VeriSign®
The Value of Trust℠

# Trust Gateway

## User's Guide

CUSTOMER MANUAL

Beta Release

**Customer Support: +1-650-426-3535 or 1-800-579-2848**

**enterprise-services@verisign.com**

**VeriSign, Inc. 00008744**

## Trust Gateway User's Guide

VeriSign, Inc. 00008744



This document supports **Trust Gateway 1.0** and all subsequent releases unless otherwise indicated in a new edition or release notes.

U.S. patent 6,324,645

### Trademark Notices



**Note** This document may describe features and/or functionality that are not present in your software or your service agreement. Contact your account representative to learn more about what is available with this VeriSign product.

# Contents

CHAPTER 1

# Introduction

Providing information and resources to your business partners, suppliers, and internal customers increasingly require that you provide access to your high-value applications and data across the Internet. For example, you may want to securely integrate your business partners' ERP systems with yours to automate procurement. In response, enterprises are increasingly turning to the emerging Web services technology to implement an XML-based framework for exchanging data between applications.

However, enterprises must also secure these applications, and their customer's communications with these applications, from unauthorized access and malicious hacking. That means authenticating the machine that is accessing the service, encrypting all communication between the services, validating the digital signature on the request, routing the incoming requests based on the service that is being accessed, and tracking the requests for subsequent audit trails and logging needs. Beyond implementing these security specifications, enterprises also require tools to simplify the management and configuration of many diverse applications over time. The cost associated with implementing and maintaining a wide variety of security specifications across all of the enterprise's technology assets and platforms can be prohibitive.

Current security solutions for Web-enabled applications focus on the transport layer. Secure Sockets Layer (SSL) along with the Transport Layer Security (TLS) and IPsec provide for transient, point-to-point security, providing data integrity, privacy, and authentication for the duration of a single session. Transport layer security is the basis of a comprehensive security solution for application integration. Most Web services will continue to rely on these technologies for many years to come.

However, Web services require additional security not provided by transport layer security. Web services require persistent, end-to-end data integrity, client authorization, and verifiable chains of evidence. This type of security is referred to as message-level or application layer security.

If your Web services rely on multi-step business processes or if you have multiple machines (such as switches or routers) between the Internet and your application, application layer security retains the data integrity and security of the message as it passes from step to step or machine to machine. Application level security enables you to provide your customers with access to the appropriate application based on their authorization. Finally, application layer security provides a mechanism for verifying that a message (such as a purchase order) has not been altered long after it has been received and processed.

Of the application layer security offerings, public key infrastructure (PKI) is the most robust. It uses digital certificates to provide persistent, end-to-end data integrity, authorization of the message sender, and clear chains of evidence after the message has been processed.

## About VeriSign's Trust Gateway

VeriSign's Trust Gateway provides the privacy and authentication features transport layer security, the persistent, end-to-end data integrity and authorization features of application layer security, into an XML-enabled, configurable, installation. VeriSign's Trust Gateway reduces the implementation costs of application layer security, and transparently uses SSL as transport layer security, enabling your organization to secure application messaging between your Web-based applications and your customers. With Trust Gateway you can:

- integrate PKI security between your internal applications and your business partners' external systems, even if they use different protocols.
- secure application messaging outside your corporate firewall, or between internal departments on corporate divisions.
- provide your business partners with access to your internal systems, without exposing those systems to unauthorized access.
- provide strong authentication, authorization, and encryption of all communication between your internal applications and your business partners.

- track the transactions performed by your business partners, as well as the activities of your own administrators.

In addition, with Trust Gateway, your business partners can enable their applications to communicate securely with you.

Trust Gateway secures machine-to-machine, XML-formatted messages sent over HTTP, and provides support for open standards such as SOAP, XML Signature, XML Encryption, and WS-Security. This open standards support increases the interoperability between your applications and those of your customers.

You can install and configure the Trust Gateway at an administrative level instead of the developer level, enabling faster deployment than traditional security solutions. Trust Gateway is highly configurable, so you can integrate it with your existing Web services and infrastructure, and add additional applications later. You can also create custom components for tighter integration with your applications.

## Components of Trust Gateway

Trust Gateway is an integrated system implemented across three primary architectures: your enterprise, the VeriSign Data Center, and your business partners. Figure 1-1 illustrates Trust Gateway and how these systems work together. These architectures are described in detail below.

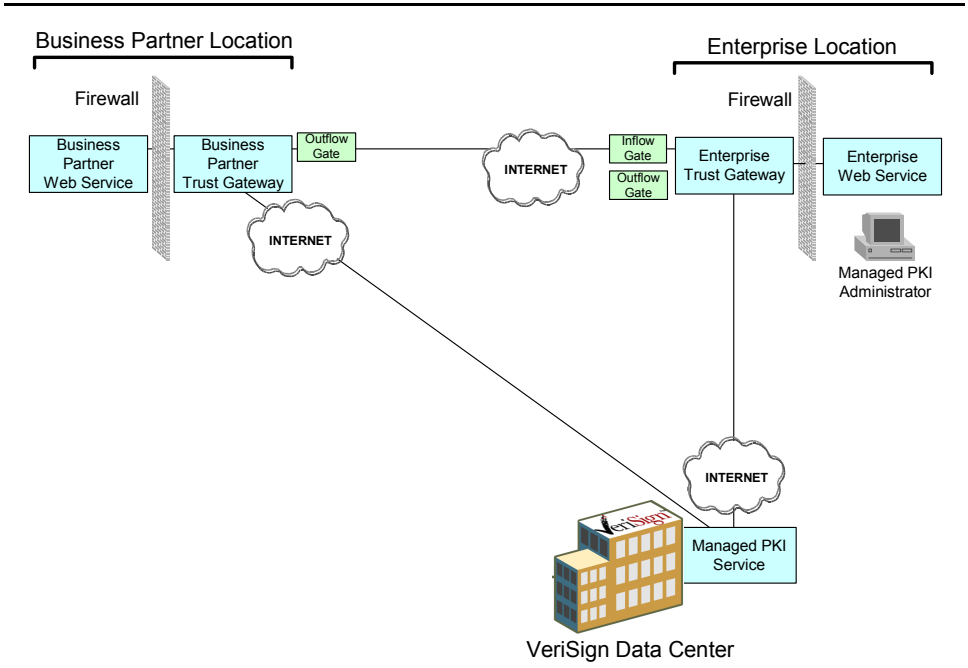


Figure 1-1 Trust Gateway components

## Enterprise Location

The enterprise location hosts the applications secured by Trust Gateway, the Trust Gateway, and your Managed PKI implementation.

- **Trust Gateway**. Server software that allows or prevents access by your business partners to a protected application on your enterprise server. The Trust Gateway performs security processing for your applications, verifying signatures, decrypting messages, and performing certificate validation and CA-based authorization on incoming messages. The Trust Gateway can also digitally sign and encrypt outgoing messages.

  The Trust Gateway is installed between your Web services and the firewall that separates your Web services from the Internet. Only transactions that are properly validated and authenticated by the Trust Gateway will be allowed to pass through the firewall to your secured Web service.

  The Trust Gateway is made up of the following components:

- Trust Gateway servlet container is the software that manages the Trust Gateway, enforcing your configuration and port settings, managing network connections and time-outs, and performing related tasks.
- Trust Gateway Administration console is the Web-based interface that you use to generate and register your default certificates, configure your business partner and service provider gates, configure port settings, and set logging options.
- Service provider (inflow) gate is the access point configured to validate and secure inbound messages made by your business partners to your Web services. The service provider gate is installed at your enterprise location.
- Business partner (outflow) gate is the access point configured to validate and secure requests made by your Web services to your business partners. A business partner gate is installed at your enterprise location as well as at your business partner location.

**IMPORTANT!** The Trust Gateway Beta release is designed to be run on a pilot system, and should not be installed on a production system. All passwords for the Trust Gateway Beta release are stored as clear text. When choosing passwords, do not use passwords that you would use on a production system.

- **Managed PKI**. VeriSign's Managed PKI service enables your enterprise to approve and issue the certificates required by the Trust Gateway to secure access to your applications. The Managed PKI administrator uses a workstation to access the Managed PKI Control Center to perform certificate management functions. This workstation can be on the same server as the Trust Gateway, or a separate computer. Refer to the Managed PKI documentation set for more information about Managed PKI.
- **Trust Gateway certificates, trust points, and keystores**. The Trust Gateway uses Trust Gateway certificates (made up of public and private key pairs) to identify the Trust Gateway to your business partner applications and secure transactions between the two. If installed in your business partner applications,

they are used to identify the business partner to your Trust Gateway. They are stored in a keystore defined by you during installation of the Trust Gateway.

The trust point is the method Trust Gateway uses to authenticate the Trust Gateway certificate. Typically, your trust point is the public portion of the issuer Certification Authority (CA) for your Trust Gateway certificates.

Both Trust Gateway certificates and trust points are stored in local keystores on that you configure. These keystores are standards Java keystores that store security resources such as digital certificates or cryptographic keys. When you install the Trust Gateway, two default keystores are created: keys and trustpoint. The keys keystore contains your initial trust Gateway certificate, and the trustpoint key store contains your initial trust point CA certificate. You can add additional keys and certificates to these keystores, or add additional keystores to your Trust Gateway.

## VeriSign Data Center

The VeriSign Data Center hosts the Web-based Managed PKI Control Center pages. Your Managed PKI administrator uses the Control Center to issue the Trust Gateway certificates used to authenticate, validate, and secure transactions from your business partners. The Control Center also enables the Managed PKI administrator to perform the certificate lifecycle functions required to manage these certificates (for example, renewing, revoking, and suspending certificates).

## Business Partner Location

Your business partners can implement the business partner gate portion of the Trust Gateway to enable secure access to your applications or Web resources. The Trust Gateway your business partners implement is functionally the same as yours, but uses certificates and software provided by your organization.

Your Managed PKI administrators use the Managed PKI Control Center to issue the certificates installed in your business partners' Trust Gateway. Your business partners do not have access to the Control Center. However, they can perform limited lifecycle functions for their certificates (such as requesting new or renewed certificates, or revoking existing ones) using the Managed PKI *Digital ID Center* pages. Refer to *Managed PKI Administrator's Handbook* for more information on the *Digital ID Center* pages.

## How Trust Gateway Processes a Transaction

When a business partner accesses your Web services through their application, the application sends a transaction to your Web service. Figure 1-2 illustrates how a transaction is processed by the Trust Gateway.

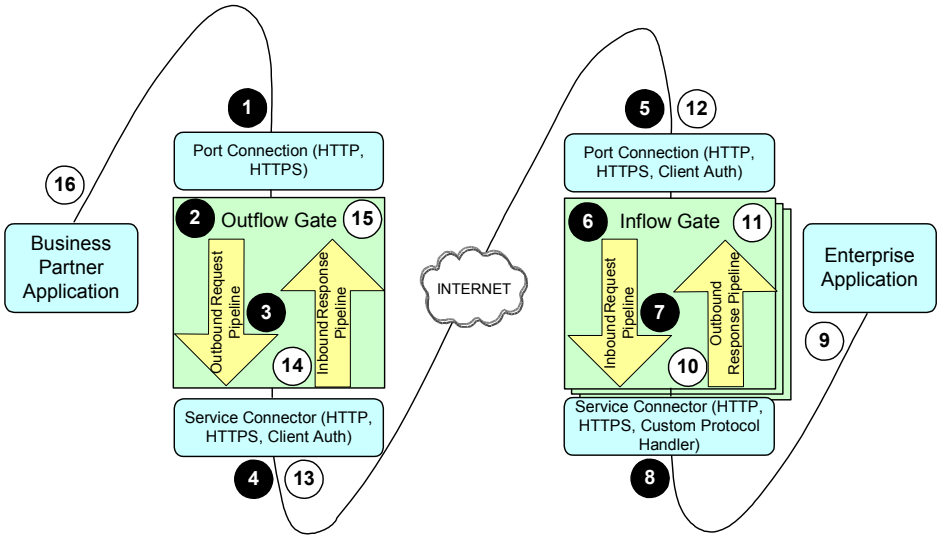


Figure 1-2 Trust Gateway transaction

1. The business partner's application sends a request to the port connection. This transaction occurs behind the firewall, and can be secured using HTTPS. The port connection routes the request to the business partner gate.
2. The business partner gate applies whatever security scheme is configured for that gate, such as signing the request or encrypting it.
3. The business partner gate sends the request through the outbound request pipeline to the service connector.
4. The service connector sends the request to the enterprise Trust Gateway over the Internet.
5. The enterprise's Trust Gateway receives the request, examines it for embedded information, and routes it to the appropriate service provider gate based on predefined routing rules.

6 The service provider gate verifies the signature on the request, and performs XKMS validation and CA-based authorization on the request's key.

7 The service provider gate applies any built-in XML transformations configured for that gate (such as removing or adding SOAP envelopes), and forwards the request to the service connector.

8 The service connector transmits the request to the appropriate application. This service connector may be a custom protocol handler, enabling support for legacy or proprietary applications.

9 The enterprise application returns a response to the service connector, which transmits the response back to the service provider gate that processed the original request.

10 The service provider gate applies any built-in XML transformations configured for that gate.

11 The service provider gate applies the security scheme configured for that gate, then sends the request through the same port connection that received the original request.

12 The port connection forwards the response back to the business partner's business partner gate over the Internet.

13 The business partner's service connector receives the response and transmits it to the business partner gate.

14 If configured to do so, the business partner gate verifies the signature on the response.

15 The business partner gate sends the response to the port connection.

16 The port connection transmits the response back to the application.

## Working with the Trust Gateway

After the Trust Gateway is configured correctly at your enterprise location and your business partner location, transactions to and from these locations are secured automatically, and require no intervention from your Managed PKI administrator or Trust Gateway administrator.

Chapter 2, “Installing the Trust Gateway,” describes how to install and configure the initial Trust Gateway and the initial business partner and service provider gates. Once you have configured these gates, your business partners can install business partner gates at their location to begin communicating securely with your protected Web services.

## Transaction Logging

The Trust Gateway provides three types of logs. All logs are written to the <Trust Gateway installation directory>/logs directory.

**Note** Managed PKI logs certificate and administrator activity associated with the Managed PKI service separately. Refer to *Managed PKI Administrator’s Handbook* for more information about these logs.

- gateway.log provides status and error information about Trust Gateway XML transactions. The gateway.log file will be rotated each day at midnight to gateway.log.YYYY-MM-DD (where YYYYMMDD is the date the log was generated). This log contains important information about XML transactions you should review this log during testing and troubleshooting. You may also choose to archive this log.
- console.log provides error information generated by the Trust Gateway Administration console. Logging information is appended to this single log file as it is generated. The console.log file is not rotated and normally does need not be examined or archived. However, you should provide this log along with any bug reports when reporting any problems with the Trust Gateway Administration console.
- server.YYYY-MM-DD.log provides status and error information generated by the servlet container. Logging information is appended to that day’s log file as it is generated. The gateway.log file will be rotated each day at midnight.

Refer to “Setting Logging Levels and Output” on page 51 for instructions on setting the level of detail generated by these logs and specifying the log output directory. Review these log files to assist you in troubleshooting the Trust Gateway. You should also review the log files periodically to ensure that the Trust Gateway is continues to function correctly.

## XML Functionality

Trust Gateway supports the following XML functionality. Unless indicated, these functions are enabled by default. Refer to Appendix B, "Configuring XML Functionality," for information on how to change these settings.

**Note** The following features may not be available in the Beta release.

Table 1-1 XML functionality supported by Trust Gateway

| Function | Description |
|---|---|
| Signature Verification | The Trust Gateway is able to verify XML signatures included in the incoming XML messages. |
| Digital Signatures on Outgoing XML messages | The Trust Gateway is able to sign the outgoing XML messages generated by the Web service(s) being served by the Trust Gateway. |
| Real-time Validation using XKMS | The Trust Gateway integrates with the XKMS real-time validation service offered by Managed PKI to validate the key used by the third party accessing the Web service using XKMS. |
| SSL server and client authentication | The Trust Gateway supports SSL server and client authentication. |
| SOAP messages signed with the WS-Security protocol | The Trust Gateway generates and consumes SOAP messages signed using the WS-Security protocol. The administrator has the option to enable or disable signing capability using the WS-Security protocol. However, the Trust Gateway is always able to process SOAP messages signed using the WS-Security protocol. |
| SOAP messages signed without the WS-Security protocol | The Trust Gateway generates and consumes SOAP messages signed using our custom protocol. If the administrator disables the option to sign using the WS-Security protocol, the Trust Gateway is able to generate SOAP messages signed using VeriSign's custom protocol. If the incoming SOAP message is signed using the WS-Security protocol, the Trust Gateway continues to handle those messages. |
| Multiple authorizations per message | The Trust Gateway supports authorizations of multiple signatures within a single XML message. |

Table 1-1 XML functionality supported by Trust Gateway (Continued)

| Function | Description |
|---|---|
| Message content based routing | The Trust Gateway is able to route the incoming XML request to the appropriate back-end application based on content of the incoming message. |
| URL-based routing | The Trust Gateway handles routing based on the URL of the application or Web service specified in the request. The administrator of the Trust Gateway is able to set the URL from the administrative console for the services that the requests are routed to. |
| Dispatch messages to legacy systems | The Trust Gateway provides APIs to support pluggable protocol adapters that support access to legacy systems. |

## Working with the Managed PKI Control Center

Although communications between your protected Web services and your business partners require no administrator intervention, the Managed PKI administrator needs to perform some certificate lifecycle functions periodically, using the Managed PKI Control Center. These functions are:

- Reviewing new certificate requests. Each new business partner requires a new Managed PKI certificate. You review, and approve or reject all new certificate requests from the Control Center.
- Reviewing certificate renewal requests. To enhance security, all Digital IDs have a limited lifetime, called its validity period. The validity period is the period of time that the certificate can be used. Once the certificate has expired, the subscriber must renew the certificate. Use the Control Center to review, and approve or reject all certificate renewal requests.
- Revoking certificates. there are some cases where a certificate should no longer be used (for instance, if the subscriber leaves the organization, or the certificate becomes corrupt or is lost). In these cases, the certificate should be revoked. The subscriber can revoke the certificate from the *Digital ID Center* pages. The Managed PKI administrator can also revoke the certificate using the Control Center.

  Once revoked, the certificate cannot be returned to valid status.

- Reviewing reports and audit trails. The Control Center provides reporting tools and audit trails. Review these regularly to keep track of the certificates issued and revoked, as well as subscriber and administrator activity.
- Assigning additional administrators. You can add additional Managed PKI administrators and configure their roles using the Control Center.

Refer to *Managed PKI Administrator's Handbook* for information on using the Control Center to perform these functions.

In addition to these certificate lifecycle functions, your organization is responsible for providing technical support to your business partners for the Trust Gateway and their certificates. Review the Managed PKI documentation set so that you are prepared to support your business partners.

## About This Guide

This handbook is a reference guide for Trust Gateway administrators—people who install and configure the Trust Gateway and provide technical support to your business partners, suppliers, and customers who access your Web services.

### Contents of This Manual

- Chapter 2, "Installing the Trust Gateway," describes the procedures for installing and configuring the basic Trust Gateway
- Chapter 3, "Configuring and Managing the Trust Gateway," provides additional configuration information, such as adding additional gateways, changing administrator passwords, and setting new default keys.
- Chapter 4, "Distribution," describes how to make the Trust Gateway available to your business partners, and overviews how your business partners install and configure their own Trust Gateway.
- Appendix A, "Service Connector API," describes how to configure additional service connectors (such as HTTPS, SSL, or a custom protocol handler) with Trust Gateway.
- Appendix B, "Configuring XML Functionality," provides instructions for configuring the XML functionality supported by Trust Gateway.

CHAPTER 2

# Installing the Trust Gateway

This chapter details the procedures you follow to install the basic Trust Gateway. Additional configuration information is provided in Chapter 3, “Configuring and Managing the Trust Gateway.”

## Installation Requirements

Before installing the Trust Gateway, you will need the following:

- Managed PKI 5.1 installed. Refer to *Managed PKI Installation and Configuration* for installation instructions. Refer to the Managed PKI documentation set for complete information. This is not required for the Beta release.
- Windows NT, 2000, or XP, Solaris 2.8 or 2.9, or Linux Red Hat 7.2.
- A key name and passcode. Create this key name and passcode by enrolling for, and approving, a certificate request with the Managed PKI Control Center. If you cannot create a passcode and associated XKMS key name, contact **xkms-interop@verisign.com** to obtain these.

### Supported Servers

The Trust Gateway has been tested against the following Web servers and application servers:

- Apache Tomcat 4.1.12 Web server
- Websphere application servers
- Weblogic application servers

# Installing the Trust Gateway

Follow these procedures to install the Trust Gateway:

1. Obtain the latest Trust Gateway installer software from the Trust Gateway CD.
2. Place the Trust Gateway CD in your CD drive (D: in this example) and run the appropriate Trust Gateway installer:
   - For Solaris machines, run TrustGateway/solaris/setup
   - For Linux machines, run TrustGateway/linux/setup
   - For Windows machines, run D:\TrustGateway\Windows\setup.exe

   **Note** For Solaris and Linux, you must be logged in as root to install the Trust Gateway.

3. Follow the onscreen prompts to install the software:
   a. Choose an installation directory.
   b. Choose **Full** or **Custom**. If you select Custom, you will be asked to select which of the following features to install. If you select **Full**, both of these components will be installed.
      – The Trust Gateway Server is the stand-alone Trust Gateway component that performs transaction processing on behalf of the enterprise's applications. With the stand-alone version, you can configure SSL from within the Trust Gateway Administration console.
      – The Trust Gateway toolkit is a version of the Trust Gateway servlet without the container. It includes developer resources such as the servlet resources and .war files, and sample applications and service connectors. The toolkit enables you to install the Trust Gateway servlet into any container, such as Websphere and Web logic. With this toolkit, you must manually configure your SSL and integrate it with the Trust Gateway.

        If you select **Custom**, this toolkit is required to test the Trust Gateway installation prior to providing it to your business partners.

c Choose an administrator name and password. This identifies the initial Trust Gateway administrator who will configure the Trust Gateway. Passwords are stored in clear text for the Trust Gateway Beta release. Do not use production passwords for the Beta.

4 The Trust Gateway software must be running to configure or use it. Start the Trust Gateway using the appropriate procedures:

**IMPORTANT!** The Trust Gateway Administration console uses port 8081. You cannot have any applications running on this port, or the Trust Gateway will not be able to start.

- For Solaris and Linux machines, run the monitor.sh script in the /bin directory.
- For Windows machines, select **Start → Programs → Trust Gateway → Start Trust Gateway**

The Trust Gateway process opens in a new window. Closing this window shuts down the Trust Gateway. This window must remain open whenever you are configuring the Trust Gateway or the Trust Gateway is in use.

5 Log in to the Trust Gateway Administration console by pointing your Web browser to **http://localhost:8081/console/** (you can replace localhost with the actual name of the machine on which the Trust Gateway is running).

Enter the administrator name and password you chose when you ran the Trust Gateway installer, and click **Submit**.

**Note** To change the administrator name and password, modify the tg-users.xml file found in the <installation directory>/conf directory.

6 The first time you access the Trust Gateway, you must register a default key. The *Register Key* page displays (Figure 2-1).

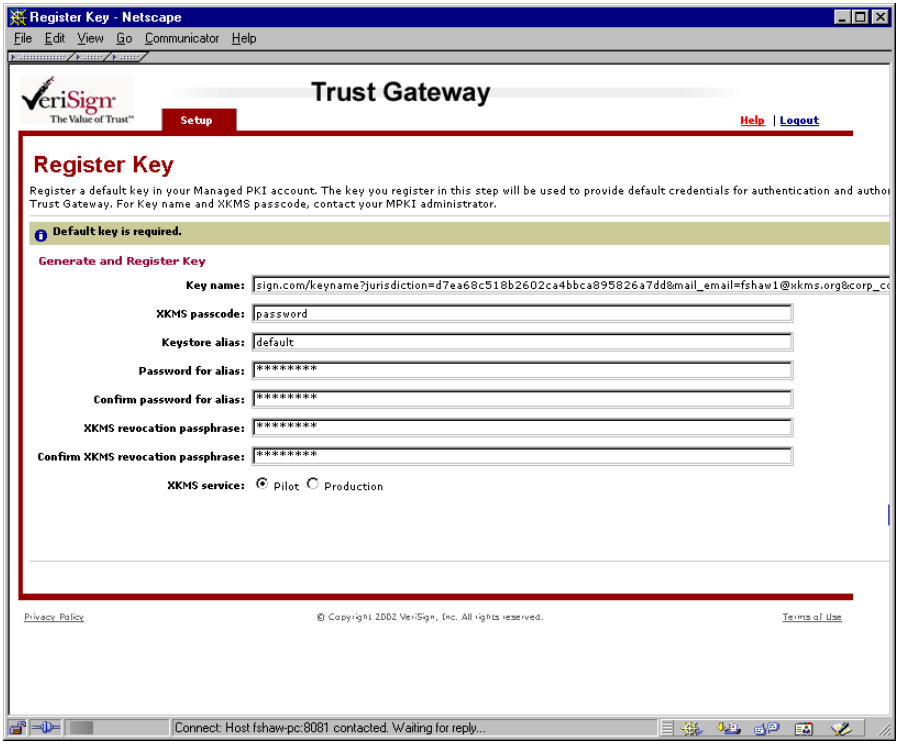


Figure 2-1 *Register Key* page

Enter the following information to register your default key:

Table 2-1 *Register Key* page fields

| Field | Input Required |
|---|---|
| Key Name | Enter the key name you created, or that you obtained from VeriSign (**xkms-interop@verisign.com**). |
| XKMS passcode | Enter the XKMS passcode you created, or that you obtained from VeriSign (**xkms-interop@verisign.com**). |
| Keystore alias | Enter a unique name for the key. Use only ASCII characters 0 - 9, and a - z. Do not use spaces, A - Z, or special characters. |

Table 2-1 *Register Key* page fields (Continued)

| Field | Input Required |
|---|---|
| Password for alias | Enter a password for the key. Use only ASCII character; do not use special characters. Passwords are case-sensitive, and should be a minimum of 6 characters.<br>You will need this password to perform any operations with this key. |
| Confirm password for alias | Re-enter the password for the key. |
| XKMS revocation password | Enter a revocation password. You will need this to revoke the keys in the default keystore. |
| Confirm XKMS revocation password | Re-enter the revocation password for the default keystore. |
| XKMS service | Select whether this key and service will be used on a pilot or production system. Select pilot for the Beta release. |

- **Continue with Configuration**

The Trust Gateway software is installed, and the *Gates* page appears (Figure 2-2). This is the home page for your Trust Gateway.

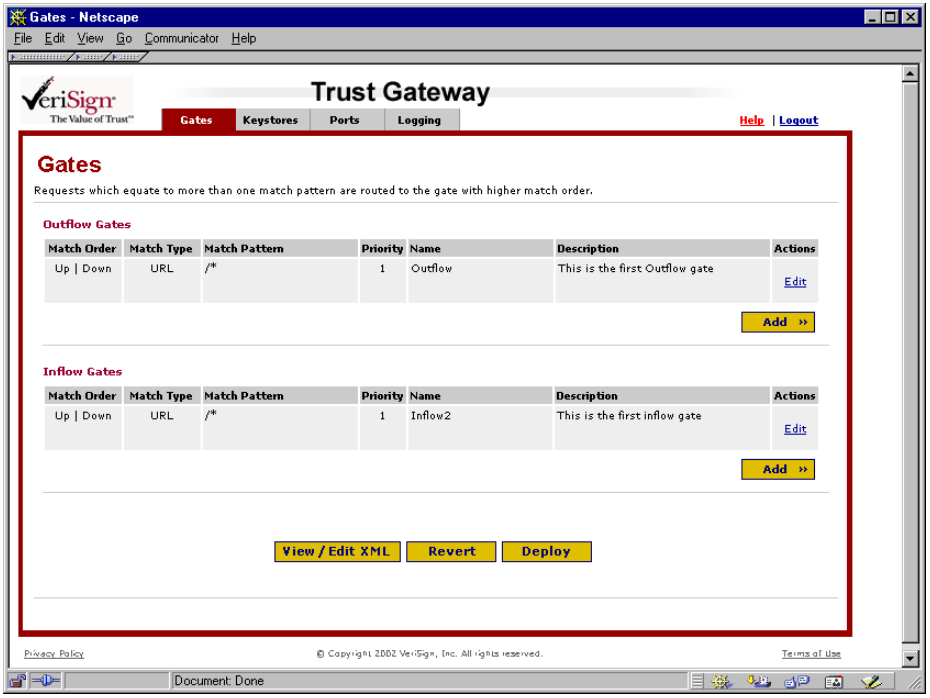


Figure 2-2 *Gates* page

To complete the installation, you must configure a service provider gate (to communicate with your business partners). Procedures for installing the initial service provider gate is the same as for configuring additional gates. Refer to Chapter 3, "Configuring and Managing the Trust Gateway," for instructions on configuring the service provider gate.

Once you have installed the service provider gate, return to the *Gates* page by selecting the **Gates** tab, and click **Deploy**. The Trust Gateway will restart and you must log back in to the Trust Gateway Administration console. The Trust Gateway is now fully installed.

**Note** For Solaris and Linux installations, you must be logged in as root to deploy a gate.

## Testing the Trust Gateway

**IMPORTANT!** You must have installed the Trust Gateway toolkit (by selecting **Custom** → **Trust Gateway toolkit** during the installation process) to use these procedures to test the Trust Gateway. The toolkit is automatically installed if you selected the Full installation.

Complete the following steps to test the Trust Gateway installation.

This test sends the file unsigned_request.xml to your business partner gate, where it is digitally signed and then sent to your service provider gate (localhost:80).

Your service provider gate verifies the digital signature, performs a real-time XKMS validation against VeriSign's Trust Service, ensures that the credential is authorized, and then sends the message to the service connector. (This service connector would typically point to a back-end application, which would perform a transaction, generate the response and then send the response to the service provider gate.)

The service provider gate then digitally signs the response and sends it to your business partner gate, which verifies the signature and then returns the message to you.

**Note** This test assumes that you have retained the default ports for your service provider and business partner gates, and your Trust Gateway Administration console.

1. Put TSIK.jar in your Classpath. TSIK.jar is located in /toolkit/tsik-1.7.zip.
2. From a command prompt, switch to the <Trust Gateway installation directory>/toolkit/samples directory. This directory is only available if you installed the Trust Gateway Toolkit in Step 3 under “Installing the Trust Gateway” on page 14.
3. Enter the following command:

```
java com.verisign.messaging.tools.SendXML http://localhost:
8080/ < unsigned_request.xml
```

CHAPTER 3

# Configuring and Managing the Trust Gateway

This chapter describes how to complete the following procedures to configure and manage the Trust Gateway:

- Starting the Trust Gateway
- Setting the match pattern order
- Adding a service provider (inflow) gate
- Adding a business partner (outflow) gate
- Editing the gateway configuration file
- Defining ports
- Setting logging levels and output

## Starting the Trust Gateway

Complete the following steps to start the Trust Gateway:

**IMPORTANT!** The Trust Gateway Administrator console uses port 8081. You cannot have any other applications running on this port, or the Trust Gateway will not be able to start.

- For Solaris and Linux machines, run the monitor.sh script in <Trust Gateway installation directory>/bin.
- For Windows machines, select **Start → Programs → Trust Gateway → Start Trust Gateway**

The Trust Gateway opens in a new window. Closing this window closes the Trust Gateway. This window must remain open whenever you are configuring the Trust Gateway or the Trust Gateway is in use.

## Setting the Match Pattern Order

When the Trust Gateway identifies a match pattern in a message, it examines the service provider and business partner gates to determine to which gate the request should be routed. The order the Trust Gateway examines these gates is the order they appear on the *Gates* page. The Trust Gateway examines the gate from the top down. If you have multiple service provider or business partner gates, the order you set may be very important.

For example, you may want to set the gate with the highest volume of transactions to the top of the list so the Trust Gateway will find it immediately. Also, if you assigned a wildcard match pattern to a gate, this gate should be at the bottom of the list, as the Trust Gateway will route all requests there, and not examine any gates below it for a better match.

Set the match pattern order from the *Gates* page by clicking **Up** or **Down** in the *Match Order* column next to the gate you wish to move.

## Adding a Service Provider (Inflow) Gate

This section describes how to create a service provider gate service to provide security and functionality for your Web services being accessed by your subscribers. Adding a service provider gate follows these steps:

1. Name the service provider gate.
2. Specify the match pattern.
3. Choose the service connector.
4. Choose a security schema.
5. Specify the trust policy.
6. Apply transforms.
7. Review and confirm the settings.

Each step is described in the following sections.

## Step 1 Name the Service Provider Gate

1 From the *Service Provider Gates* section of the *Gates* page, click **Add**. The *Add Gate: Step 1 of 7 Service Provider Gate Information* page opens (Figure 3-1).

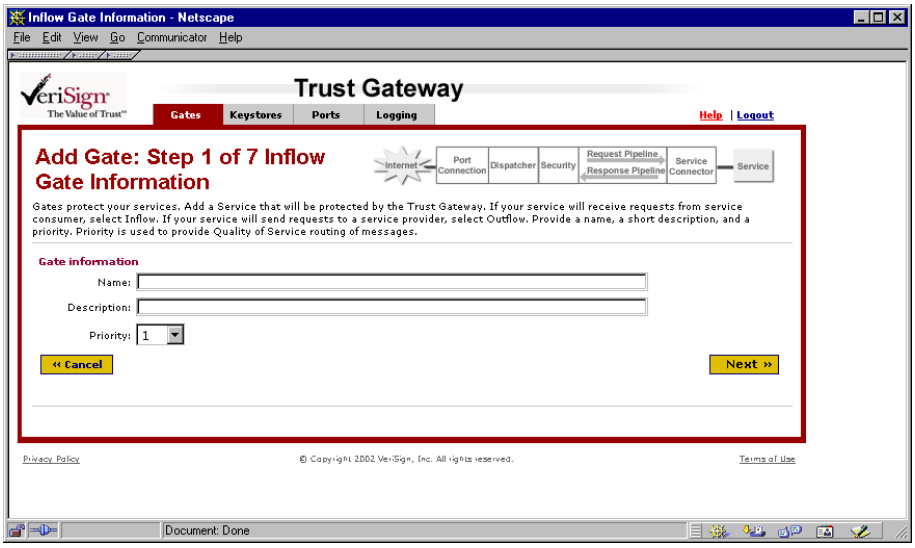


Figure 3-1 *Add Gate: Step 1 of 7 Service Provider Gate Information* page

2 Enter a name and description for the new service provider gate, and select a priority for quality of service routing. Click **Next**.

Although you can set the priority, quality of service routing is not implemented in the Beta release.

## Step 2 Specify the Match Pattern

When the Trust Gateway sends or receives a request, it examines the request for a match pattern. If you have multiple applications, the Trust Gateway can route the request to the gate associated with that application, based on the match pattern included in the request. For example, if you have set the match pattern to be a URL with the phrase /ERP appended to it, the Trust Gateway will route all requests with /ERP in the URL to that gate. For more information on how the Trust Gateway routes requests by their match patterns, refer to "Setting the Match Pattern Order" on page 22.

1 The *Add Gate: Step 2 of 7 Choose Match Pattern* page opens (Figure 3-2). Select the type of match to be used for the new business partner gate: **URL** or **XPath**.

- If you select **URL**, enter the URL into the text field.
- If you select **XPath**, either select one of the displayed choices or enter a new prefix and URI into the text fields and then click **Add**. If you do not select a displayed choice or enter a new prefix and URI, the default XPath is used.

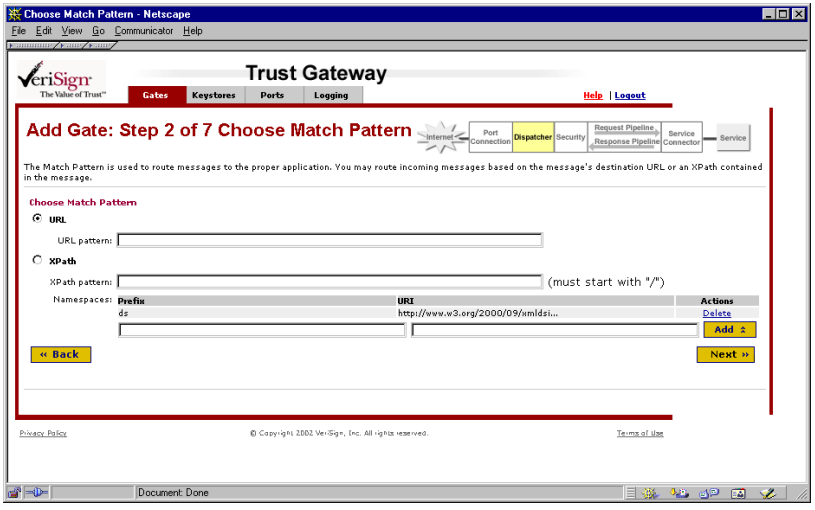


Figure 3-2 *Add Gate: Step 2 of 7 Choose Match Pattern* page

2 Click **Next**.

## Step 3 Choose the Service Connector

1 The *Add Gate: Step 3 of 7 Choose Service Connector* page opens (Figure 3-12).

- If your back-end application is a Web service, select **HTTP/HTTPS connector** and enter the URL for your backend application.
- If you back-end application uses a protocol other than HTTP/S, you must develop a custom connector to handle that protocol. Select Custom Connector, then enter the class name (without the .class extension) and the name/value properties for the component that handles the required protocol.

**Note** The Trust Gateway provides a simple custom connector, which echoes back whatever the service provider gate receives. This enables you to test the gateway without having a back-end application up and running. To implement it, select **Custom connector** and enter **EchoServiceConnector** in the text field.

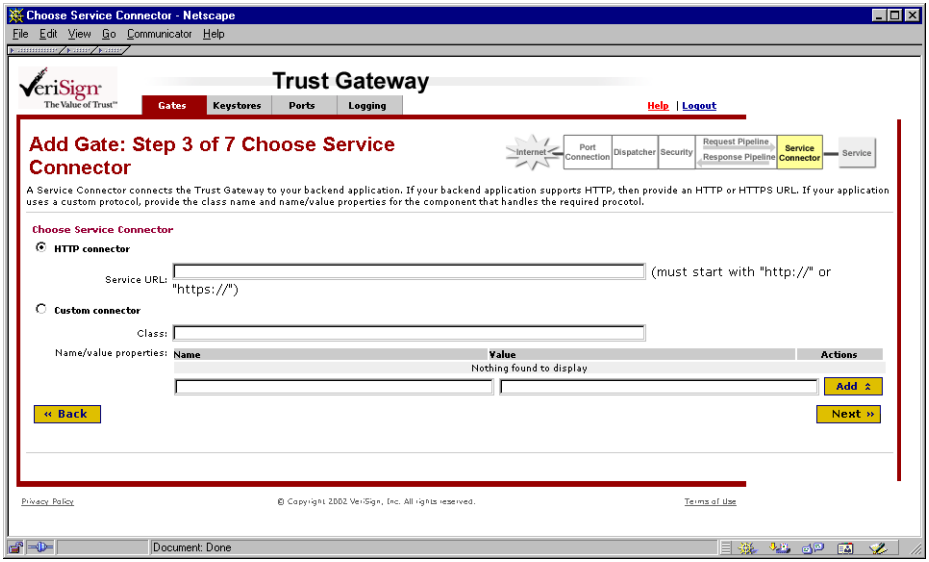


Figure 3-3 *Add Gate: Step 3 of 7 Choose Service Connector* page

2 Click **Next**.

## Step 4 Specify the Security Scheme

1 The *Add Gate: Step 4 of 7 Configure Security* page opens (Figure 3-4). Select the type of security to use for this gate. The matrix on this page describes the security features each selection provides.

**Note** If you select an SSL security type, you must configure your Web server for SSL, and update the port on the *Assign Ports* page (refer to "Defining Ports" on page 49). You will need to obtain an SSL ID for your Web server.

- **Routing Only**.
- **Routing + Message Security**.
- **SSL**.
- **SSL + Message Security**.
- **SSL + Client authentication**.

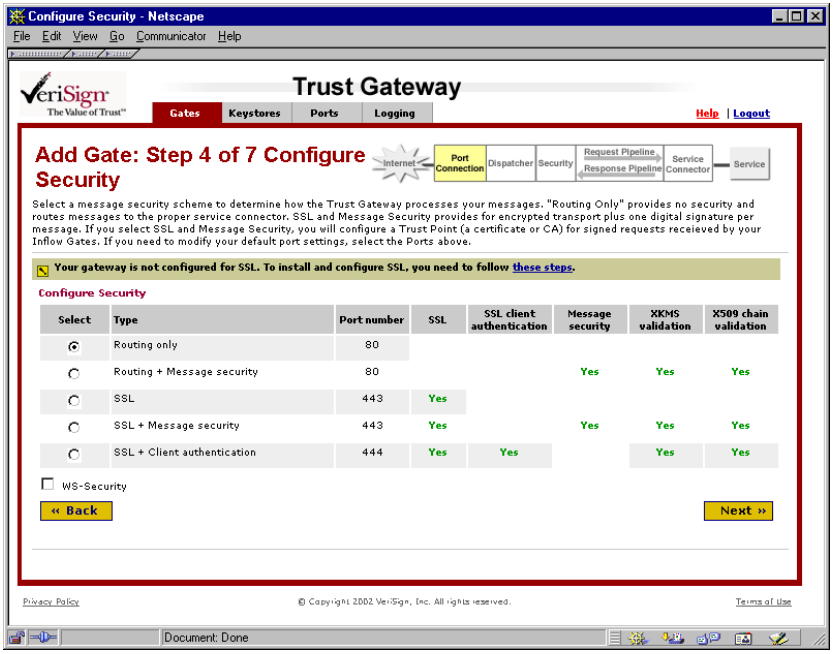


Figure 3-4 *Add Gate: Step 4 of 7 Configure Security* page

2 If you select **Message security** you have the choice of configuring WS-Security as your protocol. Select a security protocol that provides message security, and then check the WS-Security checkbox at the bottom of the page.

3 Click **Next**.

## Step 5 Specify the Trust Policy

Specify the trust policy by selecting the trust points for the certificate your business partner will use to access this service provider gate. Typically, this is the issuing CA associated with the Managed PKI account you use to issue Trust Gateway certificates to your business partners. This is typically also the CA that issued the default key you obtained when you installed the Trust Gateway.

1 The *Add Gate Step 5 of 7 Set Trust Policy* page opens (Figure 3-5). Click the **Trusted** checkbox for each trust point you want to trust. Any key issued by a trust point you set as trusted will be allowed access to this service provider gate.

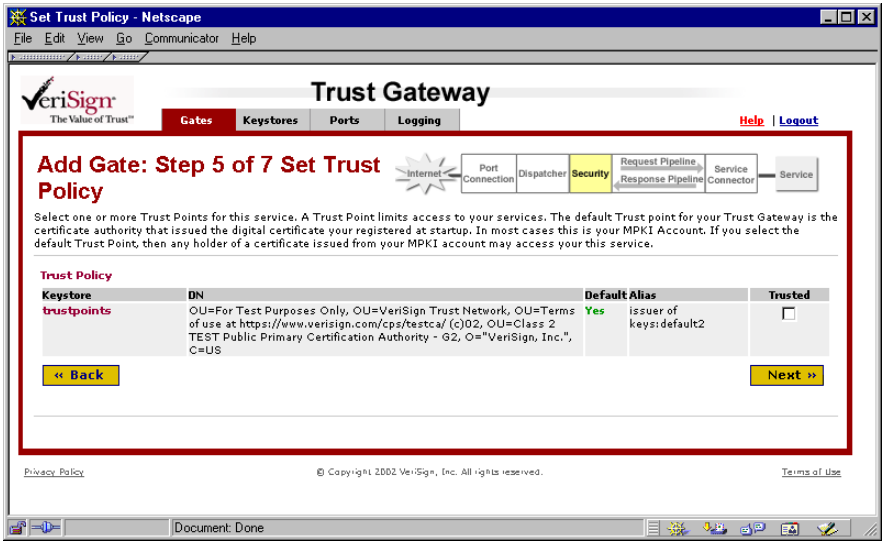


Figure 3-5 *Add Gate Step 5 of 7 Set Trust Policy* page

2 Click **Next**.

## Step 6 Apply Built-in Request Transforms

Built-in transforms are operations that change the request message in a known way prior to it being delivered to your Web service. Trust Gateway provides two XML transforms: Add SOAP envelope transform and Remove SOAP envelope transform. You can apply these transforms to incoming requests or outgoing responses.

1 The *Add Gate: Step 6 of 7 Built-In Request Transforms* page opens (Figure 3-6). Select the transforms that you want applied to messages being sent to the new gate. You can modify the sequence in which these transforms are applied in a later step. Possible choices include:

- **Add SOAP envelope transform**. This transform adds a SOAP envelope to the request message that is received by the Trust Gateway from the business partner gate. The previous request message will be inserted into the body of the new SOAP envelope. The new SOAP envelope is a generic SOAP envelope that your Web service can understand.
- **Remove SOAP envelope transform**. This transform removes any SOAP envelope that is in the request message that is received by the Trust Gateway from the business partner gate. The contents of the SOAP body become the entire message that is delivered to your Web service.

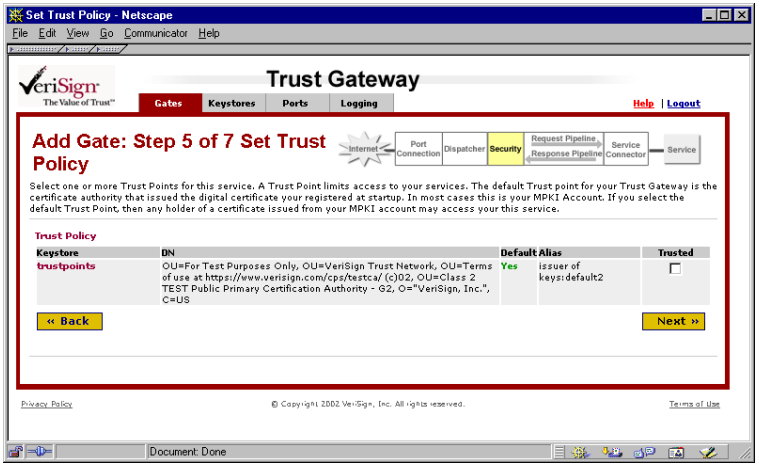


Figure 3-6 *Add Gate: Step 6 of 7 Built-In Request Transforms* page

2 Click **Next**.

## Step 7 Apply Built-in Response Transform

3 The *Add Gate: Step 7 of 7 Built-In Response Transforms* page opens (Figure 3-7). Select the transforms that you want applied to messages being sent from the new gate. You can modify the sequence in which these transforms are applied in a later step. Possible choices include:

- **Add SOAP envelope transform**. This transform adds a SOAP envelope to the response message that is sent out by the Trust Gateway to the business partner gate. The previous response message will be inserted into the body of the new SOAP envelope. The new SOAP envelope is a generic SOAP envelope that your business partner's Web service can understand.
- **Remove SOAP envelope transform**. This transform removes any SOAP envelope that is in the response message that is sent out by the Trust Gateway to the business partner gate. The contents of the SOAP body become the entire message that is delivered to your business partner's Web service.

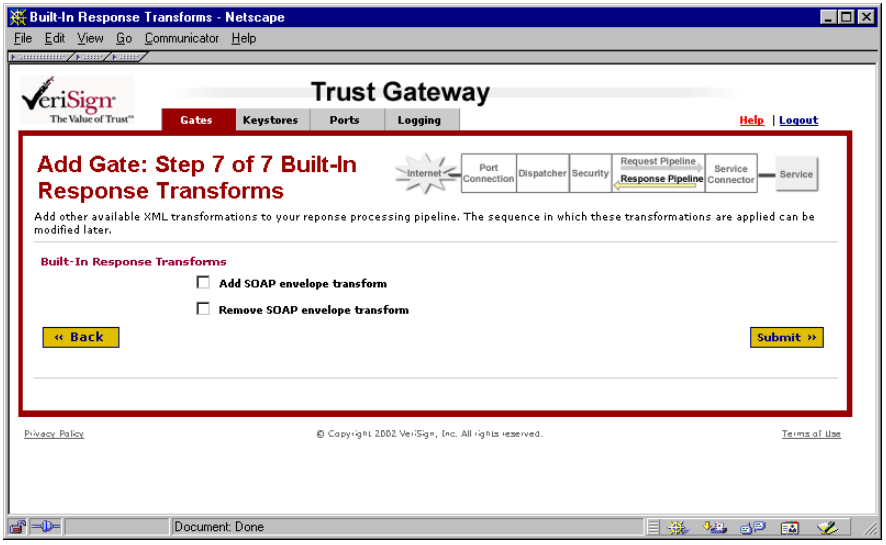


Figure 3-7 *Add Gate: Step 7 of 7 Built-In Request Transforms* page

4 Click **Submit**.

## Step 8 Review and Confirm the Settings

1 The *Edit Gates* page appears displaying the settings you configured for this service provider gate (Figure 3-8). Review the settings on this page. If you need to make any changes, click **Edit** next to the appropriate section and make the required changes. Click **Delete** to delete the entire gate.

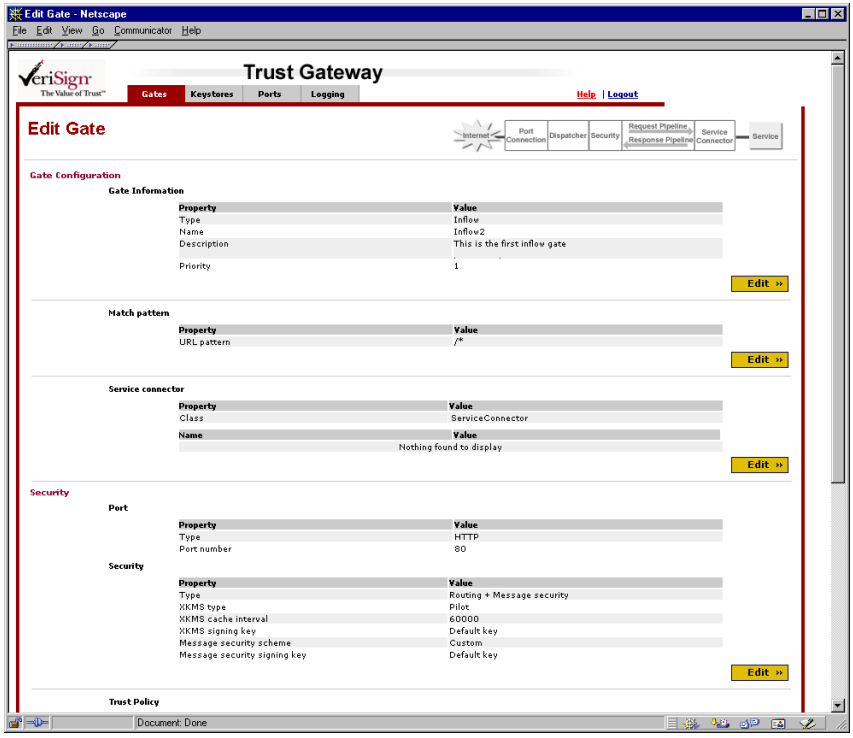


Figure 3-8 Top half of the *Edit Gate* page

2 When you are finished reviewing and editing these settings, click **Done**.

3 Click **Deploy** to restart the Trust Gateway and apply this new service provider gate. You will need to log in to the Trust Gateway once the gateway has restarted.

If you are also adding a business partner gate, you can add the business partner gate, then click **Deploy** to create both gates at one time.

**Note** For Solaris and Linux installations, you must be logged in as root to deploy a gate.

Click **Revert** to delete the changes and return to the previously saved configuration.

## Adding a Business Partner (Outflow) Gate

This section describes how to create a business partner gate service to your Trust Gateway.

Follow these general steps to configure a business partner gate:

1. Name the business partner gate.
2. Specify the match pattern.
3. Specify the port.
4. Choose the service connector.
5. Specify the signing key or client authentication certificate.
6. Apply transforms.
7. Review and confirm the settings.

Each step is described in detail in the following section.

## Step 1 Name the Business Partner Gate

1 From the *Business Partner Gates* section of the *Gates* page, click **Add**. The *Add Gate: Step 1 of 7 Business Partner Gate Information* page opens (Figure 3-9).

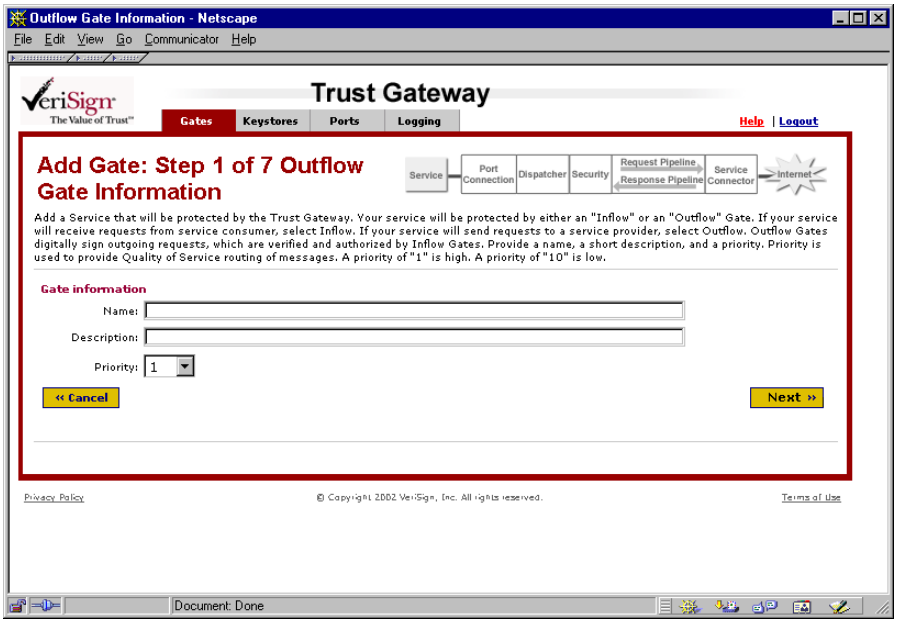


Figure 3-9 *Add Gate: Step 1 of 7 Business Partner Gate Information* page

2 Enter a name and description for the new business partner gate, and select a priority for quality of service routing. Click **Next**.

Although you can set the priority, quality of service routing is not implemented in the Beta release.

## Step 2 Specify the Match Pattern

When the Trust Gateway sends or receives a request, it examines the request for a match pattern. If you have multiple applications, the Trust Gateway can route the request to the gate associated with that application, based on the match pattern included in the request. For example, if you have set the match pattern to be a URL with the phrase /ERP appended to it, the Trust Gateway will route all requests with /ERP in the URL to that gate. For more information on how the Trust Gateway routes requests by their match patterns, refer to "Setting the Match Pattern Order" on page 22.

1 The *Add Gate: Step 2 of 7 Choose Match Pattern* page opens (Figure 3-10). Select the type of match to be used for the new business partner gate: **URL** or **XPath**.

- If you select **URL**, enter the URL into the text field. Enter /* to have all requests sent to this gate
- If you select **XPath**, enter an XPath expression. You may also need to enter a prefix/URI pair. Click **Add**.

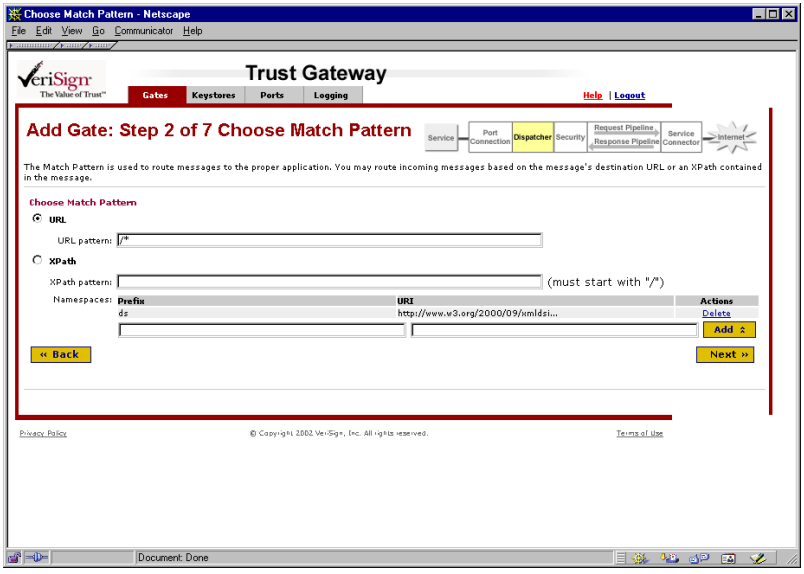


Figure 3-10 *Add Gate: Step 2 of 7 Choose Match Pattern* page

2 Click **Next**.

## Step 3 Specify the Port

1 The *Add Gate: Step 3 of 7 Choose Port* page opens (Figure 3-11). Select the port definition and how your backend application connects to this business partner gate behind the firewall. Possible choices include:

- **HTTP**.
- **HTTPS**. If you select HTTPS, you must configure your application for SSL, update the port on the *Defining Ports* page, and ensure that the key tomcat exists in the keys keystore. You will also need to obtain an SSL ID for your Trust Gateway.

**Note** The port selected depends on the type of security you select, and is not configurable from this screen. Refer to "Defining Ports" on page 49 for more information about ports and how to configure port definitions.

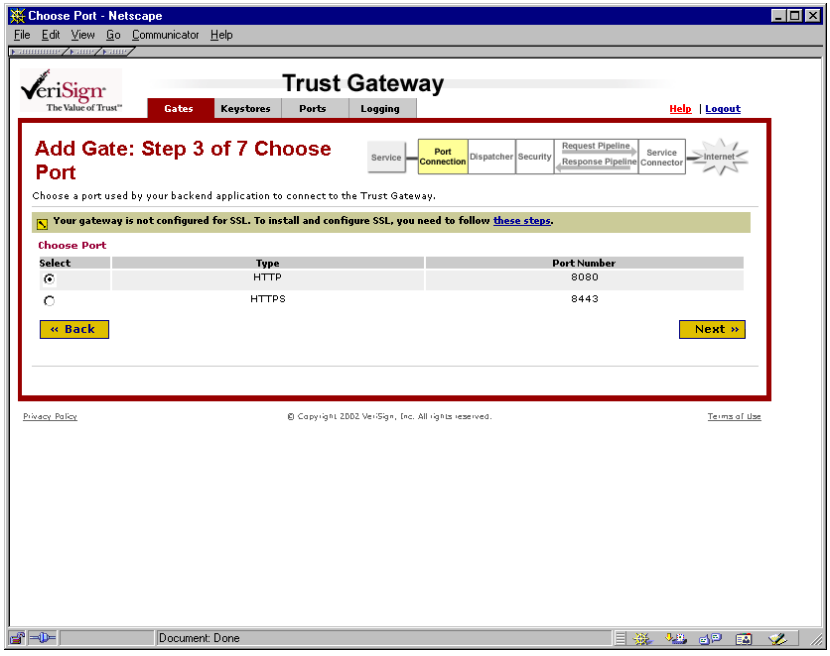


Figure 3-11 *Add Gate: Step 3 of 7 Choose Port* page

2 When you are done, click **Next**.

## Step 4 Specify the Service Connector

1 The *Add Gate: Step 4 of 7 Choose Service Connector* page opens (Figure 3-12). Enter the URL for the external service to which this business partner gate will communicate.

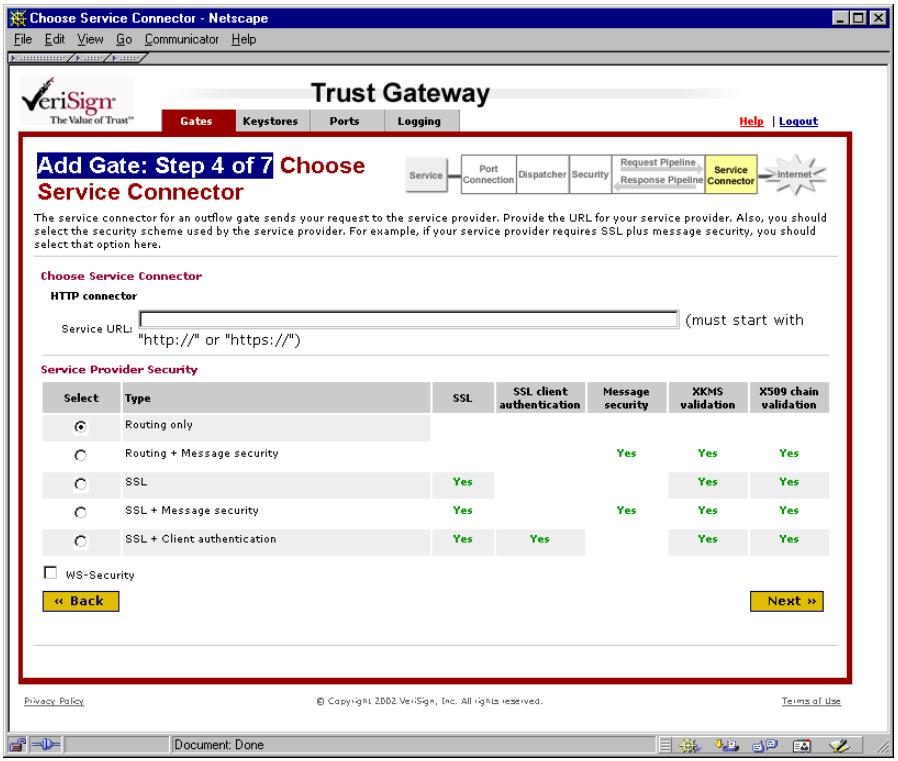


Figure 3-12 *Add Gate: Step 4 of 7 Choose Service Connector* page

2 Select the type of security to use for this gate. The matrix on this page describes the security features each selection provides.

- **Routing Only**. No security configured. Routes message to proper service connector
- **Routing + Message Security**. Routes the message to the proper service connector, digitally signs the message, and provides XKMS and X.509 chain validation.
- **SSL**. Encrypts the session using SSL.

- **SSL + Message Security**. Encrypts the session with SSL, digitally signs the message, and provides XKMS and X.509 chain validation. The trust point of the service provider gate must be configured with the issuer of this signing certificate.
- **SSL + Client authentication**. Encrypts the session with SSL, and provides client authentication.

3 Select WS-Security to implement the WS-Security protocol and process SOAP messages. You must also select **Routing + Message security** or **SSL + Message security** on this screen, and **Add SOAP envelope transform** for the request message (in Step 6 on page 39).

4 Click **Next**.

## Step 5 Specify the Signing Key or Client Authentication Certificate

Depending on the type of security you chose for this gate, you will have to specify the signing key that will be used to sign messages being sent through the business partner gate, or the certificate that will be used to authenticate the sender of the message being sent through the business partner gate.

- If you chose **Routing + Message security** or **SSL + Message security**, the *Add Gate: Step 5 of 7 Choose Signing Key* page opens (Figure 3-13).
  - Select the key that will be used to sign messages.

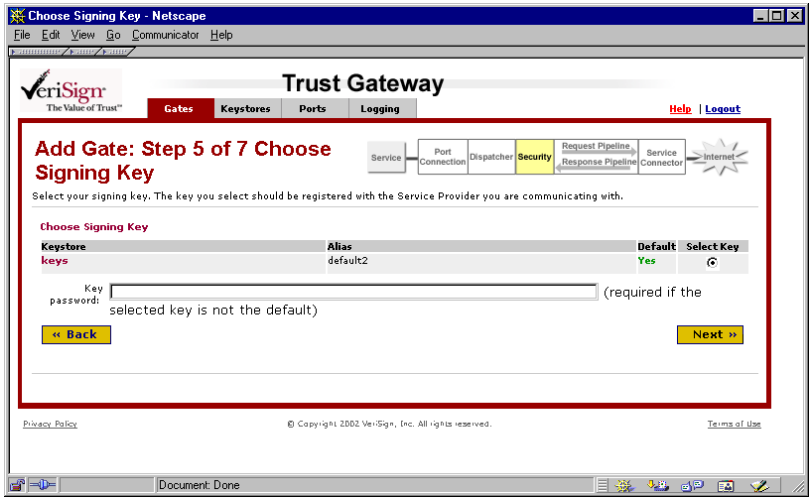


Figure 3-13 *Add Gate: Step 5 of 7 Choose Signing Key* page

  - If you selected a key that is not the default, enter the password for the keystore associated with this signing key.
  - Click **Next**.

- If you chose **SSL + Client authentication**, the *Add Gate: Step 5 of 7 Choose Certificate for Client Auth* page opens.
  - Select the certificate to be used to authenticate the sender of the message.
  - If you selected a certificate that is not the default, enter the password for the keystore associated with this certificate.
  - Click **Next**.

## Step 6 Apply Built-in Request Transform

Built-in transforms are operations that change the request message in a known way prior to it being delivered to your Web service. Trust Gateway provides two XML transforms: Add SOAP envelope transform and Remove SOAP envelope transform. You can apply these transforms to incoming requests or outgoing responses.

1 The *Add Gate: Step 6 of 7 Built-In Request Transforms* page opens (Figure 3-14). Select the transforms that you want applied to messages being sent to the new gate. You can modify the sequence in which these transforms are applied in a later step. Possible choices include:

- **Add SOAP envelope transform**. This transform adds a SOAP envelope to the request message that is sent to the business partner gate from the business partner application. The previous request message will be inserted into the body of the new SOAP envelope. The new SOAP envelope is a generic SOAP envelope.

  The request message remains in the SOAP envelope when it is sent to the Trust Gateway by the business partner gate.

- **Remove SOAP envelope transform**. This transform removes any SOAP envelope that is in the request message that is sent to the business partner gate from the business partner application. The contents of the SOAP body become the entire message that is delivered to the Trust Gateway.

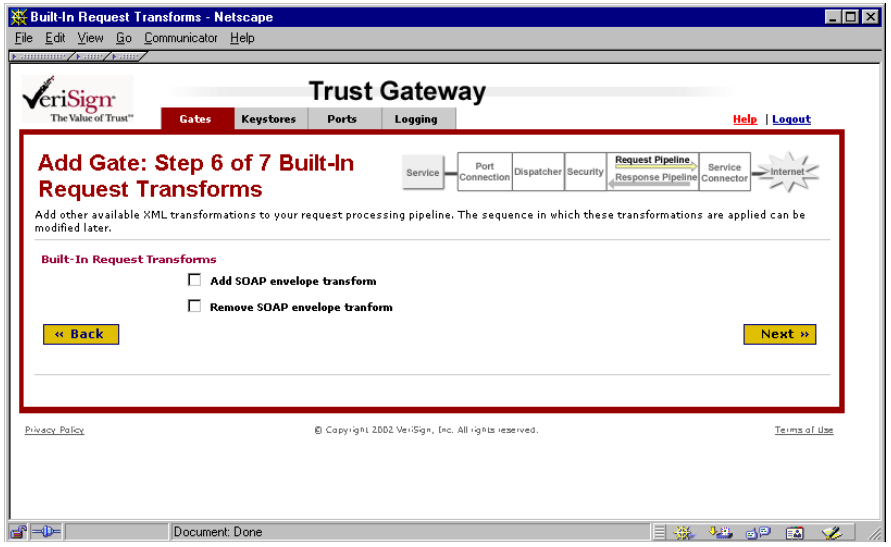


Figure 3-14 *Add Gate: Step 6 of 7 Built-In Request Transforms* page

**2** Click **Next**.

## Step 7 Apply Built-in Response Transform

1 The *Add Gate: Step 7 of 7 Built-In Response Transforms* page opens (Figure 3-15). Select the transforms that you want applied to messages being sent from the new gate. You can modify the sequence in which these transforms are applied in a later step. Possible choices include:

- **Add SOAP envelope transform**. This transform adds a SOAP envelope to the response message that is received by the business partner gate from the Trust Gateway. The previous response message will be inserted into the body of the new SOAP envelope. The new SOAP envelope is a generic SOAP envelope that your business partner's application can understand.
- **Remove SOAP envelope transform**. This transform removes any SOAP envelope that is in the response message that is received by the business partner gate from the Trust Gateway. The contents of the SOAP body become the entire message that is delivered to your business partner's application.

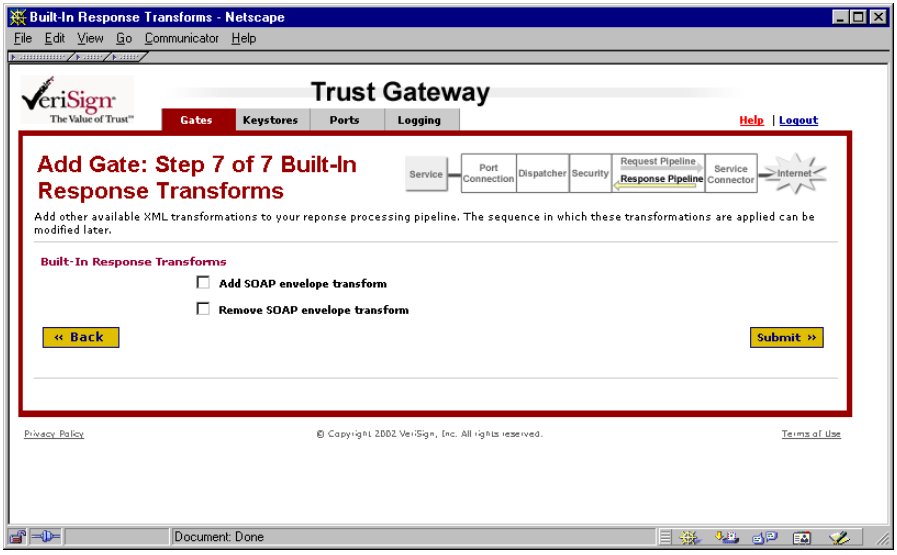


Figure 3-15 *Add Gate: Step 7 of 7 Built-In Request Transforms* page

2 Click **Submit**.

## Step 8 Review and Confirm the Settings

1 The *Edit Gates* page appears, displaying the settings you configured for this service provider gate (Figure 3-16). Review the settings on this page. If you need to make any changes, click **Edit** next to the appropriate section and make the required changes. Click **Delete** to delete the entire gate.

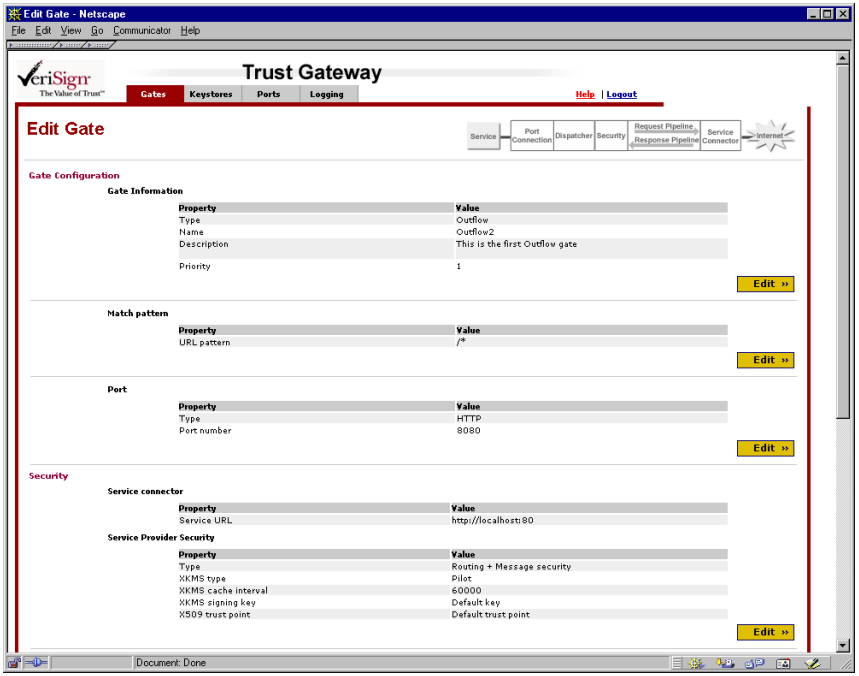


Figure 3-16 Top half of the *Edit Gate* page

2 When you are finished reviewing and editing these settings, click **Done**. The *Gates* page displays.

3 Click **Deploy** to restart the Trust Gateway and apply this new business partner gate. You will need to log in to the Trust Gateway once the gateway has restarted.

If you are also adding a service provider gate, you can add the service provider gate, then click **Deploy** to create both gates at one time.

**Note** For Solaris and Linux installations, you must be logged in as root to deploy a gate.

Click **Revert** to delete the changes and return to the previously saved configuration.

## Editing the Gateway Configuration File

You can edit the configuration file associated with the service provider and business partner gates (gateway.xml) manually. This allows you to add custom functionality to the service provider and business partner gates. You can also change any of the configuration settings you selected through the Trust Gateway Administration console.

1 To edit this configuration file, click **View/Edit XML** from the *Gates* page. The *Expert Mode* page appears (Figure 3-17), displaying the gateway.xml configuration file.

**IMPORTANT!** The gateway.xml file defines the configuration settings for all service provider and business partner gates configured in the Trust Gateway, and is in XML format. VeriSign recommends that you do not make changes to this file unless you are proficient in XML, and have a working knowledge of the Trust Gateway.

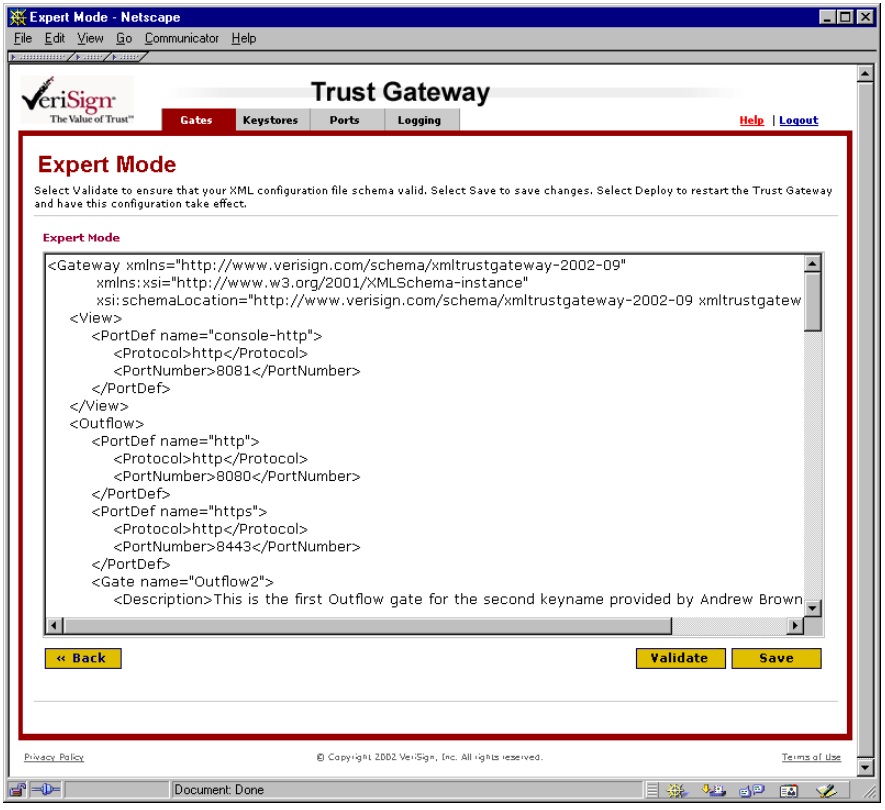


Figure 3-17 *Expert Mode* page

2 Click **Validate** to verify that any changes you made are correctly formatted. Information about the validity of the configuration file will appear in an Information bar at the top of the screen.

3 Click **Save** to save any changes you made.

4 Click **Back** or select the **Gates** tab to return to the *Gates* page.

5 Click **Deploy** to apply these changes. The Trust Gateway restarts, and you will need to log back in to the Trust Gateway.

Click **Revert** to delete the changes and return to the previous configuration.

# Managing Keys, Trust Point Certificates, and Keystores

Keystores are files containing the keys and trust point certificates (CAs) used by the Trust Gateway. You can have multiple keystores, each containing multiple CAs and keys. To manage keystores, click the **Keystores** tab. The *Manage Keystores* page opens (Figure 3-18), listing all the keystores available in the Trust Gateway.

From this page you can add keystores or view keystores (where you can add a key or trust point certificate, revoke a key or trust point certificate, generate a key, or add a certificate).

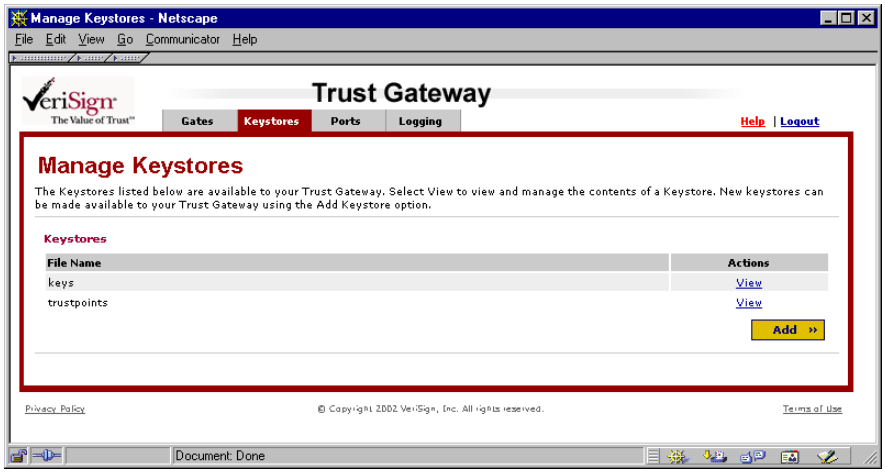


Figure 3-18 *Manage Keystores* page

## Adding a Keystore

You can add standard Sun JKS keystores using these procedures.

1 From the *Manage Keystore* page, click **Add**. The *Add Keystore* page opens.

2 Complete this page and click **Add**. Table 3-3 describes the input required for this page.

Table 3-1 *Add Keystore* page fields

| Field | Input Required |
|---|---|
| File | Enter the path to the file that contains the keystore. You can use the **Browse** button to locate this file. |
| Password | Enter the password protecting the keystore. Use only ASCII character; do not use special characters. Passwords are case-sensitive, and should be a minimum of 6 characters. |
| Confirm password | Retype the password to confirm it. |

## Viewing a Keystore

From the *Manage Keystores* page, click **View** next to the keystore you want to examine. The *View Keystore* page opens, displaying a list of all the keys or trust point certificates saved in the keystore.

From this page, you can revoke a key or trust point certificate, set it as the default, or add a key or trust point certificate.

### Setting the Default Key or Trust Point Certificate

To set a specific key or trust point certificate as the default for all outgoing messages, click the **Set As Default** link next to the key name.

### Revoking a Key or Trust Point Certificate

1 From the *View Keystore* page, click the **Revoke** link next to the name of the key or trust point certificate you want to revoke. The *Revoke Key* page opens.

2 Enter the revocation password into the text field and then select whether this key or trust point certificate was generated from a production or pilot XKMS service.

3 Click **Submit** to revoke the key or trust point certificate.

**Note** You cannot revoke the default key or trust point certificate.

## Adding a Key

You can add PKCS#12 formatted, single entry private keys (with or without the associated public key) using these procedures. There are two methods of adding a key: uploading an existing key, or enrolling for a new key.

### Uploading a Key

Complete these steps to upload an existing key. You must have the key's PKCS #12 file stored to a local drive to upload the key.

1 From the *View Keystore* page, select **Upload key** and click **Add**.

2 The *Add Key* page opens. Complete this page and click **Submit**. Table 3-2 describes the input required for this page.

**Note** You can only add a key to the keys keystore. Refer to "Adding a Trust Point" on page 49 for instruction on uploading a trust point.

Table 3-2 *Add Key* page fields

| Field | Input Required |
|---|---|
| PKCS#12 file | Enter the path to the PKCS#12 file that contains the key. You can use the **Browse** button to locate this file. |
| PKCS#12 password | Enter the password protecting the PKCS#12 file. Use only ASCII characters; do not use special characters. Passwords are case-sensitive, and should be a minimum of 6 characters. |
| Confirm PKCS#12 password | Retype the password to confirm it. |
| Save as keystore alias | Enter a unique keystore name where the key will be stored. Use only ASCII characters 0 - 9, and a - z. Do not use spaces, A - Z, or special characters. |
| Keystore password | Enter a password to protect the keystore. You will need this password to perform any operations with the keys stored in this keystore. |
| Confirm keystore password | Retype the password to confirm it. |
| Key password | Enter a password to protect this key. You will need this password to perform any operations with this key. |
| Confirm key password | Retype the password to confirm it. |

## Enrolling for a New Key

Complete these steps to enroll for a new key. You must have the key name and passcode (obtained from the Managed PKI administrator) to complete these steps.

1 From the *View Keystore* page, select **Generate and register key** and click **Add**.

2 The *Enroll for a New Key* page opens. Complete this page and click **Submit**. Table 3-3 describes the input required for this page.

The Trust Gateway generates the public portion of the key, then submits an XML certificate to VeriSign. VeriSign generates the certificate and returns it to the Trust Gateway, where it is installed in the keystore.

Table 3-3 *Generate and Register Key* page fields

| Field | Input Required |
|---|---|
| Key Name | Enter the key name you created, or that you obtained from VeriSign (**xkms-interop@verisign.com**). |
| XKMS passcode | Enter the XKMS passcode you created, or that you obtained from VeriSign (**xkms-interop@verisign.com**). |
| Keystore alias | Enter a unique name for the keystore. Use only ASCII characters 0 - 9, and a - z. Do not use spaces, A - Z, or special characters. |
| Password for alias | Enter a password for the default keystore. Use only ASCII characters; do not use special characters. Passwords are case-sensitive, and should be a minimum of 6 characters.<br>You will need this password to perform any operations with the keys stored in this keystore. |
| Confirm password for alias | Re-enter the password for the default keystore. |
| XKMS revocation password | Enter a revocation password. You will need this password in the event you need to revoke the keys in the default keystore. |
| Confirm XKMS revocation password | Re-enter the revocation password for the default keystore. |
| XKMS service | Select whether this key and service will be used on a pilot or production system. Select pilot for the Beta release. |

### Adding a Trust Point

You can add X.509 (v.1, v.2, and v.3), or Base64 encoded DER encoded ASN.1 with beginning and ending headers using these procedures.

1 From the *View Keystore* page, select **Upload Certificate** and click **Add**. The *Add Certificate* page opens.

2 Complete this page and click **Submit**. Table 3-3 describes the input required for this page.

**Note** You can only add a trust point to a trust point keystore. Refer to "Uploading a Key" on page 47 for instruction on uploading a key.

Table 3-4 *Add Certificate* page fields

| Field | Input Required |
|---|---|
| Keystore alias | Enter a name for the default keystore. Use only ASCII characters 0 - 9, and a - z. Do not use spaces, A - Z, or special characters. |
| Keystore password | Enter a password to protect the keystore. You will need this password to perform any operations with the certificates stored in this keystore. |
| Confirm keystore password | Retype the password to confirm it. |
| Upload | Select this radio button if you are uploading a certificate from a file. Enter the full path to the file in the **File name** text box (or use the **Browse** button to locate the file). |
| Cut and paste digital certificate | Select this radio button if you are pasting the contents of the certificate from the clipboard. Paste the certificate contents into the **Digital certificate** text box. Include the beginning and ending headers. Please verify. |

## Defining Ports

Which ports your Trust Gateway can use is defined according to the gate type, and the message security type used by that gate. For example, you can define port 80 to all business partner gates that use HTTP, and port 443 to all business partner

gates that use HTTPS. Each time you configure a new business partner gate for HTTPS, it will be assigned port 443.

Your applications connect to your Trust Gateway through the Business Partner ports. Your business partners connect to your Trust Gateway through the Service Provider ports. The Trust Gateway Administration console connects to the Trust Gateway server using the console port. When you installed Trust Gateway, your Trust Gateway Administration console was assigned port 8081, and your business partner gate was assigned port 8080.

You can change the port definitions for each gate and message security type, or retain the default ports. Aside from the following exceptions, the ports you define are solely at your discretion, and depend on how your hardware is installed, how your Web services are configured, and what ports you have available.

- Do not share ports with other applications. If any other application uses the same port assigned to a gate, the gate will not function correctly.
- Your business partners will need to configure their business partner gates to communicate with your service provider gates, so they will need to be aware what ports you set for your service provider gates.
- Although multiple gates can share a port, no two port definitions can share the same port. For example, your service provider HTTP port definition cannot share the same port as your service provider HTTPS port. Each row on the *Define Ports* page (Figure 3-19) is a port definition.
- If you define a port but do not configure a gate for that definition (for instance, you define both HTTP and HTTPS ports for the business partner gate, but only deploy an HTTP business partner gate), the port will not be activated.
- SSL ports are disabled until a key with the alias tomcat is added to the keys keystore.

You can change these ports, and the ports for any other gate you have installed in your Trust Gateway, using the *Define Ports* page.

1. Select the *Ports* tab. The *Define Ports* page appears.
2. Enter the port number in the text box to the right of the gate you wish to change.
3. Click **Submit**.

4 Return to the *Gates* screen (by selecting the *Gates* tab) and click **Deploy**. Ports are not active until you deploy the associated gate.

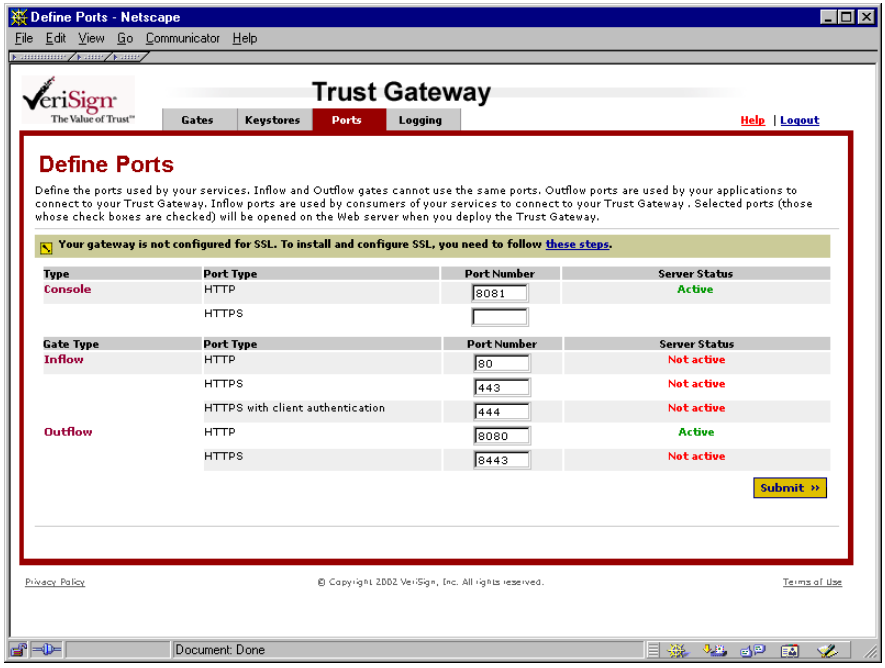


Figure 3-19 *Define Ports* page

# Setting Logging Levels and Output

The Trust Gateway logs all transactions it processes, and all events that happen to the Trust Gateway. You can set the level of detail the logs contain, as well as the location where the logs are written.

## Set Logging Level

Set the level of detail the Trust Gateway logs for each transaction using the following steps:

1 Select the **Logging** tab.

The *Logging* page opens (Figure 3-20).

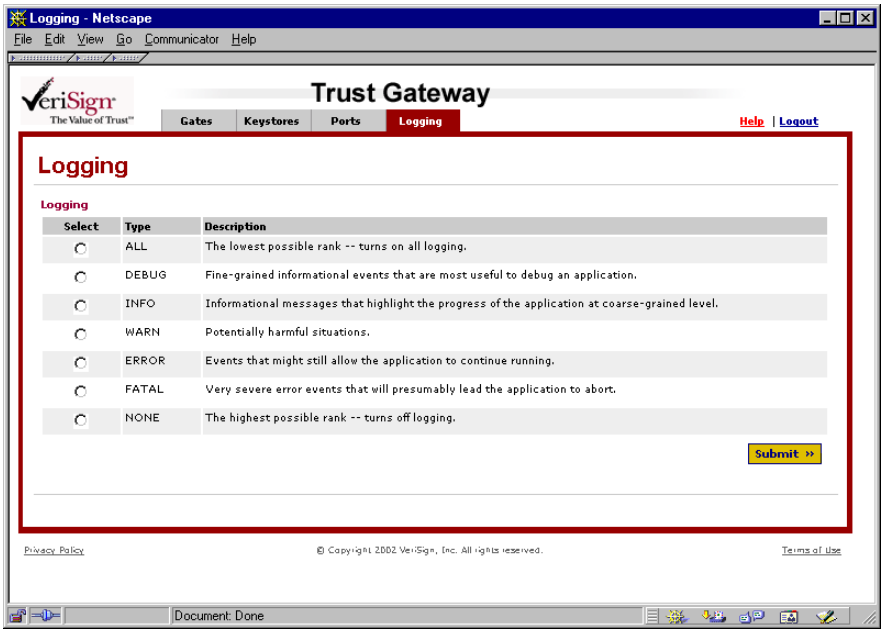


Figure 3-20 *Logging* page

2 Select the level of detail desired. The levels of detail are:

- **All**. The log will capture all possible transaction details.
- **Debug**. The log will capture the details most useful to debug the Trust Gateway.
- **Info**. The log will capture general details needed to track how the Trust Gateway is functioning.
- **Warn**. The log will capture details on potentially harmful events.
- **Error**. The log will capture details on events that hinder the Trust Gateway or transaction, but which may still allow the Trust Gateway to function.
- **Fatal**. The log will capture only severe error events that typically cause the Trust Gateway to fail.
- **None**. The log will capture no transaction details.

3 Click **Submit**.

## Set the Log File Output Directory

The Trust Gateway logs are written to <Trust Gateway installation directory>/logs by default. You can manually change the directory the log file are written to by editing the log4j.xml file.

CHAPTER 4

# Distribution

Before your business partners can access your Web services through the Trust Gateway, they must install a business partner gate at their location. This business partner gate must be configured with the same security settings as the service provider gate at your location that they will access.

You will need to provide the following to your business partners so that they can install the business partner gate.

- Trust Gateway Business Partner Gate CD, including the client business partner gateway software.
- The configuration file for the business partner gate, describing the security setting for the business partner gate
- The key name and passcode for the client certificate associated with the business partner gate (issued by Managed PKI)
- Instructions for installing the business partner gate

Additional information and the client software required to set up a business partner gate are not available with the Beta release. To set up a business partner gate at a remote location (for testing purposes only), you must install the full Trust Gateway at the remote location.

APPENDIX A

# Service Connector API

This appendix describes how to configure additional service connectors (such as HTTPS, SSL, or a custom protocol handler) with Trust Gateway.

Instructions for configuring additional service connectors is not available with the Beta release.

APPENDIX B

# Configuring XML Functionality

This feature is not available in the Beta release.

# Index

## N



## O



## P



## Q



## R



## S

## T



## U



## V

## W



## X


VeriSign®
The Value of Trust℠

www.verisign.com