CA API Management

CA API Gateway Administrators Manual

Version 8.3

This documentation and any related computer software help programs (hereinafter referred to as the "Documentation") are for your informational purposes only and are subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW OR AS AGREED BY CA IN ITS APPLICABLE LICENSE AGREEMENT, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO THE END USER OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Contents

List of Figures

List of Tables

Chapter One: Overview

About This Manual

The *CA API Gateway Administrators Manual* provides:

- Basic product information
- Gateway operations, system requirements, installation, configuration, maintenance, upgrade, and troubleshooting information and instructions
- CA API Gateway – Policy Manager installation and upgrade information and instructions
- CA API Gateway - XML VPN Client installation and upgrade information and instructions
- Technical support contact information

Note: For information on how to install, configure, and upgrade the Gateway, please refer to CA API online documentation located at wiki.ca.com/Gateway.

Audience and Assumptions

The *CA API Gateway Administrators 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 CA API Gateway 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
- Advanced knowledge of your operating system is required.

Overview of CA API Gateway Products

The CA API Gateway 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:

CA API Gateway
CA API Gateway - Policy Manager
CA API Gateway – XML VPN Client

Tip: See "Production Network Architecture" on page 7 for a diagram of the CA API Gateway products in a typical network configuration.

The **CA API Gateway** is an 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 2, "About the Gateway".

The **CA API Gateway - 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 4, "Install and Upgrade the Policy Manager".

The **CA API Gateway – XML VPN Client** is a cross-domain enablement product designed to speed and secure web services integrations spanning identity and security domains. The CA API Gateway – XML VPN Client is available as software for Red Hat Enterprise Linux or Microsoft Windows server environments. For more information, see Chapter 5, "Install and Upgrade the CA API Gateway – XML VPN Client".

Supported Standards

For a list of the system requirements for each product, please refer to the page https://wiki.ca.com/GATEWAY/Gateway+Feature+Support+Matrix on the CA API Gateway documentation site.

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 (see “Form Factors” on page 6). This Manual describes the software implementation of the Gateway.

Note: The information in this chapter applies to the three different versions of the Gateway: *API Proxy, XML Firewall,* and *SOA Gateway*. To learn about the differences in functionality between these versions, refer to “Product Summary” in the CA API Gateway online documentation located at wiki.ca.com/Gateway.

Gateway Architecture

The working unit of the Gateway is an HTTP, JMS, or FTP-accessible endpoint. Clients access the Gateway via a URI or queue 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.

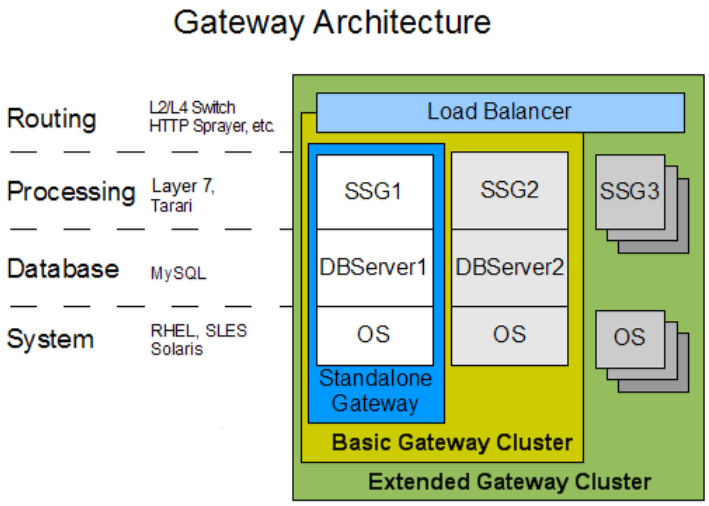

Figure 1: Overview of Gateway architecture

Routing Layer

The Routing Layer represents an industry-standard load balancer configured to provide TCP-level load balancing. 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

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 CA Single Sign-On 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 “Manage Certificates” in the CA API Gateway online documentation located at wiki.ca.com/Gateway.

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 16 .

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 “Gateway Dashboard” in the CA API Gateway online documentation located at wiki.ca.com/Gateway.

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.

There are typically two processing nodes in a cluster, both of which communicate with a single MySQL database. This database should be located on one of the processing node.

System Layer

The System Layer represents the Operating System, Java Virtual Machine, and hardware platform. The software form factor may be installed on Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), or Oracle Solaris (x86 or SPARC).

Form Factors

The Gateway is available in three different form factors:

- As software that can be installed on servers running Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Oracle Solaris (both x86 and SPARC).
- As a 64-bit appliance that requires minimal additional configuration.
- As an XML virtual appliance running under VMware. Initial configuration and setup of this product is described in the *CA API Gateway – XML Accelerator (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.ca.com/api or contact CA Technologies. To view online documentation for the CA API Gateway, please visit: wiki.ca.com/Gateway.

Production Network Architecture

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

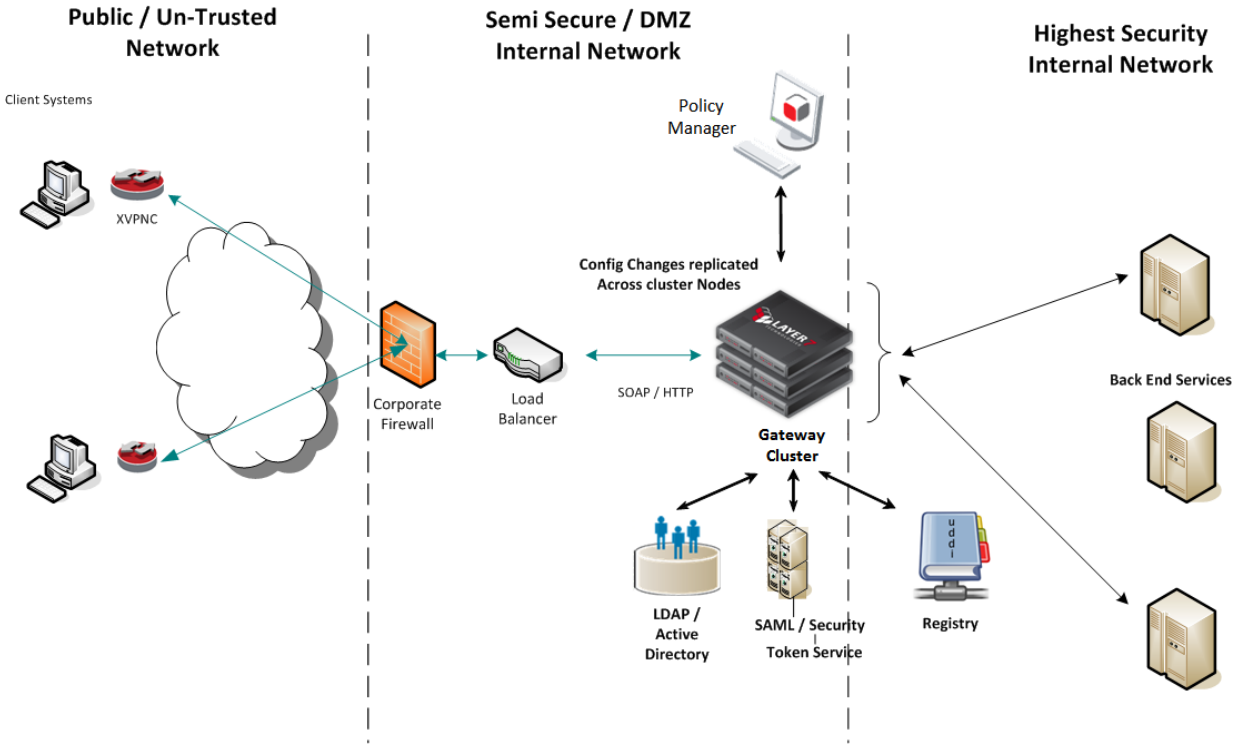

Figure 2: Production network architecture

Chapter Three: Gateway Administration

This chapter describes the various maintenance tasks related to the CA API Gateway.

Tip: The shorthand *"<ssg_home>"* is used to indicate the directory where the Gateway is installed. By default this is: */opt/SecureSpan/Gateway*.

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.

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

Viewing Logs on the Appliance Gateway

This section applies only to the Appliance Gateway.

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 Policy Manager (see "Logs" in the CA API Gateway online documentation located at wiki.ca.com/Gateway).

➢ *To view logs on the Gateway appliance:*

- Select option **9** from the Gateway main menu.

  The following options are presented:

```
This menu allows you to view log files on the
CA API 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 3: 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. **Tip:** Type **q** to exit a log.

Table 1: 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*
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 Log differs from the Audit Log. The Gateway Log includes 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 "Understanding Logging Thresholds" on page 13 on page for more information about the Audit Log.

The Gateway Log includes 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 2: 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.
ALL	All logs or audit events are logged.
OFF	No logs or audit events are logged

Note for Appliance Gateway: 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:

On the Appliance Gateway:

- **/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 Gateway main menu.
- **/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.

On the Software Gateway:

- **/opt/SecureSpan/Gateway/node/default/var/logs/ssg* :** Gateway logs are written to a log file system located 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.

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 2.

The *log.levels* cluster property defines the threshold for log events that are processed by the configured log sinks (the minimum severity that is important enough to be processed).

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 2.

For more information on log sinks, see "Manage Log Sinks" and "Log Sink Properties" in the CA API Gateway online documentation located at wiki.ca.com/Gateway.

Note: The logging levels are an advanced feature and changes should only be made under the direction of CA 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 "View Gateway Audit Events" in the CA API Gateway online documentation located at wiki.ca.com/Gateway). The Gateway logs audit events at the following default threshold levels:

Table 3: 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 B, "Gateway 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 more information, refer to the following topics in the CA API Gateway online documentation located at wiki.ca.com/Gateway:

  - For information on configuring cluster properties, see "Manage Cluster-Wide Properties".
  - For information on the audit settings that you can configure, see "Audit Cluster Properties".

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 4: 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 5: Data logged by format string index

Index Value	Data
1	JVM Time in millis
2	Java Log Level (INFO, WARNING, ...)

Index Value	Data
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 CA API Gateway online documentation located at wiki.ca.com/Gateway.

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 5 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 "Manage UDDI Registries" in the CA API Gateway online documentation located at wiki.ca.com/Gateway.

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 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 to ping the Gateway IP address or each Gateway cluster node IP address on a periodic basis.

Ping URI 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 URI in the implementation. Do not ping each Gateway node using Ping URI 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 "Manage Certificates" in the CA API Gateway online documentation located at wiki.ca.com/Gateway.

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

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

- The setting for the *pingServlet.mode* cluster property (see "Miscellaneous Cluster Properties" in the CA API Gateway online documentation located at wiki.ca.com/Gateway).
- Whether the ping URI request was submitted via standard HTTP or encrypted HTTP using SSL (see "Syntax" below)
- Whether credentials were included in the ping URI request (see "Syntax" below)

Syntax

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

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

The syntax for submitting a ping URI 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 URI 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 URI test through SSL.

Ping URI Test Results

The following table summarizes the ping URI test results based on each *pingServlet.mode* cluster property setting. For information on how to set this property, see "Miscellaneous Cluster Properties" in the CA API Gateway online documentation located at wiki.ca.com/Gateway.

Table 6: 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, and 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 19 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, and 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 "Manage Roles" in the CA API Gateway online documentation located at wiki.ca.com/Gateway.

Full Cluster Status

When the full cluster status is displayed (see Table 6), a table similar to the following is displayed in the HTML results page:

Table 7: 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:** Returns extended system information in a separate web page. You can use this information to help troubleshoot problems. This information will also

help CA Technical Support diagnose issues if you require further assistance.
Note: You need 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 7 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

W A R N I N G

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 CA 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 J, "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 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 CA API Gateway online documentation located at wiki.ca.com/Gateway.

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 "Manage Private Keys" and "Private Key Properties" in the CA API Gateway online documentation located at wiki.ca.com/Gateway.

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 CA API Gateway online documentation located at wiki.ca.com/Gateway.

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" in the CA API Gateway online documentation located at wiki.ca.com/Gateway to determine if you need one).

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.)

Appliance Gateway

Tip: You can stop and start the Gateway with a single command: **service ssg restart**

Stopping the Gateway

Either of the following methods can be used to stop a Gateway node. Use the one most appropriate to you. **Exception:** When installing a patch, you must *always* stop and start the Gateway via the menu.

- *To stop the Gateway via the menu:*

  1. Log in as *ssgconfig*. The Gateway main menu appears.
  2. Choose option **2** (Display Gateway configuration menu). The Gateway configuration menu appears.
  3. Choose option **7** (Manage Gateway status). The current status of the Gateway is displayed. Press [**Enter**] to continue.
  4. 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; "STOPPED" indicates the node has stopped).

- *To stop the Gateway via the command line:*

  1. Open a privileged shell.
  2. Run the command:

     ```
     service ssg stop
     ```

Starting the Gateway

- *To start the Gateway via the menu:*

  1. Log in as *ssgconfig*. The Gateway main menu appears.
  2. Choose option **2** (Display Gateway configuration menu). The Gateway configuration menu appears.
  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).

➢ *To start the Gateway via the command line:*

1. Open a privileged shell.
2. Run the command:

```
service ssg start
```

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.
2. Choose option **2** (Display Gateway configuration menu). The Gateway configuration menu appears.
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 CA 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.
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, 2013
3:42:24 PM com.l7tech.server.ServerConfig <init>
```

```
INFO: Couldn't find serverconfig_override.properties; continuing with
no overrides Apr 3, 2013 3:42:26 PM com.l7tech.server.boot.GatewayBoot
start
INFO: Starting SecureSpan Suite 8.0 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.

Software Gateway

Note: The gateway.sh script can only be run by *gateway* or *root* users.

Starting the Software Gateway

➢ *To start the Gateway:*

1. Log in as the *gateway* or *root* user.
2. Run the following command:

   /opt/SecureSpan/Gateway/runtime/bin/gateway.sh start

Tip: You can monitor the Gateway startup process by using the "tail" command to echo the log information to the screen:
tail -f
/opt/SecureSpan/Gateway/node/default/var/logs/ssg_0_0.log.
What to watch for: Messages containing "Warning" or a "stack trace" indicate a problem with the Gateway and require immediate attention. When you see "INFO: Server Ready", the Gateway has started successfully.

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 CA 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. Log in as the *gateway* or *root* user.
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, 2013
   3:42:24 PM com.l7tech.server.ServerConfig <init>
   ```

```
INFO: Couldn't find serverconfig_override.properties; continuing with
no overrides Apr 3, 2013 3:42:26 PM com.l7tech.server.boot.GatewayBoot
start
INFO: Starting CA API Gateway SecureSpan Suite 8.0 build ...
```

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

3. To stop the Gateway, press [Ctrl]-C.

Stopping the Software Gateway

➢ *To stop the Software Gateway:*

1. Log in as the *gateway* or *root* user. For more information, see "User Accounts" on page 11.
2. Run the following command:

   /opt/SecureSpan/Gateway/runtime/bin/gateway.sh stop

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 CA API Gateway online documentation located at wiki.ca.com/Gateway.

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 CA API Gateway online documentation located at wiki.ca.com/Gateway.

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 Policy Manager, if it is appropriate to do so. For more information, see "Manage Service Resolution" in the CA API Gateway online documentation located at wiki.ca.com/Gateway.

Step 1: Determine service based on service entity ID

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

http://gatewayhost:8080/service/123456

where *"123456"* is the entity ID of the service

These are the possible outcomes:

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

Step 2: Determine service based on URI

When the incoming URI does not contain a unique service identifier, the resolution process examines the URI 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 following elements will be treated as identical by the resolution process:

```
<a:doStuff xmlns:a="http://ns.example.com/services"/>
<b:doSomeOtherStuff xmlns:b="http://ns.example.com/services"/>
```

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 CA API Gateway online documentation located at wiki.ca.com/Gateway.

Chapter Four: 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

For a list of the system requirements, refer to the "SecureSpan Gateway (SSG) - Feature Support Matrix" page on the Customer Support Portal.

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

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 URI 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.
1. 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.
2. 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.
3. The Installation CD files appear in the target directory. To start the Policy Manager, run the following command:

   ```
   # /usr/local/securespan/Manager.sh
   ```
4. Un-mount and eject the CD-ROM as follows:

   a. Type `umount /mnt/cdrom`

   5. 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 30 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 "$HOME/securespan" installation directory by typing the following commands:
- "$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 "Start the Policy Manager" in the CA API Gateway online documentation located at wiki.ca.com/Gateway.

➢ *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 CA 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 "Oracle 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.

Upgrading the Policy Manager

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 32, then install the new version of the Policy Manager as outlined in "Installing the Policy Manager" on page 29. 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 29 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 **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.
- Online documentation located at wiki.ca.com/Gateway.

Both versions of the Policy Manager documentation contain the same content.

Chapter Five: Install and Upgrade the CA API Gateway – XML VPN Client

The CA API Gateway – 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 CA API Gateway – 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 CA API Gateway – XML VPN Client is available as Red Hat Enterprise Linux or Microsoft Windows software.

System Requirements

For a list of the system requirements, refer to the "SecureSpan Gateway (SSG) - Feature Support Matrix" page on the Customer Support Portal.

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

Installing the CA API Gateway – 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 CA API Gateway – XML VPN Client.

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

Linux Installation

Tip: Install the CA API Gateway – 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 CA API Gateway – 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:*

4. Log in as the *root* user.
5. 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.

6. 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.

7. 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 CA API Gateway – XML VPN Client documentation for configuration instructions.

8. Un-mount and eject the CD-ROM as follows:
   a. Type **`unmount /mnt/cdrom`**
   9. Eject and remove the CD.

Single User Installation–Single User on a Single Machine

To install the CA API Gateway – 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 36 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 CA API Gateway – XML VPN Client documentation for configuration instructions.

Windows Installation as Service

Install the CA API Gateway – 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 CA API Gateway – XML VPN Client as an application instead (see page 41).

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 CA API Gateway – XML VPN Client service, then running: *C:\Program Files\CA Technologies\ CA API Gateway – XML VPN Client\CA API Gateway – 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 CA API Gateway – XML VPN Client as a service:

Table 8: 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 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 CA API Gateway – XML VPN Client Performance" in the CA API Gateway – XML VPN Client documentation.

Server Certificate Discovery

In order for the CA API Gateway – 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 CA API Gateway – 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".

Note the following:

- If you are installing over an existing CA API Gateway – XML VPN Client system, make sure the service has been stopped (Start menu > All Programs > CA API Gateway – XML VPN Client > Stop CA API Gateway – XML VPN Client).
- If you are installing over an existing CA API Gateway – 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 CA API Gateway – XML VPN Client executable.
     c. The CA API Gateway – 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. Click [**Yes**] when prompted to run the CA API Gateway – XML VPN Client as a service.
5. Next, you are prompted to configure the CA API Gateway – 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 > CA API Gateway – XML VPN Client > CA API Gateway – XML VPN Client Config), then manually start the service (Start menu > All Programs > CA API Gateway – XML VPN Client > Start CA API Gateway – XML VPN Client Service).
7. The Configure CA API Gateway – XML VPN Client dialog appears. See "Configuring the CA API Gateway – XML VPN Client" on page 41 for more information.

Figure 4: Configure CA API Gateway – XML VPN Client dialog

8. When you have set up the gateway and user account, click **Continue**.
9. When prompted whether to start the service, choose one of the following:
   - Click [**Yes**] to finish the installation and start the CA API Gateway – 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 > CA API Gateway – XML VPN Client > Start CA API Gateway – XML VPN Client Service) or until the computer is restarted.

Windows Installation as Application

Install the CA API Gateway – 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 CA API Gateway – XML VPN Client as a service vs. application, refer to the table on page 38.

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 CA API Gateway – XML VPN Client as an application:*

1. Follow steps 1 to 4 under "To install the XML VPN Client as a service" on page 39. 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 CA API Gateway – XML VPN Client (Start menu > All Programs > CA API Gateway – XML VPN Client > CA API Gateway – XML VPN Client). This places the XML VPN Client icon in the system tray. Click this icon to open the main window. See "Configuring the CA API Gateway – XML VPN Client" below for information on setting up your Gateway.

Configuring the CA API Gateway – XML VPN Client

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

Configuring the XML VPN Client Application with the GUI

➢ *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 CA API Gateway – 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 *CA API Gateway – XML VPN Client User Manual* for detailed information on completing the fields.

Configuring the XML VPN Client Service with the GUI

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

1. From the Start menu, select: **All Programs** > **CA API Gateway – XML VPN Client** > **CA API Gateway – XML VPN Client Config**. The Configure CA API Gateway – 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 CA API Gateway – XML VPN Client documentation for detailed information on completing the fields.

   Note that you can also run the CA API Gateway – 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 8 on page 38). For more information, see the Tip on page 37.

Configuring the XML VPN Client with the Command Line

You can choose to configure the CA API Gateway – 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 CA API Gateway – 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 9: 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 44 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

Object Parameters

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

Table 10: Command line configuration: Object parameters

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 Parameters

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

Table 11: Command line configuration: Property parameters

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 12: 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 CA API Gateway – XML VPN Client in a Windows Domain Login configuration.

Prerequisite: The Gateway must be configured to use Windows Domain Login. For more information, refer to the topic "Configure the Gateway for Windows Domain Login" in the API Gateway online documentation located at wiki.ca.com/Gateway.

➢ *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 9 on page 44.
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 CA API Gateway – XML VPN Client documentation.
4. Verify that the policy in the Policy Manager contains the Require WS-Security Kerberos Token Profile Credentials Assertion. For more information, see the "Require WS-Security Kerberos Token Profile Credentials Assertion" in the CA API Gateway online documentation located at wiki.ca.com/Gateway.

Version Upgrades

Tip: For version-specific CA API Gateway – 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 CA API Gateway – XML VPN Client, uninstall the earlier version of the software as outlined in *Uninstall the CA API Gateway – XML VPN Client* below, then install the new version of the XML VPN Client as outlined in "Installing the CA API Gateway – XML VPN Client" on page 35. 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 CA API Gateway – 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 CA API Gateway – XML VPN Client program files, type:

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

   Note: If a different target directory was chosen for the CA API Gateway – 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 CA API Gateway – XML VPN Client" on page 35 to install the new version.

From Windows

Uninstall the CA API Gateway – 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 CA API Gateway – XML VPN Client" on page 35 to install the new version.

CA API Gateway – XML VPN Client Documentation

Two versions of the CA API Gateway – XML VPN Client documentation are available:

- A PDF "CA API Gateway – XML VPN Client User Manual".
- A program-based "CA API Gateway – XML VPN Client Help System". To access the Help System, select [**Help**] > **Help System** from the CA API Gateway – XML VPN Client Main Menu.

Both versions contain the same content.

Appendix A: Contact CA Technologies

Technical Support

At CA Technologies, our commitment to exceptional service culminates in the advanced level of technical support that we provide for our products.

You can email support at api-support@ca.com or call the number near your region.

Table 13: CA Technical Support contact numbers

Area	Phone
North America	1-800-225-5224
Federal	1-800-225-5224 (press option '7')
UK	0845 161 0038
France	081 102 5146
Germany	0800 101 4666
Italy	84032 0057
Spain	90188 8125
Switzerland	084 400 0092
Australia	1800 023 386

For more details, please refer to your Service Level Agreement.

Contact Information

CA Technologies welcomes your questions, comments, enhancement requests, and general feedback.

Table 14: CA Technologies contact information

Phone	1-800-225-5224 (North America toll free)
Web	www.ca.com/api
Email	api-info@ca.com

Appendix B: Gateway 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 CA API Gateway.

W A R N I N G

Configuring system properties should only be attempted by advanced users or as directed by CA Technical Support. Improper use may render your CA API Gateway inoperable. The list in this appendix represents only a fraction of the available system properties.

➢ *To add a Gateway 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 15: 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

Property	Description	Default
com.l7tech.common.mime.allowLaxEmptyMultipart	How empty multipart messages are treated. **true** – Incoming empty multipart messages will be treated as an empty single part message, while retaining a multipart Content Type. **false** – No change to how empty multipart messages are treated.	false
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 Gateway). The default setting of "-1" indicates that the limit should be retrieved from the cluster property *io.xmlPartMaxBytes*.	-1
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.external.assertions.ssh.server.enableMacMd5	Removes the HMAC-MD5 algorithm from the MAC algorithm list. **true** – Does not remove the HMAC-MD5 algorithm from the MAC algorithm list. **false** – Removes the HMAC-MD5 algorithm from the MAC algorithm list.	false
com.l7tech.external.assertions.ssh.server.enableMacNone	Removes the "none" MAC algorithm from the MAC algorithm list **true** – Does not remove the "none" MAC algorithm from the MAC algorithm list. The MAC algorithm is not used. **false** – Removes the "none" MAC algorithm from the MAC algorithm list.	false
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.hacounter.batchLimit	Number of individual writers to batch together before writing to the database. Lower values will cause more individual writes to the database, based on how many entries are in the queue to be written.	4096

Property	Description	Default
com.l7tech.hacounter.coreThreads	Core number of threads to have writing to the database. Do not change unless directed by CA Technical Support.	16
com.l7tech.hacounter.counterQueueSize	Counter queue size. This can be reflective of the number of requests per unit time that you expect to see. For example, with the write flush at 1, this means the Gateway can handle at most 4096 x 1 sec = 4096 requests/sec. Larger values will allow more requests through, but at the expense of more system resource usage. This setting is closely tied to the flush time for writes (*com.l7tech.hacounter.flushTimeWriteDatabase*).	4096
com.l7tech.hacounter. flushTimeWriteDatabase	Time limit until a flush of the writes to the database from the write queue. Change only if you require more or less frequent flushes. This may affect the frequency of database writes and the allowed access may exceed the permitted throughput in some instances.	1000 milliseconds
com.l7tech.hacounter.keepAliveSec	Length of time to keep alive the write to the database maximum. Do not change unless directed by CA Technical Support.	10 seconds
com.l7tech.hacounter.maxThreads	Maximum number of threads to have writing to the database. Do not change unless directed by CA Technical Support.	128
com.l7tech.hacounter. supervisorQueueSize	Supervisor queue size. The default means there can be 4096 counters, each having a counter queue size (*com.l7tech.hacounter.counterQueueSize)*. Larger values will consume more RAM. Consult with CA Technical Support before changing this.	4096
com.l7tech.hacounter. timeClearReadCache	Time limit before clearing the counter cache, which causes another read of the counter from the database. Changing the value may affect the throughput.	60000 milliseconds
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[1].	highest

*[1] 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.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		
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.detailThresholdRespected	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.policy.assertion. ServerHttpRoutingAssertion. statePool.enable	Set to "true" to ensure the Keep-alive option is respected in outbound HTTPS routing when the key is used to avoid SSL traffic. Restart the Gateway after changing this property.	false
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 CA Technical Support if connecting to more than one JMS provider.	true
com.l7tech.server.uddi.auto_republish	Republish to UDDI as needed (e.g., when the cluster hostname or port number changes)	true

Property	Description	Default
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 C: Download WSDL and Policy Documents

This appendix describes the ways to download a WSDL document or a policy document. The HTTP URIs 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 CA API 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 cluster property *service.passthroughdownloads*. By default, passthroughs are permitted only by the localhost. For more information, see "Gateway Cluster Properties" and "Manage Cluster-Wide Properties" in the CA API Gateway online documentation located at wiki.ca.com/Gateway.

Downloading WSDL Documents

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 URI:

http://*<Gateway_machine>***:8080/ssg/wsdl**

Where *"<Gateway_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 CA API Gateway.

To see a list of WSDL documents on a protected service, use this URI:

https://*<Gateway_machine>***:8443/ssg/wsdl?anon=false**

Or:

https://*<Gateway_machine>***:8443/ssg/wsil?anon=false**

You will be prompted to enter login credentials for the CA API 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 CA API Gateway online documentation located at wiki.ca.com/Gateway.

Returning WSDLs for a Specific Service

To return WSDL documents for a specific service, append the service entity ID to the URI:

```
http://<Gateway_machine>:8080/ssg/wsdl?serviceoid=1234567
```

If the service does not allow anonymous access, use this URI:

```
https://<Gateway_machine>:8443/ssg/wsdl?serviceoid=1234567
```

Using the service entity ID 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 entity ID, 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 57.

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 CA API Gateway online documentation located at wiki.ca.com/Gateway.

WSDL URI by Resolution URI

You can retrieve a WSDL by specifying the resolution URI in the URI:

```
http://<Gateway_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://<Gateway_machine>/myservice?wsdl
```

This would be translated into the equivalent request:

```
http://<Gateway_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 CA API 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[2]	Ambiguous; error is returned

Case Sensitivity in URI

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 URIs 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 "Manage Service Resolution" in the CA API Gateway online documentation located at wiki.ca.com/Gateway.

WSDL URI by Namespace

You can retrieve a WSDL by specify the namespace in the URI:

http://<*Gateway_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 CA API Gateway will respond as follows:

Scenario	Result
Only one service uses the namespace	WSDL for that service is returned
No service use the namespace	"404 Error – File Not Found" is returned

[2] Although URIs are typically used to resolve a service uniquely, they can technically resolve to multiple services in the SSG if other resolution parameters do not conflict.

Scenario	Result
Multiple services use the namespace	Ambiguous; error is returned

WSDL URI by SOAPAction

You can retrieve a WSDL by specify the SOAPAction in the URI:

http://*<Gateway_machine>*:8080/ssg/wsdl?soapaction=http://acme.com/ws/action/foo

The CA API 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 Policy Documents

To download a policy document, use this URI form from a browser:

http://*<Gateway_machine>*:8080/ssg/policy/disco?serviceoid=1234567&fulldoc=yes

Where <*Gateway_machine*> is the CA API 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 57.

Appendix D: Gateway Observer for CA Unicenter WSDM

This appendix describes how to install and configure the CA API 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 CA API 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 URI.
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. Go to the following directory on the WSDM Manager machine:

   C:\Program Files\CA\Unicenter WSDM\server\default\conf

2. Open the *WsdmSOMMA_Basic.properties* file in a text editor.
3. 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.*
4. 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 CA API Gateway once the CA WSDM Gateway Observer is installed.

Table 16: 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. 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**
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**

Name	Description
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 (URI). 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**
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**

Name	Description
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 E: Install the JMS Interface

This appendix provides a high level overview on how to add JMS support to the CA API Gateway. It assumes that the target middleware system has been correctly installed and configured and that you are familiar with the JMS specifications.

The CA API Gateway can work with a variety of message-oriented middleware (MOM) systems, including:

- TIBCO EMS
- IBM WebSphereMQ
- MQ Native
- JMS over MQ
- webMethods Broker
- WebLogic JMS
- WebSphere JMS

Please contact CA Technical Support for assistance with other JMS providers.

The MOM systems are accessed through the JMS interface. To enable JMS destinations on the CA API Gateway, the appropriate client libraries must be installed first.

Due to licensing issues, the client libraries are not included with the CA API Gateway.

Installing the Client Libraries

The client libraries must be installed in the following directory:

/opt/SecureSpan/Gateway/runtime/lib/ext/

Note: In order to use the .JAR files below, you must set the permissions to 644 and the ownership to layer7.layer7.

For WebSphere MQSeries (v7.1.x), the following libraries are installed:

MQ Native

com.ibm.mq.jar
com.ibm.mq.commonservices.jar
com.ibm.mq.headers.jar
com.ibm.mq.jmqi.jar

com.ibm.mq.pcf.jar
connector.jar

JMS using MQ

com.ibm.mq.jar
com.ibm.mq.commonservices.jar
com.ibm.mq.headers.jar
com.ibm.mq.jmqi.jar
com.ibm.mqjms.jar
connector.jar
dhbcore.jar
jms.jar
jta.jar

Note: If a .bindings file is being used to configure a JMS destination, ensure these files are also included: fscontext.jar and providerutil.jar. These files may be obtained from the IBM MQSeries client.

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 CA API Gateway.

Configuring the JMS Destinations

The JMS interface is enabled when the Gateway is restarted. You can now:

- **Configure a JMS destination**

  For details, see "Manage JMS Destinations" in the CA API Gateway online documentation located at wiki.ca.com/Gateway.

- **Add the Route via JMS Assertion to a policy**

  For details, see "Route via JMS Assertion" in the CA API Gateway online documentation located at wiki.ca.com/Gateway.

Appendix F: Install the JDBC Interface

This appendix describes how to configure the CA API Gateway to work with JDBC.

The configuration involves:

- Installing the client libraries
- White-listing the client libraries
- Enabling the client libraries

Prerequisites

- Ensure you have the necessary JDBC client libraries
- Access to the Gateway as the *ssgconfig* and *root* users

Installing the Client Libraries

➢ *To install the client libraries:*

1. Using SCP or SFTP, copy the necessary client libraries to the CA API Gateway as the *ssgconfig* user.
2. Log in to the Gateway appliance as the *root* user.
3. Change the permissions of the client libraries with this command:

   ```
   # chmod 444 /home/ssgconfig/*.jar
   ```

4. Change the ownership of the client libraries with this command:

   ```
   # chown layer7.layer7 /home/ssgconfig/*.jar
   ```

5. Move the client libraries from:

   /home/ssgconfig

   to:

   /opt/SecureSpan/Gateway/runtime/lib/ext

When this is done, follow the steps below to white-list the client libraries.

White-listing the Client libraries

➢ *To white-list the client libraries:*

1. Open the following file in a text editor:

   /opt/SecureSpan/Gateway/node/default/etc/conf/system.properties

2. Add the following line to the end of the file (these are the supported JDBC drivers by default):

   ```
   com.l7tech.server.jdbcDriver=com.mysql.jdbc.Driver\ncom.l7tech.jdbc.mysql.MySQLDriver\ncom.l7tech.jdbc.db2.DB2Driver\ncom.l7tech.jdbc.oracle.OracleDriver\ncom.l7tech.jdbc.sqlserver.SQLServerDriver
   ```

3. Append the following to the end of the line added above:

   \n*<JDBC driver class>*

   Where *"<JDBC driver class>"* is the class name string.

4. Save and exit the file.
5. Restart the CA API Gateway. You may now enable the client libraries.

Enabling the Client Libraries

➢ *To enable the client libraries:*

1. Start the Policy Manager and connect to your Gateway.
2. Select [**Tasks**] > **Manage Cluster-Wide Properties** (on the browser client, use the **Manage** menu).
3. Click [**Add**] and then choose **jdbcConnection.driverClass.defaultList** from the Key drop-down list.
4. Review the list of driver classes in the Value box. If yours is not listed, add it as a new line.
5. Save and exit all the dialogs.

The CA API Gateway is now configured to use the JDBC client libraries. You can now create JDBC connections and perform JDBC queries.

Configuring the JDBC Connections

The JDBC interface is enabled when the Gateway is restarted. You can now:

- **Configure JDBC connections and query external databases**

  For details, refer to the following topics in the Policy Manager documentation:

  Managing JDBC Connections
  JDBC Connection Properties
  Perform JDBC Query Assertion

Appendix G: Network Deployment Guide

This appendix describes the various scenarios possible for deploying the CA API 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 domain 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 CA API Gateway on your network, please contact CA 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 5 illustrates the components within a single network configuration.

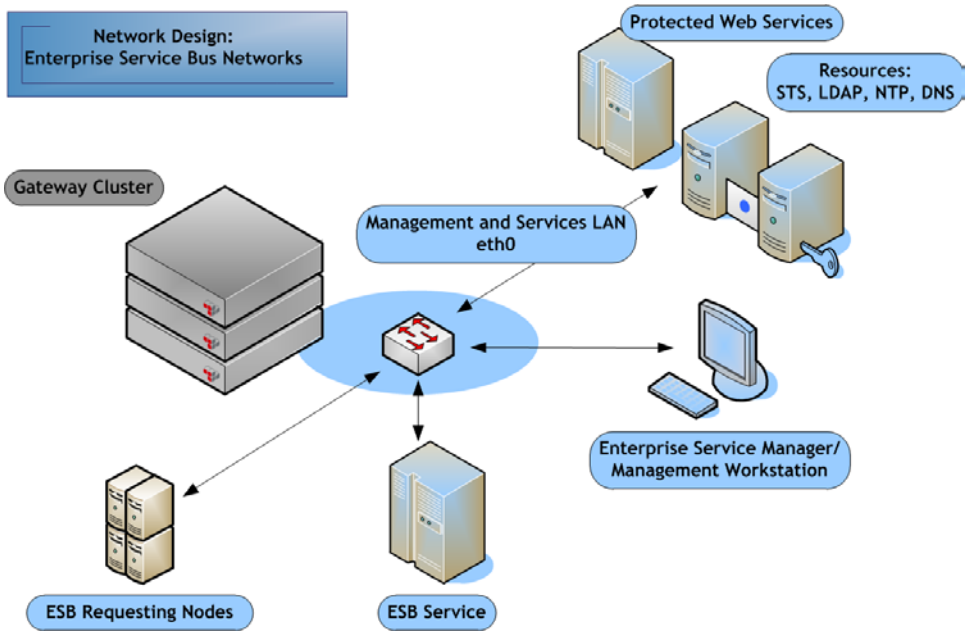

Figure 5: Network deployment: single domain network

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 6 illustrates the components within a two domain network configuration.

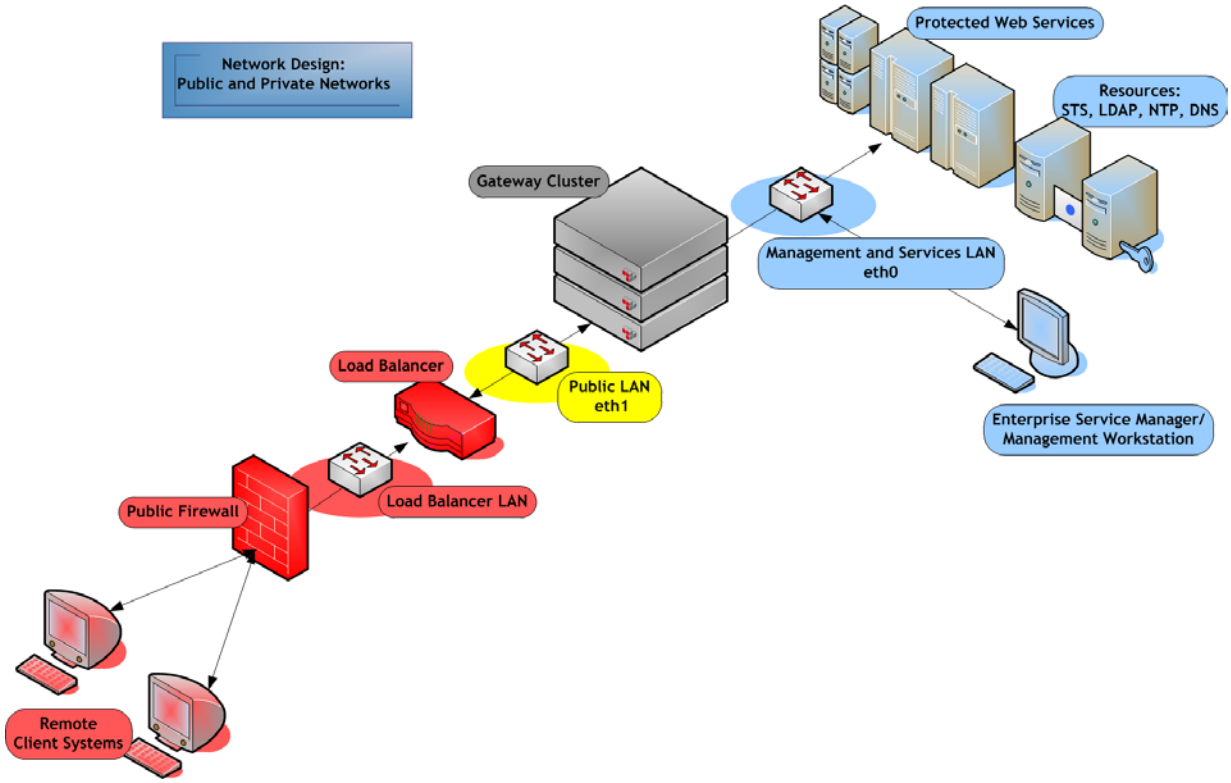

Figure 6: Network deployment: two domain network

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 7 illustrates how it is possible to separate web services from corporate resources such as LDAP using all four network interfaces.

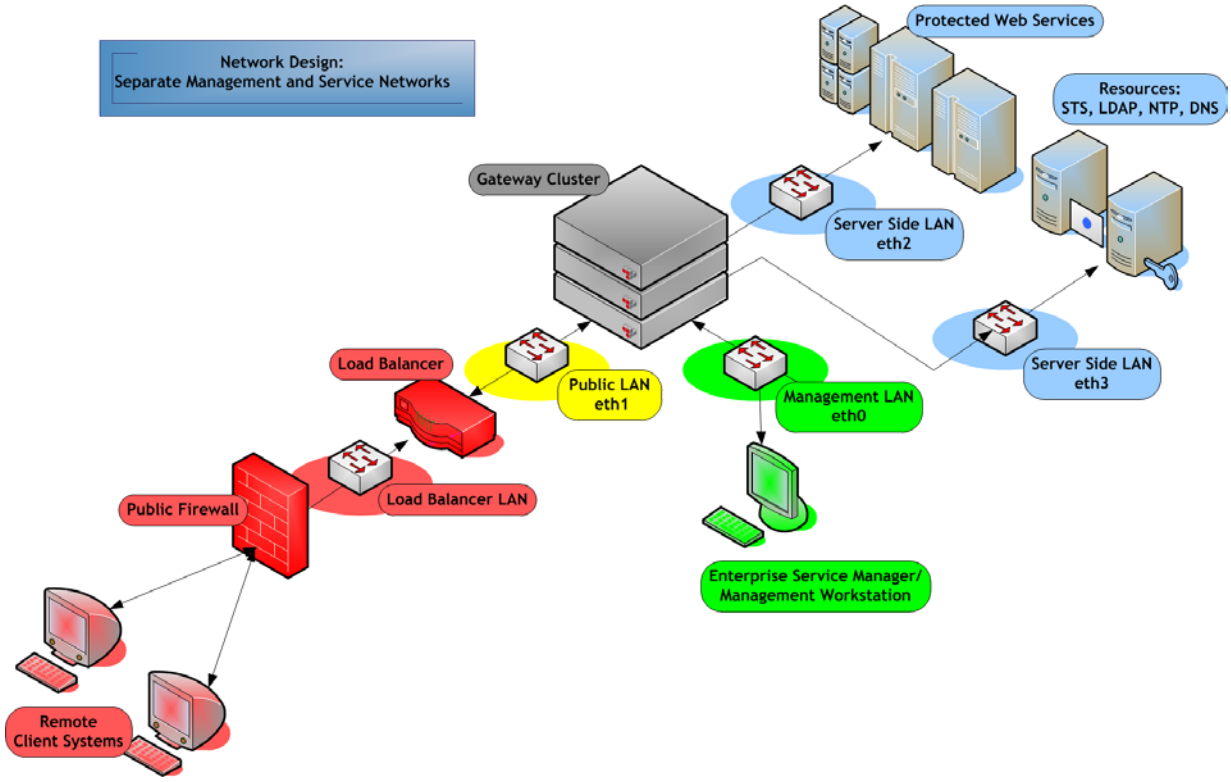

Figure 7: Network deployment: three and four domain network

Appendix H: Connect to a WebSphere JMS Provider

This appendix describes how to configure the CA API Gateway to connect to an IBM WebSphere MQ server as a JMS provider.

Prerequisites

- The WebSphere Application Server is installed
- Access to a WebSphere admin console
- Generated and downloaded keystore and trust store files
- Access to the Policy Manager
- Access to the following JAR files for MQSeries routing:

  com.ibm.ws.orb_8.5.0.jar
  com.ibm.ws.ejb.thinclient_8.5.0.jar
  com.ibm.ws.sib.client.thin.jms_8.5.0.jar
  endorsed_apis_8.5.0.jar
  mail-1.4.5.jar

  These files are located on the CD sent to you from CA Technologies.

Step 1: Set Up the Gateway

➢ *To set up the Gateway for WebSphere:*

1. Stop the CA API Gateway.
2. Copy all files under "Prerequisites" **except** for *endorsed_apis_8.5.0.jar* to the following location on the Gateway:

   /opt/SecureSpan/Gateway/runtime/lib/ext
3. Copy file *mail-1.4.5.jar* from:

   /opt/SecureSpan/Gateway/runtime/lib

   to:

   $ssgmachine//opt/SecureSpan/Gateway/runtime/lib/ext
4. Create the following directory:

   /opt/SecureSpan/Gateway/runtime/lib/ext2

5. Copy the file *javax.ws.rs-api-2.0.jar* from this directory on the Gateway:

   /opt/SecureSpan/Gateway/runtime/lib

   To the **ext2** directory:

   /opt/SecureSpan/Gateway/runtime/lib/ext2

6. Open the following file for editing:

   /opt/SecureSpan/Gateway/node/default/etc/conf/node.properties

   Then add the following line (all one line):

   ```
   node.java.opts=-Djava.ext.dirs=/opt/SecureSpan/JDK/jre/lib/ext:
   /opt/SecureSpan/Gateway/runtime/lib/ext2:/opt/SecureSpan/Gateway/
   runtime/lib/ext
   ```

7. Create this new directory on the Gateway:

   /opt/SecureSpan/Gateway/runtime/lib/endorsed

8. Copy the file *endorsed_apis_8.5.0.jar* into the newly created directory.

9. Restart the Gateway.

Step 2: Configure SSL on the Gateway

➢ *To configure SSL on the Gateway:*

1. Create the following directory: **/misc**

2. Copy the keystore and truststore files (*.jks) from the IBMV85 server to the **/misc** directory on the Gateway:

3. Copy the **ssl.client.probs** and **sas.client.props** configuration files from the WebSphere server to: /home, edit, and upload to the Gateway.

   *<IBM WebSphere install directory>***/AppServer/profiles/${profile}/properties**

4. Make the following changes to the file:

   ```
   user.root=${location of the keystore and trust store directory}
   com.ibm.ssl.protocol=SSL
   com.ibm.ssl.trustManager=SunX509
   com.ibm.ssl.keyManager=SunX509
   com.ibm.ssl.contextProvider=SunJSSE
   com.ibm.ssl.keyStoreType=JKS
   com.ibm.ssl.keyStoreProvider=SUN
   com.ibm.ssl.keyStore=${user.root}/etc/key.jks
   com.ibm.ssl.keyStorePassword=${The password for the key store}
   com.ibm.ssl.trustStoreType=JKS
   com.ibm.ssl.trustStoreProvider=SUN
   com.ibm.ssl.trustStore=${user.root}/etc/trust.jks
   com.ibm.ssl.trustStorePassword=${The password for the trust store}
   ```

   For example:

   ```
   user.root=/misc
   com.ibm.ssl.protocol=SSL
   com.ibm.ssl.trustManager=SunX509
   com.ibm.ssl.keyManager=SunX509
   com.ibm.ssl.contextProvider=SunJSSE
   ```

```
com.ibm.ssl.keyStoreType=JKS
com.ibm.ssl.keyStoreProvider=SUN
com.ibm.ssl.keyStore=${user.root}/DummyClientKeyFile.jks
com.ibm.ssl.keyStorePassword=WebAS
com.ibm.ssl.trustStoreType=JKS
com.ibm.ssl.trustStoreProvider=SUN
com.ibm.ssl.trustStore=${user.root}/DummyClientTrustFile.jks
com.ibm.ssl.trustStorePassword=WebAS
```

5. Copy the *ssl.client.props* and *sas.client.props* (also from the directory in step 3) files to the following directory on the Gateway:

   /home

The following system properties need to be added to the Gateway Java process. One way to do this is to append them to the *system.properties* file:

```
java.ext.dirs=${Gateway install Directory}/runtime/lib/ext
java.endorsed.dirs=${Gateway install Directory}/runtime/lib/endorsed
com.ibm.SSL.ConfigURI=file:///${Directory for ssl client
props}/ssl.client.props
com.ibm.CORBA.ConfigURI=file:///${Directory for sas client
props}/sas.client.props
```

6. Open the following file on the Gateway for editing:

   /opt/SecureSpan/Gateway/node/default/etc/config/system.properties

7. Add the system properties as shown above, for example:

```
java.ext.dirs=/opt/SecureSpan/Gateway/runtime/lib/ext
java.endorsed.dirs=/opt/SecureSpan/Gateway/runtime/lib/endorsed
com.ibm.SSL.ConfigURI=file:///home/ssl.client.props
com.ibm.CORBA.ConfigURI=file:///home/sas.client.props
```

8. Restart the Gateway.

Step 3: Register the JMS Destinations

This last step involves using the Policy Manager to register the JMS destinations.

➢ *To register a JMS destination:*

1. In the Policy Manager, select **[Tasks] > Manage JMS Destinations** from the main menu (on the browser client, from the **Manage** menu). The Manage JMS Destinations dialog appears.
2. Click [**Add**] to create a new JMS Destination.
3. Complete the fields are follows:
   a. In the [Basics] tab:
      - **Name:** Enter a name for the new JMS destination.
      - **Direction:** Inbound
      - **Provider Type:** Generic JMS

b. In the [JNDI] tab:

- **Initial Context Factory class name:** Enter *com.ibm.websphere.naming.WsnInitialContextFactory*
- **JNDI URI:** Enter the URI of the destination server.
- **Credentials are required to connect to JNDI:** Set as appropriate.

c. In the [Destination] tab:

- **Destination Type:** Queue
- **Connection Factory Name:** Enter a name that is used to create a connection with the JMS provider (for example, "jms/QueueConnectionFactory").
- **Destination Name:** Enter the name of the queue to use in the MQ server (for example, "samplequeue1_out").
- **Credentials are required to connect to this destination:** Set as appropriate.

4. Click [**Test Settings**] to validate your settings. The Gateway attempts to connect to the JMS destination and then displays the results.
5. After a successful test, click [**Save**] to register the JMS destination on the Gateway.

For detailed instructions on using JMS destinations with the Gateway, refer to these topics in the Policy Manager documentation:

Managing JMS Destinations
JMS Destination Properties

Appendix I: Install the CA Single Sign-On SDK

This appendix describes how to install the CA Single Sign-On SDK on a CA API Gateway running under Red Hat Enterprise Linux (RHEL) or SUSE Linux. This will enable the CA Single Sign-On functionality in the CA API Gateway.

For information about the CA Single Sign-On features, see "Working with CA Single Sign-On" in the Policy Manager online help or in the CA API Gateway online documentation located at wiki.ca.com/Gateway.

Note: The CA Single Sign-On SDK is included in the Appliance and Virtual Appliance form factors of the CA API Gateway, so separate installation is not required.

Prerequisites

- Ensure that your CA API Gateway is configured and operational.
- Ensure that you have the following file:

  siteminder-sdk_12.51_linux.tar.gz

  This file is obtained from the CA Technical Support Portal.

Known Issue

The CA Single Sign-On SDK is currently not compatible with the Solaris operating system. Please contact CA Technical Support for further instructions if you operate a Solaris Gateway and require CA Single Sign-On functionality.

Installing the SDK

➢ *To install the CA Single Sign-On SDK on a RHEL/SUSE Gateway:*

1. Copy the appropriate tar file to the machine hosting the CA API Gateway (that is, the software instance of the Gateway).
2. Create a new directory from the root and then change to it:

   ```
   # mkdir smsdk
   # cd smsdk
   ```

3. Extract the tar file with this command:

   ```
   # tar -xzf  ../siteminder-sdk_12.51_linux.tar.gz
   ```

4. Run the following script file:

```
# ./sm_sdk_install.sh
```

A success message should be displayed indicating that installation is complete.

5. Restart the Gateway with these commands:

```
# /opt/SecuraSpan/Gateway/runtime/bin/gateway.sh stop
# /opt/SecuraSpan/Gateway/runtime/bin/gateway.sh start
```

The CA Single Sign-On features in the CA API Gateway are now enabled. You may remove the directory containing the extracted files (*smsdk*).

Appendix J: Gateway MIB

This appendix applies only to Appliance Gateways.

The CA API 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 (Management Information Base) file containing the following values to enable SNMP querying (see "SNMP Monitoring" on page 20). For MIB file usage instructions, refer to the documentation accompanying your SNMP tool.

Table 17: 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 K: Gateway System Recovery

This appendix applies only to Appliance Gateways.

This appendix describes how to restore your CA API 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 CA Support to obtain this disk.

Supported Hardware

The recovery disk supports the following hardware configurations:

- Oracle X4-2, X4170, X4150 appliances, as shipped from CA Technologies
- Thales nCipher HSM

Important Notes

Please be aware of the following before proceeding:

- The recovery disk is intended for use only on CA API Gateways delivered as an appliance. It will not work on software Gateways or Virtual Appliances. **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 CA 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 "Back Up Gateways" in the CA API Gateway online documentation located at wiki.ca.com/Gateway.
- 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 CA API Gateway is part of a cluster, please contact CA 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.
2. Insert the recovery disk in the disk drive and reboot the appliance.
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 "Configure the Appliance Gateway" in the CA API Gateway online documentation located at wiki.ca.com/Gateway.
5. When configuration is complete, restore the Gateway database, if it was backed up in step 1.
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 CA 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

T

U

V

W

X