Version 7.1

Layer 7 Installation and Maintenance Manual

(Appliance Edition)

LAYER 7 TECHNOLOGIES

1.800.681.9377
info@layer7tech.com
www.layer7tech.com

Contents

List of Figures

List of Tables

Chapter One: Overview

About This Manual

The *Layer 7 Installation and Maintenance Manual* provides:

- Basic product information
- Gateway operations, system requirements, configuration, maintenance, upgrade, and troubleshooting information and instructions

> **Note:** This manual describes only the appliance form factor of the Gateway. The software form factor has more limited capabilities and is described in a separate edition of the *Layer 7 Installation and Maintenance Manual*.

- SecureSpan XML VPN Client system requirements and installation and upgrade information and instructions
- Policy Manager system requirements and installation and upgrade information and instructions
- Installation license agreement and technical support contact information.

> **Note:** This Manual does not discuss how to install or configure custom assertions on the Gateway. For this information, see the *Custom Assertion Installation Manual*. For information on using the custom assertions, see the *Layer 7 Policy Authoring User Manual*.

Audience and Assumptions

The *Layer 7 Installation and Maintenance Manual* is intended for facility coordinators, security managers, and other IT infrastructure staff familiar with:

- The hardware and software infrastructure that will be used with the Layer 7 products, such as firewalls, Layer 2 or Layer 3 switches, routers, Load Balancers, databases, identity management or access control systems, application servers, and more
- Advanced TCP-IP and internetworking concepts, web services, and user management knowledge

Overview of Layer 7 Products

The Layer 7 product suite is composed of three interoperable products that protect applications exposed as web services, connect applications across security and identity domains, and validate policy compliance across a transaction:

SecureSpan Gateway/CloudSpan Gateway
SecureSpan XML VPN Client
Layer 7 Policy Manager

Tip: See *Production Network Architecture* on page 9 for a diagram of the Layer 7 products in a typical network configuration.

The **SecureSpan Gateway/CloudSpan Gateway** is a hardware-accelerated XML firewall and service gateway designed to protect web services, accelerate XML operations, and mediate communications between SOA clients and services residing in different identity, security, or middleware domains. For more information, see *Chapter Two: About the Gateway*. (**Note:** The term “Gateway” is used throughout the remainder of this user manual to refer to both the SecureSpan and CloudSpan Gateways.)

The **SecureSpan XML VPN Client** is a cross-domain enablement product designed to speed and secure web services integrations spanning identity and security domains. The SecureSpan XML VPN Client is available as software for Red Hat Enterprise Linux or Microsoft Windows server environments. For more information, see *Chapter Six: Install and Upgrade the SecureSpan XML VPN Client.*

The **Layer 7 Policy Manager** is a GUI-based application that allows administrators to centrally define, provision, verify, and audit fine-grained security and connectivity policies for cross-domain web services and XML integrations, on the Gateway. The Policy Manager is available as software for Red Hat Enterprise Linux or Microsoft Windows server environments. There is also a browser-based version that requires no additional installation. For more information, see *Chapter Seven: Install and Upgrade the Policy Manager*.

Supported Standards

Please refer to *www.layer7tech.com* for a list of the standards supported by the Layer 7 product suite.

Gateway Licenses

WARNING

Do not modify the license XML. If the license file provided by Layer 7 Technologies is changed, then the Gateway will not be able to verify the signature and install the license.

Access to the Gateway is controlled by a signed XML license file that will be delivered separately to you. Each license file is unique to a specific Gateway installation.

If a license is not installed or if an existing license expires, then the Gateway and Policy Manager revert to unlicensed mode. In this mode, all Policy Manager features are disabled except for viewing audit logs and installing a license.

You can view the license at any time from the Policy Manager [Help] menu. See *Managing Gateway Licenses* in the *Layer 7 Policy Manager User Manual* for license installation and viewing instructions.

Layer 7 Documentation

The Layer 7 products are supported by the following documentation:

Table 1: Layer 7 Documentation

Documentation	Target Product(s)	Format(s)	Description
Layer 7 Installation and Maintenance Manual	Gateway, XML VPN Client, and Policy Manager	PDF	Installation and upgrade information for the Layer 7 products, including Gateway maintenance, operations, monitoring, and troubleshooting information and instructions. There are separate editions of this manual for the appliance (including virtual) and software Gateways.
Layer 7 Policy Manager User Manual	Policy Manager	PDF	Comprehensive user instructions for the Policy Manager (excluding documentation on policies and assertions, which are split off into the *Layer 7 Policy Authoring User Manual*).
Layer 7 Policy Authoring User Manual	Policy Manager	PDF	Comprehensive instructions on using policies and the policy assertions in the Policy Manager.
Policy Manager Help System	Policy Manager	Online help	Comprehensive user instructions for the Policy Manager (contains the contents from both the *Layer 7 Policy Authoring User Manual* and *Layer 7 Policy Manager User Manual).*

Documentation	Target Product(s)	Format(s)	Description
SecureSpan XML VPN Client User Manual	SecureSpan XML VPN Client	PDF	Comprehensive user instructions for the SecureSpan XML VPN Client.
SecureSpan XML VPN Client Help System	SecureSpan XML VPN Client	Online help	Comprehensive user instructions for the SecureSpan XML VPN Client.
Custom Assertion Installation Manual	Gateway	PDF	Instructions for installing and configuring the optional custom assertion packages on the Gateway. User instructions for the custom assertions are provided in the Policy Manager documentation.
Release Notes	All	PDF	Summarizes new features and enhancements contained in release. Lists significant bug fixes and provides upgrade instructions.
Read Me file	All	Text file	Contains the system requirements and the End User license agreement.

Chapter Two: About the Gateway

The Gateway is an XML firewall and service gateway that controls how web services are exposed to and accessed by external client applications. The Gateway provides runtime control over service-level authentication, authorization, key management, credentialing, integrity, confidentiality, schema validation, content inspection, data transformation, threat protection (including integration with external virus scanners for SOAP attachment scanning), routing, protocol switching, SLA enforcement, logging, and other functions.

Configured and managed through the GUI-based Policy Manager, the Gateway also acts as an integration point for extending existing PKI, Identity, SSO, federation and MOM infrastructures to web services, ensuring customers can leverage existing security and messaging infrastructure for web services and SOA initiatives.

The Gateway is available as a software application running on select operating system and as a preconfigured hardware appliance for optimal performance (see *Form Factors* on page 9). This Manual describes the appliance implementation of the Gateway.

Note: The information in this chapter applies to the four different versions of the Gateway: *XML Accelerator, XML Data Screen, XML Firewall and VPN,* and *SOA Networking Gateway*. To learn about the differences in functionality between these versions, refer to *Features by Product* in the *Layer 7 Policy Manager User Manual*.

Gateway Architecture

The working unit of the Gateway is an HTTP, JMS, or FTP-accessible endpoint. Clients access the Gateway via a URL or queue that is compatible with one of the above protocols. The Gateway functions as a reverse proxy for service requests and should be the single web service traffic enforcement point in a network.

Note: Due to the number of subsystems involved, changes made in the Policy Manager may require up to 15 seconds to be reflected in the Gateway.

In a typical network, the Gateway resides in the DMZ (demilitarized zone), shielding downstream services as it enforces pre-defined policy assertions on incoming and outgoing messages. In the Gateway, several interdependent layers work together to enable this end-to-end XML firewalling, security, and service protection.

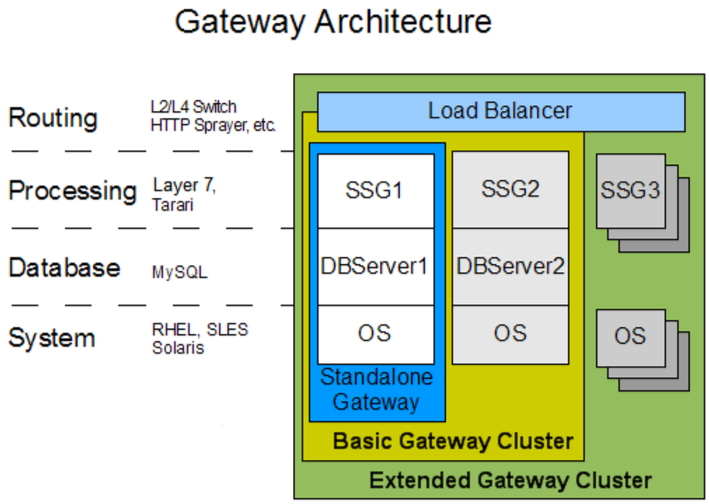


Figure 1: Overview of Gateway architecture

Routing Layer

The Routing Layer represents an industry-standard load balancer configured to provide TCP-level load balancing and failover. It is not required for a standalone Gateway.

Processing Layer

The Processing Layer represents the Gateway's core "runtime" component. When a request message is received, the Gateway executes a service resolution process that attempts to identify the targeted destination service. When a published service is resolved, the Gateway executes the Policy Manager-configured policy for the service. If the policy assertions succeed, then the request is routed; if one or more policy assertions fail, then the request is either denied with a SOAP fault or the connection is dropped.

In a Gateway cluster, systems that are installed with this runtime component are referred to as “Processing Nodes”.

The Processing Layer may also involve the following components:

- Identity Providers
- Trust Store
- UDDI
- Logging and Auditing Functionality
- Hardware Acceleration

Identity Providers

The Gateway uses identity providers to authenticate and identify users and groups when authenticating messages and administrative access. The Gateway can use its built-in identity provider (called the *Internal Identity Provider* or the *Federated Identity Provider* in an identity bridging scenario), or interface directly with any LDAP-based identity provider or, through a custom assertion, connect to and utilize an external identity management system (such as Netegrity SiteMinder or IBM Tivoli Access Manager).

Trust Store

The Gateway maintains a trust store of certificates that do not belong to it but that are trusted and used for one or more vital security functions, such as signing client certificates. Certificates are imported into the Gateway trust store via the Policy Manager. See *Managing Certificates* in the *Layer 7 Policy Manager User Manual* for more information.

UDDI

The Gateway can publish a web service by using a WSDL located in a UDDI (Universal Description, Discovery and Integration) registry. The following UDDI registries are supported:

- Systinet UDDI Registry versions 5.0 and 6.5
- CentraSite UDDI Enterprise Edition version 3.1.5.0
- CentraSite Governance Edition version 7.1

To enable UDDI registry support in the Gateway, see *Configuring UDDI Registry Searches* on page 85 .

Logging and Auditing Functionality

The Gateway provides several logging and auditing features, allowing users to monitor the activity and health of the Gateway, and the ongoing success or failure of service policy resolution. Auditing is provided for all system events, and is configurable for individual service policies. All audit records can be viewed through the Policy Manager. Gateway logging is performed during runtime, and those logs can also be viewed through the Policy Manager. The Manager also features a Dashboard that allows administrators to monitor activity through the Gateway in real-time. For more information, see *Dashboard – Service Metrics* and *Dashboard – Cluster Status* in the *Layer 7 Policy Manager User Manual*.

Hardware Acceleration

The Gateway hardware appliance is equipped with a Tarari RAX PCI-e XML Accelerator Card to enhance performance in these areas:

- XPath expressions
- XML schema validation
- XSL transformations

When the Tarari card is present, the performance of the following assertions will be enhanced:

Apply XSL Transformation
Evaluate Request XPath
Evaluate Response XPath
Protect Against Document Structure Threats
Validate XML Schema

For the most part, hardware acceleration works seamlessly in the background: if the Tarari card is present, all eligible operations are accelerated; no indication is shown on the interface. There are two exceptions: in the *Evaluate Request XPath* and *Evaluate Response XPath* assertions, two levels of acceleration are possible based on the complexity of the XPath expressions. For more information, see the *Layer 7 Policy Authoring User Manual*.

Note: It is possible to disable the Tarari card by adding the following line to the *node.properties* file: **node.tarari.enabled = false**. It is recommended that you consult Layer 7 Technical Support before taking such action.

Database Layer

The Gateway stores policies, processing audits, Internal Identity Provider, keystore, configuration details and other information in a MySQL database. In a typical configuration this database will reside on the same physical system as a Processing Node, although in rare circumstances it may reside on a separate system.

In a Gateway cluster, systems that are installed with the database component are referred to as “Database Nodes”. There will typically be two replicated Database Nodes in a cluster: Primary and Secondary. The Processing Nodes are configured to communicate with one of the Database Nodes (normally the Primary) and then fail over to the Secondary Database Node should the Primary become unavailable.

System Layer

The System Layer represents the Operating System, Java Virtual Machine, and hardware platform. The appliance form factor is based upon a hardened version of Red Hat Enterprise Linux (RHEL) operating system on a Sun Fire server.

Form Factors

The Gateway comes in three different form factors:

- As software that can be installed on servers running Red Hat Enterprise Linux version 4 or 5, SUSE Linux Enterprise Server 10, Sun Microsystems Solaris 10 (both x86 and SPARC). This version is described in the *Layer 7 Installation and Maintenance Manual (Software Edition)*.
- As a 64-bit appliance that requires minimal additional configuration. This is the version that is described in this Manual.
- As an XML virtual appliance running under VMware. Initial configuration and setup of this product is described in the *SecureSpan XML Virtual Appliance Getting Started*. Once set up, use this Manual to administer the virtual appliance.

For more information about each form factor, please visit www.layer7tech.com or contact Layer 7 Technologies.

Production Network Architecture

The unique topology of a production network determines the exact configuration of the Layer 7 products. Nevertheless, most deployments will include the Gateway, XML VPN Client, and Policy Manager in the following network configuration:

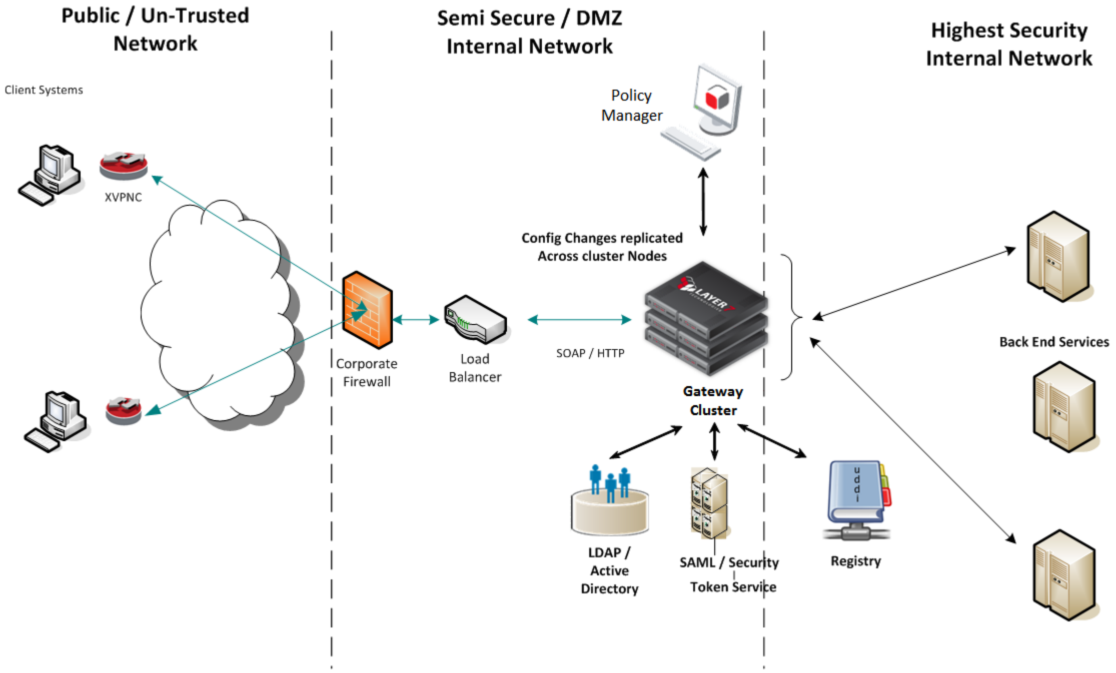

Public / Un-Trusted Network
Semi Secure / DMZ Internal Network
Highest Security Internal Network
Client Systems
XVPNC
Policy Manager
Config Changes replicated Across cluster Nodes
Corporate Firewall
Load Balancer
SOAP / HTTP
Gateway Cluster
Back End Services
LDAP / Active Directory
SAML / Security Token Service
Registry

Figure 2: Product network architecture

Gateway Documentation

There are three sources of Gateway documentation:

- As the administrative application for the Gateway, the Policy Manager documentation contains in-depth information and instructions for almost all Gateway processes, features, and functions.
- Setup and configuration information for the Gateway is described in the *Layer 7 Installation and Maintenance Manual*.
- Instructions for installing and configuring the custom assertion packages in the Gateway are provided in the *Custom Assertion Installation Manual*.

Chapter Three: Configure the Gateway

The Gateway appliance comes preconfigured with the most common settings and requires only minimal additional configuration before it can be started.

Tip: It is highly recommended that you review *Appendix I: Network Deployment Guide* first to gain a better understanding of the various network configurations. This knowledge will help you better configure your Gateways.

Accessing the Gateway Configuration Interface

The Gateway configuration interface is a menu driven wizard used to configure networking and application settings. Additionally, it provides access to the privileged (root) shell and other administrative tasks.

➢ *To access the Gateway configuration interface:*

1. Is there network connectivity to the Gateway appliance?
   - If NO, proceed with step 2.
   - If YES, proceed to step 3.
2. **At the machine (networking not yet set up):**

   If networking is not yet set up, you must either be physically at the Gateway appliance or have remote serial console access. You can access the console of the hardware appliance in one of two ways:

   - Plug in a USB keyboard and monitor.
   - Use a serial connection with the Gateway. For details, see *“Connecting via the Serial Management Port”* on page 14.

   At the login screen, log in as user **ssgconfig** using the default password **7layer**. The configuration menu in Figure 3 appears.

WARNING

You will be prompted to change the password the first time you log in as the “ssgconfig” user. The new password **must** adhere to the rules described under *Password Rules* on page 95.

The “ssgconfig” account will be locked after five (5) unsuccessful login attempts[1]. To reset this account, see *Unlocking the SSGCONFIG* on page 96.

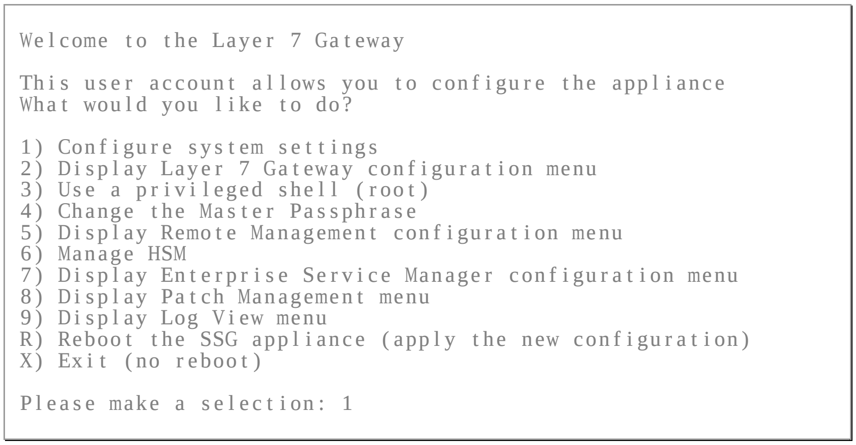
3. **Remotely (networking has been set up):**

   If networking has been set up, you can either log in locally (as described in step 2 above) or remotely connect via SSH to the Gateway as user **ssgconfig**. For example:

   - *Linux:* **ssh ssgconfig@**<*SSG_host*>
   - *Windows:* Use PuTTY or a similar utility

   Note: SSH is possible only through eth0, not eth1.

   The configuration menu in Figure 3 appears. Note that not all options are available in every system—for example, option 6 is displayed only if a Hardware Security Module (HSM) is present.



```
Welcome to the Layer 7 Gateway

This user account allows you to configure the appliance
What would you like to do?

1) Configure system settings
2) Display Layer 7 Gateway configuration menu
3) Use a privileged shell (root)
4) Change the Master Passphrase
5) Display Remote Management configuration menu
6) Manage HSM
7) Display Enterprise Service Manager configuration menu
8) Display Patch Management menu
9) Display Log View menu
R) Reboot the SSG appliance (apply the new configuration)
X) Exit (no reboot)

Please make a selection: 1
```

Figure 3: Layer 7 Gateway main menu

[1] Standard Gateways; lockout counter on custom appliances may differ.

The following table describes each option in the main menu:

Table 2: Gateway main menu

Option	Description
1) Configure system settings	Use this option to view or configure system settings on the Gateway appliance. These settings must be set up before you can configure the Gateway application. For details, see *Configuring System Settings* on page 16.
2) Display Layer 7 Gateway configuration menu	Use this option to configure the Gateway application before starting it. For details, see *Configuring the Gateway Application* on page 20.
3) Use a privileged shell (root)	Use this option to open a command shell with root user privileges. You will need this to perform certain administrative tasks in the Gateway. For more information, see *Using the Privileged Shell* on page 25. The default password is **7layer**.
4) Change the Master Passphrase *(not for nCipher HSM)*	Use this option to change the master passphrase that is used to encrypt the Gateway's database and keystore passwords. If the master passphrase has been changed from the default, you must enter the current passphrase before specifying a new passphrase. The master passphrase must be between 6 and 128 characters in length. You will be prompted to enter the new master passphrase twice. **Hint:** It is best to create a lengthy, easy-to-remember phrase using common words. Store the phrase in a safe location. The default master passphrase is **7layer**. **Note:** The "Change the Master Passphrase" option does not apply if you have a Thales nCipher HSM enabled on the Layer 7 Gateway. To change the master passphrase in this instance, simply disable and then re-enable the nCipher HSM. For more information on how to do this, see option **1** in Table 7 on page 29.
5) Display Remote Management configuration menu	Use this option to configure the Gateway node to be managed remotely. This configuration is required only if the node will be managed by the Layer 7 Enterprise Service Manager. For details, see *Configuring the Gateway for Remote Access* on page 26. **Note:** You must reboot the Gateway (using option **R** below) to apply any configuration changes.
6) Manage HSM	*This option is displayed only if an internal Hardware Security Module (HSM) is present.* Select this option to initialize, enable/disable, or back up the HSM master key to an external USB flash drive (SCA6000), or create/program into a security world (nCipher). For details, see *Managing the Hardware Security Module* on page 27.
7) Display Enterprise Service Manager configuration menu	*This option is available only if the Enterprise Service Manager has been installed on the Gateway machine.* Use this option to configure the Enterprise Service Manager. For details, see *Configuring the Enterprise Service Manager* on page 38.
8) Display Patch Management menu	Use this option to manage patches on the Gateway appliance. For details, see *Managing Gateway Patches* on page 76.

Option	Description
9) Display Log View menu	Use this option to view the various logs available in the system. For details, see *Viewing Logs on the Gateway Appliance* on page *80*.
R) Reboot the SSG appliance (apply the new configuration)	Use this option to exit the menu and reboot the appliance. Any configuration changes made will take effect when the Gateway appliance restarts. **Note:** Be sure to remove any USB flash drive before restarting to prevent boot errors.
X) Exit (no reboot)	Use this option to exit the menu without rebooting. If you have made configuration changes, they will not take effect until you reboot.

Connecting via the Serial Management Port

If your environment does not provide KVM access and DHCP is not available on the network, you can connect to the Gateway for configuration via the ILOM (Integrated Lights Out Manager) by using the Serial Management Port. Note that serial access is command line access only.

➢ *To establish a serial connection:*

1. Connect to the Serial Management Port on the back of the appliance (labeled SER MGT CAT5) using a standard Ethernet cable. This may require using the DB9-RJ45 adapter provided with the appliance. You may need to contact your IT department if you need a CAT5 to DB9 adapter, or a USB to DB9 adapter if your console device (for example, a laptop computer) does not have DB9.
2. Start your terminal program (HyperTerminal, Minicom or similar) to establish a serial connection using the following settings:

   8N1: eight data bits, no parity, one stop bit
   9600 baud
   Disable hardware flow control
   Disable software flow control

3. When the terminal screen appears, press [**Enter**] to display the login prompt. Log in with the following credentials:

   ```
   <hostname> login: root
   Password: changeme
   ```

   The ILOM Command Line Interface (CLI) is displayed. (Note that the same interface is available over SSH on the network or via a serial connection.)

Configuring the ILOM IP Address

The CLI can be used to set the IP address of the ILOM, to enable access to the Web GUI from a static IP on a laptop.

- *To configure the ILOM IP address:*

1. Enter the following command to set the working directory:

```
-> cd /SP/network
```

2. Enter the following commands to configure the network:

```
set pendingipdiscovery=static
set pendingipaddress=192.168.7.7
set pendingipnetmask=255.255.255.0
set commitpending=true
```

3. On the laptop, set the following:

   IP address: 192.168.7.8
   Netmask: 255.255.255.0

You can now access the ILOM user interface at: http://192.168.7.7. Log in with the following:

User Name: root
Password: changeme

For more information using the ILOM, please refer to the *Oracle Integrated Lights Out Manager 3.0 Documentation*, part number E19860-01, at: http://www.oracle.com/technetwork/documentation/sys-mgmt-networking-190072.html.

Preparing the Network

The default Gateway configuration listens on port 8080 for standard service requests and port 8443 for encrypted service requests over SSL. Administrative requests from the Policy Manager take place over port 8443. The browser version of the Policy Manager is accessed by either port 8443 or 9443. If the Gateway node will be configured for remote management, port 8765 is used by default. Before configuring the Gateway, you need to configure your network firewalls to allow for message and administrative traffic.

If the default endpoints are changed during configuration of the Gateway, or later by the Policy Manager, the network firewalls must be reconfigured to reflect these changes.

Cluster Considerations

In a Gateway cluster configuration, the database nodes replicate over port 3307 and are queried over port 3306. Requests between nodes for log viewing and other tasks are performed over port 2124. Replay protection synchronization between nodes is accomplished by multicast UDP port 8777 transmitted on eth0 by each cluster node. While most Gateway cluster nodes will be located in close proximity to each other on a secured network, the network administrators should be aware of these settings and prepare the network accordingly.

Configuring System Settings

The Configure System Settings option in the Gateway main menu (Table 2 on page 13) is used to view and edit the essential network settings for the Gateway appliance and to configure other system settings such as the keyboard layout. Network connectivity must be set up before you can configure the Gateway.

Tip: For illustrations on how the Gateway can be deployed on your network, see *Appendix I: Network Deployment Guide*.

Determining Whether a Default Gateway is Necessary

A default Gateway is a device that accepts packets that have destinations that do not match anything else in the routing table. Most networks do not require a default Gateway since it is implied by your IP address and the network topology.

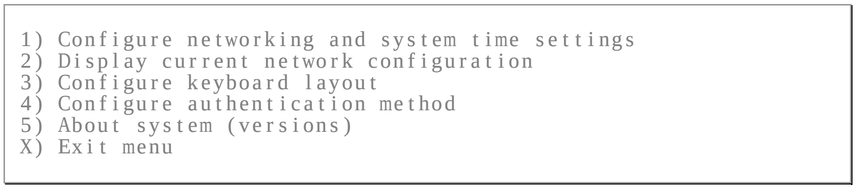
During network configuration, you will be given a chance to configure a default Gateway. Whether you choose to define one now or skip over the step depends on several factors:

- Do you have a single network environment? If so, you can most likely skip defining a default Gateway.
- Do you have a multiple network environment? If so, you may want to define a default Gateway. Network environments with more than one interface will usually have more than one network connected to the machine and the most recently configured interface automatically becomes the default. If you do *not* want this interface to be the default, then you will want to specify a default Gateway.

If in doubt, please consult your network administrator whether a default Gateway is required.

➢ *To configure system settings:*

- Choose option **1** (Configure system settings) from the Gateway main menu (Figure 3 on page 12). The following sub options are available:



```
1) Configure networking and system time settings
2) Display current network configuration
3) Configure keyboard layout
4) Configure authentication method
5) About system (versions)
X) Exit menu
```

See Table 3 below for a description of each option.

Tip: At any time during the configuration, you may type "**quit**" to exit the configuration or "**<**" to return to the previous step.

Table 3: Configure system settings

Option	Description
1) Configure networking and system time settings	User this option to configure networking, the time zone, and time synchronization on your Gateway. 1. The detected interfaces are shown, with their current configuration displayed in brackets. Enter the number of the interface to configure or choose "Configure an unlisted interface" to configure a new interface. 2. If configuring a new interface, enter the name of the interface (e.g., eth1). 3. Specify whether you are configuring an IPv4 interface. **If no, skip to step 6.** 4. Specify the boot protocol for the interface: **static** or **dhcp** (dynamic). 5. If the protocol is **static**, enter the following details for the interface: IPv4 address default IPv4 gateway netmask 6. Specify whether to configure IPv6 networking. If **yes**, continue with step 7. If **no**, you are prompted whether to configure another interface (yes = return to step 1; no = skip to step 10). 7. Specify whether to enable IPv6 auto-configuration for the interface. 8. Specify whether to enable DHCPv6 for the interface. 9. Specify whether to add static IPv6 address(es) for the interface. If **yes**, enter the address(es). If **no**, you are prompted whether to configure another interface (yes = return to step 1; no = skip to step 10). 10. Specify whether to configure a default IPv4 Gateway and interface. Configuring a default Gateway is optional. For more information, see *"Determining Whether a Default Gateway is Necessary"* on page 16. If you enter **yes**, provide the following information: a. Enter the IP address of the Gateway. b. Select the interface to use from the list displayed. c. Enter a fully qualified hostname for the Gateway (for example, *ssg1.mycompany.com*). Note that if this is part of a cluster, this is the name of the *node,* not the cluster. **Note:** If you did not configure a nameserver in step 4 or if the nameserver that was configured does not recognize the hostname entered in step 10, then the hostname may not be resolvable. To prevent this from happening, either configure a nameserver in step 4 or ensure that there is an appropriate entry in */etc/hosts* for this hostname. 11. Enter the fully qualified hostname for the Gateway. 12. Optionally specify whether to configure the DNS name servers. If yes, enter the name servers. If no, proceed to step 13. 13. Specify whether to configure the time zone for the Gateway. By default, the time zone for the appliance Gateway is "America/Vancouver", while the software Gateway uses

Option	Description
	the time zone in effect on the host machine. - If yes, keep selecting from the lists presented until your choice results in a single time zone. - If no, proceed to the next step in the configuration. 14. Specify whether to configure time synchronization on the machine. Time synchronization is an essential system setup step for clustering and replay attack prevention. - If yes, enter the IP address or hostname of the NTP time server. **Note:** If networking is already configured, you can enter the name of the timeserver here and the configurator will attempt to determine the associated address for you. - If no, proceed to the next step in the configurator. 15. Carefully review the configuration settings. - To make corrections, type **<** to return to a previous step. - To discard all your entries and exit the configurator, type **q** or **quit**. - To accept your configuration settings, press the [**Enter**] key. If the configuration results contain errors, analyze the errors and run option 1 again. **Note:** To apply the configuration changes, you must restart the Gateway. Use option **R** from Table 2.
2) Display current network configuration	User this option to see details for the current network configuration. Use it to confirm that the network was configured correctly. If changes are required, run option **1** (Configure networking and system time settings). Press [**Enter**] to return to the menu.
3) Configure keyboard layout	User this option to choose a keyboard layout for the Gateway. 1. By default, the Gateway uses the U.S. keyboard layout. If you need to load a different layout, enter **yes** or press [**Enter**] to proceed to step 2, otherwise enter **no** to skip to configuring the network interfaces. 2. The first page of keyboard choices is displayed. Enter the number for the layout to load, or press [**Enter**] to view the next page of choices. You may need to press [**Enter**] several times to find your layout.
4) Configure authentication method	Use this option to configure the authentication method for users on this machine. Choose from the following options: - **Local System:** Authenticate user accounts locally, disabling any external authentication method. This is the default. - **RADIUS only:** Authenticate users over the RADIUS protocol. You will be prompted to enter the following: address of the RADIUS Server RADIUS shared secret RADIUS timeout (in seconds) **Note:** Using RADIUS-only authentication provides only a basic means to create a centralized authentication service that is not as secure as other methods.

Option	Description
	• **LDAP(S) only:** Authenticate users against an LDAP(S) server. You will be prompted to enter the following: Specify if directory service used is Active Directory use LDAP securely address of the LDAP server LDAP server port LDAP base DN LDAP Bind DN (if not enabling Anonymous Bind) LDAP Bind Password (if not enabling Anonymous Bind) LDAP Group Name (contains the users granted access to the Gateway) LDAP Group ID (contains the users granted access to the Gateway) LDAP object used to find password for users LDAP object used to find groups for users LDAP object used to find shadow entries for users LDAP server CA certificate location URL of the PEM containing certificate File containing PEM formatted certificate LDAP TLS option Handling the server's certificate Customize the PAM login attribute name PAM login attribute name • **RADIUS with LDAP(S):** Authenticate users over the RADIUS protocol with user information coming from LDAP(S). You will be prompted to enter the following: use LDAP securely address of the RADIUS Server RADIUS shared secret RADIUS timeout (in seconds) address of the LDAP server LDAP server port LDAP base DN LDAP bind DN (if "no anonymous bind" set to NO) LDAP bind password (if "no anonymous bind" set to NO) LDAP Group Name (contains the users granted access to the Gateway) LDAP Group ID (contains the users granted access to the Gateway) LDAP object used to find password for users LDAP object used to find groups for users LDAP object used to find shadow entries for users LDAP Server CA certificate location: URL of the PEM containing certificate File containing PEM formatted certificate LDAP TLS option Handling the server's certificate Customize the PAM login attribute name PAM login attribute name Review the configuration summary and press [**Enter**] to continue. **Notes:** (1) When authenticating using RADIUS and/or LDAP, authentication will fall back to local authentication if communication with RADIUS or LDAP is not possible or if authentication fails. (2) You must restart the Gateway appliance after changing authentication methods. Use option "**R**" from the Gateway main menu (see Figure 3 on page 12). After the system restarts, the chosen authentication method becomes the default.

Option	Description
5) About system (versions)	Use this option to view the version numbers of the installed Layer 7 software.

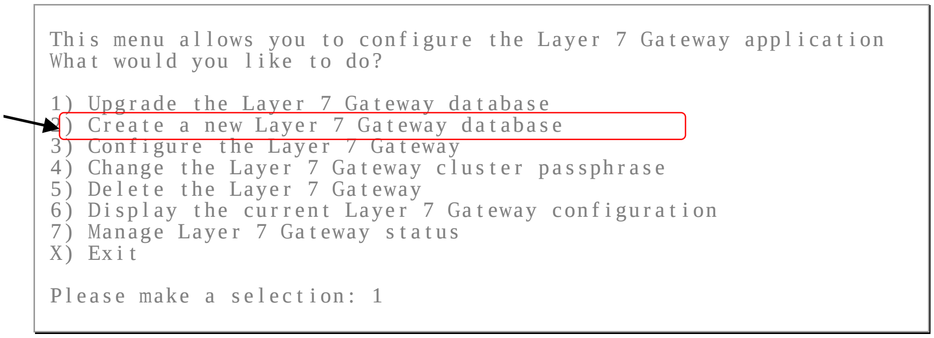
Configuring the Gateway Application

Note: The procedure described in this section is suitable for configuring a single stand-alone Gateway or to configure the first node of a cluster of Gateways after replication has been configured. If you are configuring a cluster of Gateways, be sure to read *Chapter Four: Configure a Gateway Cluster* for instructions on setting up replication and configuring the processing nodes.

WARNING

If you are configuring the first node of a cluster, ensure that the database layer has been properly configured for replication and tested. Failure to do this will require complex steps to enable proper operation of the cluster. Replication is described in *Configuring Database Replication* on page 51.

To configure a single Gateway or the first processing node of a cluster, select option 2 from the Gateway main menu (Figure 3 on page 12). You are presented with the following options:



```
This menu allows you to configure the Layer 7 Gateway application
What would you like to do?

1) Upgrade the Layer 7 Gateway database
2) Create a new Layer 7 Gateway database
3) Configure the Layer 7 Gateway
4) Change the Layer 7 Gateway cluster passphrase
5) Delete the Layer 7 Gateway
6) Display the current Layer 7 Gateway configuration
7) Manage Layer 7 Gateway status
X) Exit

Please make a selection: 1
```

Use this option to configure a new stand-alone Gateway or the first processing node of a Gateway cluster.

Figure 4: Configure Layer 7 Gateway menu

Using the Embedded Database

When creating a new Gateway database, you have the option of configuring a connection to a MySQL database or using the built-in embedded (non-MySQL) database on the Gateway.

The embedded database is designed for environments where it is not possible to have a separate MySQL instance. For example, your security policy may forbid operating MySQL or any other network-accessible SQL database, even on *localhost*.

The embedded database is also ideal for testing or evaluating the Layer 7 Gateway, as it can be set up quickly, without relying on an external database.

Note the following limitations when an embedded database is in effect:

- Multi-node clustering is not available—the Gateway will behave as a single-node cluster.
- Service metrics are not available (see "Dashboard – Service Metrics" in the *Layer 7 Policy Manager User Manual).*
- The Audit Archiver is not available (see "FTP Audit Archiver" in the *Layer 7 Policy Manager User Manual*).
- The Layer 7 OAuth Toolkit can be used on a Gateway with an embedded database only if MySQL is also available.

The following table describes each menu option from Figure 4. When configuring a new stand-alone Gateway or first processing node of a Gateway cluster, you only need to use option **2**, *Create a new Gateway database*.

Table 4: Configure Gateway menu options

Option	Description
1) Upgrade the Layer 7 Gateway database	Select this option to upgrade the Gateway database to the current software version. This is required only if you've installed a new version of the Gateway. If an upgrade is not required, you will be notified by a message on the screen.
2) Create a new Layer 7 Gateway database	Select this option to create a database for the first (or only) Gateway node in the cluster. When configuring a database connection, you will be guide through the following steps: • Set Up the Gateway Database • Set Up the Gateway Failover Database • Set Up the SSM Administrator • Set Up the Gateway Cluster • Set Up the Gateway Node Fewer prompts are displayed when using the embedded database. **Note:** Once the new Gateway database is created, you can no longer use option 2 on that cluster. To modify the configuration afterwards or to add additional processing nodes, use option 3, *Configure the Gateway*. To delete the Gateway configuration and start over again, use option 5, *Delete the Gateway*.
2) Create a new Layer 7 Gateway database → **Database Connection**	Enter **yes** to configure a connection to a MySQL database. This is the default. Enter **no** to use the embedded database (see "Using the Embedded Database" on page 20). The first prompt you will see is "Set Up the SSM Administrator" (page 22).
2) Create a new Layer 7 Gateway database → **Set Up the Gateway**	Enter information about the new MySQL database: • **Database Host:** Enter the name of the database host. If the database is installed on the same server as the Gateway, you can press [**Enter**] to accept

Option	Description
Database *(Only applies to MySQL database connections)*	**localhost**. If setting up the first node of a cluster, accept "localhost" as the primary database node. You can enter the secondary database node in the next step ("Set Up the Gateway Failover Database"). • **Database Port:** Enter the port number or press [**Enter**] to accept the default port **3306**. • **Database Name:** Enter a distinct name to define the Gateway database name or press [**Enter**] to accept the default name **ssg**. • **Database Username:** Enter the name of the user who has access to the database. The default name is **gateway**. • **Database Password:** Define a password for the database user, then retype to confirm. • **Administrative Database Username:** Enter the username of the root MySQL user. The default user is **root**. • **Administrative Database Password:** Enter the password for the root MySQL user.
2) Create a new Layer 7 Gateway database → **Set Up the Gateway Failover Database** *(Only applies to MySQL database connections)*	For MySQL database connections, you can optionally configure a failover database. • **Configure Database Failover Connection:** Enter **yes** to configure a database failover connection or press [**Enter**] to enter "no" and skip to the next part of the configuration. • **Database Failover Host:** Enter the host name of the machine that will serve as a database failover. • **Database Failover Port:** Enter the port number to use on the failover host, or press [**Enter**] to accept the default port **3306**.
2) Create a new Layer 7 Gateway database → **Set Up the SSM Administrator**	Create a Policy Manager administrative user account: • **SSM Username:** Enter the name of the Policy Manager administrative user. • **SSM Password:** Define a password for the administrative user, then retype to confirm. For information on logging in with these credentials, see *Connecting to the Gateway* in the *Layer 7 Policy Manager User Manual*.
2) Create a new Layer 7 Gateway database → **Set Up the Gateway Cluster**	Enter the host name and password for the Gateway cluster. **Note:** A stand-alone Gateway or a Gateway with an embedded database is considered to be a "cluster" of one. • **Cluster Host:** Enter the Gateway cluster fully qualified domain name (FQDN) used to identify the Gateway and to generate the SSL certificate. An example of a hostname: *clusterhostname.mycompany.com*. • **Cluster Passphrase:** Enter a passphrase to protect the cluster, between 6-129 characters. Retype to confirm. **Tip:** If you need to change the cluster hostname, you cannot do it using this menu option once it has been set. Instead, perform these steps using the Layer 7 Policy Manager to change a cluster host name:

Option	Description
	1. Set the cluster property *cluster.hostname* to the new name of the host. 2. Create a new private key using the *Manage Private Keys* task. Be sure to set this key as the default SSL key. For more information, see *Creating a Private Key* and *Private Key Properties* in the *Layer 7 Policy Manager User Manual*. 3. Restart all nodes in the cluster for the new cluster host name to take effect.
2) Create a new Layer 7 Gateway database → **Set Up the Gateway Node**	Set up the Gateway node: • **Enabled:** Press [**Enter**] to enable the node, or enter **no** to leave the node disabled after configuration is complete. The configuration summary is displayed. Carefully review the settings and then press [**Enter**] to confirm. To make corrections, enter **<** to return to the appropriate step in the wizard.
2) Create a new Layer 7 Gateway database → **Configuration Results**	The configuration results show either: • **Success:** Press [**Enter**] to return to the Configure Gateway menu. Enter **X** to exit the menu, and then enter **R** on the main menu to reboot the appliance. You may now start the Gateway (see page 39). • **Errors encountered:** Copy and paste the log messages from the command window into a text file. Analyze the errors and run the wizard again. If you require assistance, contact Layer 7 Technical Support.
3) Configure the Layer 7 Gateway	Use this option to do one of the following: • Edit the settings for a Gateway node that has already been configured. • Add a new processing node to a cluster. Select which settings to change: • Enter **1** to change the database connection. For details, see *"Create a new Gateway database → Database Connection"* above. • Enter **2** to change the database failover connection. For details, see *"Create a new Gateway database → Set Up the Gateway Failover Database"* above. • Enter **3** to change the password for the cluster. For details, see *"Create a new Gateway database → Set Up the Gateway Cluster"* above. • Enter **4** to change the node configuration. For details, see *"Create a new Gateway database → Set Up the Gateway Node"* above. When this option is used to add a new processing node to a cluster, you are prompted to enter the following: Database Host Database Port Database Name Database Username Failover Database Host (optional) Failover Database Port (optional) Cluster Password For more information on each of these fields, see *Configuring Subsequent Gateway*

Option	Description
	Processing Nodes on page 55.
4) Change the Layer 7 Gateway cluster passphrase	Select this option to change the passphrase for the Gateway cluster. a. Type the existing password. b. Enter the new password, between 6 to 128 characters. c. Retype the password to confirm. **IMPORTANT NOTE FOR SAFENET LUNA HSM:** If the Gateway is using the SafeNet HSM device, you must disable support for the SafeNet HSM prior to changing the master passphrase, then re-enable support afterwards. To do this, use the *Manage Keystore* task in the Policy Manager. For more information, see *Managing Keystore* in the *Layer 7 Policy Manager User Manual*.
5) Delete the Layer 7 Gateway	Select this option to delete the configuration for the Gateway node. • If the node being deleted is also the host for the primary database, the database can be optionally deleted by entering database administration credentials. • If the database is not deleted, you can reuse it at a later time by using option 3, *Configure the Gateway*. **IMPORTANT:** Deleting the configuration is permanent. All information in the database will be lost. Enter **yes** to proceed with the deletion.
6) Display the current Layer 7 Gateway configuration	Select this option to view the current Gateway configuration. The following information is displayed: • Database hostname • Database port • Database name • Database user name • Whether the node is enabled
7) Manage Layer 7 Gateway status	Select this option to view the current Gateway status or to stop/restart the Gateway. The following information is displayed initially: • Current status of the Gateway node, which is one of: • STARTING – Node is starting up • WONT_START – Node encountered an unrecoverable error when starting • RUNNING – Node is running normally • ABNORMAL_SHUTDOWN – Node shut down unexpectedly • STOPPING – Node is stopping • STOPPED – Node is stopped • Current time stamp • When the node was started Press [**Enter**] to display options that allow you to: • Stop the Gateway (if currently running)

Option	Description
	• Start the Gateway (if currently stopped) • Restart the Gateway **IMPORTANT:** You should always stop and restart the Gateway using these menu options or by using the command line equivalents (*“service ssg stop”* and *“service ssg restart”*). *Never* stop a Gateway by turning off the appliance or use the appliance power switch to restart the Gateway.

Using the Privileged Shell

The Gateway uses menus to help guide you through most of the configuration tasks. However, it may be necessary to access the command line of the underlying Red Hat Enterprise Linux OS to accomplish specific configuration and administration tasks. This is the purpose of the privileged shell. This shell is identical to logging in as the root user of the OS and grants you complete control of the system. **It is assumed that anyone entering the privileged shell is familiar with the Linux command line and is comfortable with executing commands.**

➢ *To use the privileged shell:*

1. Select option **3** (Use a privileged shell) from the Gateway main menu (see Figure 3 on page 12).
2. Enter the required commands.
3. Enter **exit** to close the shell.

WARNING

When using the privileged shell, you must exercise ***extreme*** caution, as an incorrect or mistyped command may render the system unusable.

WARNING

Changes made at the OS level may be lost when the system is upgraded. It is important to accurately record any privileged shell actions for reimplementation after an upgrade has been performed.

Root User Password

You will be required to change the password the first time you log in as the root user. The new password must adhere to the rules described under *Password Rules* on page 95.

WARNING

The root account will be locked after five (5) unsuccessful login attempts. If this happens, please contact Layer 7 Technical Support for assistance.

Configuring the Gateway for Remote Access

If the Gateway node will be managed remotely by the Layer 7 Enterprise Service Manager, select option **5** from the Gateway main menu (Figure 3 on page 12) and then complete the options in Table 5.

Note: You must restart the Gateway for configuration changes to take effect. Use option **R** in Table 2.

Table 5: Configure Gateway for remote access

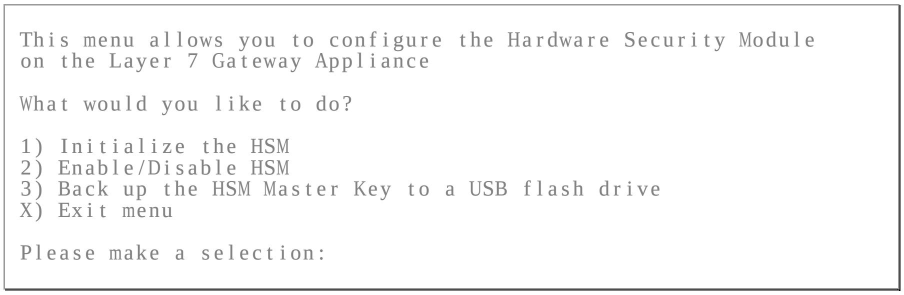
Option	Description
1) Listener IP Address	Select this option to enter the IP address of the Internal Management LAN. This is the "eth0" interface shown in the diagrams under "Network Deployment Guide", located in Appendix J. **Tip:** If the IP of eth0 is not readily available or if your deployment contains only a single network interface, enter "*****" (asterisk) or "**localhost**" as the listener IP address.
2) Listener Port	Select this option to change the listening port from the default "8765". **Note:** Ensure that the IP address/port number combination is valid and is not used by another process. **Tip:** The listen port is stored in the cluster property *node.processControllerExternalPort*. You can update this listen port in the future by modifying the cluster property.
3) Remote Node Management Enabled	Select this option to enable or disable remote management for the node: • To enable remote management, enter **yes**. • To disable remote management, enter **no**. By default, remote management is disabled on all nodes.
4) New Trusted Certificate 4) Delete Trusted Certificate	Select this option to enable trust between the node and the Enterprise Service Manager that will be remotely controlling it. Option 4 will read "**New Trusted Certificate**" if trust has not yet been established. Once trust is established, it will read "**Delete Trusted Certificate**".

Option	Description
	To enter a new trusted certificate: 1. Do one of the following: • Enter the URL from which to download the trusted certificate; for example: *https://acmecorp.domain.com:8182* This downloads the certificate from the Enterprise Service Manager and stores it as a trusted certificate on the Gateway. **Tip:** The ESM port number is defined using option **7** (Display Enterprise Service Manager configuration menu) in Table 2 on page 13. • Enter the thumbprint of the SSL certificate from the Enterprise Service Manager. This thumbprint is visible on the [Settings] tab > System Settings page of the ESM. This thumbprint method offers the flexibility of establishing trust without dealing with firewall issues associated with opening another port. **Note:** If you enter a thumbprint, you can only review the thumbprint—the other certificate details are not yet available. 2. Examine the certificate details and enter **y** to accept it. **Note:** A node can be remotely managed by only one Enterprise Service Manager at (ESM) a time. To change the ESM that is managing a node, first delete the trusted certificate and then add a new trusted certificate. *To delete a trusted certificate:* • Enter **y** to confirm the deletion. Once the certificate is deleted, you can use option 4 again to enter the trusted certificate from another ESM.

Managing the Hardware Security Module

If a Hardware Security Module (HSM) is installed on the Gateway appliance, you can use option **6** from the Gateway main menu (Figure 3 on page 12). Refer to the section for your HSM.

Sun Crypto Accelerator 6000 PCIe HSM



```
This menu allows you to configure the Hardware Security Module
on the Layer 7 Gateway Appliance

What would you like to do?

1) Initialize the HSM
2) Enable/Disable HSM
3) Back up the HSM Master Key to a USB flash drive
X) Exit menu

Please make a selection:
```

Figure 5: Configure SCA6000 HSM menu

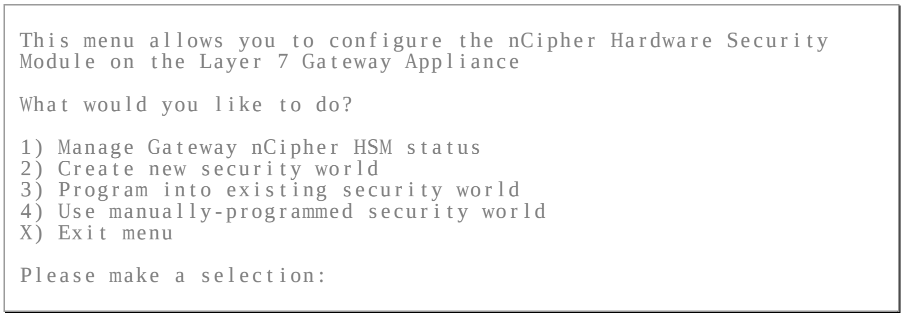
Refer to the following table for a description of each menu option:

Table 6: Managing the SCA6000 card

Option	Description
1) Initialize the HSM	Select this option to initialize (restart) the SCA6000. You are warned that initializing the HSM will delete all data. • Enter **1** to generate a new master key. • Enter **2** to import an existing one from a USB flash drive (be sure drive is plugged in) and then enter the master key password when prompted.
2) Enable/Disable HSM	Select this option to disable or enable the HSM. A Hardware Security Module must be present and configured. Press [**Enter**] to confirm the enable/disable. • When the HSM is enabled, either the SCA6000 or SafeNet Luna HSM (if available) is used. For more information, see *Managing Keystores* in the *Layer 7 Policy Manager User Manual*. • When the HSM is disabled, the software keystore becomes the system default. **Tip:** If you have the SafeNet Luna HSM, ensure the Luna jar files are copied over to the Gateway prior to enabling the HSM: cd /usr/lunasa/jsp/lib cp libLunaAPI.so Luna*.jar /opt/SecureSpan/JDK/jre/lib/ext
3) Back up the HSM Master Key to a USB flash drive	Select this option to back up the master key to an external USB flash drive. Ensure the USB flash drive is plugged in before proceeding. You will be prompted to enter a password to protect the master key backup.

Thales nCipher HSM

Note: The Gateway does not currently support AES-GCM when using a Thales nCipher Hardware Security Module with a custom FIPS level 3 security world.



```
This menu allows you to configure the nCipher Hardware Security
Module on the Layer 7 Gateway Appliance

What would you like to do?

1) Manage Gateway nCipher HSM status
2) Create new security world
3) Program into existing security world
4) Use manually-programmed security world
X) Exit menu

Please make a selection:
```

Figure 6: Configure nCipher HSM menu

Refer to the following table for a description of each menu option:

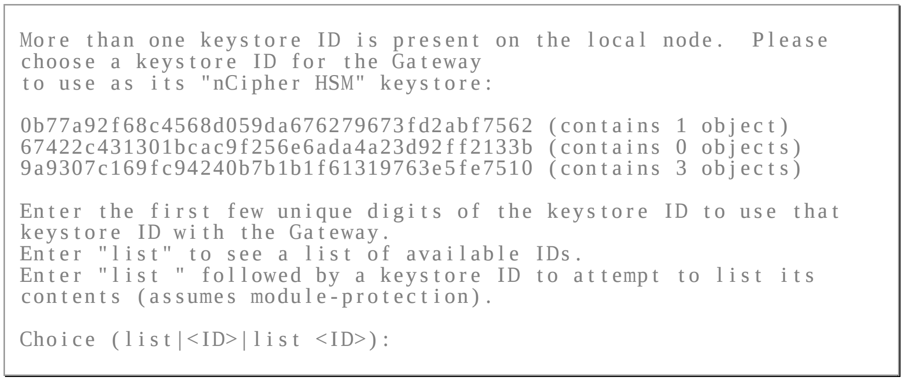
Table 7: Managing the nCipher card

Option	Description
1) Manage Gateway nCipher HSM status	Select this option to enable or disable Gateway use of nCipher. • Enter **1** to enable Gateway use of the nCipher HSM. Enabling nCipher on a Gateway will generate a new random master passphrase, using the nCipher module's hardware random number generator. The database password and the cluster passphrase are automatically re-encrypted with the new master passphrase. • Enter **2** to disable Gateway use of the nCipher HSM. Disabling nCipher on a Gateway will reset the master passphrase back to the default **7layer**. You can change the passphrase using option 4 in Table 2 on page 13. When nCipher is disabled, the Gateway will revert to using the software DB as its default keystore. If a SafeNet Luna HSM has been configured, it is used instead.
2) Create new security world	Select this option to initialize the nCipher card and create a new security world cardset. You will choose this option if there is no existing security world in which to program the card. 1. Ensure that the card read is connected to the nCipher HSM and that the module switch on the HSM is in the "I" position (pre-initialization mode). The initialization will require at least three blank cards. 2. Press [**Enter**] to proceed. 3. Insert the blank cards when prompted and be sure to make note of the passphrase used to protect each card. These will be needed to program additional modules (or to reprogram this one) into the security world. 4. When the initialization is complete, set the module switch to the "O" position (operational mode). 5. Disconnect the card reader and then enable the HSM as prompted using option **1** (Manage Gateway nCipher HSM Status). 6. Exit to the Gateway main menu (Figure 3 on page 12). Select option **2** (Display Layer 7 Gateway configuration menu) to display the Configure Layer 7 Gateway menu (Figure 4 on page 20). Select option **7** (Manage Layer 7 Gateway status) to restart the Gateway. **Note:** If you lose access to the security world, you will need to re-enter the database password and cluster passphrase. If you no longer have the cluster passphrase, please contact Layer 7 Technical Support.

Option	Description
3) Program into existing security world **Note:** To use this option, the Gateway node should be configured to use a database that already contains a security world.	Select this option to program the nCipher card into an existing security world. You will need at least two cards from the security world's cardset, along with the passphrases. 1. Ensure that the card reader is connected to the nCipher HSM and that the module switch on the HSM is in the "I" position (pre-initialization mode). 2. Press [**Enter**] to proceed. 3. Insert the cards and enter the passphrase as prompted. 4. When the initialization is complete, set the module switch on the HSM to the "O" position (operational mode). 5. Disconnect the card reader and then enable the HSM as prompted using option **1** (Manage Gateway nCipher HSM Status). 6. Exit to the Gateway main menu (Figure 3 on page 12). Select option **2** (Display Layer 7 Gateway configuration menu) to display the Configure Layer 7 Gateway menu (Figure 4 on page 20). Select option **7** (Manage Layer 7 Gateway status) to restart the Gateway.
4) Use manually-programmed security world **Note:** To be able to use this option, you must either have manually created a new security world on the nCipher module or programmed the module into an existing security world. For details, see *"How to Manually Set Up the nCipher Card"* on page 31.	Select this option to direct the Gateway to use a security world that has already been manually programmed. Press [**Enter**] to proceed. The configurator checks the status of a security world in the database and takes the following actions: • **No world information present in database:** If the database does not contain an nCipher security world, the new world is simply copied to the database. Press [**Enter**] to continue when prompted. • **Matching world information already in database:** If the database already contains a matching security world, no further action is required. Press [**Enter**] to continue when prompted. • **Conflict with security world in database:** If the database already contains a different security world, you are prompted to delete it and replace it with the security world on the disk. Type "**proceed**" (without the quotes) to continue. Entering anything else will cancel the process. **Note:** You may be prompted to choose a keystore ID. For details, see *"Choosing a Gateway Keystore"* on page 30.

Choosing a Gateway Keystore

When enabling nCipher support with a manually-programmed security world (option **4** in Table 7), you may be prompted to choose a keystore ID to be used by the Gateway as the "nCipher HSM" keystore. This will occur if the database does not yet contain a designated keystore ID and more than one keystore ID is present.



```
More than one keystore ID is present on the local node.  Please
choose a keystore ID for the Gateway
to use as its "nCipher HSM" keystore:

0b77a92f68c4568d059da676279673fd2abf7562 (contains 1 object)
67422c431301bcac9f256e6ada4a23d92ff2133b (contains 0 objects)
9a9307c169fc94240b7b1b1f61319763e5fe7510 (contains 3 objects)

Enter the first few unique digits of the keystore ID to use that
keystore ID with the Gateway.
Enter "list" to see a list of available IDs.
Enter "list " followed by a keystore ID to attempt to list its
contents (assumes module-protection).

Choice (list|<ID>|list <ID>):
```

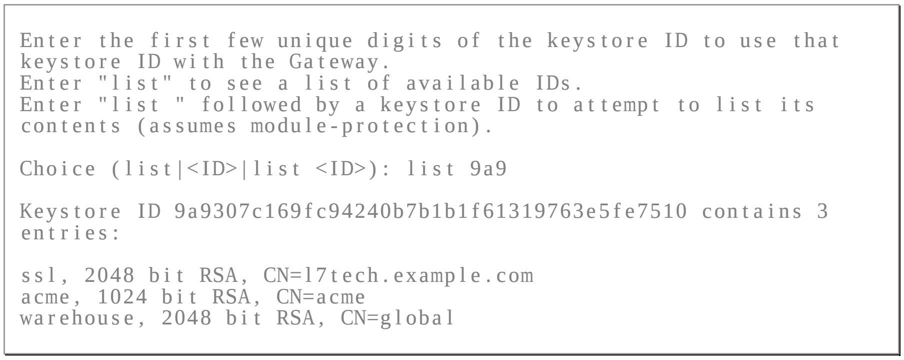
Figure 7: Choosing a Gateway keystore

Select one of the following:

- Enter **list** to redisplay the list of available keystore IDs.
- Enter **list** *<ID>* to view the contents of a particular keystore ID (see below for details)
- Enter the *<ID>* of a keystore to select it. You do not need to enter the entire ID—just the first few unique characters. Using the example IDs shown in Figure 7, simply entering the first character of the ID would be sufficient.

Using the "list <ID> command

You may be able to inspect the contents of a particular keystore by entering "list" followed by the first few unique characters of the keystore ID—for example: **list 9a9**.



```
Enter the first few unique digits of the keystore ID to use that
keystore ID with the Gateway.
Enter "list" to see a list of available IDs.
Enter "list " followed by a keystore ID to attempt to list its
contents (assumes module-protection).

Choice (list|<ID>|list <ID>): list 9a9

Keystore ID 9a9307c169fc94240b7b1b1f61319763e5fe7510 contains 3
entries:

ssl, 2048 bit RSA, CN=l7tech.example.com
acme, 1024 bit RSA, CN=acme
warehouse, 2048 bit RSA, CN=global
```

Figure 8: Using the "list <ID>" command

After inspecting the keystore, you can either enter its ID to select it, or use the **list** command to redisplay the list of available keystore IDs or inspect another keystore.

How to Manually Set Up the nCipher Card

In order to use option **4** ("Use manually programmed security world") in Table 7, there must either be a manually created security world on the nCipher module or a module has been programmed into an existing security world. Follow the appropriate scenario below.

Setting Up NetHSM and nShield Connect

For instructions on how to manually configure a NetHSM or nShield Connect, please refer to the user documentation provided by Thales. When you have completed setting up the nShield Connect and configuring the security world, the Layer 7 Gateway will be ready to work with nShield Connect; you only need to use option **4** in Table 7 to instruct the Gateway to use the manually preconfigured security world.

Scenario 1: Your Gateway appliance or soft appliance is using a network-attached nShield Connect

Note: Use of an nShield Connect from a Gateway appliance that is already equipped with an internal HSM is not supported.

Please refer to the *nShield Connect Quick Start Guide* provided by Thales for information on setting up the Gateway to use nShield Connect. Note the following however:

- Clear any existing data in *kmdata/local* using these commands:

  a. Log in as *ssgconfig* and open a privileged command shell from the Gateway configuration menu (see Figure 3 on page 12).

  b. At the command prompt, enter:

  ```
  # cd /opt/nfast/kmdata/local
  # rm –f *
  ```

- You do not need to install the nfast client software, as it will already be present on appliances that were shipped with nCipher cards.

- If you are using the Gateway as an RFS server, you must configure the Gateway's IP-level firewall to permit access. See *"Using the Gateway as an RFS Server"* on page 33 for more details.

- If you are using the Gateway as a client only (relying on another Gateway to be the RFS server), do the following:

  a. Perform the steps under *"Setting up client cooperation"* in the *nShield Connect User Guide*. This sets up the client to synchronize with the RFS server.

  b. Log in as *ssgconfig* and open a privileged command shell from the Gateway configuration menu (see Figure 3 on page 12).

  c. Run the following command to update the RFS files to local storage:

  ```
  # /opt/nfast/bin/rfs-sync –-update
  ```

  d. Run the following command to set the permissions for the updated files:

  ```
  # chown gateway.nfast key_jcecsp*
  ```

  These steps populate *kmdata/local* with the *kmdata/local* files from the RFS server.

Other notes to consider:

- If the nShield Connect is not yet initialized, see “Basic configuration of the nShield Connect” under “Basic software setup” in the nShield Connect Quick Start Guide.
- To configure the nfast client software to use the nShield Connect, see *“Configuring cooperation”* under *“Basic software setup”* in the *nShield Connect Quick Start Guide*.

You can verify that the nfast client software on the Gateway appliance is correctly configured to use a security world with nShield connect by running the following commands after restarting the Gateway appliance:

```
# /opt/nfast/bin/enquiry
# /opt/nfast/bin/nfkminfo
```

For the “enquiry” command, look for these lines:

```
Module #1:
[…]
mode            operational
```

For the “nfkminfo” command, look for these lines:

```
World
[…]
state       […] Usable […]
[…]
Module #1
State       […] Usable
```

Once verified, you can configure the Gateway to use the HSM by running option **4** in Table 7.

Using the Gateway as an RFS Server

To use the Gateway appliance as an RFS (Remote File System) server, you will need to allow access through the Gateway's IP firewall. You can do this by either by temporarily turning off the firewall or by adding a rule to allow incoming RFS connections.

➢ *To turn off the Gateway’s IP firewall:*

1. Log in as *ssgconfig* and open a privileged command shell from the Gateway configuration menu (see Figure 3 on page 12).
2. At the command prompt, enter:

```
# service ssg stop
# service iptables stop
```

This turns off the firewall. The firewall will be automatically re-enabled the next time the Gateway appliance is restarted.

Note: Confirm with your system administrator that it is safe to disable the Gateway's IP firewall.

➢ *To edit the firewall to permit incoming RFS connections:*

1. Locate and open the following file in a text editor:

   /etc/sysconfig/iptables

2. Add an allow rule for the desired port on the desired interface about the line "ADD CUSTOM ALLOW RULES HERE".

   For example, to allow inbound RFS connections on the default port of 9004 on the appliance's private-side network interface, add a rule similar to the following:

```
# Allow inbound nShield Connect RFS connections on private interface
[0:0] -A INPUT -i eth0 -p tcp -m tcp --dport 9004 -j ACCEPT
#
# ADD CUSTOM ALLOW RULES HERE
#
```

3. Save and close the *iptables* file and then enter the following command to make the changes effective:

```
# service iptables restart &
```

Scenario 2: Your Gateway appliance has an internal nShield HSM

The instructions in this section are intended only for an internal nCipher module and not a NetHSM or nShield Connect. For information about setting up one of these other products, please refer to the nCipher documentation.

➢ *To manually create a new security world on a Gateway appliance internal HSM:*

Tip: You do not need to manually create a security world if you are using a Gateway appliance internal nCipher HSM unless you wish to customize the security world settings.

1. Before deleting any existing world from the module, ensure you have performed any administrative operations that require the security world. (For example, erasing any operator cards you may have manually created. Note that worlds created via the nCipher HSM menu (Figure 6) only use administrator cards and do not use any operator cards.) If the existing security world will be reused, ensure that its administrator cards are stored in a safe place and that the previous contents of *kmdata/local* are backed up.

   If necessary, clear any existing nCipher data from the Gateway database using the instructions under *"How to Manually Clear the Database" on page 37"*.

2. Log in as *ssgconfig* and open a privileged command shell from the Gateway configuration menu (see Figure 3 on page 12).

3. At the command prompt, enter the following commands to delete any existing data in *kmdata/local*:

```
# cd /opt/nfast/kmdata/local
# rm –f *
```

4. Ensure that the module switch on the back of the HSM is in the “I” position (pre-initialization mode).

Tip: You can query the current status of the module switch by running these commands:

```
# /opt/nfast/bin/nopclearfail ca
# /opt/nfast/bin/enquiry -m 1 | grep mode
```

The screen will display messages such as “mode operational” or “mode pre-initialization” depending on the position of the switch.

5. Reset the module by entering this command:

```
# /opt/nfast/bin/nopclearfail ca
```

6. Create a new security world with this command:

```
# /opt/nfast/bin/new-world -m 1 -s 0 -Q 2/3 -k rijndael
```

This creates a world on the first module that is FIPS Level 2 compliant, creating three administrator cards, any two of which must be inserted in order to authorize certain administrative actions.

7. Follow the instructions displayed by the new-world command, inserting administrator cards as prompted.

8. Change the module switch on the back of the HSM to the "O" position (operational mode).

9. Reset the module again:

```
# /opt/nfast/bin/nopclearfail ca
```

10. Check the security world with this command:

```
# /opt/nfast/bin/nfkminfo
```

The “World” section at the top should show a “state” similar to:

```
Initialised Usable Recovery !PINRecovery !ExistingClient RTC NVRAM
FTO SEEDebug StrictFIPS140
```

➢ *To manually program a Gateway appliance internal nCipher HSM into an existing security world:*

Tip: You do not need to manually program an existing security world if you are using a Gateway appliance internal nCipher HSM and are configuring a node from a cluster that already contains nCipher security world information in its database.

1. Before deleting any existing world from the module, ensure you have performed any administrative operations that require the security world. (For example, erasing any operator cards you may have manually created. Note that worlds created via the nCipher HSM menu (Figure 6) only use administrator cards and do not use any operator cards.) If the existing security world will be reused, ensure that its administrator cards are stored in a safe place and that the previous contents of *kmdata/local* are backed up.

2. If necessary, clear any existing nCipher data from the Gateway database using the instructions under *"How to Manually Clear the Database" on page 37*.

3. Log in as *ssgconfig* and open a privileged command shell from the Gateway configuration menu (see Figure 3 on page 12).

4. At the command prompt, enter the following commands to delete any existing data in *kmdata/local*:

```
# cd /opt/nfast/kmdata/local
# rm –f *
```

5. Copy the following files to */opt/nfast/kmdata/local*.

   - Your existing security world's "world" file.

   - *(Optional)* A single "key_jcecsp_*YYYY*" file (where "YYYY" is the keystore ID) for your existing keystore ID created within the existing security world either by the Gateway or by a Java program using the KeyStore.nCipher.sworld KeyStore type

   - *(Optional)* One or more "key_jcecsp_*YYYY*-key-*ZZZZ*" files (where "ZZZZ" is a hexadecimal identifier), one for each private key entry within your existing keystore ID.

Note: The owner and group of all the *key_jcecsp* files must be *gateway* and *nfast*, respectively. If not, permission denied errors will occur when the Gateway is restarted. To set this, use the following command:

```
# chown gateway.nfast key_jcecsp*
```

6. Ensure that the module switch on the back of the HSM is in the "I" position (pre-initialization mode). To check the current status of the module switch, see the "Tip" in step 4 on page 35.

7. Reset the module by entering this command:

   ```
   # /opt/nfast/bin/nopclearfail ca
   ```

8. Program the module into the existing security world with this command:

   ```
   # /opt/nfast/bin/new-world --program --module=1
   ```

9. Follow the instructions displayed by the new-world command, inserting existing administrator cards as prompted.

10. Change the module switch on the back of the HSM to the "O" position (operational mode).

11. Reset the module again:

    ```
    # /opt/nfast/bin/nopclearfail ca
    ```

12. Check the security world with this command:

    ```
    # /opt/nfast/bin/nfkminfo
    ```

    The “World” section at the top should show a “state” similar to:

    ```
    Initialised Usable Recovery !PINRecovery !ExistingClient RTC NVRAM
    FTO SEEDebug StrictFIPS140
    ```

How to Manually Clear the Database

If the Gateway database contains an existing keystore ID within the desired security world, it will use that keystore ID instead of one that may already be present in *kmdata/local*.

➢ *To clear all nCipher security world and keystore information from the database:*

, issue the following two commands as root on one of the cluster nodes (after the node has already been configured into the cluster):

1. On a configured cluster node, log in as *ssgconfig* and open a privileged command shell from the Gateway configuration menu (see Figure 3 on page 12).

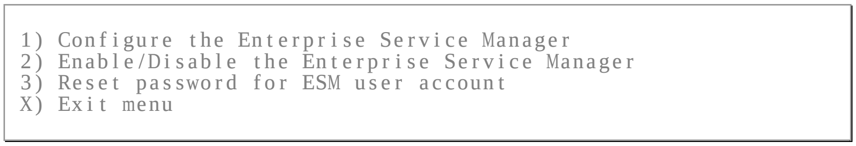
2. At the command prompt, enter the following two commands (note each command is entered on a single line):

   ```
   # /opt/SecureSpan/Appliance/libexec/ssgconfig_launch -keystoreProperty
   clear 4 worldb64
   ```

   ```
   # /opt/SecureSpan/Appliance/libexec/ssgconfig_launch -keystoreProperty
   clear 4 databytes
   ```

Configuring the Enterprise Service Manager

The Enterprise Service Manager is a separate application from Layer 7 Technologies that can remotely manage Gateway clusters located anywhere in the world. To configure the Enterprise Service Manager prior to first use, select option **7** from the Gateway main menu (Figure 3 on page 12). The following sub options are available:



```
1) Configure the Enterprise Service Manager
2) Enable/Disable the Enterprise Service Manager
3) Reset password for ESM user account
X) Exit menu
```

- Select **1** to configure the administrator credentials and listener port for the Enterprise Service Manager. Refer to Table 8 to complete the configurator.
- Select **2** to disable or re-enable the Enterprise Service Manager. This will take effect after the appliance is rebooted (option “R” in Table 2 on page 13).
- Select **3** to reset the password for any Enterprise Service Manager user. Use this option if the password is forgotten. The Enterprise Service Manager must not be currently running. Enter the **ESM Username** and new **ESM Password** when prompted, and then press [**Enter**] again to confirm the change.

Table 8: Configure Enterprise Service Manager

Configurator Step	Description
Set Up the Enterprise Service Manager Administrator	Create the ESM administrative user account. • **ESM Username:** Enter the name of the ESM administrator, between 3-128 characters. • **ESM Password:** Enter the password for the ESM user, between 6-128 characters. Retype to confirm.
Set Up the ESM HTTPS Listener	Next, you are prompted for the server settings for the Enterprise Service Manager. By default, the factory settings are: monitor all IP addresses (*) over port 8182. • To accept the factory settings or to configure the settings later, press [**Enter**] to indicate that you are not overriding the defaults. • To override the factory settings, type **yes** and then press [**Enter**]. • Enter the IP address for the HTTPS listener or press [**Enter**] to use all available addresses. • Enter the port number for the HTTPS listener or press [**Enter**] to use the default port “8182”. **Remember this port number.** **Tip:** Ensure that the port number is not currently in use. Do not use any reserved port numbers such as 8080, 8443, 9443, etc.
Configuration Summary	The configuration summary is displayed. If any changes are required, type “**<**” to go to the previous step or press [**Enter**] to apply the configuration.

Configurator Step	Description
Configuration Results	The configuration results should show that the settings were applied successfully. Press [**Enter**] to return to the previous menu, then enter [**x**] to return to the Gateway main menu. From the main menu, enter **R** to reboot the Gateway appliance and then enter **yes** to confirm.

Once the initial setup is complete, the next step is to configure each Gateway node to allow it to be remotely managed by Enterprise Service Manager. For details, see *Configuring the Gateway for Remote Access* on page 26.

Starting and Stopping the Gateway

The Gateway may need to be stopped and restarted when performing certain maintenance tasks. (Note that as a service, the Gateway does not log messages to the console or screen.)

Stopping the Gateway

➢ *To stop the Gateway:*

1. Log in as *ssgconfig*. The Gateway main menu appears (see Figure 3 on page 12).

1. Choose option **2** (Display Gateway configuration menu). The Gateway configuration menu appears (see Figure 4 on page 20).

2. Choose option **7** (Manage Gateway status). The current status of the Gateway is displayed. Press [**Enter**] to continue.

3. Select the option to stop the Gateway. It may take a moment for the Gateway to stop completely. Use option **7** to monitor the stoppage ("STOPPING" indicates the node is still stopping; "SDTOPPED" indicates the node has stopped).

Tip: You can also run "service ssg stop" from a privileged shell to stop the Gateway node.

Starting the Gateway

➢ *To start the Gateway:*

1. Log in as *ssgconfig*. The Gateway main menu appears (see Figure 3 on page 12).

2. Choose option **2** (Display Gateway configuration menu). The Gateway configuration menu appears (see Figure 4 on page 20).

3. Choose option **7** (Manage Gateway status). The current status of the Gateway is displayed. Press [**Enter**] to continue.

4. Select the option to start the Gateway. It may take a moment for the Gateway to fully start. Use option **7** to monitor the startup ("STARTING" indicates the node is still starting; "RUNNING" indicates the node is up and running normally).

Tip: You can also run "service ssg start" from a privileged shell to start the Gateway node.

Configuring Autostart on Reboot

The Gateway normally starts automatically after the appliance is rebooted.

➢ *To disable autostart on reboot:*

1. Log in as *ssgconfig*. The Gateway main menu appears (see Figure 3 on page 12).
2. Choose option **2** (Display Gateway configuration menu). The Gateway configuration menu appears (see Figure 4 on page 20).
3. Choose option **3** (Configure the Gateway).
4. Choose option **4** (Change node configuration).
5. Enter **no** to disable the node. The Gateway will no longer start automatically upon reboot.

➢ *To enable autostart on reboot:*

- Repeat the steps under "disable autostart" above. In step 5, enter **yes** to enable the node. The Gateway will automatically start upon reboot.

Troubleshooting Gateway Start

If you are attempting to debug Gateway start issues, you can use the "run" mode to log each step of the startup sequence. This log will help Layer 7 Technical Support troubleshoot your issue.

Note: The "run" option described below should only be used while troubleshooting; it is not intended for production use.

➢ *To start the Gateway in debug mode:*

1. Open a privileged shell. For more information, see *Using the Privileged Shell* on page 25.
2. Enter the command:

```
./runtime/bin/gateway.sh run
```

You will see messages similar to:

```
[gateway@ssg Gateway]$ ./runtime/bin/gateway.sh run Apr 3, 2009
3:42:24 PM com.l7tech.server.ServerConfig <init>
INFO: Couldn't find serverconfig_override.properties; continuing with
no overrides Apr 3, 2009 3:42:26 PM com.l7tech.server.boot.GatewayBoot
start
INFO: Starting Layer 7 SecureSpan Suite 5.0 build ...
```

These messages are output to the console as well as recorded in the log file.

3. To stop the Gateway and exit the debug mode, press [Ctrl]-C.

Using Windows Domain Login

Using the Gateway in a Windows Domain Login configuration requires configuring the Active Directory server, then installing the keytab file.

Note: Ensure that any user who requires access to the Windows service has a domain account.

➢ *To configure the Gateway to use Windows Domain login:*

1. On the Active Directory machine, create a principal for the Windows service and then map it to the host using the **ktpass** command:

   ```
   ktpass –princ http/<Gateway_host>@<Realm> –mapuser <userName> -pass
   <userPassword> –out <keytab_name>
   ```

   For example:

   ```
   ktpass -princ http/gateway.domain.com@DOMAIN.COM -mapuser gateway
   -pass password -out kerberos.keytab
   ```

   This produces the output file *kerberos.keytab*.

2. Install the keytab file using the “Manage Kerberos Configuration” task in the Layer 7 Policy Manager.

   For more information, see “Managing Kerberos Configuration” in the *Layer 7 Policy Manager User Manual*.

Working with Multiple Service Principal Names

The Layer 7 Gateway can be configured to handle multiple Service Principal Names in a Kerberos keytab file. This will allow the Gateway to perform Kerberos authentication in these scenarios:

- One Gateway cluster which has been assigned multiple DNS host names, each with their own Virtual IP (VIP):

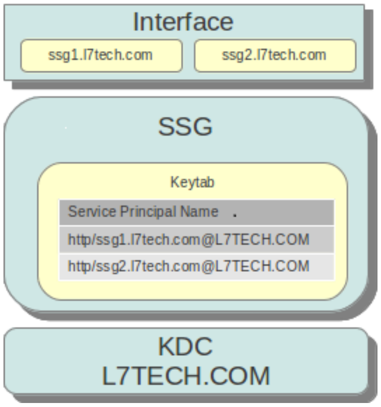


Figure 9:Kerberos multiple hostnames

- Multiple domains:

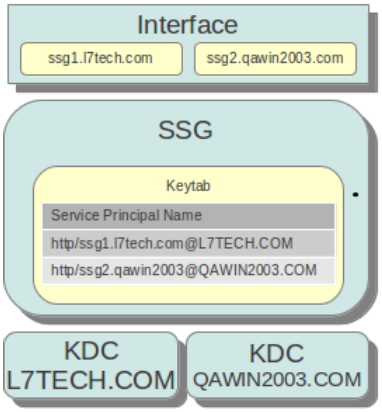


Figure 10: Kerberos multiple domains

- Routing to multiple domains (via the [Target] tab in the *Route via HTTP(S)* assertion).

How the Principal is Determined

When multiple service principals are defined, this is how the Gateway determines which principal in the keytab to use:

Require Windows Integrated Authentication Credentials Assertion

For this assertion, the Gateway will use the request URL to determine which principal in the keytab will be used to handle the Windows authentication.

Example: For a request for the *http://ssg1.acmecorp.com/test.html* page, the Gateway will look up the service principal *http/ssg1.acmecorp.com* from the keytab file.

Route via HTTP(S) Assertion

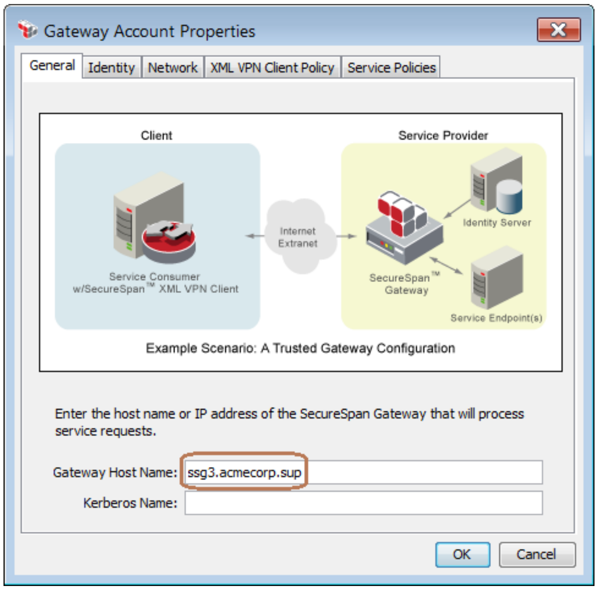
For this assertion, the Gateway will use the routing URL to determine which principal in the keytab will be used to hand the Windows authentication.

Example: Route to http://ssg1.acmecorp.com/test.html page, will look up the service principal http/ssg1.acmecorp.com from the keytab file.

Require WS-Security Kerberos Token Profile Credentials Assertion

This assertion requires the use of the SecureSpan XML VPN Client (XVC).

The Gateway will use the Gateway host name entered in the Gateway Account Properties to determine which principal in the keytab to handle the Windows authentication. For example in Figure 11, the Gateway will look up *http/ssg3.acemecorp.sup* from the keytab file.



Enter the host name or IP address of the SecureSpan Gateway that will process service requests.

Gateway Host Name: ssg3.acmecorp.sup

Kerberos Name:

Figure 11: Gateway Host Name in the XVC

Note: The Kerberos Name is not required unless the Kerberos name does not match the standard naming pattern "http/<GatewayHostName>". Please contact Layer 7 Technical Support if this applies to you.

➢ *To create multiple service principals in the keytab file (Windows):*

- On the Active Directory machine, run the following command:

```
ktpass –princ http/<Gateway_host>@<Realm> –mapuser <userName> -pass
<userPassword> -in <kerberos_file_to_merge> –out <keytab_name>
```

For example:

```
ktpass -princ http/gateway.domain.com@DOMAIN.COM -mapuser gateway
-pass password –in kerberos.keytab -out kerberosMerged.keytab
```

This produces the output file *kerberosMerged.keytab* which contains the multiple service principals.

➢ *To create multiple service principals in the keytab file (Linux):*

- On the Active Directory machine, run the following commands:

```
ktutil
ktutil: read_kt <Kerberos keytab file>
ktutil: read_kt <Kerberos keytab file>
...
ktutil: write_kt <Kerberos keytab file containing multiple principle>
quit
```

Once this is done, install the keytab file using the "Manage Kerberos Configuration" task in the Layer 7 Policy Manager.

About the krb5.conf File

When a keytab is loaded via the *Manage Kerberos Configuration* task in the Layer 7 Policy Manager, the Gateway automatically generates a *krb5.conf* file and places it in the following directory:

/opt/SecureSpan/Gateway/node/default/var

The first service principal in the keytab file will be used as the default realm. For example, a keytab file contains the following service principals:

```
KVNO Principal
---- ------------------------------------
   2 http/ssg1.acmecorp.com@ACMECORP.COM
   4 http/ssg3.abccorp.sup@ABCCORP.SUP
   3 http/ssg4.sup.widgetcorp.sup@SUP.WIDGETCORP.SUP
```

In the krb5.conf file, "ACMECORP.COM" will be listed as the default realm.

Chapter Four: Configure a Gateway Cluster

A Gateway cluster consists of multiple Gateway nodes that, through a Load Balancer, present a unified network interface to client systems and software. Loosely-coupled yet synchronized through the replicated database, the Gateway cluster shares the service policies, identity providers, and configuration settings administered in the Policy Manager. This dramatically increases the scalability, processing power, and reliability of the Gateway implementation.

The Gateway cluster is an intelligent information propagation system that distinguishes between time-sensitive data that must be updated synchronously, data that is node-specific, and data that must be commonly available yet updated asynchronously. For example, policy and configuration setting changes are automatically propagated to each cluster node asynchronously within five seconds of the change in the Policy Manager. In contrast, replay attack data and SLA counters require instantaneous synchronized cluster-wide updates for them to be useful.

Tip: Complete the Cluster Configuration Worksheet in Appendix H while preplanning your cluster. This will help you complete the wizard more quickly when it comes time to configuring the first Gateway processing node (see page 55).

Note: Gateway clustering is not available if an embedded database is in use. For more information, see “Using the Embedded Database” on page 20.

System Requirements

Gateway cluster node requirements are the same as those for a stand-alone Gateway. In addition to the installation scenario requirements outlined in *Chapter Three: Configure the Gateway*, a cluster also requires:

- An industry-standard Load Balancer device installed and configured on the network that can provide TCP-level load balancing and failover
- Each Gateway that will become a node in the cluster must possess its own host name, IP address, and original node address within the Load Balancer. The cluster must also possess a host name and IP address in the Load Balancer (see *Configuring the Load Balancer* on page 48)
- Two nodes of the cluster must be installed and configured with the MySQL database with known root user names and root user passwords (see *Configuring Database Replication* on page 51).

Overview

The following is an overview of creating a new Gateway cluster:

1. Install and configure the Load Balancer on the network (see page 48).
2. Configure database replication on both Gateway database nodes (see page 51).
3. Configure the first Gateway processing node (see page 55).
4. Configure subsequent Gateway processing nodes (see page 55).
5. Start the Gateway cluster (see page 56).
6. Create a CA key for the cluster if the cluster will be communicating with the XML VPN Client (see page 56). This applies even if the "cluster" is a single Gateway.

Note: If you need to cluster existing stand-alone Gateways, please contact Layer 7 Technical Support for assistance.

Clustered Network Architecture

The following diagram shows the general network configuration for a Gateway cluster.

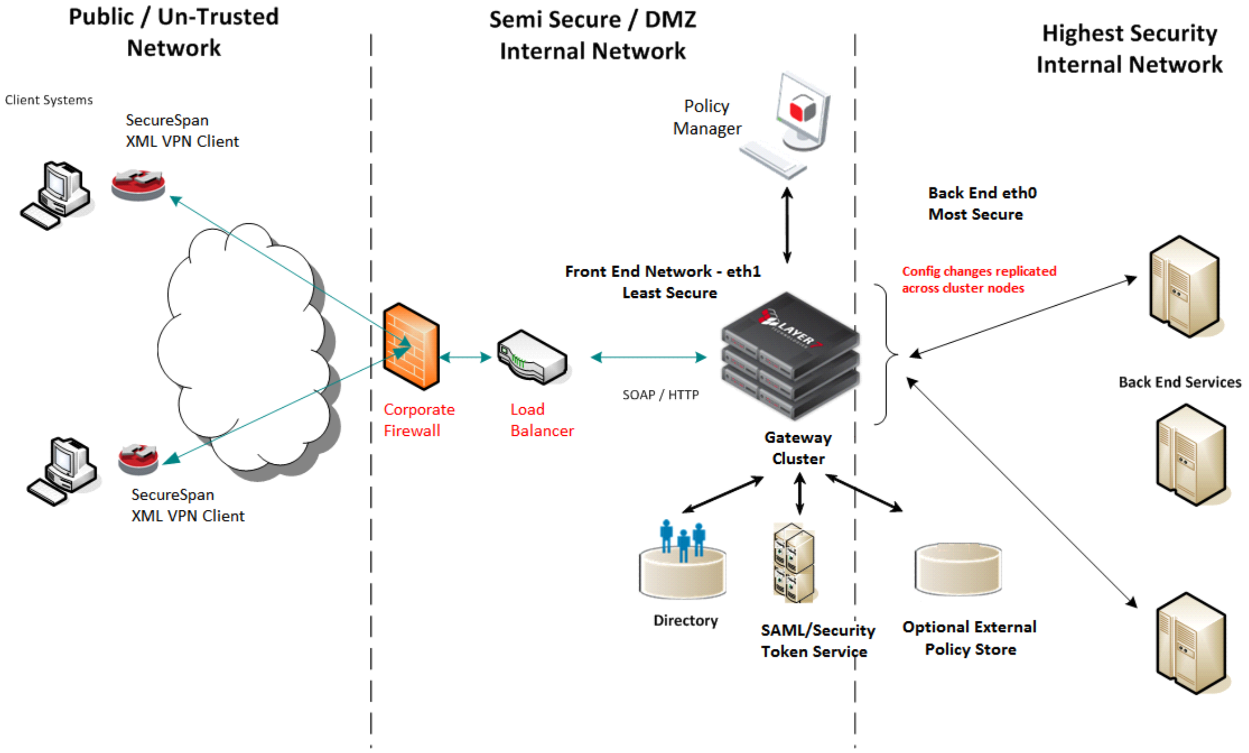

Public / Un-Trusted Network
Semi Secure / DMZ Internal Network
Highest Security Internal Network
Client Systems
SecureSpan XML VPN Client
Policy Manager
Back End eth0 Most Secure
Front End Network - eth1 Least Secure
Config changes replicated across cluster nodes
Corporate Firewall
Load Balancer
SOAP / HTTP
Back End Services
Gateway Cluster
SecureSpan XML VPN Client
Directory
SAML/Security Token Service
Optional External Policy Store

Figure 12: Clustered network architecture

Configuration Examples

These instructions describe how to configure a new cluster consisting of newly installed Gateway appliances. For brevity, clarity, and consistency, the following example values are used where applicable throughout the following sections. Other example values are used and referenced when necessary.

Table 9: Cluster configuration example

Description	Example Value
Gateway cluster Fully-Qualified Domain Name (FQDN)	clusterhostname.mycompany.com
IP address for clusterhostname (load balancer)	10.0.0.10
Gateway node host names	ssg1.mycompany.com, ssg2.mycompany.com
IP addresses for nodes	10.0.0.11, 10.0.0.12
MySQL database nodes	ssg1.mycompany.com, ssg2.mycompany.com
MySQL root user name	root
MySQL root user password	7layer
MySQL database replication username	repluser
MySQL database replication password	replpass
Gateway database name	ssg
Gateway database user	gateway
Gateway database password	7layer
Keystore password	7layer
Cluster Configuration passphrase	7layer

Configuring the Load Balancer

Note: This Manual does not provide Load Balancer configuration information or instructions. Only the specialized configuration settings required to connect the Load Balancer to a Gateway cluster are provided. Please consult your Load Balancer device documentation for detailed configuration instructions.

In a Gateway cluster, a Load Balancer device provides the vital load balancing and failover protection functions that allow the cluster to act as a unified interface, enabling the enhanced scalability, processing power, and reliability of the Gateway implementation. In a Gateway cluster, the Load Balancer device specifically:

- Listens for incoming network messages on its external interface.
- Evenly distributes its received messages to the Gateway processing nodes in the cluster, ensuring that the workload between the cluster nodes is balanced.
- Provides failover protection. If a Gateway processing node in the cluster fails, then the Load Balancer automatically directs incoming request messages to another processing node in the cluster.
- Provides failover detection. The Load Balance detects service availability by periodically polling the Gateway processing nodes. ICMP detection is minimal, and HTTP polling is preferred.
- Provides client-transparent TCP connectivity for the Gateway cluster.

To connect to the Gateway cluster, the Load Balancer device must contain special settings in four configuration areas:

- IP address determination
- virtual server configuration
- session persistence configuration
- service availability determination configuration

Use the following sections in conjunction with your Load Balancer's documentation to help you configure the Load Balancer device.

Determining the IP Address

IP addresses for the cluster and cluster nodes must be determined by and set in the Load Balancer.

Cluster IP Addresses

The Gateway cluster is accessed by the XML VPN Client, the Policy Manager, and external client systems and software at a single network address. The Network

Administrator determines this static IP address, commonly on the non-secure client-facing side of the enterprise network.

Cluster Node IP Address

The Load Balancer evenly delegates workload to the individual Gateway processing nodes in a cluster. In order to do so, each processing node in the cluster must be identified by a unique static IP address within the Load Balancer's secure subnet. Define and set these IP addresses, as necessary, in the Load Balancer. For example, with a cluster origin IP address of "10.0.0.10", the cluster node IP addresses would be "10.0.0.11" and "10.0.0.12" for the Gateway processing nodes "SSG1" and "SSG2", respectively.

Note: In more secure network configurations, a second IP address is required for the Gateway cluster to connect to back-end services. This secure network is generally not routable by the Load Balancer, preventing insecure messages from entering the back-end secure network. If a secure network exists, then the back-end service IP address must be assigned to "eth0" in Load Balancer, and any less secure network IP address must be assigned to "eth1". By default, the Gateway cluster will use the more secure network for inter-node communication if available; otherwise, the cluster will use the Load Balancer.

Configuring the Virtual Server

The load balancer for the Gateway cluster listens for incoming messages on TCP ports 8080 and 8443 and forwards the traffic to the processing nodes at the static IP addresses defined in *Cluster IP Addresses* on page 48.

WARNING

Use the IP addresses defined in *Determining the IP Address* on page 48 when configuring forwarding for ports 8080 and 8443. Do not use secure network IP addresses, if they exist.

Configuring Session Persistence

When the Load Balancer transmits an incoming message to a particular processing node, a session is opened between the client application and the node. Session persistence ensures that the session remains open for the duration of the transaction. To ensure session persistence, configure the Load Balancer session timeout limit to 30 minutes.

Configuring Service Availability Determination

Note: Not all Load Balancer models check for service availability, and those that do so will likely use a different term for the feature. Consult your Load Balancer documentation to determine whether it will check for service availability.

In a Gateway cluster, the Load Balancer device provides failover detection as part of its failover protection function. Using service availability determination, the Load Balancer can assess the availability of a Gateway service instead of just assessing whether the processing node is alive on the network. This feature also permits the Policy Manager to connect to the Gateway cluster when a processing node is down.

To check for service availability, configure ports 8080 and 8443 with the following parameters:

Note: The actual terminology used by your Load Balancer may differ from the parameter terms used below. Consult your Load Balancer documentation for the proper configuration information and instructions.

- Set the frequency of checking setting to 120 seconds. Setting a lower value will provide faster failure detection, but will cause excessive load on the Gateway cluster
- Set the response timeout to 120 seconds
- For port 8080, set the communication type to “Normal”
- For port 8443, set the communication type to “SSL”
- Configure ports 8080 and 8443 to check the URL “/ssg/ping”. By default, the “/ssg/ping” URL responds only when the request is submitted using SSL on port 8443, with HTTP basic credentials in the request. To enable non-SSL response without credentials, please refer to the *pingServlet.mode* property in *Gateway (Cluster) Properties* of the *Layer 7 Policy Manager User Manual*.

  Note: In some Load Balancers, you may have to enter a “send string” of “GET /ssg/ping” or an HTTP location of http://machine_ip:portnumber/ssg/ping”. Consult the Load Balancer documentation for device-specific configuration information and instructions.

- An “OK” message will appear when the Gateway is able to successfully connect the cluster storage, thereby determining that the service is working. If the connection fails, then a “The server is not in an operational state” message will appear after about 20 seconds.

  Note: In some Load Balancers, the success text feature is called a “receive rule”. Consult your Load Balancer documentation for device-specific terminology.

Configuring Database Replication

Note: In the following instructions, the terms "DBServer1" and "DBServer2" are used to represent each database node that will form the replicated pair in the example cluster.

Regardless of the number of Gateway processing nodes in a cluster, a maximum of two MySQL database servers can be configured for database replication in a Gateway cluster (for example, "DBServer1" and "DBServer2"). Each peered database unit becomes both a slave and master to the other unit. This configuration is often referred to as "master-master replication". The Gateway cluster is configured to use one as the primary database node and then fail over to the secondary database node in case of problems.

Background replication between the database nodes occurs constantly, with updates to the secondary node happening milliseconds after the primary node. If the primary node fails, then the Gateway processing nodes will invalidate previous connections to that database node before automatically connecting to the secondary database node.

Two main configuration tasks are required to configure database replication in a new cluster: configure the replication settings and synchronize the content of the two database nodes.

System Requirements

The following items and information are required to configure database replication:

- Host names for DBServer1 and DBServer2 configured in DNS or "/etc/hosts", or their respective IP addresses
- MySQL service for DBServer1 and DBServer2 is running
- Both Gateway services stopped
- Time synchronization configured amongst all Gateway nodes (for more information, see Table 3 on page 17)

Configure Replication

The database content must be synchronized between DBServer1 and DBServer2. This creates a replicated pair, ensuring that changes in one database are automatically propagated to the other.

Note: It is highly recommended that you set up synchronization before configuring any Gateway nodes.

➢ *To configure replication:*

1. Run the following script against the local database on each node of the cluster:

   ```
   /opt/SecureSpan/Appliance/bin/add_slave_user.sh
   ```

   The *add_slave_user.sh* script adds permissions for the users to MySQL.

2. Complete the following prompts in the script:

   a. **Enter hostname or IP for the <target>:** Enter either the hostname or IP address for the target machine being configured. In almost all cases, this is the other peer node. For example, if running the *add_slave_user.sh* script on the primary node, you would enter the hostname or IP address of the secondary node.

   b. **Enter replication user:** Enter the user account in the MySQL database that is used for replication. The default username is **repluser**.

   c. **Enter replication password:** Enter the password for the replication user.

   d. **Enter MySQL root user:** Enter the user account for the root MySQL user.

   e. **Enter MySQL root password:** Enter the user account for the root MySQL password.

   f. **Is this the Primary (1) or Secondary (2) database node?** Enter **1** or **2** to indicate the type of node.

   A message will confirm that MySQL is properly configured for replication and that slave permissions have been granted.

3. Run the following script against each database node of the cluster:

   ```
   /opt/SecureSpan/Appliance/bin/create_slave.sh
   ```

   The *create_slave.sh* script sets up the replication to run between the two databases, using the user configured in *add_slave_user.sh.*

   Tip: The *create_slave.sh* script is always run against the ***other*** node in a 2-node database cluster. In other words, you are setting up the other node as the master. Since this script is run on both nodes, each node gets the other one set up as its master, thus creating the master-slave relationship.

4. Complete the following prompts in the script:

   a. **Enter hostname or IP for the MASTER:** Enter either the hostname or IP address for the target machine being configured. In almost all cases, this is the other peer node. For example, if running the *add_slave_user.sh* script on the primary node, you would enter the hostname or IP address of the secondary node.

b. **Enter replication user:** Enter the account used in MySQL for replication. This should be the same user as entered when configuring the replication user in the first script (*add_slave_user.sh)*.

c. **Enter replication password:** Enter the password for the replication user.

d. **Enter MySQL root user:** Enter the user account for the root MySQL user.

e. **Enter MySQL root password:** Enter the user account for the root MySQL password.

f. **Do you want to clone a database?**

- If you have a pre-existing database and wish to keep its contents, enter **yes** and then enter the name of the database to clone. Be sure the slave is not currently running on the master.
- If you are following these steps for the first time or if you want to discard the existing database and create a new one, enter **no**.

This script then clones the database and starts the slave.

Tips: (1) To verify that replication has started, run the following command on each node: mysql;show slave status\G;
You should see the following:

```
    Slave_IO_Running: Yes
    Slave_SQL_Running: Yes
```

(2) If there is a problem with replication, you can restart it by running this script:

```
opt/SecureSpan/Appliance/bin/create_slave.sh
```

When replication is configured, you may proceed to configure the first Gateway processing node.

Monitor Replication Failure

The Gateway uses the following cluster properties to configure monitoring of replication delays or failures:

- *db.replicationDelayThreshold:* This property defines the threshold before the Gateway audits a warning for slow or failed replication. The default is 60 seconds.
- *db.replicationErrorAuditInterval:* This property defines the minimum interval between database replication failure audits. The default is 60 minutes.

For more information, see *Gateway (Cluster) Properties* in the *Layer 7 Policy Manager User Manual*.

The following replication events will be audited:

- **Replication failure:** When replication has been delayed beyond the value specified in *db.replicationDelayThreshold,* the Gateway will log audit message 2381 (“Replication failing for host/database”).

- **Replication recovery:** When replication recovers, audit message 2382 ("Replication recovered for host/database") is logged.
- **Database failure:** If either the primary or secondary database fails, audit message 2380 ("Error accessing host/database") is logged.

Tip: If the Gateway cluster is being managed by the Enterprise Service Manager, replication delay can also be monitored on the Monitor page under the Manage Gateways tab, with optional alerts when the delay exceeds the threshold. For more information, see *Monitor Page* in the Enterprise Service Manager documentation.

Restart Replication

If replication stops working for whatever reason, you can restart it by running the *restart_replication.sh* script.

Note: Replication must already be correctly configured and previously running before you can restart it.

➢ *To restart replication:*

1. Run the following script against the local database on each node of the cluster:

   ```
   /opt/SecureSpan/Appliance/bin/restart_replication.sh
   ```

2. Complete the following prompts in the script:

   a. **Enter hostname or IP for the MASTER:** Enter either the hostname or IP address for the master machine.

   b. **Enter replication user:** Enter the account used in MySQL for replication.

   c. **Enter replication password:** Enter the password for the replication user.

   d. **Enter MySQL root user:** Enter the user account for the root MySQL user.

   e. **Enter MySQL root password:** Enter the user account for the root MySQL password.

When replication is successfully restarted, you should see the message *"Slave successfully started."*

Configuring the First Gateway Processing Node

Configuring the first node of the cluster will create and initialize the database on both database nodes and establish basic configuration of the Gateway cluster.

Prerequisite: Before configuring the first processing node, make sure that database replication has been correctly configured (see page 51). ***This step is very important—failure to do so will require complex steps to enable proper operation of the cluster.***

Tip: If you completed a Cluster Configuration Worksheet (see Appendix H), use the values from that worksheet.

➢ *To configure the first Gateway processing node:*

1. Log into DBServer1 as *ssgconfig*. The Gateway main menu appears (see Figure 3 on page 12).
2. Select option **2** (Display Gateway configuration menu). The Configure Gateway menu appears (see Figure 4 on page 20).
3. Select option **2** (Create a new Gateway database). The database configurator starts. Refer to Table 4 on page 21 for instructions on completing this configurator.

Once this initial node is configured, follow the next section to add subsequent processing nodes.

Configuring Subsequent Gateway Processing Nodes

Once the first processing node has been configured, adding new nodes to the cluster simply involves configuring the Gateway on each subsequent node.

Prerequisite: The first node of the cluster must already be configured using the instructions under *Configuring the First Gateway Processing Node* on page 55.

➢ *To configure subsequent Gateway processing nodes:*

1. Log into DBServer2 as *ssgconfig*. The Gateway main menu appears (see Figure 3 on page 12).
2. Select option **2** (Display Gateway configuration menu). The Configure Gateway menu appears (see Figure 4 on page 20).
3. Select option **3** (Configure the Gateway). The Gateway configurator starts. Refer to Table 4 on page 21 for more information about this option, but note the following:
    - For **Database Host:** Enter the hostname for DBServer1 (the initial processing node)—for example, *ssg1.mycompany.com*.

- For **Database Name**: Enter the name that was used to create the database when configuring the first Gateway node.
- For **Database Username** and **Database Password**: Enter the values used when configuring the first Gateway processing node.
- For **Cluster Password**: Enter the password that was defined when configuring the first Gateway processing node. This is required to extract the settings from the database.

4. Ensure the node is enabled and then press [**Enter**] at the configuration summary.
5. Return to the Gateway main menu and use the **R** option to restart the appliance. The node will join the cluster when it is started.

Repeat this procedure for each new processing node to add to the cluster.

Configuring Name Resolution

It is expected that each node of the Gateway cluster can resolve the IP address of the cluster and all other nodes by DNS. If DNS is not configured to provide this, then each node must do so via the "/etc/hosts" file.

Starting the Gateway Cluster

To start the Gateway cluster, start the individual Gateway nodes as outlined on page 25.

In a cluster environment, each node needs to be started individually. As each node comes up, it will join the cluster.

Configuring a CA Key for the Cluster

You will need to configure a CA key for the cluster if <u>both</u> the following apply:

- The Gateway cluster will be communicating with the XML VPN Client.
- You expect to use the automatic client certificate provisioning feature in the XML VPN Client.

You do not need to configure a CA key for the cluster if <u>either</u> of the following applies:

- The Gateway cluster will not be communicating with the XML VPN Client.
- Client certificates have been manually imported into the XML VPN Client.

To configure a CA key for the cluster, use the *Manage Private Keys* task in the Policy Manager to create a new CA-capable key and then set it as the default. For more information, see *Managing Private Keys* and *Private Key Properties* in the *Layer 7 Policy Manager User Manual*.

Deactivating a Cluster Node

Deactivating a cluster node requires access to the Gateway configuration menus and to the Policy Manager.

➢ *To temporarily deactivate a Gateway node:*

This procedure will deactivate the node until the Gateway is restarted, at which point the node is automatically reactivated. For a more permanent deactivation, see *"To disable a Gateway node"* below.

1. Access the Gateway main menu on the node to be deactivated—see Figure 3 on page 12.
2. Select option **2** ("Display Layer 7 Gateway configuration menu").
3. Select option **7** ("Manage Layer 7 Gateway status"). The status is displayed after a few seconds. Press [Enter] to continue.
4. Select option **1** ("Stop the Layer 7 Gateway").
5. Exit all the menus and leave the Gateway main menu using option **X** ("Exit (no reboot)").

➢ *To disable a Gateway node:*

This procedure will disable a node until you manually re-enable it by running this procedure again and entering **Yes** in step 5.

1. Access the Gateway main menu on the node to be deactivated—see Figure 3 on page 12.
2. Select option **2** ("Display Layer 7 Gateway configuration menu").
3. Select option **3** ("Configure the Layer 7 Gateway"). The configuration details are displayed after a few seconds.
4. Select option **4** ("Node Configuration").
5. Enter **No** to disable the node.
6. Select option **S** ("Save and exit"), then press [**Enter**] to acknowledge the change.
7. Exit all the menus and leave the Gateway main menu using option **X** ("Exit (no reboot)").

➢ *To remove a node from the cluster:*

Once a node has been deactivated or disabled, you can remove it from the cluster using the Layer 7 Policy Manager.

1. Open the Dashboard in the Policy Manager and select the [Cluster Status] tab.
2. In the Gateway Status list, right-click on the inactive node and then select **Delete Node**. (Note that only inactive nodes can be deleted.)

The node will reappear in the list once it is active again.

Chapter Five:
Maintain and Upgrade the Gateway

This chapter describes the tasks to maintain the Gateway and how to upgrade to a newer version of the Gateway:

- Backing up, restoring, migrating the Gateway
- Configuring the Gateway Logging Functionality
- Configuring the Gateway Audit Functionality
- Configuring UDDI Registry Searches
- Upgrading the Gateway
- System Health Test
- Rebooting the Gateway
- Regenerating Expired Keys
- Understanding the Service Resolution Process
- Troubleshooting Password Issues

Maintenance Tasks

In general, the Gateway requires minimal direct maintenance. The few required maintenance tasks, such as database audit purging, are initiated from the Policy Manager. Other normal maintenance tasks, such as log rollover, are handled automatically by the Gateway when required.

Even when grouped, the Gateway cluster is self-managing and healing. If a cluster node fails, for example, then the Load Balancer device simply moves traffic to the other cluster nodes, minimizing service interruptions. Automatic background database replication in a cluster occurs constantly, with updates to the secondary node happening milliseconds after the primary node.

For more information about the user-initiated Gateway maintenance tasks, see the Policy Manager documentation.

Backing Up the Gateway

There are two ways to back up your data in the Gateway:

- **Back up using a browser:** This is a quick, one-step process that backs up to a .ZIP file: the Gateway database, all configuration files, custom and modular assertions, and optionally audits. You can optionally create a script that triggers the backup.
- **Back up using the command line:** This offers greater flexibility in specifying what to back up.

Backups are specific to a node. To back up all nodes in a cluster, run the backup on each individual node (if using the command line) or click the button for each node (if using a browser).

Note: The Gateway must be correctly configured before it can be backed up.

Back Up Using a Browser

There are two ways to use the browser-based Backup Service:

- **Method 1:** Run a backup on demand using a web browser. With this method, you can back up a Gateway node at any time.
- **Method 2:** Perform a backup using a script. With this method, the backup is performed every time the script is run.

All backup attempts using the browser are recorded in the audit log.

IMPORTANT: The backup is stored in an unencrypted zip file and contains sensitive information such as passwords and passphrases. It is highly recommended that you store the backup in a secure location.

Prerequisites:

- The person performing the backup has the role “Administrator” (must be able to Read and Write all entity types).
- The Gateway is running.

Backup Log Files

When backing up using a browser, the backup log files are stored in the same location as the Gateway log files. For more information, see *Logging Levels* on page 81.

Method 1: Back up on demand

➢ *To perform an on-demand backup using a web browser:*

1. Start the browser and navigate to:

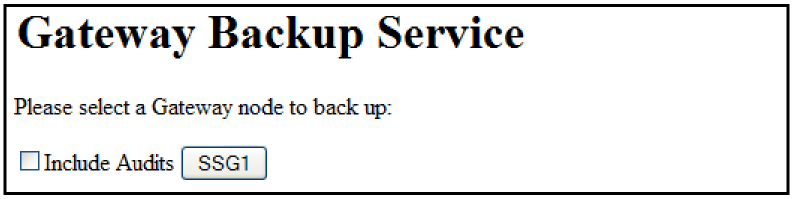
   https://*<SSG_host_name>***:***<port>***/ssg/backup**

   where the default "<*port*>" is 8443.

   Note: If a user has a client certificate registered on the Gateway, then the user is required to use the client certificate when performing a backup.

2. Enter the user name and password when prompted.

   The Gateway Backup Service page is displayed:



Gateway Backup Service

Please select a Gateway node to back up:

□ Include Audits

Figure 13: Gateway Backup Service web page

3. Select the [**Include Audits**] check box to include audit records in the backup.

   Note: Including audits will increase the time to complete the backup and may greatly increase the size of the backup .ZIP file.

4. Click the button corresponding to the Gateway node to back up. If you are not running a cluster of Gateways, only one button is displayed.

   Note: The database is only included in the backup of the node hosting the database. For example, if there are three nodes in the cluster and all three are backed up, then only one backup image will contain a database (and audits) in the backup.

5. Select "Save to Disk" and then specify a name and location for the backup file when prompted.

Method 2: Back up using a script

The backup process can be invoked from a script. You will need to obtain the URL of the Gateway node to back up, then write a script to perform an HTTP GET at the URL.

To include audits, use this URL in the script:

https://*<SSG_host>***:***<port>***/ssg/backup?node=***<node_name>***&audits=true**

To exclude audits, use this URL in the script:

https://*<SSG_host>***:***<port>***/ssg/backup?node=***<node_name>***&audits=false**

Note: The script will need the user name and password to access the Backup Service. To maintain security, you should write the script in such a way as to not expose the password to other users.

Best practices when using a script

The Gateway Backup Service was designed to be available remotely via HTTP with a standard tool such as *wget,* or via a scriptable command line tool. This means the backup can be automated by using a cron job or with any other scheduling tool.

When using a script, care must be taken to ensure information security. Tools like *wget* can have credentials passed on the command line. These credentials may be exposed in UNIX systems if someone uses the “ps” command to view the process status. To prevent passwords from being revealed, store them in “.wgetrc” or “.netrc” and protect those files with the “chmod” command.

For example, the following cron job entry securely backs up the Gateway on a daily basis (the entry should be all on one line):

```
02 4 * * * /usr/bin/wget --tries=10 --output-document=Gateway1.zip
--output-file=backup.log https://<host>:<port>/ssg/backup?node=Gateway1
```

In this script, the username and password are saved in ~/.wgetrc in the format:

```
http_user=admin
http_password=password
```

Back Up Using the Command Line

The command line utilities offer more configurability for backing up settings and data from a Gateway node compared to backing up using a browser.

There are two ways to perform a backup using the command line:

- *Standard backup:* most inclusive; used most often
- *Custom backup:* lets you select which components to back up

Performing a Standard Backup

A standard backup will back up every applicable component except for audits (which may be included using the “-ia” switch). The following components may not be applicable for a standard backup:

- The database files is included only if the database is local to the node
- Custom assertions are backed up if installed
- The Enterprise Service Manager can be included if the “-esm” switch is used

Examples of a standard backup:

- A standard backup: ssgbackup.sh -image name.zip
- A standard backup including audit records:

```
ssgbackup.sh -image name.zip -ia
```

Performing a Custom Backup

A custom backup includes only specific components. A custom backup is created when any of these switches are used:

-os: back up OS configuration files
-config: back up Gateway configuration files
-maindb: back up the Gateway database, excluding audit data
-audits: back up the database audits
-ext: back up the contents of the *Gateway/runtime/lib/ext* directory (**Note:** The backup will exclude files in the "ext" directory if both the following conditions apply: (1) the file begins with the characters "jms" and (2) the file is owned by an rpm which starts with the letters "ssg".)
-ca: back up custom assertions
-ma: back up modular assertions

For more information on these switches, see Table 10 on page 64.

You can combine any of these switches to create a custom backup containing exactly what you want.

Examples of a custom backup:

- Custom backup of only the database components:

  ```
  ssgbackup.sh -image name.zip -maindb -audits
  ```

- For custom backups, the "-ia" switch is not used, so this command will not include audits:

  ```
  ssgbackup.sh -image name.zip -os -config -maindb -ia
  ```

  The correct version to include audits:

  ```
  ssgbackup.sh -image name.zip -os -config -maindb -audits
  ```

Note: The Gateway license file is not backed up, however if the Enterprise Service Manager is included in the image, its license file *is* backed up.

Backup Log Files

Backup log files can be found in the following location:

```
/opt/SecureSpan/Gateway/config/backup/logs
```

➢ *To back up the Gateway from the command line:*

1. Log in as *ssgconfig* and open a privileged command shell from the Gateway configuration menu (see Figure 3 on page 12).
2. Run the following command:

```
/opt/SecureSpan/Gateway/config/backup/ssgbackup.sh [options]
```

Refer to Table 10 for the available *[options]*. Separate each option with a space. You must specify the “-image” switch.

Table 10: Command line backup options

Option	Description
-image <*file_name.zip* >	Save the backup to the specified image file. Be sure to add the zip extension as the backup image is a zip file. If saving to an FTP server, this is the name of the image on the FTP server and any path information is relative to the FTP server. If the path is not specified, the image is saved to /opt/SecureSpan/Gateway/*config/backup/images* A timestamp is added as a prefix to the image name to ensure uniqueness: *yyyyMMddHHmmss_imagename.zip* If backing up to an FTP server and no path is specified, then the image will be transferred to the login directory of the “**-ftp_user**”.
-ia	Include audit tables in the image. By default, audit tables are not included during backups because of the space they may consume.
-it <*output_template_file_path*>	Create a template mapping file. You then edit the template to populate it with the appropriate values to create the final mapping file. See *Creating a Mapping File* on page 75 for more details. **Note:** You should use the “**-it**” option only if you also intend to use the backup image for migration purposes. For more information, see *Migrating the Gateway* on page 71.
-v	Display verbose backup progress information on the screen.
-halt	Fail the entire backup when the first failure is encountered. This prevents an incomplete backup from being created. If this option is not specified, the backup script will attempt to back up each component separately. Components that failed to back up will be noted in the log and on the console. For a custom backup, “-halt” also means to fail if a requested component is not applicable. In this example, if an applicable component fails to backup, the backup image will contain everything else which successfully backed up: ssgbackup.sh –image name.zip In this example, if any applicable component fails to backup, the entire backup will fail: ssgbackup.sh -image name.zip -halt In this example, the backup image will contain all components which completed successfully. If the database is not local, it will not be included: ssgbackup.sh -image name.zip -maindb -os -config In this example, the entire backup will fail if the database is not local. Reason:

Option	Description
	A component was explicitly requested which was not applicable and the "-halt" switch was used. ssgbackup.sh -image name.zip -maindb -os -config -halt Failed components are displayed on the screen.
-ftp_host *<FTP_host_machine>:[port]*	Create the backup image on the specified FTP host; can optionally specify a port number. **Note:** Secure FTP (FTPS) is not supported. Protocol must be FTP.
-ftp_user *<user_name>*	Username to log onto FTP host.
-ftp_pass *<password>*	Password for username on FTP host.
Using any of the following options will create a custom backup that includes only the specified components:	
-audits	Include the database audit files in a custom backup. The "-maindb" option (include database) must always accompany "-audits". **Note:** The "-audits" option differs from the "-ia" switch, which includes the audit records but does not cause a custom backup. If both switches are present, the "-audits" option takes precedence and a custom backup will be created.
-ca	Include the custom assertion jar and properties files in a custom backup.
-config	Include the Gateway configuration files in a custom backup.
-ext	Include the directory *Gateway/runtime/lib/ext* in a custom backup.
-ma	Include the modular assertion jar files in a custom backup.
-maindb	Include the Gateway database in a custom backup, excluding audit data. This switch is valid only if the database is local to the node being backed up.
-os	Include the operating system configuration files in a custom backup.
The following option can be used for a standard or custom backup:	
-esm	Include the Enterprise Service Manager (ESM) in the backup, if present. The ESM must be installed on the same node and not currently running.

When the backup is complete, the console displays whether the backup was a success, partial success, or failure.

Restoring the Gateway

Restoring the Gateway recovers the entire Gateway environment. It is useful for initializing a new cluster node or to recover data back to an existing cluster node after a major error.

You can choose to restore the entire image or only select components within the backup image. Restoration can be to the same Gateway node or to a different node. Each item in the backup image file can be restored independently. The backup image file may reside locally or on an FTP server.

Note: If you need to restore but do not have a backup image, you can revert your Gateway to a “as shipped from the factory” state. For more information, see *Appendix J – Gateway Recovery*.

Tip: If you need to make configuration changes to a restored Gateway, be sure to restart the Gateway first *before* reconfiguring. Otherwise, the settings in the restored image will overwrite any configuration changes made through the Gateway Main Menu (see Figure 3 on page 12).

nCipher HSM users: Please be prepared to enter the database password and cluster passphrase after performing a restore.

Prerequisites:

- MySQL must be installed and configured and running on the Gateway node being restored.
- The target Gateway rpm files must be installed, but it does not need to be configured (see page 20). This assumes the backup image contains all required files to recover the configuration.

Full Restore vs. Custom Restore

A *full* restore restores all applicable components found in the backup image. To perform a full restore, use any of the following combinations:

- Default restore: **ssgrestore.sh -image -dbu –dbp**
- Default restore from FTP:

  ssgrestore.sh -image -ftp_host -ftp_user -ftp_pass -ftp_dir -dbp –dbu

Tip: When no information is found for a particular component during a full restore, this is logged as an INFO log event and will not affect the restore. For example, if no modular assertions are present in the image, a full restore will log the fact that modular assertions are not being restored because none were present in the image. This also applies when a component found in the image is not applicable (for example, OS data is found but the appliance Gateway is not present).

A *custom* restore includes only specific components. A custom restore is performed when any of these switches are used:

-os: restore the OS configuration files
-config: restore the Gateway configuration files
-maindb: restore the Gateway database, excluding audit data
-audits: restore the database audits
-ext: restores the contents of the *Gateway/runtime/lib/ext* directory
-ca: restore the custom assertions
-ma: restore the modular assertions

For more information on these switches, see Table 11 on page 68.

You can combine any of these switches to create a custom restore from the backup image.

Examples:

- Custom restore only the database, including audit records:

  ssgrestore.sh -image name.zip -maindb –audits -dbu -dbp

- Custom restore only the custom assertions and modular assertions:

  ssgrestore.sh -image name.zip -ca -ma

Note: When no information is found for a requested component in a custom restore, this will be logged as a WARNING audit and will be displayed on the screen. If the “-halt” switch is used, the restore will stop.

IMPORTANT: When restoring the database, the image completely overwrites the destination Gateway's database—data is *not* merged. Audits are always deleted with the “**-maindb**” switch. In particular, the license on the target node will need to be reinstalled after a restore of the database component since the license file is not included in the backup image.

Restore Log Files

Restore log files can be found in the following location:

/opt/SecureSpan/Gateway/config/backup/logs

➢ *To restore a backup image:*

1. Stop the target Gateway node (see page 41).
2. Log in as *ssgconfig* and open a privileged command shell from the Gateway configuration menu (see Figure 3 on page 12).
3. Run the following command:

   ```
   /opt/SecureSpan/Gateway/config/backup/ssgrestore.sh [options]
   ```

   Refer to Table 11 for the available *[options]*. Separate each option with a space.
4. **Restoring a previous version of the Gateway:** If restoring an image created in a previous version of the Gateway, you must upgrade the database after the restore is complete. To do this:
   a. Start the Gateway main menu (see Figure 3 on page 12).
   b. Select option **2** (Display Gateway configuration menu). This displays options to configure the Gateway application (Figure 4 on page 20).
   c. Select option **1** (Upgrade the Gateway database). Follow the prompts on the screen to upgrade the database.
5. Restart the Gateway node.

Table 11: Restore Utility options

Option	Description
-image *<image_file_path>*	Full path to the image file to be restored. The path can be relative to the working directory. When restoring from an FTP server, this is the path and name of the file to download. **Note:** The image must be located in a directory accessible by the **layer7** user, for example the default location used by the backup command: /opt/SecureSpan/Gateway/config/backup/images/ Restoration will fail if the image is in a directory that is only accessible (for example) by the root user.
-dbu *<admin_db_username>*	Name of the database admin user.
-dbp *<admin_db_password>*	Password for the database admin user. **Tips:** (1) The "-dbp" option is not required if the admin database password is blank. (2) If the password contains special characters (for example, a semicolon), enclose the password within quotes; for example: *"pass;word"*.

Option	Description
-halt	Fail the restore when the first error is encountered. This will result in a partially restored system. If the error was caused by requesting a component that was not present in the backup image, run the restore again with the correct options. If an unexpected error occurred, contact Layer 7 Technical Support for further assistance. The Restore Utility always attempts each component independently. If "-halt" is not specified, a failure of one component does not affect other components from being tried. Failed components are displayed on the screen.
-v	Display verbose restoration progress information on the screen.
-ftp_host *<FTP_host_machine>:[port]*	If the backup image is on an FTP host, specify the host name and optionally the port number.
-ftp_user *<user_name>*	Username to log onto FTP host.
-ftp_pass *<password>*	Password for username on FTP host.
-gdbu *<gateway_name>*	The database user for the Gateway node. **Note:** The "-gdbu" option must be used when doing a restore when a Thales nCipher HSM is present.
-gdbp *<gateway_password>*	The password for the database user for the Gateway node. **Tip:** If the password contains special characters (for example, a semicolon), enclose the password within quotes; for example: *"pass;word"*. **Note:** The "-gdbp" option must be used when doing a restore when a Thales nCipher HSM is present.
-os	Overwrite OS-level files during restore. You must restart the Gateway appliance to complete the restoration of OS-level files. Applies only for appliance Gateways. **Note:** The "-os" option should only be used for the same Gateway type (for example, do not back up a VMware Gateway and then attempt to restore to a hardware appliance).
The following options are used to perform a custom restore:	
-audits	Include the audit records in a custom restore. The "**-maindb**" option must always accompany "-audits".
-ca	Include custom assertions and their associated property files in a custom restore.
-config	Include the Gateway configuration files in a custom restore.
-ext	Include all files from the *Gateway/runtime/lib/ext* directory in the backup image.
-ma	Include modular assertions in a custom restore.

Option	Description
-maindb	Include the database configuration in a custom restore, excluding audits.
The following option can be used for a standard or custom restore:	
-esm	Include the Enterprise Service Manager (ESM) in the restore.

When the restore is complete, the console displays whether the restoration was a success or failure.

Advanced Tip: Restoration of *node.properties* and *omp.dat*

Table 12 summarizes how the configuration files *node.properties* and *omp.dat* are treated after ssgrestore.sh is run.

Note: When the *node.properties* is generated on the restore host, the node database username and cluster passphrase will always be encrypted.

Table 12: Restoration of node.properties and omp.dat

Scenario	Result
Scenario 1: Backup image does not contain node.properties or omp.dat. OR Image does contain the files but a custom restore is performed with no “-config” component.	The *node.properties* and *omp.dat* from the restore host is used.
Scenario 2: Backup image contains *node.properties*.	The *node.properties* from the image copied to the restore host. The treatment of *omp.dat* depends on whether it is present in the image: • If *omp.dat* is in the image, it is used to decrypt values from *node.properties* from the image and to encrypt values when writing to the restore host. • If omp.dat is not in the image, then the Gateway attempts to decrypt/encrypt using the *omp.dat* on the restore host. This will then only succeed when the omp values are the same between the image and the host.

Migrating the Gateway

Migrating a Gateway is used to transfer select data and some settings between Gateway environments—for example, from a testing environment to a production environment. When migrating, you can specify:

- A list of tables to exclude when migrating the database, in file *exclude_tables*. Please contact Layer 7 Technical Support if you need to exclude tables.
- A list of files to exclude when migrating the configuration files, in file *exclude_files*.
- A mapping file that describes the corresponding values between source and target systems (using the "**-mapping**" option)

Both the *exclude_tables* and *exclude_files* files are stored in this directory:

/opt/SecureSpan/Gateway/config/backup/cfg

The *exclude_files* file is a text file that lists all the files that will not be restored after migration is complete. These files can include:

- **Gateway configuration files** (e.g., node*.properties*): Add the name of the file to exclude; no path is required.
- **OS files** (e.g., any files in *backup_manifest*): Add the entire file name and path of the actual file; for example, to exclude the file */etc/hosts* from being copied from the backup image onto the host, add */etc/hosts* as a new line in *exclude_files*.
- **Database files** (e.g., *my.cnf*): Same as "OS files" above.

Tip: To see a list of which files were copied or ignored, refer to the *ssgrestore*.log* files in */opt/SecureSpan/Gateway/config/backup/logs*.

Tip: If you need to make configuration changes to a migrated Gateway, be sure to restart the Gateway first *before* reconfiguring. Otherwise, the settings in the migrated image will overwrite any configuration changes made through the Gateway Main Menu (see Figure 3 on page 12).

Prerequisites:

- Both the source and target Gateways are configured and operational.
- A backup image that has these components present: Gateway Database ("-maindb") and Gateway configuration files ("-config").
- MySQL must be installed and configured and running on the Gateway node being restored.
- The target Gateway must be installed, but it does not need to be configured (see page 20).

Tip: Reusing Migration Scripts from Previous Releases

The Migration Utility preserves the migration behavior from previous release of the Gateway. If you have created scripts using “ssgrestore.sh -migrate” in the previous release and wish to reuse these scripts, simply update the name of the script being called,

from: **ssgrestore.sh**

to: **ssgmigrate.sh**

None of the script arguments from the previous version *ssgrestore.sh* need to be changed.

➢ *To migrate a backup image:*

1. Stop the target Gateway node (see page 41).
2. Log in as *ssgconfig* and open a privileged command shell from the Gateway configuration menu (see Figure 3 on page 12).
3. Run the following command:

```
/opt/SecureSpan/Gateway/config/backup/ssgmigrate.sh [options]
```

   Refer to Table 13 for the available *[options]*. Separate each option with a space.

4. **Migrating a previous version:** If migrating an image created in a previous version of the Gateway, you must upgrade the database after the migration is complete. To do this:
   a. Start the Gateway main menu (see Figure 3 on page 12).
   b. Select option **2** (Display Gateway configuration menu). This displays options to configure the Gateway application (Figure 4 on page 20).
   c. Select option **1** (Upgrade the Gateway database). Follow the prompts on the screen to upgrade the database.
5. Restart the target Gateway node.

Note: In Table 13 below, the following options will be written to the migrated host’s *node.properties*, or to a new *node.properties* file if one doesn’t exist: -db, -newdb, -dbh, -gdbu, -gdbp, -cp.

Table 13: Migrate Utility options

Option	Description
-image *<image_file_path>*	Full path to the image file to migrate. The image cannot be located on an FTP server. **Note:** The image must be located in a directory accessible by the **layer7** user. Migration will fail if the image is in a directory that is only accessible (for example) by the root user.

Option	Description
-mapping *<mapping_file_path>*	Location of the mapping template file. This file is created by the "**-it**" option when the backup was performed (see Table 10 on page 64). Use of this switch is optional. For more information, see *Creating a Mapping File* on page 75.
-dbu *<admin_db_username>*	Name of the database admin user.
-dbp *<admin_db_password>*	Password for the database admin user. **Tips:** (1) The "-dbp" option is not required if the admin database password is blank. (2) If the password contains special characters (for example, a semicolon), enclose the password within quotes; for example: *"pass;word"*.
-dbh *<host_name>*	The database server host name.
-db *<database_name>*	The name of the Gateway database.
-config	Include the Gateway configuration files in the migration, excluding the database. Use of this switch is optional. **Tip:** As the Migrate Utility will never migrate a database if it is not local, the "-config" switch lets you run ssgmigrate.sh with an image containing a backed up database without it failing when the database is attempted to be restored.
-os	Overwrite OS-level files during migration. You must restart the Gateway appliance to complete the migration of OS-level files Applies only for appliance Gateways. Use of this switch is optional. **Note:** The "-os" option should only be used for the same Gateway type (for example, do not back up a VMware Gateway and then attempt to migrate to a hardware appliance).
-cp *<passphrase>*	The cluster passphrase for the resulting database.
-gdbu *<gateway_name>*	The database user for the Gateway node.
-gdbp *<gateway_password>*	The password for the database user for the Gateway node. **Tip:** If the password contains special characters (for example, a semicolon), enclose the password within quotes; for example: *"pass;word"*.
-newdb *<database_name>*	Create a new database with the specified name. The database must not exist.

When the migration is complete, the console displays whether the migration was a success or failure.

Advanced Tip: Migration of *node.properties* and *omp.dat*

If the backup image contains no configuration component or "-config" was not specified during migration AND all database command line parameters are supplied, then the following occurs:

- If *node.properties* on the migration target does not exist, it will be created and a node.id will be automatically generated.

- If *node.properties* on the migration target does exist, then it is updated with the command line parameters. The target host's current *omp.dat* is always used in this case.

Note: When the *node.properties* is generated on the migration target host, the node database username and cluster passphrase will always be encrypted.

Tips for Migrating Policies between Environments

Migration Alternative

The Enterprise Service Manager provides comprehensive migration capabilities in a simple to use browser interface. For more information on this product, please contact Layer 7 Technologies.

This section provides some useful tips reducing the overall effort when using the Migrate Utility (ssgmigrate.sh) to migrate between environments.

Note: If your goal is to *initialize a new cluster* using a backup image, you should use the Restore Utility (ssgrestore.sh) instead. For more information, see *Restoring the Gateway* on page 66.

When migrating between environments, the backend server names and service URLs will usually differ. To best handle this, avoid using explicit values in the service policies. Use context variables in the Route via HTTP(S) Assertion instead of explicit URLs. The following is an example:

1. In the routing assertions, you might use the "${gateway.*cluster_property*_name}" context variable instead of explicit hostnames or IP addresses. For example, use "http ://${gateway.*back_end_app_server*}/Url/" in the Route via HTTP(S) Assertion instead of the actual URL.
2. Using the *Manage Cluster-Wide Properties* task, define *back_end_app_server* as a new cluster property with the name of the source server as its value—for example: *DEVappserver.company.com*.
3. Follow the steps under *Backing up the Gateway* and *Migrating the Gateway* to migrate the policy between the testing and production servers.
4. When the migration is complete, update the value of the cluster property used for the routing URL in the mapping file—for example: *QAappserver.company.com.*

Repeat these steps each time you need to migrate to a different environment. Using context variables and cluster properties in this manner will reduce the amount of service policy editing following the migration.

Creating a Mapping File

When migrating an image, you can use the "**-mapping**" option to supply an XML file that describes the corresponding values between the source data (in the image being imported) and the target system.

There are two categories of information that can be mapped between source and target systems:

- IP addresses referred to in routing assertions in the policies of published services
- Values of cluster-wide properties

➢ *To create a mapping file:*

1. Use the Backup Utility with the "**-it**" option. See Table 10 on page 64.
2. Open the mapping file in a text editor and replace *only* the placeholders with your values. The placeholders are indicated by "**_add_your_value_**" within the mapping file. Do not change anything else.
3. Once the mapping file is edited, you specify it using the "**-mapping**" option of the Migration Utility.

Figure 11 shows an example of the mapping file template.

```
<?xml version="1.0" encoding="UTF-8"?>
<L7flash:ssgimportmapping xmlns:L7flash="http://www.layer7tech.com/migration/stagingmapping">
    <L7flash:backendipmapping>
        <L7flash:ipmap sourcevalue="_add_your_value_" targetvalue="_add_your_value_"/>
        <L7flash:ipmap sourcevalue="_add_your_value_" targetvalue="_add_your_value_"/>
    </L7flash:backendipmapping>
    <L7flash:globalvarmapping>
        <L7flash:varmap name="babou" sourcevalue="_add_your_value_" targetvalue="_add_your_value_"/>
    </L7flash:globalvarmapping>
</L7flash:ssgimportmapping>
```

Figure 14: Mapping file template sample

Note: If a mappable value is present in the imported image but is not referenced in the mapping file, then it will be imported with its original value. Similarly, when you import without a mapping file, all values that would otherwise be mappable are imported as is.

Please refer to the Policy Manager documentation for more information on:

Route via HTTP(S) Assertion
Managing Cluster-Wide Properties
Context Variables (using the *${gateway.cluster_property_name}* variable)

Managing Gateway Patches

The Gateway provides a patch management feature to help you organize the incremental patches for the Gateway appliance. These patches are issued by Layer 7 Technologies to update functionality on the Gateway appliance.

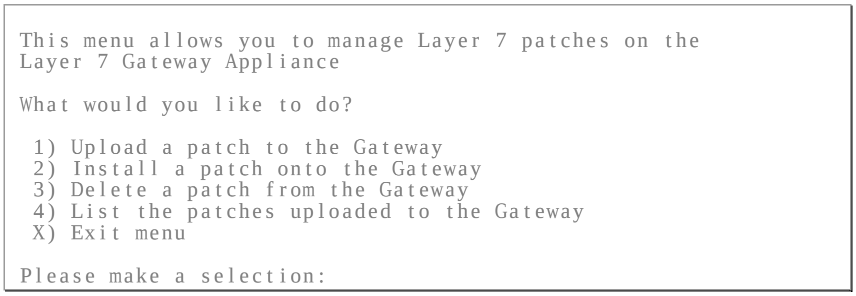
IMPORTANT: It is highly recommended that you back up your Gateway before installing a patch. For information on how to do this, see *Backing Up the Gateway* on page 60. Be prepared to restart the Gateway if the patch requires it.

Prerequisite: A patch must be copied to the appliance using the SCP command before it can be uploaded or installed. The recommended directory is */home/ssgconfig*, however it is possible to upload patches from another directory.

➢ *To access the patch management menu,*

- Select option **8** from the Gateway main menu (Figure 3 on page 12).

  The following options are presented:



```
This menu allows you to manage Layer 7 patches on the
Layer 7 Gateway Appliance

What would you like to do?

 1) Upload a patch to the Gateway
 2) Install a patch onto the Gateway
 3) Delete a patch from the Gateway
 4) List the patches uploaded to the Gateway
 X) Exit menu

Please make a selection:
```

Figure 15: Patch Management menu options

Refer to the following table for a description of each option:

Table 14: Patch management menu options

Option	Description
1) Upload a patch to the Gateway	This option scans the directory */home/ssgconfig* for eligible patches and lists them on the screen: 1. Enter the number next to the patch you wish to upload to the Gateway. 2. Press [**Enter**] to confirm the uploading of the patch. 3. A message will indicate that the patch was successfully registered. Press [**Enter**] to return to the previous menu. If the patch you wish to upload is not currently *in /home/ssgconfig,* use option **S** to enter a path to the patch to use. **Notes:** Uploading a patch does not install it—you must use option **2** to do this. Placing a patch file into */home/ssgconfig* does not make the Gateway aware of it until you use the option **1** to upload it.

Option	Description
2) Install a patch onto the Gateway	This option installs an uploaded patch. A list of eligible patches is displayed. 1. Enter the number next to the patch you wish to install. **Note:** If the patch you want is not listed, enter **X** to exit and then use option **1** to upload it first. 2. Press [**Enter**] to confirm the installation of the patch. 3. A message will indicate that the patch was successfully installed. If further configuration is required or if a Gateway restart is necessary, this will be noted on the screen. For example, the following text may be displayed after installing a custom assertion: *Please check the Gateway logs and, if the observer for CA Unicenter WSDM is NOT enabled, customize the manager SOAP endpoint by editing the cluster property cawsdm.managerSoapEndpoint and then restart the Gateway.* 4. Press [**Enter**] to return to the previous menu. 5. If a restart was indicated, return to the Gateway main menu and use option **R** to restart the appliance. **Note:** Once a patch is installed, it cannot be uninstalled unless you obtain a rollback patch (if one is available) from Layer 7 Technical Support.
3) Delete a patch from the Gateway	This option deletes an uninstalled patch from the list of registered patches on the Gateway. It physically deletes the patch from the internal repository, but not from the original pre-upload location. You will delete a patch if it has been rolled back and thus no longer required, or if a patch was uploaded in error. Note the following when deleting a patch: • Only patches in the UPLOADED or ROLLED_BACK states can be deleted. • Deleting a patch only sets its state to NONE—the patch itself is not physically removed from the appliance. • A deleted patch may be uploaded and installed again if necessary. • Deleting a patch does not "uninstall" it. If you must uninstall a patch, contact Layer 7 Technical Support for the availability of a rollback patch (not all patches can be rolled back).
4) List the patches uploaded to the Gateway	This option lists all the patches currently registered on the Gateway and their statuses. For a description of the statuses, see *Understanding the Patch States* on page 79. **Note:** Only patches that have been registered using option 1 will be shown. Patches simply copied to */home/ssgconfig* will not be listed.

Patching Using the Command Line

Patches may also be applied using the following command:

/opt/SecureSpan/Controller/bin/patch.sh *<target> <action>*

Where:

- *"<target>"* is either the patch API endpoint URL or the Process Controller home directory; if not specified, the <target> defaults to:

  https://localhost:8765/services/patchServiceApi

- *"<action>"* is one of the actions from Table 15.

When you are installing a patch, you may be prompted to restart the Gateway.

Table 15: Patcher command line actions

Action	Description
upload *<filename>*	Uploads the patch named *<filename>* to the Gateway.
install *<patch_ID>*	Installs the patch with the identifier <patch_ID>. This patch must already be uploaded using the **upload** action. A message will indicate that the patch was successfully installed. If further configuration is required or if a Gateway restart is necessary, this will be noted on the screen. For example, the following text may be displayed after installing a custom assertion: *Please check the Gateway logs and, if the observer for CA Unicenter WSDM is NOT enabled, customize the manager SOAP endpoint by editing the cluster property cawsdm.managerSoapEndpoint and then restart the Gateway.* **Note:** Once a patch is installed, it cannot be uninstalled unless you obtain a rollback patch (if one is available) from Layer 7 Technical Support.
delete *<patch_ID>*	Removes an uninstalled patch from the list of registered patches on the Gateway. It physically deletes the patch from the internal repository, but not from the original pre-upload location. Note the following when deleting a patch: • Only patches in the UPLOADED or ROLLED_BACK states can be deleted. • Deleting a patch only sets its state to NONE—the patch itself is not physically removed from the appliance. • A deleted patch may be uploaded and installed again if necessary. • Deleting a patch does not "uninstall" it. If you must uninstall a patch, contact Layer 7 Technical Support for the availability of a rollback patch (not all patches can be rolled back).
list	Lists all the patches currently registered on the Gateway and their statuses. For a description of the statuses, see *Understanding the Patch States* below.

Understanding the Patch States

The state of a patch is displayed when you run the **list** action or use the "**List the patches uploaded to the Gateway**" menu command. A patch can be in any of these states:

Table 16: Patch states

State	Description
NONE	The patch is unknown to the Gateway. This state is returned if you query an unknown patch_ID or query a patch that was uploaded and then deleted without being installed. It is also the result of deleting a ROLLED_BACK patch.
UPLOADED	The patch has been uploaded to the Gateway and its signature has been verified. The patch is available for other operations, but it is not installed yet.
INSTALLED	The patch has been installed successfully. Note that only UPLOADED patches may be installed.
ROLLED_BACK	The patch has been "uninstalled" by means of a roll-back patch. A rolled-back patch can be installed again.
ERROR	The patch installation has failed. Please contact Layer 7 Technical Support if this happens.

Viewing Patch Log Files

Log file for the patching process is located here:

/opt/SecureSpan/Controller/var/logs/patches.log

When the command line patcher is used, additional application logs can be found here:

/opt/SecureSpan/Controller/var/logs/patch_cli*.log

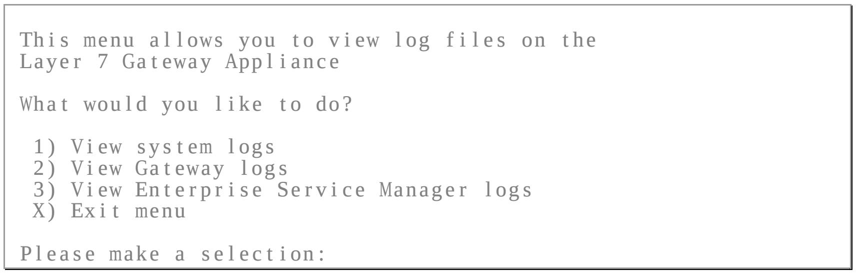
Viewing Logs on the Gateway Appliance

The Gateway appliance maintains a comprehensive set of logs that can help you troubleshoot issues. These logs can be viewed on the appliance from the Gateway main menu; many logs can also be viewed from the Layer 7 Policy Manager (see *"Viewing Logs"* in the Layer 7 Policy Manager User Manual for more information).

➢ *To view logs on the Gateway appliance:*

- Select option **9** from the Gateway main menu (Figure 3 on page 12).

  The following options are presented:



```
This menu allows you to view log files on the
Layer 7 Gateway Appliance

What would you like to do?

 1) View system logs
 2) View Gateway logs
 3) View Enterprise Service Manager logs
 X) Exit menu

Please make a selection:
```

Figure 16: View Logs menu options

Note that option "3" is available only when the Enterprise Service Manager has been installed.

Refer to the following table for a description of each option:

Table 17: Viewing each log type

Option	Description
View system logs	Use this option to view the various system logs: • **View main log:** Displays the logs from */var/logs/messages.** • **View security log:** Displays the logs from */var/log/secure.** • **View command log:** Displays the logs from */var/log/bash_commands.log.** • **View MySQL log:** Displays the log from */var/log/mysqld.log*
View Gateway logs	Use this option to view the various Gateway logs: • **View node log:** Displays the default logs from: */opt/SecureSpan/Gateway/node/default/var/logs/ssg_X_0.log* • **View host log:** Displays the logs from: */opt/SecureSpan/Controller/var/logs/sspc_X_0.log* • **View patch history log:** Displays the log from: */opt/SecureSpan/Controller/var/logs/patches.log* • **View patch client log:** Displays the logs from: */opt/SecureSpan/Controller/var/logs/patch_cli_X_0.log* • **View patch verifier log:** Displays the logs from: */opt/SecureSpan/Controller/var/logs/patch_verifier_X_0.log*

Option	Description
View Enterprise Service Manager Log *(only if ESM is present)*	Use this option to view the Enterprise Service Manager logs (if present): */opt/SecureSpan/EnterpriseManager/var/logs/ssem_X_0.log*

Configuring the Gateway Logging Functionality

Note: The Gateway Logs differs from the Audit Log. The Gateway Logs include fine-grained Gateway activity messages, whereas the Audit Log contains audit messages about more general runtime events and can only be viewed from within the Policy Manager. See *Configuring the Gateway Audit Functionality* on page 83 for more information about the Audit Log.

The Gateway Logs include fine-grained operational information such as the start-up of services within the Gateway; database connection attempts and their results; request message arrival, processing, and outcome information; errors; exceptions; and optional detailed debugging information.

Logging Levels

The Gateway uses standard Java logging levels, in both its logging and auditing:

Table 18: Java logging levels

Logging Level	Description
FINEST	Reserved for code details that are generally not required for the day-to-day running of the Gateway. Normally not logged by the Gateway or audited.
FINER	Reserved for code details that are generally not required for the day-to-day running of the Gateway. Normally not logged by the Gateway or audited.
FINE	Reserved for code details that are generally not required for the day-to-day running of the Gateway. Normally not logged by the Gateway or audited.
CONFIG	Normal running events. First level of logging that is on by default.
INFO	Normal running events. First level of system auditing that is on by default.
WARNING	Events that do not always cause errors, but that could help you find other errors. For example, a policy assertion that fails will generate a WARNING log. In this case, the Gateway did not fail, but an expected result—the success of the policy assertion—caused the warning. First level of message-level auditing that is on by default.
SEVERE	Level for serious or fatal errors in the Gateway, that either lead to inability to startup or inability to continue operating correctly. The Gateway failed on an essential operation.

Logging Level	Description
ALL	All logs or audit events are logged.
OFF	No logs or audit events are logged

When the logging subsystem on the Gateway receives messages from various sources, these messages refer to a "facility", which can represent entities such as "authpriv", "kern", "user", "daemon", etc. Based on the facility, the logging subsystem determines where the message should be stored—for example, messages from the "authpriv" facility normally goes to *a /var/log/secure.** log, while the */var/log/messages.** files store the majority of the messages.

By default, the Gateway is configured to provide logging at default set levels that should be sufficient for day-to-day operation of the Gateway. The Gateway will log events/messages to the following locations:

- **/var/log/messages.*:** These logs contain messages related to starting and stopping the Gateway, private authentication messages, and error conditions regarding the Gateway service. These logs also record the commands issued at the terminal.
- **/var/log/secure.*:** These logs contain commands entered at the terminal and all messages pertaining to authentications.
- **/var/log/bash_commands.log:** This log lists the bash commands entered at the terminal. Also records all activity from the Layer 7 Gateway main menu (see Figure 3 on page 12).
- **/opt/SecureSpan/Controller/var/logs/** : These logs contain messages generated by the process controller.
- **/opt/SecureSpan/Gateway/node/default/var/logs/ssg***: After system startup, further Gateway logs are written to log files in this directory. The logs are maintained and rolled over by the Gateway process (starting with ssg_0_0.log, up to ssg_0_9.log). By default, there are 10 log files of 20 MB each, which are used and rolled over as they fill up. The "default_startup_0_0.log" file stores startup log information.

Logs are created on startup, and logging continues between startup and shutdown. They can be manually deleted when the Gateway is not running.

Understanding Logging Thresholds

The Gateway generates log events with a range of severities, as described in *Table 18: Java logging levels* on page 81.

The *log.levels* cluster property defines the threshold for log events that are processed by the configured log sinks (that is, the minimum severity that is important enough to be processed). For more information about this property, see *Gateway (Cluster) Properties* in the *Layer 7 Policy Manager User Manual*.

Note that the *log.levels* property will control which log events are propagated to the configured log sinks. Each log sink has a "threshold": only events that meet or exceed the threshold will be processed by the log sink; all others are ignored.

If the log event severity is higher than the log level threshold, then the log event is propagated to the log sinks.

In order for a log event to be processed by a log sink, the severity of the event must meet or exceed the threshold defined by both the *log.levels* cluster property and by the log sink.

To alter the logging level threshold, modify the value of the *log.levels* cluster property and set the "<new_level>":

com.l7tech.level = *<new_level>*

to the desired value from Table 18 on page 81.

For more information on log sinks, see *Managing Log Sinks* and *Log Sink Properties* in the *Layer 7 Policy Manager User Manual*.

Note: The logging levels are an advanced feature and changes should only be made as directed by Layer 7 Technical Support.

Configuring the Gateway Audit Functionality

In the Gateway, audit events are saved in the database and viewed in the Policy Manager's View Audit Events window (see *Gateway Audit Events* in the *Layer 7 Policy Manager User Manual*). The Gateway logs audit events at the following default threshold levels:

Table 19: Default audit thresholds

Audit Events Category	Default Setting	Configurable?
System	ALL	No
Administrative	INFO	Yes
Message	WARNING	Yes
Associated	INFO	Yes

The defaults for the event thresholds can be overridden from the following locations:

- **The system.properties file:** This file controls the behavior of the particular Gateway or Gateway node (if part of a cluster).

  For more information on configuring this file, see *Appendix D: System Properties*. The audit thresholds are controlled by these system properties:

  com.l7tech.server.audit.messageThreshold
  com.l7tech.server.audit.adminThreshold
  com.l7tech.server.audit.detailThreshold
  com.l7tech.server.audit.hinting
  com.l7tech.server.audit.assertionStatus
  com.l7tech.server.audit.detailThreshold Respected
  com.l7tech.server.audit.purgeMinimumAge

- **Cluster Properties:** Cluster property settings apply to all Gateway nodes in a cluster. Audit settings configured here will override the same settings in the *system.properties* file.

  For information on configuring cluster properties, refer to *Managing Cluster-Wide Properties* in the *Layer 7 Policy Manager User Manual*. For information on the audit settings that you can configure, refer to “Audit Settings” under *Gateway (Cluster) Properties* in the *Layer 7 Policy Manager User Manual*.

Configuring the Log Message Format

The Gateway log message format can be configured by editing the following properties in the *ssglog.properties* file:

sink.format.<*format*>
sink.format.<*log sink name*>**.**<*format*>

Examples:

- *sink.format.VERBOSE* formats VERBOSE level messages for all Log Sinks
- *sink.format.MyErrorSink.RAW* formats messages for the Log Sink named “MyErrorSink”.

The following table describes the default format strings:

Table 20: Default log format strings

Log Format	Format String
RAW	`%4$s`
STANDARD	`%2$s %3$s: %4$s`
VERBOSE	`[%8$s] %2$s %3$s %6$s: %4$s`

The format string is a Java *String.format* formatting string. The following table lists the items that are available to be logged, with each referenced by number in the format string.

Table 21: Data logged by format string index

Index Value	Data
1	JVM Time in millis
2	Java Log Level (INFO, WARNING, ...)
3	Logger Name (Class originating the log message)
4	Message logged
5	Thread ID (Note this is already written to Syslog via a lower level)
6	Source Method originating the log message
7	Exception message (this is automatically added when required, don't use)
8	Log Sink Name

For information on where the log formats are used, see “Log Sink Properties” in the *Layer 7 Policy Manager User Manual*.

Configuring UDDI Registry Searches

Note: The instructions below assume that the UDDI registry product has been correctly installed, configured, and is accessible to the Gateway. See *UDDI* on page 7 for the supported registries.

You can search and publish a web service that is listed in a supported UDDI registry. The Gateway can use the APIs in a supported UDDI registry product to retrieve WSDL information about the web services registered in the UDDI registry. UDDI search results are initiated and displayed in the Policy Manager’s *Publish to UDDI Settings* and *Publish SOAP Web Service Wizard*.

➢ *To configure UDDI registry searches:*

- In the Policy Manager, use the Manage UDDI Registries task to define the UDDI registries to search. For more information, see *Managing UDDI Registries* in the *Layer 7 Policy Authoring User Manual*.

Upgrading the Gateway

Upgrades to the Gateway will be made available in accordance to your service agreement.

The following directions describe how to upgrade a standalone Gateway or a cluster of Gateways with replication enable.

Note: It is highly recommended that upgrades are performed across a secure network.

If Custom Assertions are present

If your installation includes any custom assertions, please verify with Layer 7 Technical Support prior to upgrading that you are running the most recent version and that your particular custom assertion will not cause issues during the Gateway upgrade.

Determine the Existing Version

Before upgrading, you can use the procedure below to verify the version of the Gateway application currently installed on the appliance. After upgrading, you can use these steps to validate that the installation packages were installed correctly.

➢ *To determine the version of the Gateway:*

1. Log in as *ssgconfig* and open a privileged command shell from the Gateway configuration menu (see Figure 3 on page 12).
2. At the command prompt, type:

   ```
   rpm –q ssg
   ```

   This will display the version of the Gateway currently installed.

➢ *To upgrade the Gateway:*

1. For clustered Gateways, if replication is in effect, stop the slave in MySQL on all nodes in the cluster.
2. Back up the Gateway. For more information, see page 60.
3. Disable the Gateway using option **7** (“Manage Layer 7 Gateway status”) in Table 4 on page 21.
4. Upload the relevant patch files to the Gateway. These files are available from the Layer 7 Technical Support site. ***Refer to the Release Notes for a list of the patch files required for your installation.***

   For more information on uploading patch files, see option **1** in Table 14 on page 76. For the command line equivalent, see Table 15 on page 78.

5. If platform upgrades are required, install these files first and then restart the Gateway.
6. Install the remaining patch file(s). Unless noted otherwise, the patch files may be installed in any order.

   For more information on installing patch files, see option **2** in Table 14 on page 76. For the command line equivalent, see Table 15 on page 78.
7. Restart the MySQL service on all nodes in the cluster with this command:

   ```
   service mysql restart
   ```
8. Restart the Gateway, using option **R** from Table 2. **Tip:** there may be a slight delay when restarting a virtual appliance, as the *vmware-tools_reconf_once* service takes a moment to prepare the VMware tools for the new OS kernel.
9. Choose one of the following, depending on the type of database the Layer 7 Gateway has been configured to use:
   - **MySQL database:** Upgrade the Gateway database on the node hosting the primary database. For more information, see option 1 in Table 4 on page 21.
   - **Built-in embedded database:** No further action is required. This database is updated automatically upon Gateway restart.
10. Enable the Gateway using option **7** ("Manage Layer 7 Gateway status") in Table 4 on page 21. For clustered Gateways with replication in effect, the secondary database will be replicated from the primary database.

System Health Tests

Tip: Access the Gateway IP address or the individual Gateway cluster node IP addresses from the public side of the network to test the connectivity of both the public and higher security networks.

This section describes the tests that you can run to assess the health and performance of the Gateway and your Layer 7 implementation.

ICMP Ping Test

To determine whether an individual Gateway machine is accessible through the network, use a monitoring tool (for example, *Big Brother* from www.bb4.org) or the cluster Load Balancer (see page 48) to ping the Gateway IP address or each Gateway cluster node IP address on a periodic basis.

Ping URL Test

Tips: (1) To catch potential network issues early and maximize uptime, configure a monitoring schedule of once a minute or more for each Gateway Ping URL in the implementation. Do not ping each Gateway node using Ping URL more often than once every five seconds, as doing so will affect the performance of the system. (2) For the Ping service to work successfully in a cluster over SSL, ensure that nodes in a clustered environment have been configured to trust each other. For more information, see "Managing Certificates" in the *Layer 7 Policy Manager User Manual*.

To initiate a system sanity check that tests the policy engine container and the connection to the database or replicated cluster database pair, use a monitoring tool or the Load Balancer to access the ping URL of each Gateway or each node in a Gateway cluster. The ping URL response is returned as an HTML page.

The following factors determine the outcome of a call to the ping URL:

- The setting for the *pingServlet.mode* cluster property (see *Managing Cluster-Wide Properties* in the *Layer 7 Policy Manager User Manual*)
- Whether the ping URL request was submitted via standard HTTP or encrypted HTTP using SSL (see *Syntax* below)
- Whether credentials were included in the ping URL request (see *Syntax* below)

Syntax

The syntax for submitting a ping URL test via standard HTTP:

http://*<ssghost>*:8080/*ssg*/ping

The syntax for submitting a ping URL test via encrypted HTTP using SSL:

(without credentials) https://*<ssghost>*:8443/*ssg*/ping

(with credentials) https://*<user>*:*<password>*@*<ssghost>*:8443/*ssg*/ping

Note: In Internet Explorer, embedding the username and password in the URL is not supported after installing *MS04-004 Cumulative Security Update for Internet Explorer* (832894). For more information, please see http://support.microsoft.com/kb/834489.

Where:

- *<ssghost>* is the name of the machine hosting the Gateway, in the format: *hostname.domain.com*
- *<user>* is the user ID for logging into the Gateway
- *<password>* is the password for the user ID

Note: If a user has a client certificate registered on the Gateway, then the user is required to use the client certificate when performing a ping URL test through SSL.

Ping URL Test Results

The following table summarizes the ping URL test results based on each *pingServlet.mode* cluster property setting. For information on how to set this property, see *Managing Cluster-Wide Properties* in the *Layer 7 Policy Manager User Manual*.

Table 22: Gateway ping results

Cluster Property	Description
OFF	All pings are discarded, regardless of the protocol used.
REQUIRE_CREDS (default)	For pings submitted via SSL with credentials, the following is returned: Gateway state, full cluster status, build number. For pings submitted via SSL without credentials, a "401 Unauthorized" is returned. All other ping attempts are discarded. **Note:** In REQUIRE_CREDS mode, user must belong to a role with read access to cluster node information. See *Roles and Permissions* on page 89 for more information.
OPEN	For pings submitted via standard HTTP, the Gateway state is returned. For pings submitted via SSL, the following is returned: Gateway state, full cluster status, build number. Note that credentials are not required for the OPEN setting.

Roles and Permissions

When the *pingServlet.mode* cluster property is set to REQUIRE_CREDS, the user must belong to a role with read permissions for cluster node information in order for the ping to be acknowledged. The predefined roles that include this permission are:

Administrator
Operator
Manage Cluster Status
View Audit Records and Logs
View Service Metrics

If the correct permission is not present, ping attempts from that user are discarded.

For more information about roles and permissions, see *Managing Roles* in the *Layer 7 Policy Manager User Manual*.

Full Cluster Status

When the full cluster status is displayed, a table similar to the following is displayed in the HTML results page:

Table 23: Sample full cluster status display

Node	Uptime	Status	System Info
SSG1	1 day 3 hours 2 mins	OK	SSG1
SGG2	2 days 2 hours 39 mins	Warning	SSG2
SSG3	?	FAIL	SSG3

Where:

- **Node:** Name of the Gateway node
- **Uptime:** Time duration since Gateway process startup on this node, rounded to the nearest minute. If a node has failed, the uptime will show a question mark ("?") instead.
- **Status:** Each node in the cluster updates the timestamp in the database periodically. If a node is down, the timestamp will begin to fall behind compared to the current time. The status indicators are:
  - **OK** = Timestamp is no older than 30 seconds
  - **Warning** = Timestamp is older than 30 seconds but younger than 1 hour
  - **FAIL** = Timestamp is older than 1 hour; when a node has failed, the uptime cannot be determined
- **System Info:** Click to display extended system information in a separate web page. You can use this information to help troubleshoot problems. This information will also help Layer 7 Technical Support diagnose issues should you require further assistance. **Note:** You have the roles *Administrator* or *Operator* to view extended system information.

Database Failure

If the nodes are active but the database has failed, the full cluster status shown in Table 21 will not be displayed. Instead, one of the following messages will be returned:

> *FAILURE*
>
> *FAILURE: Cannot connect to database from <machinename.domain.com>*

Tip: To verify that the Gateway is working correctly, you can configure a monitoring application to search for the string "OK" or the protocol status "200" in the HTML results page. If not found, then the monitoring system should proceed to raise an alert.

SNMP Monitoring

WARNING

SNMP support is an optional Gateway configuration with inherent security implications. The procedures required to configure the Gateway as an SNMP Agent are dependent on site and network factors and must be implemented in consultation with a Professional Services Specialist. For more information, contact Layer 7 Technologies.

For system analysis and monitoring purposes, the Gateway can act as an SNMP (Simple Network Management Protocol) Agent in an SNMP-enabled network. Using an existing tool like SNMPWALK from the Net-SNMP tool kit (http://net-snmp.sourceforge.net) configured with the MIB (Management Information Base) information in *Appendix C: Gateway MIB*, you can construct various "SNMP GET" queries or requests for Gateway CPU load, network traffic, and other basic statistical information. When queried, the Gateway will return an SNMP trap notification with the required counter data. Since the SNMP query and response processes are executed independently from the standard Gateway functionality, they will not affect the performance of the Layer 7 implementation.

The configured threshold of the Gateway's Audit Log determines the type and depth of audit records that are accessible by the SNMP queries.

Tip: Related to but separate from the Gateway's SNMP Agent functionality, you can configure a Send SNMP Trap Assertion in the Policy Manager. When encountered in a policy path, the Send SNMP Trap Assertion instructs the Gateway to broadcast an SNMP trap event to a predefined network address. The event could be an alert based on the processing result of a previous assertion, or an alert based on another policy processing outcome. For more information, see *Send SNMP Trap Assertion* in the *Layer 7 Policy Authoring User Manual*.

Rebooting the Gateway

Note: The performance of the Gateway will be slightly slower after a reboot, but will return to normal efficiency after receiving a few service requests.

You can use either of the following methods to reboot the Gateway:

- **HMI Reset Button:** A small reset button is provided on the front panel of the Gateway appliance. Press the button to reboot the system.

- **System Configuration Menu:** Use option 5 from the System Configuration Menu (see Figure 3 on page 12).

The Gateway is mostly self-healing after a system shut down. The file systems are log structured for quick recovery and reliability, services are configured for resume, and a clustered configuration will reinstate itself within minutes of the reboot. Overall, a system shut-down due to a power failure or an operator-assisted reboot will restart within five minutes, fully recovering and checking the file system and database.

Regenerating Expired Keys

Private keys in the Gateway usually have a lifetime of five years and will not require regeneration prior to their expiration date unless the Gateway host name or cluster host name changes within the active period.

To regenerate an expired key, use the *Manage Private Keys* task in the Policy Manager. This task allows you to create any number of keys and designate one to be the default SSL or default CA key.

For more information, see *Managing Private Keys* and *Private Key Properties* in the *Layer 7 Policy Manager User Manual*.

Tip: When a CA key is regenerated, certificates issued by a previous CA are still valid. All new certificates will be issued with the new CA key.

If both the CA and SSL keys required regeneration, you need to do the following:

- Refresh any Gateway or backend service has used the old SSL certificate or CA certificate to set up a trust relationship.
- Update any affected Federated Identity Provider to use the new certificates. Use Step 2 of the Federated Identity Provider Wizard to remove the old certificates and add the new ones. For more information, see *Federated Identity Provider Wizard* in the *Layer 7 Policy Manager User Manual*.

Note: A default SSL key is automatically created the first time the Gateway is started. A default CA key is not created—see *Configuring a CA Key for the Cluster* on page 56 to determine if you need one.

Understanding the Service Resolution Process

When a request is received by the Gateway, the service resolution process determines the target web service and ultimately, the policy that will be enforced by the Gateway.

Note: The resolution process does not ensure that the messages are valid or meaningful. It is recommended that your policy includes a *Validate XML Schema* assertion to ensure compliance. For more information, see *Validate XML Schema Assertion* in the *Layer 7 Policy Authoring User Manual*.

By default, Web services are accessed through the URI */ssg/soap*. However, it is recommended that you assign a custom resolution URI as opposed to using this default value. There are benefits to using a custom URI—for example, to allow the same WSDL to be published more than once. To learn how to define a resolution URI, see *Service Properties* in the *Layer 7 Policy Authoring User Manual*.

To determine the correct Web service, the resolution process uses the following steps to narrow down the possible targets. When the list of possible targets is reduced to a single Web service, the resolution is a success and the request can be routed. If no service is found, the resolution fails and an error is returned to the requestor.

Tip: Any of the following resolution logic can be disabled through the Layer 7 Policy Manager, if it is appropriate to do so. For more information, see *Managing Service Resolution* in the *Layer 7 Policy Manager User Manual*.

Step 1: Determine service based on service OID

Initially, the resolution process attempts to match the unique identifier of a service from the URL. It seeks URLs in this format:

http://gatewayhost:8080/service/123456

where *"123456"* is the OID of the service

These are the possible outcomes:

- *The URL contains a service OID and it matches a service:* The request succeeds and the appropriate policy is executed (pending *SOAP Verification*, if necessary).
- *The URL contains a service OID that does not match any service:* The resolution process fails and an error is returned to the requestor.
- *The URL does not contain a service OID:* The resolution process moves to Step 2.

Step 2: Determine service based on URI

When the incoming URL does not contain a unique service identifier, the resolution process examines the URL for a custom routing URI, for example: *http://gatewayhost:8080/customURI*.

These are the possible outcomes:

- A custom routing URI matches a single service assigned to this URI: The request succeeds and the appropriate policy is executed (pending *SOAP Verification*, if necessary).
- A custom routing URI matches more than one service with this URI: The resolution process moves to Step 3.
- A custom routing URI does not match any service: The resolution process fails and an error is returned to the requestor.
- There is no custom routing URI (i.e., the default "/ssg/soap" is used): The resolution process moves to Step 3.

Step 3: Determine service based on SOAPAction

In this step, the resolution process searches for a SOAPAction accompanying the incoming message. SOAPActions are associated with a service during publication time using a service description document provided by the administrator.

These are the possible outcomes:

- *The SOAPAction matches a published service:* The request succeeds and the appropriate policy is executed (pending *SOAP Verification*, if necessary).
- *The SOAPAction does not match any service:* The resolution process fails and an error is returned to the requestor.
- *There is no SOAPAction:* The resolution process moves to Step 4.

Step 4: Determine service based on SOAP payload namespace

In this step, the resolution process examines the namespace of the first element in the message body and tries to match it against known namespaces from the list of published services.

Note that for the purposes of service resolution, only the namespace URIs of the SOAP payload element(s) are considered, not the local names or namespace prefixes. For example, the elements *<a:doStuff xmlns:a="http://ns.example.com/services"/>* and *<b:doSomeOtherStuff xmlns:b="http://ns.example.com/services"/>* will be treated as identical by the resolution process.

These are the possible outcomes:

- *The namespace matches a published service:* The request succeeds and the appropriate policy is executed.
- *The namespace does not match any service:* The resolution process fails and an error is returned to the requestor.

Partial Matches

The resolution process routes requests to target services as quickly and efficiently as possible. It is designed to stop once it finds a single web service within Steps 1 to 4 that matches the contents of the request. This may result in only a partial match because there is no guarantee that the request will have passed any subsequent checks. For example, a request is successfully routed based on its URI (Step 2), but that does not means its SOAPAction (Step 3) or SOAP payload namespace URI (Step 4) will match the target web service.

SOAP Verification

If the request is resolved to a SOAP service (that is, one published with a WSDL), the following additional verification is performed. The Gateway will verify that:

- The request is SOAP, and
- The payload elements in the request correspond to an operation defined in the WSDL.

If both of these are satisfied, the request is routed to appropriate service.

Note: The SOAP Verification process may be overridden on a service-by-service basis. For more information, see the "WSDL" tab under *Service Properties* in the *Layer 7 Policy Manager User Manual*.

Troubleshooting Password Issues

To maintain the security of your Gateway appliance, stringent password rules are enforced for the *ssgconfig* and *root* user accounts.

Note: The stringent rules apply only to the passwords for the *ssgconfig* and *root* user accounts. Other passwords used by the Gateway are not affected and will not be locked out after unsuccessful attempts.

Password Rules

You will be required to change the password for the *ssgconfig* and *root* accounts upon first use and every 60 days thereafter. The new password must adhere to the following rules:

- Minimum 9 characters in length
- Contains at least two upper and two lowercase characters
- Contains at least two digits
- Contains at least two special characters

The new password must not be a repeat of any of the five most recent passwords and at least 24 hours must have elapsed since the last password change.

WARNING

The Gateway automatically locks the *ssgconfig* or *root* account after five unsuccessful login attempts. To restore *ssgconfig* access, see *Unlocking the SSGCONFIG Account* below. A locked root account will be unlocked automatically after 20 minutes. For instructions on restoring a locked root account immediately, contact Layer 7 Technical Support.

Unlocking the SSGCONFIG Account

Re-enabling the *ssgconfig* account requires physical access to the Gateway appliance and knowledge of the root password.

➢ *To unlock the ssgconfig account:*

1. At the console, log in as the root user.
2. Type the following command at the command prompt:

```
pam_tally2 --user ssgconfig --reset
```

You may now log in using the *ssgconfig* account. Note that lockout will again occur after five unsuccessful attempts.

Changing the SSGCONFIG Password

Changing the *ssgconfig* password requires physical access to the Gateway appliance and knowledge of the root password.

Note: You cannot change the password for an *ssgconfig* account that is currently locked.

➢ *To change the ssgconfig password:*

1. At the console, log in as the root user.
2. Type the following command at the command prompt:

```
passwd ssgconfig
```

   Follow the prompts on the screen to change the password. Note that the new password must conform to *Password Rules* on page 95.

Chapter Six: Install and Upgrade the SecureSpan XML VPN Client

The SecureSpan XML VPN Client enables fast and flexible partner or portal connectivity in XML and web services environments. Deployed as software in partner and portal environments, the SecureSpan XML VPN Client provides a code-free mechanism for managing PKI, single sign-on, federation, client-side credential management, and security change management in cross-domain and portal web services integrations.

The SecureSpan XML VPN Client is available as Red Hat Enterprise Linux or Microsoft Windows software.

System Requirements

Note: System requirements are partially determined by the nature of your Gateway deployment. Layer 7 Technologies' Professional Services Specialists will help determine any system requirements beyond the following list.

Ensure that the following system requirements are met on the target machine before installing the SecureSpan XML VPN Client:

- □500 MHz or faster processor
- 256 MB available RAM
- Hard disk with 200 MB free space
- CD-ROM reader
- □Adobe Reader for viewing PDFs (free download from www.adobe.com)
- Red Hat Linux with X-Windows or Microsoft Windows Server 2003 or Microsoft Windows XP
- Java Runtime Environment (JRE) or Java SE Development Kit (JDK) version 1.7
- Network access to a Load Balancer or Gateway on port 8080 (HTTP) and port 8443 (HTTPS)

Note: Port 8080 (HTTP) and port 8443 (HTTPS) are the default ports used by the XML VPN Client to route service messages to the Gateway. If your network set-up requires different ports, then you can change the default port settings when configuring the Gateway Account in the XML VPN Client. See the SecureSpan XML VPN Client documentation for more information.

Installing the SecureSpan XML VPN Client

Note: Ensure that the target machine meets the requirements in *System Requirements* above before you install the XML VPN Client. It is recommended that you install and configure the Gateway with one or more valid routing paths prior to installing the SecureSpan XML VPN Client.

Install the SecureSpan XML VPN Client on the same physical machine as the client application that will consume Gateway-protected services.

Linux Installation

Tip: Install the SecureSpan XML VPN Client on a modern file system like ext2/ext3 that supports full Linux file semantics instead of a FAT32/NTFS partition. The FAT32/NTFS partition does not allow uid, gid, and symlinks.

Install the SecureSpan XML VPN Client on a multi-user or a single-user Linux with X-Windows machine.

Common Installation–Multiple Users on a Single Machine

Note: The following instructions assume a root user common installation on a modern Linux system. Some of the command options may vary on Solaris, AIX, and FreeBSD.

➢ *To install the XML VPN Client for all users on a multi-user machine:*

1. Log in as the root user.
2. Insert the installation CD into the CD-ROM drive. One of the following will occur:
   - If automatic mounting is enabled, proceed to step 3
   - If automatic mounting is not enabled, type the following to mount the CD-ROM contents:

     ```
     mount -t auto /dev/cdrom /mnt/cdrom
     ```

     Proceed to step 3.

Note: The mounting command assumes that the "/mnt/cdrom" directory exists. If the directory exists but is not empty, then delete any files in the directory and re-mount the installation CD. If the directory does not exist, create it by typing “mkdir /mnt/cdrom" and then repeat the mounting command.

3. The Client.tar.gz file appears in the “/mnt/cdrom” directory To uncompress and unpack the tarball into a new local installation directory, Run the following command:

   ```
   mkdir /usr/local/securespan
   cd /usr/local/securespan/
   tar -xzvf /mnt/cdrom/ Client-<version>.tar.gz
   cd ~
   ```

   Note: The last command returns you to the default directory. It is recommended that you create and unpack the installation files into the “/usr/local/securespan/” directory. If you choose to use a different directory, then replace the "/usr/local/securespan" path with your chosen directory path in the command line. If you choose to create a different directory, then do so before using the command line. Unpacking the tarball signifies your acceptance of the terms and conditions in the License Agreement.

4. The Installation CD files appear in the target directory. To run the XML VPN Client GUI, Run the following command:

   ```
   /usr/local/securespan/Client.sh
   ```

   Consult the SecureSpan XML VPN Client documentation for configuration instructions.

5. Un-mount and eject the CD-ROM as follows:

   a. Type `unmount /mnt/cdrom`

   b. Eject and remove the CD.

Single User Installation–Single User on a Single Machine

To install the SecureSpan XML VPN Client on a single machine with single user access rights, perform steps 1 through 5 outlined in *Common Installation–Multiple Users on a Single Machine* on page 98 with the following exceptions:

- In step 1, log in with your personal user name and password
- In step 3, unpack and uncompress the installation CD files into the "$HOME/securespan" install directory by typing the following commands:

  ```
  mkdir $HOME/securespan
  cd $HOME/securespan
  tar -xzvf /mnt/cdrom/Client-<version>.tar.gz
  cd ~
  ```

- In step 4, type **$HOME/securespan/XML VPN Client.sh** to run the XML VPN Client GUI. Consult the SecureSpan XML VPN Client documentation for configuration instructions.

Windows Installation as Service

Install the SecureSpan XML VPN Client as a service under Windows when you wish to run the XML VPN Client in a non-interactive mode (for example, another service will be acting as the client). If the XML VPN Client will be securing an interactive application running on the same machine, you should install the SecureSpan XML VPN Client as an application instead (see page 104).

Tip: Even when the XML VPN Client is installed as a service, you can still run it in "application" mode by first manually stopping the SecureSpan XML VPN Client service, then running: *C:\Program Files\Layer 7 Technologies\SecureSpan XML VPN Client\SecureSpan XML VPN Client.exe*. This allows you to take advantage of the benefits offered by both modes of operation.

Refer to the following table to help you decide whether to install the SecureSpan XML VPN Client as a service:

Table 24: Installing the XML VPN Client as a Service vs. Application

XML VPN Client installed as a service	XML VPN Client installed as an application
Configuration changes take effect within 5 seconds, without needing to restart the XML VPN Client	Configuration changes take effect immediately, without needing to restart the XML VPN Client
No logon prompt. If the preconfigured user name or password is incorrect, or the current identity is not authorized to use a service, the request will fail.	Prompted for login information as required. User receives feedback if credentials are incorrect. User is prompted if credentials are needed and: ▪ they have not been entered in the current session (if "Save password to disk" is not selected), OR ▪ they have not been entered at all (if "Save password to disk" is selected), OR ▪ existing credentials were rejected for the operation that is currently being attempted
No prompt for trusting the server certificate. If the server certificate is configured improperly and the automatic certificate discovery fails, the request will fail. For more information, see *About Server Certificate Discovery* below.	Prompted with "Do you trust this server certificate?" if the automatic certificate discovery fails. Allows user to examine the certificate and take the appropriate action. For more information, see *About Server Certificate Discovery* below

XML VPN Client installed as a service	XML VPN Client installed as an application
XML VPN Client runs all the time. Any process running on the machine under any user ID can access the XML VPN Client through the localhost socket and issue requests using the credentials managed by the XML VPN Client.	XML VPN Client is available only when explicitly run. Though the same security risks are present, they are lessened because the XML VPN Client is not running as often.
Cannot view message activity.	Can see recent activity by selecting [**Window**] > **Recent Message Traffic** from the main menu. For more information, see *Analyzing SecureSpan XML VPN Client Performance* in the SecureSpan XML VPN Client documentation.

About Server Certificate Discovery

In order for the SecureSpan XML VPN Client to operate correctly, it needs a known good copy of the server certificate from the Gateway with which it is communicating. For example, in order to open an SSL/TLS connection, the XML VPN Client must discover the server certificate before it can use HTTPS.

The SecureSpan XML VPN Client can discover a good copy of the server certificate automatically if the Gateway can prove that it already knows the account password. During this process, the XML VPN Client also ensures that the certificate has not been tampered with or replaced.

- If the automatic certificate discovery succeeds, the certificate is imported without further prompting. If the automatic certificate discovery fails, the following will occur:
- If the XML VPN Client is running as a service, the request will fail.

If the XML VPN Client is running as an application, you are prompted to manually verify that you trust the server certificate

Automatic server certificate discovery works with internal users and any LDAP identity providers where the HTTP-Digest-style password hash H(A1) is available to the Gateway. On the Gateway, automatic certificate discovery is enabled only when the built-in service “Policy download service” is enabled and the cluster property *services.certificateDiscoveryEnabled* is set to “true”.

Notes:

- If you are installing over an existing SecureSpan XML VPN Client system, make sure the service has been stopped (Start menu > All Programs > SecureSpan XML VPN Client > Stop SecureSpan XML VPN Client).
- If you are installing over an existing SecureSpan XML VPN Client system that was installed as an application, be sure to uninstall the existing version first. Otherwise, you will have two instances of the XML VPN Client running.

- If your security application requests permission to install software from "Multiplan Consultants Ltd", allow it to proceed.

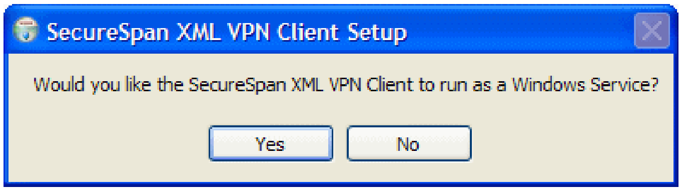
➢ *To install the XML VPN Client as a service:*

1. Close all open programs on the target machine.
2. Insert the installation CD into the CD-ROM drive. One of the following will occur:
   - The XML VPN Client Setup wizard appears. Proceed to step 3.
   - The XML VPN Client Setup wizard does not appear. Do the following:
     a. Navigate to the CD-ROM drive in Windows Explorer.
     b. Double-click on the XML VPN Client executable.
     c. The SecureSpan XML VPN Client Setup wizard appears. Proceed to step 3.
3. Follow the wizard instructions through the License Agreement, Choose Install Location, and Choose Start Menu Folder screens. The installation begins.

   If installing over an existing system, you are prompted to overwrite and reminded that the current service must be stopped.

   Note: Avoid installing the same version of the XML VPN Client more than once across different folders. If this happens, the Add/Remove Programs applet will be able to remove only the most recently installed instance of the XML VPN Client. To remove the other instances, you must manually run "Uninstall.exe" from the installation folders of the other XML VPN Client instances.

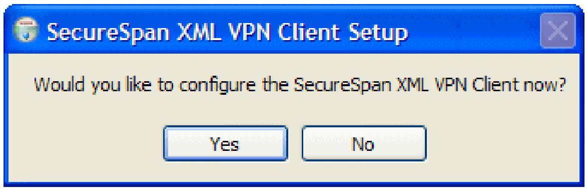
4. You are prompted whether to run the SecureSpan XML VPN Client as a service:


SecureSpan XML VPN Client Setup

Would you like the SecureSpan XML VPN Client to run as a Windows Service?

Figure 17: Running the XML VPN Client as a service

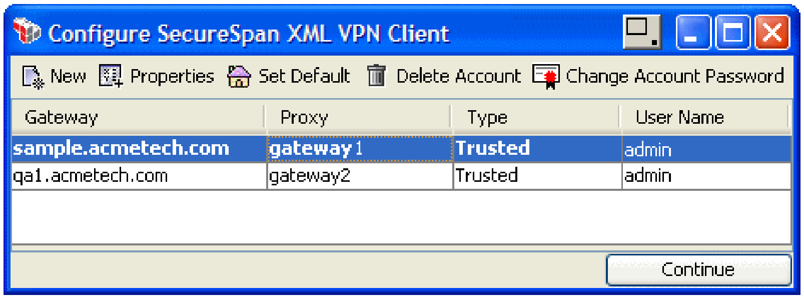
5. Click [**Yes**]. Next, you are prompted to configure the SecureSpan XML VPN Client service:


SecureSpan XML VPN Client Setup

Would you like to configure the SecureSpan XML VPN Client now?

Figure 18: Configuring the XML VPN Client

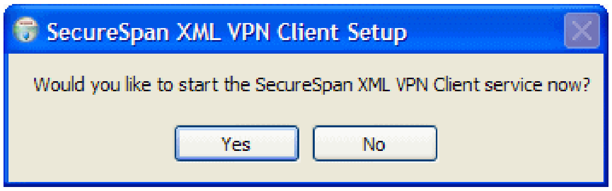
6. Choose one of the following:
   - Click [**Yes**] to configure the XML VPN Client right now. Continue with step 7.
   - Click [**No**] if you wish to configure the XML VPN Client later. If you choose this, the installation will end. You will need to manually start the configuration screen (Start menu > All Programs > SecureSpan XML VPN Client > SecureSpan XML VPN Client Config), then manually start the service (Start menu > All Programs > SecureSpan XML VPN Client > Start SecureSpan XML VPN Client Service).
7. The Configure SecureSpan XML VPN Client dialog appears. See *Configuring the SecureSpan XML VPN Client* on page 104 for more information on setting up your gateway.



Gateway	Proxy	Type	User Name
sample.acmetech.com	gateway1	Trusted	admin
qa1.acmetech.com	gateway2	Trusted	admin

Figure 19: Configure SecureSpan XML VPN Client dialog

8. When you have set up the gateway and user account, click **Continue**.
9. You are prompted whether to start the service:



Would you like to start the SecureSpan XML VPN Client service now?

Figure 20: Starting the XML VPN Client

10. Choose one of the following:
    - Click [**Yes**] to finish the installation and start the SecureSpan XML VPN Client service. You are now connected to the Gateway.
    - Click [**No**] to finish the installation without starting the service. You are not connected to the Gateway until the service is started (via Start menu > All Programs > SecureSpan XML VPN Client > Start SecureSpan XML VPN Client Service) or until the computer is restarted.

Windows Installation as Application

Install the SecureSpan XML VPN Client as a normal application if you wish to control when the XML VPN Client is running. This method is also useful for corporate environments that require a minimal number of background services running. When installed as an application, all configuration changes require that you shut down and restart the XML VPN Client before the changes take effect.

For more information on the differences between running SecureSpan XML VPN Client as a service vs. application, refer to the table on page 101.

Notes:

- If you are installing over an existing XML VPN Client system, make sure the current version is not running.
- If you are installing over an existing XML VPN Client system that was installed as a service, be sure to uninstall the existing version first. Otherwise, you will have two instances of the XML VPN Client running.
- If your security application requests permission to install software from “Multiplan Consultants Ltd”, allow it to proceed.

➢ *To install the SecureSpan XML VPN Client as an application:*

1. Follow steps 1 to 4 under “To install the XML VPN Client as a service” on page 102. In step 4, be sure to select No when prompted to install as a service.

   If installing over an existing system, you are prompted to overwrite and reminded that the current version must not be running.

2. Click Close to finish the installation.

When installation is complete, you should start the SecureSpan XML VPN Client (Start menu > All Programs > SecureSpan XML VPN Client > SecureSpan XML VPN Client). This places the XML VPN Client icon in the system tray. Click this icon to open the main window. See *Configure SecureSpan XML VPN Client* below for information on setting up your gateway.

Configuring the SecureSpan XML VPN Client

This section provides an overview on how to set up your gateway account on the SecureSpan XML VPN Client after installation is complete. For detailed information on using the XML VPN Client, please refer to the *SecureSpan XML VPN Client User Manual*.

Note: If you have installed the XML VPN Client over an existing version, your previous configuration is preserved. You will not need to configure unless any of your settings have changed.

GUI Configuration, Windows and Linux (XML VPN Client as Application)

➢ *To configure XML VPN Client using the graphical interface when installed as an application:*

1. Start the XML VPN Client, if it is not already started.
2. Click the XML VPN Client icon in the system tray. The SecureSpan XML VPN Client dialog appears.
3. Click **New** to create a new gateway account. The Create Gateway Account dialog appears.
4. Refer to *Creating a Trusted Gateway Account* in the *SecureSpan XML VPN Client User Manual* for detailed information on completing the fields.

GUI Configuration, Windows (XML VPN Client as Service)

➢ *To configure XML VPN Client using the graphical interface when installed as a service:*

1. From the Start menu, select: **All Programs** > **SecureSpan XML VPN Client** > **SecureSpan XML VPN Client Config**. The Configure SecureSpan XML VPN Client dialog appears.
2. Click **New** to create a new gateway account. The Create Gateway Account dialog appears.
3. Refer to *Create Trusted Gateway Accounts* in the SecureSpan XML VPN Client documentation for detailed information on completing the fields.

   Note that you can also run the SecureSpan XML VPN Client as an application, even when it is installed as a service. This allows you to take advantage of features not available in the service mode (see Table 22 on page 100). For more information, see the Tip on page 35.

Command Line Configuration, Windows and Linux

You can choose to configure the SecureSpan XML VPN Client from the command line, without using the graphical interface. Changes made via the command line take effect immediately, with no restart required of the XML VPN Client.

The commands do not require that the SecureSpan XML VPN Client be running.

➢ *To configure the XML VPN Client from the command line:*

1. Start the XML VPN Client Configuration Editor using one of the following commands:
   - *Windows:* Run **`ssxvcconfig.bat`**
   - *Linux:* Run **`./Client.sh –config`**
2. Enter the appropriate commands.

   Refer to the following tables for command and object information.
3. Enter **`quit`** when done.

Global Commands

The following global commands are used to create, modify, and delete information about your gateways. Note the following:

- All the commands can be abbreviated. You can either use the suggested abbreviations shown, or any other unambiguous abbreviation. For example: the "show" command can be entered as "sho" or "sh".
- The "<object>" parameter can be entered either before or after the command. For example, the "show" commands are identical:

  show gateway3 clientCert
  gateway3 show clientCert

Table 25: Command line configuration: Global commands

Command	Abbr	Description	Usage

help	h	Shows command usage information	`help`
			`help <global command>`
			`help <object>`
			`help <object> <property>`
			`help <object> <special command>`
			Examples:
			help gateway1
			h g3 disco

show	sh	Shows information about an object	`show <object>`
			`show <object> <property>`
			Examples:
			show gateways
			sh g3 clientCert

Command	Abbr	Description	Usage

set	se	Sets an object property	`set <object> <property> <value>`
			`set <object> <property>`
			Examples:
			set gateway1 defaultGateway true
			set gateway5 password s3cr3t

create	cr	Creates a new object	`create <object>`
			`create <object> <property> [<property> [<property]]]`
			Examples:
			create gateway 192.168.1.57
			create gateway ssg.example.com jsmith password123

delete	del	Deletes an object and its properties	`delete <object>` **Example:** delete gateway37
kerberos	k	Manually configure the KDC and realm to enable Kerberos. This enables the "Use Windows Domain Login" option under the [Identity] tab of the Gateway Account properties. Only required if user is not logged into a domain. This command is not required if XML VPN Client is running as an application that is logged into a domain. See also *Windows Domain Login Configuration* on page 109 for more information.	`kerberos <kdc-host> <realm>` **Example:** kerberos 10.0.0.1 DOMAIN.COM **Note:** If running the VPN XML Client as an application, need to restart the VPN XML Client before the "Use Windows Domain Login" option becomes available.
quit	q	Exit the configuration editor	quit

Objects

The following items can be used in the <object> parameter of the global commands.

Table 26: Command line configuration: Global commands, <object> parameter

Object	Abbr	Description
gateways	g	The set of all configured Gateway Accounts. Use with the show global command: *show gateways* lists the available gateways *show gateway5* shows only Gateway Account #5 *sh g5* is the same as above *create gateway* creates a new Gateway Account
gateway	g1, g2, g3, etc.	A specific Gateway Account. The gateways are automatically numbered as they are created. *show gateway3* shows info about Gateway Account #5 *sh g3* shows info about Gateway Account #3 *create gateway* creates a new Gateway Account

Properties

The following items can be used in the <property> parameter of the global commands.

Table 27: Command line configuration: Global commands, <properties> parameter

Property	Abbr	Description
hostname	host	Hostname or IP address of Gateway
username	user	Username of account on this Gateway
password	pass	Password of account on this Gateway
chainCredentials	chain	Chain credentials from client (HTTP Basic)
savePassword	save	Whether to save the password in the configuration file
preferSsl	prefer	Use SSL unless a policy says otherwise
serverCert	server	Gateway X.509 SSL certificate
clientCert	client	XML VPN Client X.509 client certificate
default	def	Make this the default Gateway Account

Gateway Commands

The following commands can be used to manipulate specific gateways.

Table 28: Command line configuration: Gateway commands

Command	Abbr	Description	Usage

discover	disco	Discover Gateway SSL certificate	`<gateway> discover serverCert`
			`<gateway> discover serverCert <thumbprint>`
			Examples:
			gateway1 discover serverCert
			g5 disco serv 4d7721111be8b56c

request	req	Request client certificate	`<gateway> request clientCert` **Example:** gateway1 request clientCert
changePass	change	Change password and revoke client cert	`<gateway> changePass <new password>` **Example:** gateway1 changePass abc123

import	imp	Import a client or server certificate	`<gateway> import serverCert <PEM or DER file>`
			`<gateway> import clientCert <PKCS#12 file> <passphrase> [<alias>]`
			Example:
			gateway3 import serverCert /tmp/cert.pem
			g7 import clientCert alice.p12 fooSecret alice

copyTo	co	Copy this configuration over top of another account	`<gateway> copyTo <target gateway>` **Example:** g7 copyTo g4

Windows Domain Login Configuration

Perform the following if using the SecureSpan XML VPN Client in a Windows Domain Login configuration.

Prerequisite: The Gateway must be configured to use Windows Domain Login. For more information, see *Using Windows Domain Login* on page 41.

➢ *To configure the XML VPN Client to use credentials from a Windows domain login (Kerberos credentials):*

1. Run the following file located in the XML VPN Client installation directory:

```
enableKerberos.reg
```

2. If not using a domain or if Linux is involved, run the **kerberos** command at the command line. For details, see Table 23 on page 107.
3. When creating a Trusted Gateway, be sure to select the [**Use Windows Domain Login**] check box on the [Identities] tab. For more information, see *Creating Trusted Gateway Accounts* in the SecureSpan XML VPN Client documentation.
4. Verify that the policy in the Policy Manager contains the Require WS-Security Kerberos Token Profile Assertion. For more information, see the *Require WS-Security Kerberos Token Profile Assertion* in the *Layer 7 Policy Authoring User Manual*.

Version Upgrades

Tip: For version-specific SecureSpan XML VPN Client information, see the Read Me file on the installation CD.

To upgrade from an earlier version to a new version of the SecureSpan XML VPN Client, uninstall the earlier version of the software as outlined in *Uninstall the SecureSpan XML VPN Client* below, then install the new version of the XML VPN Client as outlined in *Installing the SecureSpan XML VPN Client* on page 98. When installed, the new version will automatically import the Gateway Accounts configured in the previous version. It is strongly recommended that you review the details of each previously configured Gateway Account to ensure that it is accurate.

Uninstalling the SecureSpan XML VPN Client

From Linux

- *To remove the XML VPN Client from a Linux system:*

1. Log in as the root user (common installation) or with your personal user name and password (single user installation).
2. To remove the directory containing the SecureSpan XML VPN Client program files, type:

```
rm -ri usr/local/securespan/
```

Note: If a different target directory was chosen for the SecureSpan XML VPN Client installation files, then replace the “usr/local/securespan” in the command line with the alternate directory name. The command will remove the specified directory as well as its files and sub-directories. Ensure that you type the command line exactly as shown. If you make an error when using the “rm –r” command with root access, you could delete your entire system.

3. A prompt appears asking you to confirm the deletion. Enter [**Y**] for yes to proceed.
4. If upgrading the XML VPN Client, proceed to *Installing the SecureSpan XML VPN Client* on page 98 to install the new version.

From Windows

Uninstall the SecureSpan XML VPN Client from a Microsoft Windows system with the Add or Remove Programs feature, or navigate to the XML VPN Client installation folder to directly initiate the Uninstall Wizard. If upgrading the XML VPN Client, proceed to *Install the SecureSpan XML VPN Client* on page 98 to install the new version.

SecureSpan XML VPN Client Documentation

Two versions of the SecureSpan XML VPN Client documentation are available:

- A PDF and print-based “SecureSpan XML VPN Client User Manual”. The PDF version is included on the installation CD. To request a printed manual, please contact Layer 7 Technologies (see page 120)
- A program-based “SecureSpan XML VPN Client Help System”. To access the Help System, select [**Help**] > **Help System** from the SecureSpan XML VPN Client Main Menu.

Both versions contain the same content.

Chapter Seven:
Install and Upgrade the Policy Manager

The Policy Manager connects to one or more Gateways or clusters of Gateways. The GUI-based application enables administrators to centrally define, manage, verify, and audit fine-grained security and integration policies for Gateway-protected web services and XML applications. Through the Policy Manager, administrators connect to shared services, establish trust and identity sources with existing infrastructure, use these sources to define personalized policies through a declarative and rich policy language of assertions, and provision policies to existing clients.

The Policy Manager is available as Red Hat Enterprise Linux or Microsoft Windows software.

System Requirements

Note: System requirements are partially determined by the nature of your Gateway deployment. Layer 7 Technologies' Professional Services Specialists will help determine any system requirements beyond the following list.

Ensure that the following system requirements are met on the target machine before installing the Policy Manager:

- Dedicated workstation

WARNING

To minimize security risks, install the Policy Manager software on a dedicated work station.

- □500 MHz or faster processor
- 256 MB available RAM
- Hard disk with 200 MB free space
- CD-ROM reader
- □Plug-in: Adobe Reader for viewing PDFs (free download from www.adobe.com)
- Red Hat Linux with X-Windows, Solaris 10 (x86 or SPARC), or Microsoft Windows operating system installed with administrative access
- Java Runtime Environment (JRE) or Java SE Development Kit (JDK) version 1.7
- If running the Policy Manager on Linux or Solaris, the JAVA_HOME environment must point to a version 7 Sun Microsystems JDK.

- Network access to one or more Gateways through port 2124.

Installing the Policy Manager

Note: Ensure that the target machine meets the requirements in *System Requirements* above before you install the Policy Manager. It is recommended that you install and configure the Gateway with a valid HTTPS URL and port prior to installing the Policy Manager.

Install the Policy Manager on a dedicated machine on the internal local area network.

Linux/Solaris Installation

Tip: Install the Policy Manager on a modern file system like ext2/ext3 that supports full Linux file semantics instead of a FAT32/NTFS partition. The FAT32/NTFS partition does not allow uid, gid, and symlinks.

Install the Policy Manager on a multi-user or a single-user Linux machine.

Common Installation–Multiple Users on a Single Machine

Note: The following instructions assume a root user common installation on a modern Linux system. Some of the command options may vary on Solaris, AIX, and FreeBSD.

➢ *To install the Policy Manager for all users on a multi-user machine:*

1. Log in as the root user.
2. Insert the installation CD into the CD-ROM drive. One of the following will occur:
   - If automatic mounting is enabled, proceed to step 3
   - If automatic mounting is not enabled, type **mount -t auto /dev/cdrom /mnt/cdrom** to mount the CD-ROM contents. Proceed to step 3.

   Note: The mounting command assumes that the "/mnt/cdrom" directory exists. If the directory exists but is not empty, then delete any files in the directory and re-mount the installation CD. If the directory does not exist, create it by typing "mkdir /mnt/cdrom" and then repeat the mounting command.

3. The Manager.tar.gz file appears in the /mnt/cdrom directory. To uncompress and unpack the tarball into a new local install directory, Run the following command:

```
mkdir /usr/local/securespan
cd /usr/local/securespan/

tar -xzvf /mnt/cdrom/Manager-<version>.tar.gz
cd ~
```

Note: The last command returns you to the default directory. It is recommended that you create and unpack the installation files into the "/usr/local/securespan/" directory. If you choose to use a different directory, then replace the "/usr/local/securespan" path with your chosen directory path in the command line. If you choose to create a different directory, then do so before using the command line. Unpacking the tarball signifies your acceptance of the terms and conditions in the License Agreement.

4. The Installation CD files appear in the target directory. To run the Policy Manager, Run the following command:

   ```
   /usr/local/securespan/Manager.sh
   ```

5. Un-mount and eject the CD-ROM as follows:

   a. Type `umount /mnt/cdrom`

   b. Eject and remove the CD.

Single User Installation–Single User on a Single Machine

To install the Policy Manager on a single machine with single user access rights, perform steps 1 through 5 outlined in *Common Installation–Multiple Users on a Single Machine* on page 114 with the following exceptions:

- In step 1, log in with your personal user name and password
- In step 3, unpack and uncompress the installation CD files into the "$HOME/securespan" installation directory by typing the following commands:

  ```
  mkdir $HOME/securespan
  cd $HOME/securespan
  ```

  ```
  tar -xzvf /mnt/cdrom/Manager-<version>.tar.gz
  cd ~
  ```

- In step 4, type `$HOME/securespan/Manager.sh` to run the Policy Manager. Consult the Policy Manager documentation for configuration instructions.

Windows Installation

Note: Only the desktop client version of the Policy Manager requires installation. The web client version of the Policy Manager can be run from any approved browser without installation. For more information, see *Starting the Policy Manager* in the *Layer 7 Policy Manager User Manual*.

➢ *To install the Policy Manager under Windows:*

1. Close all open programs on the machine.
2. Insert the installation CD into the CD-ROM drive. One of the following will occur:

- If autorun is enabled, then the Policy Manager Setup wizard will automatically appear. Proceed to step 3.
- If autorun is not enabled, then do the following:
    a. Navigate to the CD-ROM drive in Windows Explorer.
    b. Double-click on the Policy Manager executable.
    c. The Policy Manager Setup wizard appears. Proceed to step 3.

3. Follow the wizard instructions through the License Agreement, Choose Install Location, and Choose Start Menu Folder screens. When completed, click [**Install**].

Note: To install more than one Policy Manager on the same host machine, carefully observe the following: (1) Each installation must be in a different folder; (2) Each installation must have a unique Start Menu Folder name.

4. The wizard uses a status bar to track the installation process. An Installation Complete screen will appear when completed. Click [**Close**] to close the wizard.
5. Start the Policy Manager.

Policy Manager Logs

The Policy Manager logs are stored in the following location:

- *Windows:* **C:\Documents and Settings\***<user>***\.l7tech** (default path)
- *Linux:* **/home/***<user>***/.l7tech**
- *Solaris:* **/export/home/***<user>***/.l7tech**

There may be one or more log files, named *ssm0.log*, *ssm1.log*, etc. You only need to refer to these log files when instructed to by Layer 7 Technical Support.

Note: The Policy Manager browser client does not write to the local log files on the disk. To see a record of the web client's activity, show the Java console. To do this, either:

- Select "Sun Java Console" in your browser's Tools menu if available, or
- Open the Java control panel. Select the [Advanced] tab > **Java console** > **Show console**. Restart the browser if necessary.

Version Upgrades

Tip: For version-specific Policy Manager information, see the *Read Me* file on the installation CD.

To upgrade from an earlier version to a new version of the Policy Manager, uninstall the earlier version of the software as outlined in *Uninstalling the Policy Manager on page 117*, then install the new version of the Policy Manager as outlined in *Installing the Policy Manager on page 114*. When installed, the new version will automatically import the services, security policies, identities, and other settings configured in the previous version.

Uninstalling the Policy Manager

From Linux/Solaris

➢ *To uninstall the Policy Manager:*

1. Log in as the root user (common installation) or with your personal user name and password (single user installation).
2. To remove the directory containing the Policy Manager program files, Run the following command:
   - *Linux:* `rm -ri usr/local/securespan/`
   - *Solaris:* `rmdir /path/to/dir`

   Note: If a different target directory was chosen for the Policy Manager installation files, then replace the “usr/local/securespan” in the above command with the alternate directory name. The above command will remove the specified directory as well as its files and sub-directories. Ensure that you type the command line exactly as shown. If you make an error when using the “rm –r” command with root access, you could delete your entire system.
3. A prompt appears asking you to confirm the deletion. Enter [**Y**] for yes to proceed.
4. If upgrading the Policy Manager, proceed to *Installing the Policy Manager* on page 114 to install the new version.

From Windows

➢ *To uninstall the Policy Manager:*

1. Click [**Start**] > **Control Panel** > **Add or Remove Programs**.
2. From the Add or Remove Program dialog, select **Layer 7 Policy Manager**.

3. Click [**Change/Remove**].

Policy Manager Documentation

Two versions of the Policy Manager documentation are available:

- A program-based online help system that can be accessed by either selecting [**Help**] > **Help System** from the Policy Manager or by clicking the [**Help**] button in a dialog.
- Two PDF-based user manuals: *Layer 7 Policy Manager User Manual* and *Layer 7 Policy Authoring User Manual*. These PDFs are included on the installation CD. If you require printed copies, please contact Layer 7 Technical Support.

Both versions of the Policy Manager documentation contain the same content.

Appendix A: Contacting Layer 7 Technologies

Technical Support

At Layer 7 Technologies, our commitment to exceptional service culminates in the advanced level of technical support that we provide for our Layer 7 products.

Support is provided via email and telephone:

Table 29: Layer 7 Technical Support contact numbers

Area	Phone
North America	1-888-681-9377 (toll free) 1-604-683-9330 (local)
Federal	1-800-207-8659
UK	08002796218
France	0800914728
Germany	08001827694
Italy	800789738
Spain	900987899
Switzerland	0800836638
Australia	1800621963
Email	support@layer7tech.com

For more details, please refer to your Service Level Agreement.

Contact Information

Layer 7 Technologies welcomes your questions, comments, enhancement requests, and general feedback.

Table 30: Layer 7 Technologies contact information

Phone	604-681-9377 (General) 1-800-681-9377 (North America toll free)
Fax	604-681-9387
Web	www.layer7tech.com
Email	info@layer7tech.com

Appendix B: Layer 7 Gateway Hardware Specifications

The following table summarizes the hardware specifications for the Gateway appliance.

Tip: For complete specifications for the Sun Server X3-2, see: http://www.oracle.com/us/products/servers-storage/servers/x86/sun-server-x3-2-ds-1683091.pdf

Table 31: Gateway appliance specifications

Server type	Sun Server X3-2: 1 RU base chassis with motherboard
Processor	Dual Intel Xeon E5-2640 6-core 2.5 GHz
Memory	32GB DDR2-1600 DIMM
Storage:	Sun Storage 6GB SAS PCIe HBA, Internal: 8 port 2 x 300GB 10,000RPM 2.5-inch SAS-2 HDD 4 x 2.5 inch drive slots and 1 DVD-RW disk cage
Network	4 x GE/FE NIC (dual socket systems) 2 x GE/FE NIC (single socket systems) 4 x 10GbE ports Dedicated 10/100 Base-T Ethernet network manage port
Power source	• Dual-redundant, hot-swappable power supply, 600W maximum output per power supply • Maximum AC input current at 100V AC and 600W output: 7.2A • Power supply efficiency at 600W (100%) load: 91%
Operating temperature (single, non-rack system)	• 5°C to 35°C (41°F to 95°F) • 10% - 90% relative humidity, non-condensing
Non-operating temperature (single, non-rack system)	• -40°C to 70°C (-40°F to 1587°F) • Up to 93% relative humidity, non-condensing
Operating Altitude (single, non-rack system)	Operating altitude: up to 3,000m (9,840 ft), maximum ambient temperature is derated by 1°C per 300m above 900m

Non-Operating Altitude (single, non-rack system)	Up to 12000m (39,370ft)
Acoustic noise (single, non-rack system)	7.61 Bels A weighted operating, 5.28 Bels A weighted idling

Appendix C: Gateway MIB

Note: You require a file with the following MIB (Management Information Base) information to configure an SNMP tool. For assistance, contact Layer 7 Technologies. For MIB file usage instructions, refer to the documentation accompanying your SNMP tool.

The Gateway can act as an SNMP Agent, allowing SNMP queries of basic statistical information in an SNMP-enabled network. Configure the SNMP tool with an MIB file containing the following values to enable SNMP querying (see page 91).

Table 32: Gateway Management Information Base information

IANA Organization Number	17304 as referenced in: www.iana.org/assignments/enterprise-numbers

SNMP Query Entry Point	1.3.6.1.4.1. based on:
	internet OBJECT IDENTIFIER ::= { iso(1) org(3) dod(6) 1 }
	private OBJECT IDENTIFIER ::= { internet 4 }
	enterprises OBJECT IDENTIFIER ::= { private 1 }
	l7 OBJECT IDENTIFIER ::= { enterprises 17304 }
	(1.3.6.1.4.1.17304)

Gateway SNMP Root (Main Object)	ssgmgt OBJECT IDENTIFIER ::= { l7 7 } (1.3.6.1.4.1.17304.7)
Published Services and Statistics Root	1.3.6.1.4.1.17304.7.1 field index is x: 1.3.6.1.4.1.17304.7.1.x service index is y: 1.3.6.1.4.1.17304.7.1.x.y service oid 1.3.6.1.4.1.17304.7.1.1.y service name 1.3.6.1.4.1.17304.7.1.2.y number of requests (counter) 1.3.6.1.4.1.17304.7.1.3.y authorized requests (counter) 1.3.6.1.4.1.17304.7.1.4.y completed requests (counter) 1.3.6.1.4.1.17304.7.1.5.y Alternate: service id 1.3.6.1.4.1.17304.7.1.1.x service name 1.3.6.1.4.1.17304.7.1.2.x number of requests (counter) 1.3.6.1.4.1.17304.7.1.3.x authorized requests (counter) 1.3.6.1.4.1.17304.7.1.4.x completed requests (counter) 1.3.6.1.4.1.17304.7.1.5.x
Audit Records Root	1.3.6.1.4.1.17304.7.2
Outgoing Traps Root	1.3.6.1.4.1.17304.7.3

Appendix D: System Properties

The following table lists the properties that can be used in the *system.properties* file. These properties are used to override the default behavior of the Gateway.

➢ *To add a system property:*

1. Locate and open the following file in a text editor:

   /opt/SecureSpan/Gateway/node/default/etc/conf/system.properties

2. Add a line in the format:

   ```
   [system property name] = [value]
   ```

3. Save and exit the file, then stop and restart the Gateway.

Note: In the following table, <SSG> is the home directory for the Gateway: */opt/SecureSpan/Gateway*.

Table 33: System properties

Property	Description	Default
com.l7tech.common.http.prov.apache. CommonsHttpClient.staleCheckCount	Number of stale checked connections per interval	1
com.l7tech.common.http.prov.apache. CommonsHttpClient.useExpectContinue	Use the “Expect: 100-continue” header during HTTP routing.	false
com.l7tech.common.http.prov.apache. CommonsHttpClient.noKeepAlive	Permits use of persistent connections.	false
com.l7tech.common.http.strictCookieExpiryFormat	How to respond if date format of cookie is not recognized: **true** – An exception is thrown, event is logged, and cookie is not sent **false** – No exception thrown, cookie returns to client with a max age of “0”	true
com.l7tech.external.assertions.rawtcp. defaultRequestSizeLimit	The maximum number of bytes in a raw TCP routing request (to the backend service).	1048576
com.l7tech.external.assertions.rawtcp. defaultResponseSizeLimit	The maximum number of bytes in a raw TCP routing response (returned to the Layer 7 Gateway). The default setting of “-1” indicates that the limit	-1

Property	Description	Default
	should be retrieved from the cluster property *io.xmlPartMaxBytes*.	
com.l7tech.external.assertions.samlpassertion. validateSSOProfile	Whether the *Build SAML Protocol Response Assertion* should validate profile rules. **true** – Rules are validated; if a rule is broken, assertion will fail and warning audit is logged **false** – Rules are not validated	true
com.l7tech.gateway.config.backuprestore. nouniqueimagename	Make the backup image name unique. **true** – Prefix the image name with a timestamp *yyyyMMddHHmmss* **false** – Do not add a timestamp to the image name (default)	
com.l7tech.kmp.properties	Location of *kmp.properties* file, either absolute or else relative to the directory where *omp.dat* would normally be found. The default value assumes this file is located in the same directory as the *omp.dat* file.	kmp.properties
com.l7tech.ncipher.preference	This property automatically applied when Gateway use of nCipher is enabled via the Gateway main menu, if using a FIPS level 3 security world. Manually adding this system property should not be necessary unless upgrading an existing Gateway[2].	highest
com.l7tech.security.secureconversation. defaultDerivedKeyLengthInBytes	Add these properties to change the derived key length for the default WS-SecureConversation. **Note:** The following property must also be set in the XML VPN Client: *com.l7tech.security.secureconversation.defaultDerivedKeyLengthInBytes* =16	32
com.l7tech.security.secureconversation. defaultSecretLengthInBytes		

[2] You can cause this property to be applied after an upgrade by disabling and re-enabling Gateway use of nCipher after the upgrade—see option **1** in Table 7.

Property	Description	Default
com.l7tech.server.attachmentDirectory	Directory for caching large SOAP attachments	<SSG>/node/default/ var/attachments/
com.l7tech.server.audit.messageThreshold	Minimum level required of a Message Audit record for it to be saved to the database	WARNING
com.l7tech.server.audit.adminThreshold	Minimum Level required of an Admin Audit record for it to be saved to the database	INFO
com.l7tech.server.audit.detailThreshold	Minimum Level required of an audit detail message for it to be saved to the database	INFO
com.l7tech.server.audit.hinting	Enable audit messages to provide hints for audited information (such as request XML)	true
com.l7tech.server.audit.assertionStatus	Use the highest assertion status level when checking if a record should be saved	true
com.l7tech.server.audit.detailThreshold Respected	Use the audit detail level when checking if a record should be saved	true
com.l7tech.server.audit.purgeMinimumAge	Minimum age of audit records that can be purged (in hours)	168 (1 week)
com.l7tech.server.configDirectory	Directory for Gateway configuration files	<SSG>/node/default/ etc/conf
com.l7tech.server.documentDownload.maxSize	Maximum default size (in bytes) of a document download. A value of "0" (zero) indicates unlimited size.	10485760
com.l7tech.server.home	Home directory for Gateway files	<SSG>
com.l7tech.server.hostname	Gateway hostname	OS hostname
com.l7tech.server.httpPort	HTTP port used by Gateway **Note:** Must update **server.xml** as well.	8080
com.l7tech.server.httpsPort	HTTPS port used by Gateway **Note:** Must update **server.xml** as well.	8443

Property	Description	Default
com.l7tech.server.jdbcDriver	Override default JDBC Driver class setting (as defined in *serverconfig.properties*, "jdbcConnection.driverClass.whiteList") Require Gateway restart to take effect.	
com.l7tech.server.keystore.enablehsm	Indicates whether an internal Hardware Security Module is present	false
com.l7tech.server.ldapTemplatesPath	Path to LDAP templates	
com.l7tech.server.maxLdapSearchResultSize	Number of max results in an identity provider search result operation	50
com.l7tech.server.metrics.fineBinInterval	Time period for fine Service Metrics bins (milliseconds)	5000
com.l7tech.server.multicastAddress	Multicast address for server cluster	randomly created
com.l7tech.server.outConnectTimeout	I/O timeout for outbound connection (milliseconds)	30000
com.l7tech.server.outTimeout	I/O timeout for outbound response (milliseconds)	60000
com.l7tech.server.rateLimit	Minimum permissible rate for incoming requests (bytes per second)	1024
com.l7tech.server.rateTimeout	I/O timeout for incoming request rate checking (milliseconds)	60000
com.l7tech.server.serverID	Numeric server identifier	IP address of Gateway
com.l7tech.server.timeout	I/O timeout for incoming requests (milliseconds)	60000
com.l7tech.server.transport.jms.detectJmsTypes	Auto detect JMS provider type, if using ActiveMQ or WebLogic. **true** – Auto detect the JMS type (either queue or topic). If unable to detect the type, generic JMS connection type is used. **false** – Do not auto detect the JMS type; always use generic JMS connection type. **Note:** Contact Layer 7 Support if connecting to more than one JMS provider.	true

Property	Description	Default
com.l7tech.server.uddi.auto_republish	Republish to UDDI as needed (e.g., when the cluster hostname or port number changes)	true
com.l7tech.util. allowDuplicateIdAttrsOnElem	Allow messages with an element that has duplicate ID attributes **Tip:** For greater security, set this property to “false” to reject any message with an element that has more than one attribute recognized as an ID attribute.	True
policyValidation.maxPaths	The maximum number of possible paths through a policy before the policy is considered to be too complex to attempt server-side validation.	500000

Appendix E: WSDL Proxy & Policy Downloads

This appendix describes the ways to download a WSDL document or a policy document. The HTTP URLs described here can resolve a service WSDL, even if the initial service is deleted and a new service based on the same backend service is added.

Configuring Gateway Passthrough

You can configure the Gateway to allow particular IP addresses and/or subnets to retrieve WS-Policy and/or WSDL documents without authentication. Requests originating from these exempted addresses will pass through unchallenged; requests from other addresses will be required to provide credentials corresponding to users authorized to consume the published service. If a service is accessible anonymously, the corresponding WSDL and Policy documents will always be downloadable without the need to provide credentials.

To configure a passthrough, modify the gateway cluster property *service.passthroughdownloads*. By default, passthroughs are permitted only by the localhost. For more information, see *Gateway (Cluster) Properties* and *Managing Cluster-Wide Properties* in the *Layer 7 Policy Manager User Manual*.

Downloading a WSDL

Tip: WSDL documents for secure services will only be provided over SSL.

There are several ways to retrieve a WSDL document. The simplest method is to use this URL:

http://*<SSG_machine>***:8080/ssg/wsdl**

Where “*<SSG_machine>*” is the Gateway host name (for example, “ssg.acme.com”). This will display a list of all WSDL documents that correspond to anonymous services published on the Gateway.

To see a list of WSDL documents on a protected service, use this URL:

https://*<SSG_machine>***:8443/ssg/wsdl?anon=false**

Or:

https://*<SSG_machine>***:8443/ssg/wsil?anon=false**

You will be prompted to enter login credentials for the Gateway.

Note: By default, you cannot download WSDL and policy documents from a disabled service. You can override this behavior using the *service.disabledDownloads* cluster property. For more information, see *Gateway (Cluster) Properties* in the *Layer 7 Policy Manager User Manual*.

Returning WSDLs for a Specific Service

To return WSDL documents for a specific service, append the service OID to the URL:

```
http://<SSG_machine>:8080/ssg/wsdl?serviceoid=1234567
```

If the service does not allow anonymous access, use this URL:

```
https://<SSG_machine>:8443/ssg/wsdl?serviceoid=1234567
```

Using the service OID is the most reliable mechanism for retrieving a specific WSDL for a service, as more than one service can have the same URI, SOAPAction, or namespace. If you do not know the service OID, you can still use one of the following methods to attempt to retrieve the WSDL.

Note: If you attempt a download from a machine that does not qualify for a passthrough, the WSDL download may fail. For more information, see *Configuring Gateway Passthrough* on page 131.

WS Policy Attachments

When an Enforce WS-Security Policy Compliance Assertion is present in the policy when the WSDL document is downloaded, the WS-Security Policy translation of the services policy is appended to the WSDL document. If the original WSDL contains a WS-SP policy, it is removed.

For more information, see *Enforce WS-Security Policy Compliance Assertion* in the *Layer 7 Policy Authoring User Manual*.

WSDL URL by Resolution URI

You can retrieve a WSDL by specifying the resolution URI in the URL:

```
http://<SSG_machine>:8080/ssg/wsdl?uri=/xml/foo
```

You can also retrieve the WSDL by appending “?wsdl” to the services resolution path. Such requests are translated into requests for the WSDL proxy; for example:

```
http://<SSG_machine>/myservice?wsdl
```

This would be translated into the equivalent request:

```
http://<SSG_machine>/ssg/wsdl?uri=/myservice
```

When the WSDL does not permit anonymous access, use “?wsdl&anon=false” to force an authentication challenge.

Notes: (1) The “?wsdl” suffix works only when If there is a single web service published at any given path. (2) Downloading the WSDL using the “?wsdl” suffix may be disabled using the *service.wsdlQueryEnabled* cluster property.

The Gateway will respond as follows:

Scenario	Result
One service resolves at specified URI	WSDL for that service is returned
No service resolves at specified URI	*404 Error – File Not Found* is returned
Multiple services resolve at specified URI[3]	Ambiguous; error is returned

Case Sensitivity in URL

By default, the services are matched in a case sensitive manner. If case sensitivity for service resolution is disabled, then services are matched accordingly.

For example, consider the following URLs for requesting a WSDL:

http://localhost:8080/ssg/wsdl?uri=/warehouse
http://localhost:8080/warehouse?wsdl

In the examples above, the value “warehouse” will be compared case sensitively or case insensitively, depending on the resolution settings.

For information on case sensitivity during service resolution, see *Managing Service Resolution* in the *Layer 7 Policy Manager User Manual*.

WSDL URL by Namespace

You can retrieve a WSDL by specify the namespace in the URL:

```
http://<SSG_machine>:8080/ssg/wsdl?ns=http://acme.com/ns/ws/foo
```

This namespace, sometimes called the SOAP payload namespace URI, corresponds to a namespace used by the child elements under the Body element of the SOAP envelope.

The Gateway will respond as follows:

Scenario	Result
Only one service uses the namespace	WSDL for that service is returned

[3] Although URIs are typically used to resolve a service uniquely, they can technically resolve to multiple services in the Gateway if other resolution parameters do not conflict.

Scenario	Result
No service use the namespace	*404 Error – File Not Found* is returned
Multiple services use the namespace	Ambiguous; error is returned

WSDL URL by SOAPAction

You can retrieve a WSDL by specify the SOAPAction in the URL:

http://*<SSG_machine>***:8080/ssg/wsdl?soapaction=http://acme.com/ws/action/foo**

The Gateway will respond as follows:

Scenario	Result
Only one service uses the SOAPAction	WSDL for that service is returned
No service use the SOAPAction	*404 Error – File Not Found* is returned
Multiple services use the SOAPAction	Ambiguous; error is returned

WSDL Resolution Using a Combination

You can further refine the WSDL to retrieve by using a combination of the above proxies. For example:

http://ssg.acme.com:8080/ssg/wsdl?ns=namespace1&uri=/xml/foo

The WSDL for that service is returned if found, otherwise an error is returned.

Note: If a *serviceoid* is specified, that takes precedence over any other parameter.

Downloading a Policy Document

To download a policy document, use this URL form from a browser:

http://*<SSG_machine>***:8080/ssg/policy/disco?serviceoid=1234567&fulldoc=yes**

Where <*SSG_machine*> is the Gateway host name (for example, “ssg.acme.com”) and “1234567” is the unique ID of the published service.

Note: If you attempt a download from a machine that does not qualify for a passthrough, you may receive an authentication challenge. For more information, see *Configuring Gateway Passthrough* on page 131.

Appendix F: Gateway Observer for CA Unicenter WSDM

This appendix describes how to install and configure the Gateway Observer for CA Unicenter WSDM version 3.50.

Note: Be sure the CA Unicenter WSDM product has been installed and configured before continuing.

This appendix contains the following sections:

- Installing the Gateway Observer
- Configuring the Gateway Observer
- Configuring the WSDM Manager
- Disabling the Gateway Observer

Installing the Gateway Observer

Linux Installation

➢ *To install the Gateway Observer under Linux:*

1. Log in as root on the Gateway. Enter your user name and password at the prompts. The Gateway command shell appears.
2. Locate the **CaWsdmAssertion-4.2.0.aar** file and then copy it into the */opt/SecureSpan/Gateway/runtime/modules/assertions* directory on each Gateway machine in the cluster
3. If the Gateway is not currently running, start the Gateway. Otherwise, wait 10 seconds for the running Gateway to pick up the new module.
4. Reconnect the Policy Manager to the Gateway, then do the following:
   a. From the Tools menu (Manage menu from the browser client), select **Manage Cluster-Wide Properties**.
   b. Click [**Add**]. The New Cluster Property dialog appears.
   c. Review the Key drop-down list to ensure that the new CA WSDM properties, including “cawsdm.managerSoapEndpoint” are present.

Windows Installation

The Windows installation procedure is the same as Linux, except in step 2, the .aar file should be copied to this folder:

C:\Program Files\Gateway\modules\assertions

Configuring the Gateway Observer

➢ *To configure the Gateway Observer:*

1. From the Tools menu (Manage menu from the browser client), select **Manage Cluster-Wide Properties.**
2. In the property **cawsdm.managerSoapEndpoint**, enter the actual hostname of the WSDM Manager in the URL.
3. Review the other cluster properties with the prefix “cawsdm” and modify as required.
4. Restart the Gateway.

Proceed to *Configuring the WSDM Manager* next.

Configuring the WSDM Manager

➢ *To configure the WSDM Manager to recognize the Gateway Observer type:*

1. Locate the following file on the WSDM Manager machine and open it in a text editor:

   ```
   C:\Program Files\CA\Unicenter
   WSDM\server\default\conf\WsdmSOMMA_Basic.properties
   ```

2. Add the following line:

   ```
   observertype.777=Gateway
   ```

   The number “777” is used as an example. If that value is already used, choose a different one. The value used here must match the cluster property *cawsdm.observerType.*

3. Restart the WSDM Manager.

Disabling the Gateway Observer

➢ *To temporarily disable the Gateway Observer for CA Unicenter WSDM:*

1. Create an empty file with the same name as the CA WSDM .aar file but with the additional suffix “.DISABLED”:

   ```
   /opt/SecureSpan/Gateway/runtime/modules/assertions/CaWsdmAssertion-
   4.2.0.aar.DISABLED
   ```

2. Wait 10 seconds.

To re-enable the Gateway Observer, delete the .DISABLED file and wait 10 seconds.

Using the Gateway Observer Cluster Properties

The following table summarizes the cluster properties added to the Gateway once the CA WSDM Gateway Observer is installed.

Notes: For more information about cluster properties in general, see *Gateway (Cluster) Properties* in the *Layer 7 Policy Manager User Manual*. For more information about the Gateway Observer properties, see “Parameters” in “Chapter 10: Deploying a .NET Observer” of the *Unicenter Web Services Distributed Management Implementation Guide*.

Table 34: Gateway Cluster Properties - Audit settings

Name	Description
cawsdm.autoDiscover	Determines whether the Observer reports all newly discovered WSDLs and then registers them with the Catalog. If this property is set to “no”, all new WSDL files must be manually imported into the Catalog for the services to be registered. Values are yes/no. For a description of this functionality, see “Maintaining the Catalog” in the CA Unicenter WSDM online help. Default: **yes**
cawsdm.blockUnknown	Determines whether all requests arriving at the Observer will be allowed through, even if the request was not previously identified in the Manager Catalog. If this property is set to “yes”, the Observer will not process unidentified requests. Values are yes/no. Default: **no**
cawsdm.log.echo.debug	Logs debug information to the console. Value is a Boolean. On the Gateway, items logged to the console can be found in this directory: */opt/SecureSpan/Gateway/node/default/var/logs* Default: **false**
cawsdm.log.echo.error	Logs error information to the console. Value is a Boolean. Default: **true**
cawsdm.log.echo.info	Logs info details to the console. Value is a Boolean. Default: **false**
cawsdm.log.echo.warn	Logs warning information to the console. Value is a Boolean. Default: **true**

Name	Description
cawsdm.log.enable.debug	Logs debug information to the log file. Value is a Boolean. On the Gateway, the log files can be found in this directory: */opt/SecureSpan/Gateway/*node/default/var/logs/ca_wsdm_observer/ Default: false
cawsdm.log.enable.error	Logs error information to the log file. Value is a Boolean. Default: true
cawsdm.log.enable.info	Logs info details to the log file. Value is a Boolean. Default: false
cawsdm.log.enable.warn	Logs warning information to the log file. Value is a Boolean. Default: true
cawsdm.log.file.maxsize	Sets the maximum size of the Observer log files (bytes). Default: 10485760
cawsdm.logSoap	Determines whether SOAP messages are logged: • yes = All SOAP messages passing through the Observer will be sent to the WSDM Manager for logging; SOAP messages are included in the local log records. **Note:** Setting this property to "yes" may cause excessive logging. • no = Only fault messages and messages that violate single transaction threshold monitors will be sent to the WSDM Manager; SOAP messages are omitted from the local log records. Default: no
cawsdm.managerSoapEndpoint	The WSDM Manager endpoint address (URL). This is required; if not specified, the Observer will be disabled. Default: http://hostname:8282/wsdm35mmi/services/WSDM35MMI
cawsdm.messageBodyLimit	Maximum number of characters per message body to send to the WSDM Manager, if sending is enabled. The purpose of this property is to prevent excessive network usage. Default: 5000
cawsdm.observerType	The Observer type to display in the WSDM Manager (integer). Be sure to add the following entry to the *\Program Files\CA\Unicenter WSDM\server\default\conf\WsdmSOMMA_Basic.properties* file on the WSDM Manager: `observertype.777=Gateway` Default: 777

Name	Description
cawsdm.queueSizeMax	The maximum number of messages permitted in the queue. **Note:** If no maximum value is specified, a memory error may occur under heavy traffic load. Conversely, setting the maximum too low may result in loss of data when the upper limit is exceeded. Adjust this parameter to define an appropriate maximum queue size for your environment. Default: 0 (no limit)
cawsdm.queueSizeMin	The minimum number of messages that must be stored before messages are transmitted. This allows for transaction-based buffering of data at the Observer level before it is sent to the Manager. Default: 1
cawsdm.sendSoap	Determines whether SOAP messages are sent: • no = SOAP messages will not be sent to the Manager. When set to "no", this parameter takes precedence over the cawsdm.logSoap parameter to ensure that no SOAP messages are sent to the Manager. • yes = sending of SOAP messages to the Manager is determined by the cawsdm.logSoap parameter. **Note:** Setting this parameter to "yes" will increase CPU and network load on the Gateway. Default: no
cawsdm.standaloneMode	Specifies whether the Observer logs messages without Manager availability. Set this as resources permit. Value is yes/no. Default: no
cawsdm.waitPeriod	The maximum amount of time (in minutes) to wait before the Observer tries to resend data to the Manager if the connection between the two has been broken. Set this as system resources permit. Default: 5

Appendix G: Installing the JMS Interface

This appendix provides a high level overview on how to add JMS support to the Gateway. It assumes that the target middleware system has been correctly installed and configured and that you are familiar with the JMS specifications.

Introduction

The Gateway can work with a variety of message-oriented middleware (MOM) systems, including:

- TIBCO EMS
- IBM WebSphereMQ
- FioranoMQ
- webMethods Broker
- WebLogic JMS

Please contact Layer 7 Technical Support for assistance with other JMS providers.

The MOM systems are accessed through the JMS interface. To enable JMS queues on the Gateway, the appropriate client libraries must be installed first.

Due to licensing issues, the client libraries are not included with the Gateway.

Installing the Client Libraries

The client libraries must be installed in the following directory:

```
/opt/SecureSpan/Gateway/runtime/lib/ext/
```

For WebSphere MQSeries, the following libraries are installed:

com.ibm.mq.jar
com.ibm.mqbind.jar
com.ibm.mqjms.jar
connector.jar

For TIBCO EMS, the following libraries are installed

tibjmsapps.jar
tibjmsadmin.jar
tibrvjms.jar

tibjms.jar
tibcrypt.jar

Tip: It is recommended to use the SFTP, SCP, or similar methods to copy the library files.

Once the libraries are installed, restart the Gateway.

Configuring the JMS Queues

The JMS interface is enabled when the Gateway is restarted. You can now:

- **Configure a JMS queue**

  For details, see *Managing JMS Queues* in the *Layer 7 Policy Manager User Manual*.

- **Add the Route via JMS Assertion to a policy**

  For details, see *Route via JMS Assertion* in the *Layer 7 Policy Authoring User Manual*.

Appendix H: Cluster Configuration Worksheet

Use the following worksheet to record configuration information during the cluster preplanning stage and to assist you when configuring the cluster (see *Configuring the First Gateway Processing Node* on page 55).

Table 35: Cluster configuration worksheet

Description	Example Value	MY VALUE
Gateway cluster Fully-Qualified Domain Name (FQDN)	clusterhostname.mycompany.com	
IP address for clusterhostname (load balancer)	10.0.0.10	
Gateway node host names	ssg1.mycompany.com, ssg2.mycompany.com	
IP addresses for nodes	10.0.0.11, 10.0.0.12	
MySQL database nodes	ssg1.mycompany.com, ssg2.mycompany.com	
MySQL root user name	root	
MySQL root user password	password	
MySQL database replication username	repluser	
MySQL database replication password	replpass	
Gateway database name	ssg	
Gateway database user	gateway	
Gateway database password	7layer	
Keystore password	7layer	
Cluster Configuration passphrase	7layer	

Appendix I: Network Deployment Guide

This appendix describes the various scenarios possible for deploying the Gateway within a network. In particular, it may be necessary to separate service networks from management networks to increase organizational security.

The following scenarios are described:

- **Single network:** All network communication is handled within the Internal Management LAN (“eth0”).
- **Two domain network:** Two networks are used: a Wide Area Network representing the public side (“eth1”) and the Internal Management LAN for the private side (“eth0”).
- **Three and four domain network:** Three or more networks are used: a Wide Area Network for the public side (“eth1”), Internal Management LAN for the private side (“eth0”), and one or two Internal Service LANs (“eth2” and “eth3”)

The following pages describe each scenario in more detail.

For additional assistance in deploying the Gateway on your network, please contact Layer 7 Technical Support.

Single Domain Network

The single network configuration is used in scenarios where is no need to separate management and message and back end traffic (for example, proof of concept, development, and testing setups, or an ESB deployment). In this configuration, all networking occurs within the Internal Management LAN (eth0).

The single network configuration is simple and straightforward, but is not a common production deployment.

Figure 18 illustrates the components within a single network configuration.

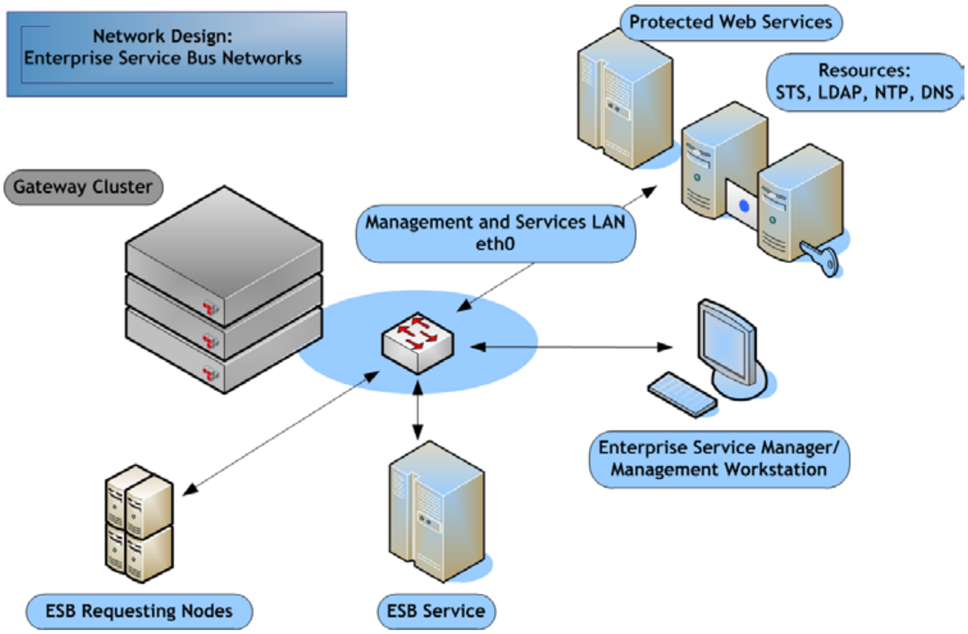


Figure 21: Network deployment: single domain network

Two Domain Network

The two domain network is used in more complex layouts, where the service consumers are separate from the services protected by the Gateway cluster. In this layout, the services and management are connected to the Internal Management LAN (eth0), while the "public side" is connected to the WAN (eth1).

This layout assumes that no workstations on the public side are allowed to access management functions. A load balancer may be used on the public side to provide load sharing and high availability.

Figure 19 illustrates the components within a two domain network configuration.

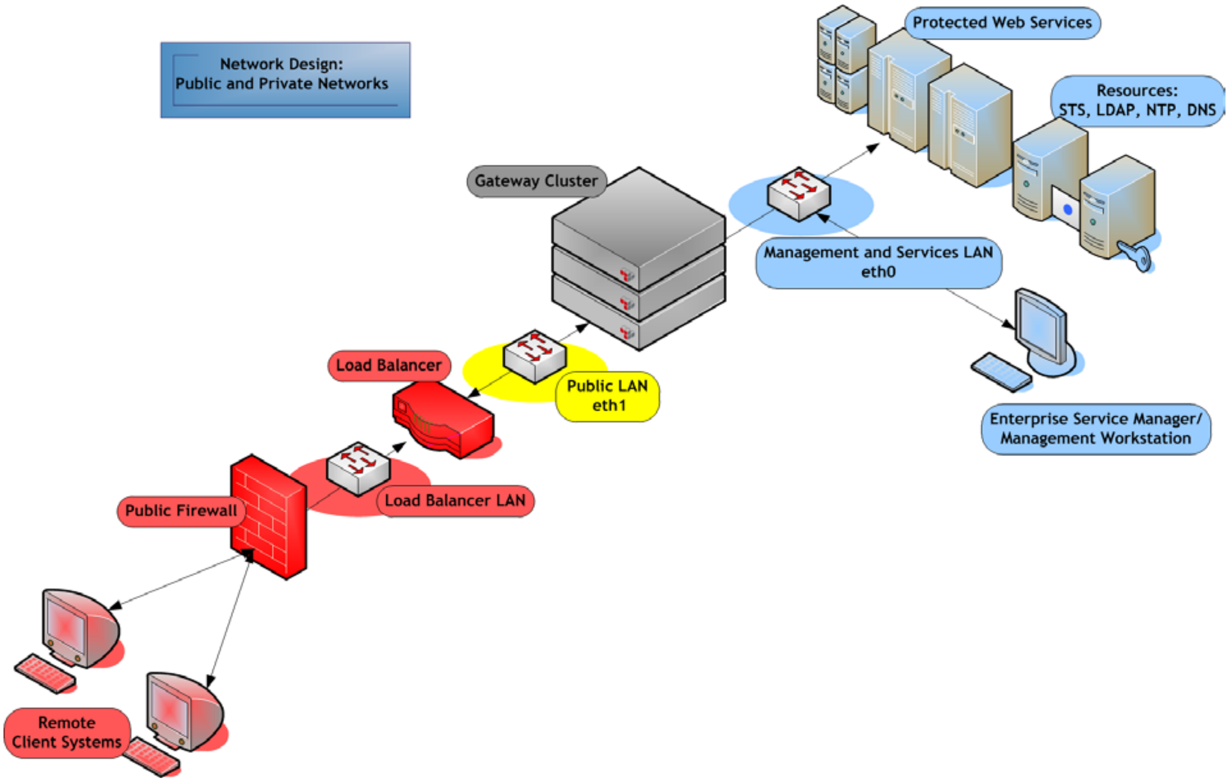


Figure 22: Network deployment: two domain network

Three and Four Domain Network

In high security environments, management workstations may be separated from services networks. In this multi-network setting, the “public side” is expected to have a load balancer and be on the WAN (eth1), while the management network is on the Internal Management LAN (eth0). The service networks are on the Internal Service LANs (eth2, eth3), so that there is no direct access from management nodes to the service systems, except via the Gateway cluster.

Figure 20 illustrates how it is possible to separate web services from corporate resources such as LDAP using all four network interfaces.

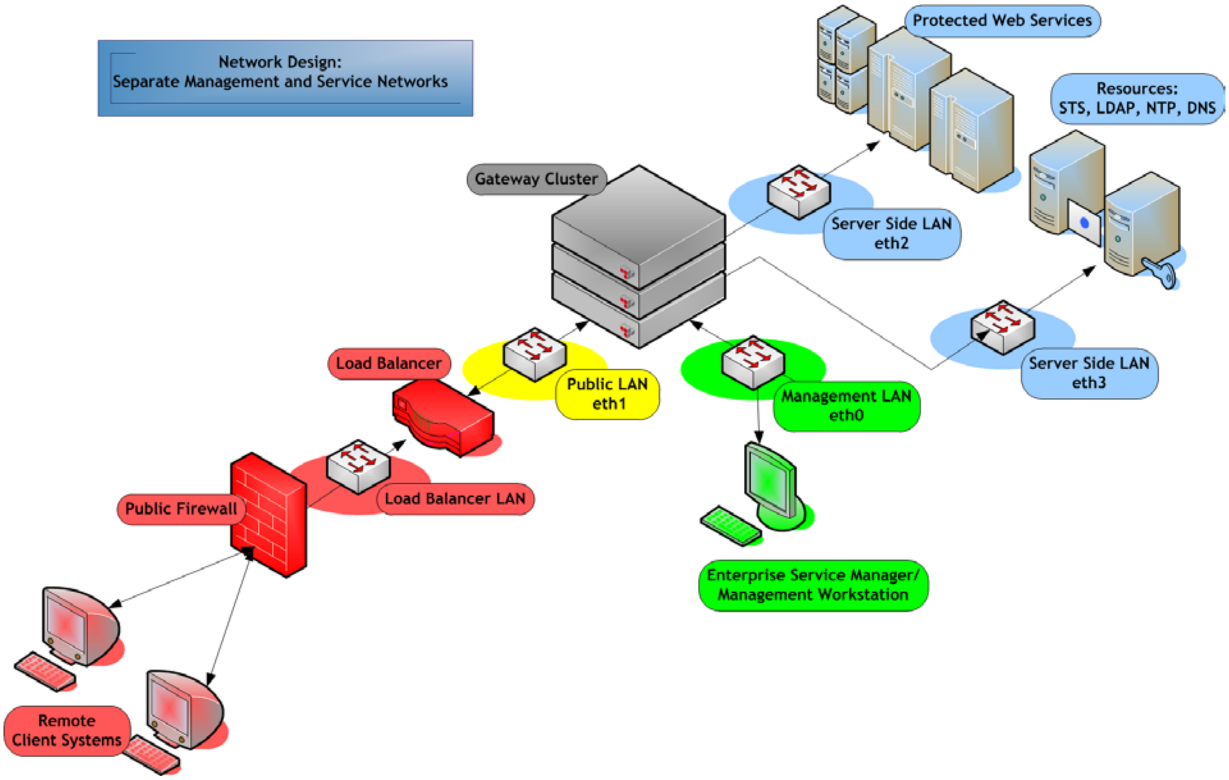


Figure 23: Network deployment: three and four domain network

Appendix J: Gateway System Recovery

This appendix describes how to restore your Gateway using the *Gateway Recovery Disk*. This disk will restore a Gateway to its factory state, erasing all information on the hard drive. Use it when you need to do the following:

- The Gateway appliance needs to be rolled back because of a failed upgrade, or as part of a disaster recovery plan.
- The Gateway appliance becomes corrupted for whatever reason or a faulty hard drive is replaced.
- The Gateway needs to be restored to a baseline state when running in a test environment or when moving from a test environment to a production environment.

Note: The Gateway Recovery Disk is not shipped with the appliance. Please contact Layer 7 Technical Support to obtain this disk.

Supported Hardware

The recovery disk supports the following hardware configurations:

- Sun X4100 and X4150 appliances, as shipped from Layer 7 Technologies
- Tarari PCI card
- Sun Crypto Accelerator 6000 PCIe HSM (SCA6000)
- Thales nCipher HSM

Important Notes

Please be aware of the following before proceeding:

- The recovery disk is intended for use only on Gateways delivered as an appliance. It will not work on software Gateways or VMware Gateways. **DO NOT USE THE RECOVERY DISK ON NON-GATEWAY MACHINES. THE RECOVERY WILL FAIL AND ALL DATA ON THE NON-GATEWAY MACHINE'S HARD DRIVE WILL BE LOST.**
- Hardware added to the appliance after delivery by Layer 7 Technologies is not supported.
- The recovery process erases the *entire* hard drive, not just the current partition. Anything stored in other partitions on the hard drive will be lost.

- If possible, back up the Gateway database first. You will be able to restore the database and configuration files when recovery is complete. For more information, see *Backing Up the Gateway* on page 60.
- Be sure you have a copy of the Gateway license file stored elsewhere for safekeeping. The license is stored with the database, so if you have backed up the database file first, the license will be applied upon restoration of the database.

Using the Recovery Disk

IMPORTANT: If your Gateway is part of a cluster, please contact Layer 7 Technical Support for information on removing the Gateway from the cluster prior to reimaging.

➢ *To recover the Gateway using the recovery disk:*

1. Back up the database, if possible. See *Backing Up the Gateway* on page 60.
2. Insert the recovery disk in the disk drive and reboot the appliance. See *Starting and Stopping the Gateway* on page 39.
3. Follow the prompts on the screen to begin the recovery process. You can choose to either have the appliance reboot or shut down after the recovery is finished. When the recovery is complete, the appliance is restored to a factory-shipped state.
4. Configure the restored Gateway. For more information, see *Chapter Three: Configure the Gateway*.
5. When configuration is complete, restore the Gateway database, if it was backed up in step 1. For more information, see *Restoring the Gateway* on page 66.
6. Redo any additional configuration that was made since the Gateway was installed, for example: SNMP, static routing, Gateway redirect rules, keyboard settings, database replication, etc. For assistance, please contact Layer 7 Technical Support.

Note: The recovery process cannot be interrupted. If recovery was unsuccessful, the hard drive has already been erased. The only option is to run the recovery disk again.

Index