this permission.

The specific preloaded e-Invoice permissions in the Sterling e-Invoice Gateway are as follows:

Permission Name	Action(s) Permission Allows
elvoicing	Displays the elvoicing menu in the application user interface.
elvoicing Configuration	Displays the Configuration option in the elvoicing menu.
elvoicing Archive	Displays the Integrated Archive option in the elvoicing menu.
elvoicing ALL BUYERS	View/access buyer invoices only.
elvoicing ALL SUPPLIERS	View/access supplier invoices only.
elvoicing DELETE AGREEMENTI	Delete agreements. Note: This permission works in conjunction with the UI OPERATIONS permission to enable a user to delete agreements.
elvoicing DOWNLOAD INVOICE	Download raw invoices and evidence.
elvoicing CREATE/EDIT AGREEMENT	Create and edit agreements.
elvoicing REVALIDATE INVOICE	Revalidate invoices.
elvoicing VIEW AGREEMENT	View the Agreements menu link and user interface, and view agreements.
elvoicing VIEW INVOICE	View raw invoices, evidence, and audit entries.
elvoicing IDENTITY_[identity] VAT_[VAT_ID]	Access the VAT ID for the specified identity. Note: To create and edit identities, a user must also be assigned the permission UI Advanced Trading Profile Setup . Each agreement must reference a pair of identities with valid VAT IDs.
elvoicing ALL SUPPLIERS	View all supplier-side invoices in the search result page. Note: This permission works in conjunction with elvoicing ALL BUYERS to enable a user to view any VATs.
elvoicing ALL BUYERS	View all buyer-side invoices in the search result page. Note: This permission works in conjunction with elvoicing ALL SUPPLIERS to enable a user to view any VATs.

Managing role-based security for the Sterling e-Invoice Gateway includes the following sequential tasks to create user accounts and assign the appropriate permissions:

- ◆ Create permissions according to the modules the users require access to.
- ◆ Create groups according to the permissions you created.
- ◆ Create a password policy to assign to user.
- ◆ Create the user account using the permissions, groups, and password policy you created.

Creating Permissions for Sterling e-Invoice Gateway Users

When you create a permission, you set access to an application module that can be assigned to different users.

To create a permission:

1. From the **Administration** menu, select **Accounts > Permissions**.
2. In the Create section, next to Create a new Permission, click **Go!**
3. In the Permissions page, complete the following fields and click **Next**.

Parameter	Definition
Permission ID	Permission ID for the permission you are creating. Permission ID is the name of the business process, XSLT document, Web template, or resource for which you are setting the permission. Include the extension for the resource after the ID. Required.
Permission Name	Name of the permission you are creating. Required.
Permission Type	Select eInvoicing Entity as the permission type of the permission you are creating. Required.

4. Click **Finish** to create the permission.

Creating Groups for Sterling e-Invoice Gateway Users

Groups allow you to maintain access permissions for several users from a single place. Groups minimize the amount of work involved with maintaining accounts, especially when several users perform the same job function. You can associate many permissions to different users by creating groups for each job function instead of each user. At a minimum, you need to create the following groups:

- ◆ Group for buyers
- ◆ Group for suppliers

You must have already created an identity for the e-Invoice buyer and e-Invoice supplier.

To create the necessary groups:

1. From the **Administration** menu, select **Accounts > Groups**.
2. In the Create section, next to Create a new Group, click **Go!**
3. In the Permissions page, complete the following fields and click **Next**.

Parameter	Definition
Group ID	Unique identifier for the group you are creating. Required.
Group Name	Name of the group you are creating. Required. Note: You need to create one group for buyers and one group for suppliers.

Parameter	Definition
Owner	Name of the owner for the group. The group owner has two primary roles: <ul style="list-style-type: none"> ◆ Administrative contact for the group when changes to the group are needed. The owner contacts the system administrator to request changes. ◆ Routing device. For example, if a group is created for a development department and all development department employees send time sheets using the application, the Owner field can be used to route all of the time sheets to the departmental manager. Required.
Identity	Select the identity you created for buyers or for suppliers. Required.

4. In the Assign Subgroups page, if you want to filter groups by name, under Filter Data in the **By Name** field, type either a portion of the name or the entire name of the group you want to filter for and click the filter button to the right of the field. If you do not want to filter groups by name, select the group or groups you want to assign to this group.
5. Complete one of the following actions and click **Next**.
 - ◆ Click the right double-arrow to move all groups from the Available pane to the Assigned pane.
 - ◆ Click the right single-arrow to move selected groups to the Assigned pane.
 - ◆ Click the left double-arrow to move all groups from the Assigned pane to the Available pane.
 - ◆ Click the left single-arrow to move selected groups to the Available pane.
6. In the Assign Permissions page in the Available pane, select the permission or permissions you want to assign to this group.

Note: If you want to filter by e-Invoicing Entity type to include the permission you just created, select **eInvoicing Entity** and click the filter button to the right of the field.
7. Complete one of the following actions and click **Next**.
 - ◆ Click the right double-arrow to move all permissions from the Available pane to the Assigned pane.
 - ◆ Click the right single-arrow to move selected permissions to the Assigned pane.
 - ◆ Click the left double-arrow to move all permissions from the Assigned pane to the Available pane.
 - ◆ Click the left single-arrow to move selected permissions to the Available pane.

Note: By default, the permissions associated with the subgroups assigned to this group are already selected. The associated permissions do not display in the available column; the associated permissions display in the confirm page.
8. In the Confirm page, review the permission settings, and click **Finish** to save the new group.
9. Complete steps 2 through 8 for each group you need to create.

Creating a Password Policy

You create a password policy to assign the policy to user accounts to simplify your security operations when adding new users. You do not need to associate a password policy with a user account, but it helps you to manage your security. A user account cannot have more than one password policy associated with it.

To create a password policy:

1. From the **Accounts** menu, select **Password Policy**.
2. In the Password Policy page, next to **Create a new Password Policy**, click **Go!**
3. In the Password Policy page, complete the following fields and click **Next**.

Field	Description
Policy ID	Identifier that identifies the password policy in the database.
Policy Name	User-friendly name that displays in the user interface when any reference is made to the password policy.
Number of days valid	Number of days that a user password is valid. The user is prompted to change the password when this time period expires. The default is 0, which means the password never expires. You can change this number to any number you want; there is no maximum. The expiration countdown starts the first time a user logs in to the application after a password is assigned to the user account.
Minimum Length	Minimum length that the password must be. Required. Valid values are any numerals. This number must be set to at least the number 6. The default value is 6. If no policy is applied, the application enforces a minimum length of 6.
Maximum Length	Maximum length that the password can be. Required. Valid values are any numerals. This number must be set to at least the same number as the minimum length. The default value is 28
Number of passwords kept in history	Number of passwords to keep in the PWD_HISTORY table in the database for a user. After this number of passwords is exceeded, the oldest password is removed from the table and can be re-used by the user. The default value is 5.
Password required to contain special characters	Specifies that the password must contain at least one special character, such as numeral, capital letter, !, @, #, \$, %, ^, &, or *.
Required password change on first login attempt	Specifies that the user must change the default password after the initial login. This prompts the user to change the password after logging in for the first time.

4. In the Confirm page, review the password policy settings and click **Finish**.

Creating User Accounts with e-Invoicing Permissions

User accounts work with permissions to provide security for the Sterling e-Invoice Gateway and your organization. These features make it possible to regulate which users have access to each feature in the Sterling e-Invoice Gateway and what functions each user can perform.

When you create a user account, you specify a login ID and password, permissions, and contact information for a specific user.

The way in which User Permissions are configured consists of certain dependencies. For example if a user was assigned permissions to only view invoices, the set of permissions to be assigned to that user account is as follows:

- ◆ eInvoicing
- ◆ eInvoicing Archive
- ◆ eInvoicing View Invoice

In addition, this user must also be given permissions for entity level permissions, which are permissions that are automatically created when a user entity (supplier or buyer) is created. These permissions are in the format **eInvoicing IDENTITY_[identity] VAT_[VAT_ID]**.

To create a user account and assign it the proper Sterling e-Invoice Gateway permissions:

1. From the Accounts menu, select **User Accounts**.
2. In the Create section, next to **Create a new Account**, click **Go!**
3. In the New Account page, select the type of authentication for the user:
 - ◆ Local - Authentication is completed against the application database and the Sterling e-Invoice Gateway archive database.
 - ◆ External - Authentication is completed against an LDAP server. External authentication does not require the application LDAP adapter, which is used with business processes and enables the application to communicate with local or remote LDAP servers using a Java Naming Directory Interface (JNDI).
4. Complete the following fields and click **Next**.

Field	Description
User ID	User ID for the user account you are creating. The user ID must be at least five characters long. Required
Password (Local only)	Password for the user account you are creating. The password must be at least six characters long. Required for local users. This field does not display for external users.
Confirm Password (Local only)	Type the password a second time. Required for local users. This field does not display for external users.
Policy (Local only)	Password policy to associate with this user account. From the list, select from the policy you want to associate. Optional. This field does not display for external users. The application calculates the expiration date from the first date that the user logs on with this password.
Authentication Host (External only)	The Lightweight Directory Access Protocol (LDAP) server on which the user is being authenticated. The server(s) listed in this field are specified in the authentication_policy.properties.in file.
SSH Authorized User Key	Public key used to authenticate remote users. Obtain this key from your trading partner. Key must be checked in prior to creating the user account, then select the correct one from the list.

Field	Description
Session Timeout	Amount of time that you cannot interact with the application before you have to log in again. Time is in minutes. Required.
Accessibility	<p>Portion of the dashboard user interface that the user account has access to. Optional. The following are accessibility options:</p> <ul style="list-style-type: none"> ◆ Admin UI - Access to only the Admin Console pane in the application dashboard. ◆ AS2 UI - Access to only the AS2 Edition interface. ◆ Dashboard UI - Access to dashboard interface. You refine this choice by choosing a dashboard theme below.
Dashboard Theme	<p>Predefined dashboard that the user account has access to. Required if accessibility is set as Dashboard UI. The following are dashboard theme options:</p> <ul style="list-style-type: none"> ◆ Operator ◆ Participant ◆ Participant Sponsor ◆ Sponsor

5. In the Groups page, complete one of the following actions and click **Next**.
 - ◆ Click the right double-arrow to move all groups from the Available pane to the Assigned pane.
 - ◆ Click the right single-arrow to move selected groups from the Available pane to the Assigned pane.
 - ◆ Click the left double-arrow to move all groups from the Assigned pane to the Available pane.
 - ◆ Click the left single-arrow to move selected groups from the Assigned pane to the Available pane.
 6. In the Permissions page, complete one of the following actions and click **Next**.
 - ◆ Click the right double-arrow to move all permissions from the Available pane to the Assigned pane.
 - ◆ Click the right single-arrow to move selected permissions from the Available pane to the Assigned pane.
 - ◆ Click the left double-arrow to move all permissions from the Assigned pane to the Available pane.
 - ◆ Click the left single-arrow to move selected permissions from the Assigned pane to the Available pane.
- Note:** By default, the permissions associated with the groups this user is assigned to are already selected. You can assign to the user permissions not associated with a group.
7. In the User Information page, complete the following fields and click **Next**.

Field	Description
First Name	User's first name. Required.

Field	Description
Last Name	User's last name. Required.
E-mail	User's e-mail address.
Pager	User's pager number.
Preferred Language	User's preferred language. English or Japanese.
Manager ID	Identifier of the user's manager.
Identity	<p>Identity of the trading partner to associate with the user account. This is an identity you have already created.</p> <p>Note: Only one trading partner can be associated with a user account. A user account can be associated with many groups, each with its own trading partner identity association. This enables a user account to be associated with more than one trading partner. The Identity field is used for routing messages in Mailbox.</p>

8. In the Confirm page, review the user account settings, and click **Finish** to create the user account. The application creates the user account and displays the message: *The system update completed successfully.*

Creating Maps for Use with the Sterling e-Invoice Gateway

Overview

Some tax laws require that you must be able to present an e-Invoice in a human-readable format. Other laws or tax authority practices may require that the invoice be machine-readable. In addition, Buyer invoice processing applications may require a machine readable format. The Sterling e-Invoice Gateway provides a signed invoice that can be processed by tax authorities and applications by using XML and style sheets.

Note: You may need to keep the canonical maps you create for archival purposes so that they can be inspected by an auditor.

The Map Editor enables you to create a map to translate documents from your format to the canonical invoice format required by TrustWeaver. The Map Editor generates a Canonical Invoice Format file layout from the information that is preloaded when you install Map Editor.

Note: You need to download the Map Editor component to use it.

Our Canonical Invoice Format implementation conforms to the rules of the XML language 1.0 specification, as published by the World Wide Web Consortium (W3C). However, to be more flexible, the application diverges slightly from the W3C base 1.0 XML specification. Our implementation enables you to do the following with XML:

- ◆ Specify the number of times that a group can repeat.
- ◆ Specify the number of times an element in a mixed group can repeat.
- ◆ Repeat an element (with a structure different from the structure of the original element) in a different part of the document.

Map Editor allows you to modify the map components by using the Deactivate, Promote, Split, Copy, Cut, and Paste functions.

Note: We provide you with a sample map (X12_810_To_Canonical.xml). This map is located in the <Map Editor Install Dir>/Samples/maps directory. You can use this map as an example to create your map for converting your invoice format to the canonical format.

If the translation produces no output, the business process is halted to give you the opportunity to either modify your map or provide a different map, and then resume the business process, if desired.

Canonical Invoice Format Components in the Map Editor

The following table lists the components that make up the Canonical Invoice Format layout in the Map Editor, the icons that represent the components, and descriptions of the components.

Component	Description
Canonical Invoice Format root element	The <i>Canonical Invoice Format root element</i> represents the Canonical Invoice Format document that the application is mapping. The Canonical Invoice Format root element is a looping structure that contains elements and content particles that repeat in sequence until either the group data ends or the maximum number of times that the loop is permitted to repeat is exhausted. The root element cannot be referenced by standard rules or links.
Element	An <i>element</i> contains related elements and content particles. In addition, an element can contain one pcd data and one attribute container. These objects repeat in sequence until either the element data ends or the maximum number of times that the loop is permitted to repeat is exhausted. A repeating element that contains another repeating element corresponds to a nested looping structure. The Canonical Invoice Format Element object cannot be referenced by standard rules or links.
Abstract element	An <i>abstract element</i> is an inconcrete element from an XML schema (for example, the term “appliance” may be considered an abstract element while “dishwasher” is a concrete one). An abstract element must be substituted with a non-abstract element for a map to be successfully compiled.
Content particle	A <i>content particle</i> contains related subordinate objects that define either a choice, a sequence, or an all. A content particle can contain only one pcd data. If specified, these objects can repeat in sequence until either the content particle data ends or the maximum number of times that the loop is permitted to repeat is exhausted. If you create a content particle that is subordinate to another content particle, the content particle corresponds to a nested looping structure (a loop within a loop). A content particle cannot be referenced by standard rules or links.
Pcd data	A <i>pcdata</i> contains character data in a Canonical Invoice Format document. Only one pcd data can be defined per element or content particle. The application automatically names the pcd data with the name of the parent element or content particle. When a pcd data has a link performed against it, a red check mark appears over the pcd data icon. When a pcd data contains an extended rule or a standard rule, an asterisk appears to the right of the pcd data icon.
Attribute container	An <i>attribute container</i> does not correspond to an XML function. The application uses attribute containers to contain the attributes of an element. The attribute container has no properties. When you create the first attribute of an element, the Map Editor automatically creates an attribute container object. An element can have only one attribute container, but the attribute container object can enclose many attribute objects.

Component	Description
Attribute	<p>An <i>attribute</i> specifies information associated with an element that further defines the element. The attribute is located within an attribute container. Attributes do not have to occur in sequence in the input data.</p> <p>When an attribute has a link performed against it, a red check mark appears over the attribute icon.</p> <p>When an attribute contains an extended rule or a standard rule, an asterisk appears to the right of the attribute icon.</p>

Creating a Canonical Invoice Format Map

When you create a new map, you can either manually create a Canonical Invoice Format layout or you can use a wizard that creates a layout for you based on the Canonical Invoice Format standard. The wizard saves you time and effort and minimizes the risk of having an invalid standard format.

To create a Canonical Invoice Format map:

1. From the Map Editor **File** menu, select **New**.
2. In the **New Map Wizard**, complete the questions in the first window and click **Next**.

Note: Be sure that **Sterling Integrator** is selected in the **What kind of map are you creating** list.

3. In the Input Format window (**Create a New Data Format Using this Standard** option) select your format using one of the following:
 - ◆ Create a new data format using this standard

Note: This selection allows you to use a preloaded standard (that is, you do not have to load the data format for the standard to the Map Editor).

- a. Select the standard and click **Messages**
- b. Complete the Map Wizard
 - ◆ Load the data format from a saved definition

Note: This selection allows you to use an existing file format.

- a. Type the path and file name of the saved definition (.ddf or .ifd extension).
- b. Click **Browse** to display the **Open File Definition** dialog box.
 - ◆ Create a new data format using this syntax

Note: For your format on the input side of the map, you need to choose whether you want to use a preloaded standard, an existing file format, or want to create a new file format for that side of the map (including selecting from standards that you have previously downloaded to the standards database). The preloaded standards are downloaded when you download the Map Editor to your machine or any optional standards.

4. Click **Finish** to load the message.
5. Click **Next** to select the Output Format.

6. In the Output Format window (**Create a New Data Format Using this Standard** option) select **Sterling Message Format** and click **Messages**.
7. Select the version of the standard (Version 1.0) and the message (Canonical Invoice) you want to use and click **Next**.
8. For the **Choose sub-elements to be included in the map** list, click **Next**.

Note: Do not clear any of the checkboxes. De-selecting critical elements such as Invoice Number or VAT ID may cause the application to not function correctly.

9. Click **Finish** to load the message.

10. Click **Next**.

11. Click **Finish**. The Map Editor displays the new map in the Map Editor window.

Note: Prior to opening an .xml (XML-formatted) file, the Map Editor verifies that you have the Microsoft XML Core Services (MSXML) 4.0 installed on the same computer as Map Editor. If you do not have the Microsoft XML Core Services (MSXML) 4.0 installed, the Map Editor cannot save or load .xml source files.

12. Map the appropriate components from the input side of the map (your format) to the canonical invoice format. See *Map Editor Guide* for more information.