FORUM SYSTEMS SENTRY™ VERSION 8.1 SYSTEM MANAGEMENT GUIDE

Table of Contents

List of Figures

INTRODUCTION TO THE SYSTEM MANAGEMENT GUIDE

Audience for the System Management Guide

The *Forum Systems Sentry™ Version 8.1 System Management Guide* is for System Administrators who will manage:

- General system monitoring information.
- Global Device Management (GDM) for managing more than one system (Agent machine).
- Global Device Management (GDM) for managing more than one Agent Group.
- Import / Export configuration of the system.
- Import / Export HSM configuration for existing or new Security Worlds.
- Import Global Device Management (GDM) Agent and Agent Groups.
- System Settings configuration.
- Network Settings configuration.
- Global response processing setting.
- Licensing information for the product.
- Transfer WSDL or XML Policies to an Agent Group.
- Import WSDL or XML Policies via GDM into the product.
- Export WSDL or XML Policies to a local file system.
- Upgrading Forum software on the system.
- Contacting Forum Systems Customer Support.
- System Troubleshooting tasks.
- Failover.

Conventions Used in the System Management Guide

A red asterisk (*) aligned with a field term means that this field is required. In this and other documentation, the Web Administration Interface is referred to as the WebAdmin and the Forum XML Security Appliance™ is referred to as the 'device', 'product' or 'system'.

In this document, all data or commands that must be entered or selected are displayed in boldface. Example:

> User name: **johnsmith**
> Password: ********

UI screens which display a STATUS column represent the following states:

- Green status light = enabled policy.
- Yellow status light = a required functional element of this policy is disabled.
- Red status light = disabled policy.

Throughout this and other documents in the Documentation Set, repetitive actions such as:

- View / edit a policy.
- Enable / disable a policy.
- Delete a policy.
- Rename a policy.
- Limit display of policies with Search or Max Results fields.

are not shown. For more information, refer to the Common Operations section of the *Forum Systems Sentry™ Version 8.1 Web-based Administration Guide.*

Customers with plug-in licenses on the system, confirm that your Integration License is visible on the General Info screen under the SUPPORTED FEATURES section.

Any specifications and constraints referenced in this volume appear in the Appendices of this volume.

Session Timeout Cautionary
Any action that causes an interaction with the server affects session timeout.

When the session timeout is adjusted, the adjustment does not affect the currently logged in Administrators on the WebAdmin. They are still subject to the previous session timeout value until they login again.

Note: For more information about adjusting Session Timeout, refer to the Session Timeout section of this document.

GENERAL INFORMATION

The General Info screen displays detailed information on resources and server load such as CPU utilization, system memory, application memory and enabled HTTP Network policies.

View Utilization

The Utilization Memory section of the General Info screen includes:

- DB Queue – the percentage of the the database queue for entries waiting to be written to the database

View Application Memory

The Application Memory section of the General Info screen includes:

- Total – the total memory in use by the application.
- Free – physical RAM not in use by the application.
- Used – physical RAM currently in use by the application.

Monitor Enabled Network Policies

The following graphic displays the Network Policy section of the General Info screen after enabled Network policies were created. This area captures all enabled Network policies, activity and configuration data on each listed Network policy.

NETWORK POLICY	# REQ	# CONN	# REQ/CONN
FTP_DomesticTransports	0	0	0
FTP_SSL_DomesticVendors	0	0	0
QAGroupOne-Listener	0	0	0
TemperatureService-Listener	0	0	0
mustUnderstandAttrib-Listener	0	0	0

The following table describes each column in the Network policies section and a description of the status of HTTP activity on the network:

FIELD	DESCRIPTION
Network Policy	Name of each Network policy currently enabled.
# Req	The total number of requests passed to this Network policy since it was last enabled.
# Conn	Number of connections made to this Network policy.
# Req / Conn	Sliding average number of requests per connection since this Network policy was last enabled.

The remainder of the General Info screen displays specific firmware data on your particular system.

Licensing Information

The General Info screen also displays a series of license and version data for the system.

```
Forum Systems Model: 1500
Serial Number: 0000
Licensed to: Developer
License Expiration: Jun 1, 2006
Firmware Version: 6.0
Product Version: 6.0.469
Server Date/Time: Wed, 15 Feb 2006 03:15:46 PM GMT-05:00
Server Start Date/Time: Wed, 15 Feb 2006 11:40:54 AM GMT-05:00
Server Up-Time: 0 years, 0 months, 0 days, 3 h, 35 min, 52 s, 552 ms
```
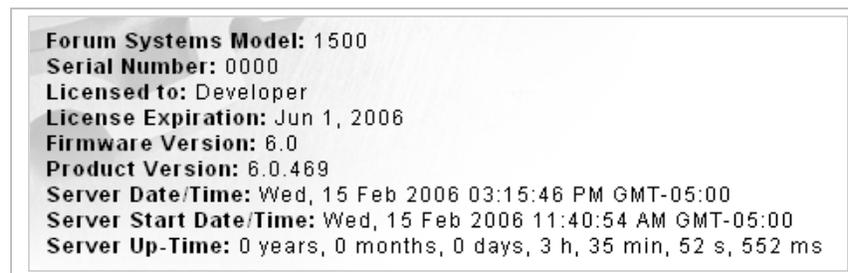
License Manager Terms

The following table displays the terms and definitions included in the License Manager:

LICENSE TERM	LICENSE ELEMENT
Forum Systems Model	Platform identification for the software.
Serial Number	Unique server identification.
Licensed to	Company name which software is registered to.
License Expiration	Date license expires.
Firmware Version	Version number of the firmware.
Product Version	Version number of the product.
Server Date / Time	Current date and time on the system.
Server Start Date / Time	Date and time the software was installed on the server.
Server Up-Time	Length of time that has been running since the last restart.

Licensing Your Forum Software

The Forum Systems product license file may be imported to the product. For customers who have an system, login to the WebAdmin interface, and from the **General Info** screen, under REGISTER, click Browse to locate and highlight the provided license file from your installation CD, and then click **Import** to import the license file.

Note: For more information, refer to the *Forum Systems Sentry™ Version 8.1 Hardware Installation Guide.*

Software Product Versions

Once your company's Primary Contact has received the Forum Systems's product license file, the license.xml file needs to be copied to the server running the Forum Systems software product. From the **General Info** screen, under REGISTER, click **Browse** to navigate your file system to the provided license file.

Note: For more information, refer to the *Forum Systems Sentry™ Version 8.1 Software Installation Guide.*

Upgrade to Versions or Licensed Features

Login to the WebAdmin interface, and from the **General Info** screen, under REGISTER, click browse to locate and highlight the provided license file, and then click **Import** to import the new version or license file.

Note: For more information, refer to the *Forum Systems Sentry™ Version 8.1 Hardware Installation Guide.*

Administration Domain

The Active Domain is displayed at the bottom of the WebAdmin UI. After installation of the system, the default Domain, labeled Default, is visible.

Note: For more information, refer to the Overview of MultiDomain Administration or the Domains sections of the *Forum Systems Sentry™ Version 8.1 Access Control Guide.*

OVERVIEW OF GLOBAL DEVICE MANAGEMENT

Global Device Management (GDM) has a notion of one Policy Server machine (MASTER) that holds all the policies used in your business processes. The system provides the ability to push an existing or updated configuration (.fsx / .fsg files) from the Policy Server machine to any number of managed Agent machines. Additionally, all Agents retain the ability to customize their own system to their specific IPs and ports.

GDM FULL CONFIGURATION TRANSFERS THROUGH AGENTS

Manage Agents Through the Policy Server Machine

The Agents screen provides a method of securely transferring policy configuration information from a Policy Server machine to any number of Agents. This transfer can be from any Forum Systems form factor to another with the exception that HSM-enabled systems can only import to another HSM-enabled system on the same Security World.

Note: Forum System recommends that both Forum Systems installations run the same version of Forum Systems software.

All values listed on the Agents screen are specific to each targeted Agent machine policy. All data is transferred among Agent machines securely via SSL.

Additionally, you may also export a configuration file from the Policy Server machine or any Agent(s) machine(s). The configuration file may be exported to a local file system or stored on an external file server. The system supports importing configurations created on other systems up to one major version release behind the target system version.

Note: When working on the system with Version 5.1.234 of the software, for example, Administrators may import any configuration version between 4.0.0 and 5.1.234. Likewise, Version 8.1.789 will be able to import any configuration between 7.0.0 and 8.1.789. Any exported configuration file built more than one major version prior will fail to import into the system.

Every policy in the system is transferred during a GDM transaction with the following exceptions:

- All network information from the Network screen of the product.
- Network routes, host routes and host entries.
- When on FIA Gateway, the FIPS policy.
- The SNMP policy.
- Managed Machine policies (from GDM).

Agents Screen Terms

While working with the Agents screen, please consider the following:

FIELD NAME	DEFINITION
Agent Name	The name of an Agent machine.
Host Name IP Address	The host name or IP address of the Agent.
Agent Info	The information that is on the Agent includes the platform, software version, machine model and product name of the Agent. Selecting the Retrieve link displays the collected information in the WebAdmin UI.
Time Last Exported	A date/timestamp for the last time a given Agent policy was exported.

Note: The **Test** button on the AGENT DETAILS screen requests authentication of the appropriate credentials (user name and password) on the Agent machine before that Agent machine is allowed to accept a configuration transfer from the Policy Server. The **Save** button on the AGENT DETAILS screen saves the entered data in the Agent policy.

Once the Agent policy is saved, click on the **Agent machine name link** to view the policy and then select the "**Edit Policy Values**" button. The EDIT POLICY VALUES screen lists all network interface policies that will be applicable on the Agent machine.

From the Policy Server machine, the ORIGINAL VALUE column of the EDIT POLICY VALUES screen displays the current policy network interfaces. To prevent using duplicate IPs and Ports on Agent machines, enter new values in the OVERRIDE VALUE column applicable for the Agent machines. The OVERRIDE VALUE column stores replacement IPs and Ports of existing policies before a configuration transfer is performed from the Policy Server machine to an Agent machine.

Note: Forum Systems recommends configuring Network listener policies using the Device IP. If the Use device IP setting is selected, there is no need to overwrite IPs and Ports.

Determine if Multiple Systems are in Same Security World

To determine if two or more systems are on the same Security World, from the **General Info** screen, verify that each of the Security World ID names match. You may also determine this from the CLI start up screen, or by using the **show hsm security-world-id** command. For more information on Security Worlds, refer to the *Forum Systems Sentry™ Version 8.1 Guide to Security Worlds.* For users working with Luna HSM systems, refer to the *Forum Systems Sentry™ Version 8.1 SafeNet Luna® Integration Guide.*

Agents Policy Terms

While working with the Agents policy screen, please consider the following:

FIELD NAME	DEFINITION
Agent Name	A name for the targeted Agent machine.
Host Name or IP Address	The host name or IP address of the targeted Agent machine.
Web Admin Port	Default port of 5050 for all managed Agents.
GDM Port	Default port of 5070 for all managed Agents.
GDM User	User name of a user with privileged access enabled. For partial GDM, the user name of the user with Write access is sufficient.
GDM Password	Password for the GDM user.
SSL Signer Group	The SSL Signer Group policy user to verify the SSL connection.
Verify Hostname	With Verify Hostname checked, this setting will verify the hostname on incoming certificate.

GDM Full Configuration Transfer Examples For Agent Machines

Examples for Agent policies and GDM full configuration transfers for Agent Machines include:

- Add an Agent Machine Policy.
- Edit an Agent Machine Policy.
- Transfer Configuration to Another Agent Machine.
- Delete an Agent Machine Policy.

Add an Agent Machine Policy

Adding an Agent Machine policy involves three steps:

1. Adding the Agent Machine policy.
2. Editing the Agent Machine policy (optional).
3. Transferring a configuration to an Agent Machine.

Note: Forum Systems recommends that both machines run the same Forum Systems software version.

Adding an Agent Machine Policy

- From the Navigator on the Policy Server machine, select **Agents.** Click **New**.
- On the AGENT DETAILS screen, in the Agent Name field, enter the **name** of an Agent machine to manage.
- In the Host name or IP Address field, enter the **host name** or **IP address** of the targeted managed machine.
- In the WebAdmin Port field, retain the default **port** for the WebAdmin of a managed machine.
- In the GDM Port field, retail the default **port** for the targeted Global Device Machine.

- From the GDM User drop down list, select the **user name** of a user having privileged access (or Write access for partial GDM) enabled for the targeted Agent machine.
- In the GDM Password field, enter the **password** of the GDM User.
- In the SSL Signer Group drop down list, select a Signer Group used to authenticate the SSL session.
- Check the **Verify Hostname** checkbox.
- Click **Test**. A connection is attempted to the Agent machine with the provided authentication credentials.
- When the "Test successful" message appears, click **Create**.

Editing an Agent Machine Policy

Edit an Agent Machine policy to map new IP addresses and ports to the IPs and ports applicable on the target Agent Machine. When the configuration is transferred, the applicable policy, IP and port information will be changed for the targeted machine.

- From the Navigator on the Policy Server machine, select **Agents**.
- Under the AGENT NAME column, click an **Agent machine name** link.
- On the AGENT DETAILS screen, click **Edit Policy Values**.
- On the EDIT POLICY VALUES screen, in the OVERRIDE VALUES column, enter any values to be modified. This example changes the **Listener IP** and **Listener Port** for the Listener policy and the **Remote IP** and **Remote Port** for the Remote policy.
- Click **Save**.
- On the AGENT DETAILS screen, click **Test**.
- A connection is attempted to the Agent machine with the provided authentication credentials.
- When the "Test successful" message appears, click **Save**.

Transferring Configurations to Another Agent Machine

Using the Transfer command, an Agent Machine may transfer their configuration to another Agent Machine. Follow these steps to transfer configurations from the Policy Server machine to an Agent Machine:

- From the Navigator on the Policy Server machine, select **Agents**.
- Under the AGENT NAME column, check the checkbox aligned with the targeted Agent machine to receive the configuration. Click **Transfer**.
- The "Are you sure you want to overwrite the configurations of the selected agents?" message appears. Click **OK**. The progress bar appears.
- When the progress bar has completed, the AGENTS screen refreshes with a date/time stamp visible in the TIME LAST EXPORTED column.

Note: Users may also transfer configurations to Agent Groups. For more information, refer to the GDM Full Configuration Transfers Through Agent Groups section of this document.

Delete an Agent Machine Policy

Follow these steps to delete an Agent Machine policy:

- From the Navigator on the Policy Server machine, select **Agents**.
- Under the AGENT NAME column, check the **checkbox** aligned with the targeted Agent machine to delete.
- Click **Delete**. The "Are you sure you want to delete the selected agents?" message appears. Click **OK**.

GDM FULL CONFIGURATION TRANSFERS THROUGH AGENT GROUPS

Agent Groups are a collection of one or more Agents. Using the Transfer command, an Agent Group can transfer the configuration (FSX file) of the current Agent to all members of the selected Agent Group.

GDM Full Configuration Transfer Examples for Agent Groups

Examples for Agent Group policies and GDM full configuration transfers for Agent Groups include:

- Add an Agent Group Policy.
- Edit an Agent Group Policy.
- Transfer Configuration to Agent Group.
- Delete an Agent Group Policy.

Add an Agent Group Policy

This instruction assumes that at least one Agent machine policy was previously created.
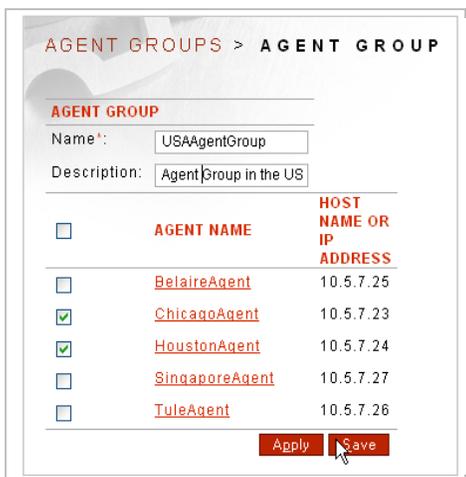
- From the Navigator on the Policy Server machine, select **Agent Groups**.
- Select **New**.
- On the AGENT GROUP screen, in the Agent Name field, enter the **name** of an Agent Group machine to manage.
- In the Description field, enter a **description** of this Agent group (optional).
- Check the **checkbox**(**es**) prefacing the Agent policy name(s) to be added to this Agent Group.
- Select **Save**.

Edit an Agent Group Policy

- Edit an Agent Group policy by selecting the **Agent Group name** link.
- From the Agent Group screen, make **changes**, and then select **Save**.

Transfer Configuration to an Agent Group

When transferring configuration to an Agent Group, you are overwriting the configuration FSX file of all members of the selected Agent Group with the configuration of the current Agent machine.

- From the Navigator on the Policy Server machine, select **Agent Groups**.
- On the AGENT GROUPS screen, select **New**.
- Check the **checkbox**(**es**) prefacing the Agent Group name(s) whose current configuration is to be overwritten by the configuration being transferred.
- The "Are you sure you want to overwrite the configurations of the selected agent?" message appears. Select **OK**.
- Select **Save**.

Delete an Agent Group Policy

Follow these steps to delete an Agent Group policy:

- From the Navigator on the Policy Server machine, select **Agent Groups**.
- Under the AGENT GROUP column, check the checkbox aligned with the targeted Agent Group to delete.
- Click **Delete**. The "Are you sure you want to delete the selected agent groups?" message appears.
- Click **OK**.

GDM PARTIAL CONFIGURATION TRANSFERS

Users may transfer one or more WSDL or XML policies from one Agent machine to another Agent machine with the Transfer command visible on the WSDL Policies or XML Policies screen. This type of transfer is referred to as a GDM partial configuration transfer.

Overview of GDM Partial Configuration Transfer

The product allows transferring configurations from one system to another. The transfer includes the entire configuration from the source system and overwrites the configuration of the target system.

```
 ----------                      ----------
| Source |     ----> | FSX | -----> | Target |
 ----------                      ----------
```

Sending the entire configuration does not work when multiple developers are working on separate parts of the overall configuration. Every developer or business unit has its own set of WSDL or XML policies that need to be aggregated on a target system. Since the product only allows transferring an entire configuration, there is no way to automatically aggregate the different WSDL or XML from individual developers into one final configuration.

Partial GDM was built to address this use case. Partial GDM allows a system to transfer one or more of the configured WSDL or XML policies on a source system to a target system without overwriting the entire configuration of the target machine. This allows Administrators to have multiple groups working on different web services and later aggregate the web services policies on a central system. The central system can then be used for testing and later put into production.

```
 ----------
| Source1 |     ----> | FSG1 | ----->|
 ----------                          |
 ----------                          |        ----------
| Source2 |     ----> | FSG2 | ----->|--->    | Target |
 ----------                          |        ----------
 ----------                          |
| Source3 |     ----> | FSG3 | ----->|
 ----------
```
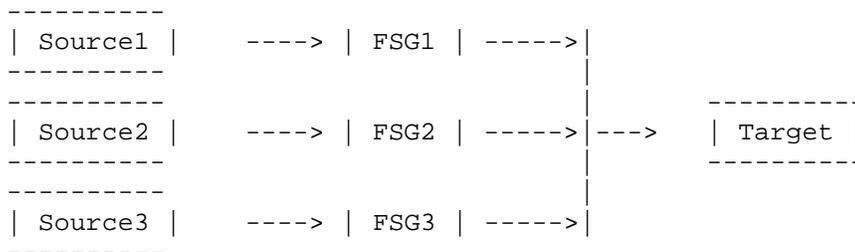
A typical use case is to have developers working on product software instances. In their own sandboxes, developers will secure and customize the different IDP Rules and Task Lists according to their particular requirements. Once completed, the developer can push its WSDL or XML policy and associated dependencies to a staging system where all WSDL or XML policies will be united.

Using Partial GDM

Requirements on the target system:

- Network accessibility
- A user account with Write permissions. The user account can be a privileged user or an Admin user with Write permissions.

Requirements on the source system:

- Network connectivity
- A configured Agent pointing at the desired target.
- An Agent Group containing at least one Agent.
- A WSDL or XML Policy

The developer on the source machine can select one or more WSDL or XML policies to transfer from the list of WSDL or XML Policies. The configuration will be sent to all Agents in the selected Agent Group. If the source and target machines are not on the same network, the configuration can be exported to a file, and later imported manually into the target machine.

About FSG Files

An FSG file contains one or more WSDL or XML policies and its set of dependencies. For example, after creating a WSDL or XML Policy from the wizard, creating an FSG file will include the following:

- WSDL or XML Policies
- Listener Policies
- Remote Policies
- Request Filters
- Default WSDL or XML Policy IDP Group
- IDP Rules associated with the IDP Group
- IDP Actions associated with the IDP Rules
- IDP Schedules associated with the IDP Rules

The process of building an FSG involves finding every dependency required for the proper functioning of a WSDL or XML policy. If a Task List is added to a message node, the Task List will be part of the FSG file.

How Transfers Work

The source machine initiates an SSL connection to the target machine. After the connection has been established, the target machine verifies the credentials presented by the source machine. This is analogous to the login procedure in the Web Admin. After the credentials have been verified the user is assigned an active domain.*

The target system will walk the list of dependencies and update the configuration on the target machine. If the configuration in the FSG file did not exist on the target machine, it will be added. If a configuration already exists, it will be updated. This allows developers to send their configuration and later update it as needed.

If the target system is configured to use multiple Domains, all the policies in the transfer will be assigned the Domain of the logged in GDM user at the target machine. The Active Domain of the configuration or the user logged at the source machine, is not relevant to the transfer. The functionality allows changing the Domain of the configuration only on the target machine.

* If the authenticated GDM user belongs to multiple Domains, the first Domain to grant Write access will be used. `Forum Systems` recommends using users with access to a single Domain when multiple Domains are configured on the target machine.

Caveats for GDM Partial Transfers

The following list of caveats must be adhered to when making a GDM partial transfer for WSDL or XML policies:

- If multiple users are working on different WSDL or XML policies, `Forum Systems` recommends prefixing the names of their policies with a unique identifier as a standard practice to help the administrator easily distinguish different policies. It addition, this action helps to prevent a developer from overwriting the configuration of a different developer because they happen to use the same name for the same policy type. Keep in mind that when updating configurations or WSDL or XML policies, users will want to push the same-named files to force an overwrite.

- Several policies in the system are considered system defaults. A privileged user can update the configuration of a system default policy on a target system. The update for the default policy will be included in the FSG file, but it will be ignored if the logged in GDM user at the target machine has insufficient privileges to update it.
- A transfer will never leave the configuration of the target machine in a corrupt state. The target machine will stop updating the configuration at the first error and abort the rest of the transfer. Once the error is fixed the configuration can be resent. `Forum Systems` recommends taking production system offline before updating their configuration.
- If during a transfer, the Agent on the target Agent machine is not a superuser, and one of the policies that you depend upon is a system default (such as the Default key pair), the dependency will be ignored and the transfer will continue and not fail. System defaults will not fail an upgrade from a transfer because of permissions.

GDM Partial Configuration Transfer Examples

The example for a GDM partial configuration transfer is Transfer a WSDL or XML Policy.

Transfer a WSDL or XML Policy

Users may transfer one or more WSDL or XML policies to an Agent Group. Policies are transferred to the agent members of the Agent Group. This instruction assumes that at least one Agent Group exists on the source Agent machine. This instruction displays transferring a WSDL policy.

- Navigate to the **WSDL Policies** screen.
- Check the **checkbox** aligned with the WSDL policy to transfer.
- Select **Transfer**.
- On the TRANSFER screen, from the Agent Group drop down list, select an **Agent Group** to transfer the WSDL policy to, and then click **Next**.
- The TRANSFER IN PROGRESS screen appears, and closes when the transfer is complete.

GDM FULL CONFIGURATION IMPORTS

Import on Non-HSM-enabled and HSM-enabled Platforms

The system provides a method for importing system configuration information, including policies, device setup, namespace and key data. The Import / Export screen provides a means of importing system configuration information from their local file systems.

From the Import / Export screen, users may import their full system configuration.

Only one configuration may be active on the system at one time. Importing a new configuration file (i.e. <filename>.fsx) will override the currently active configuration file. Configuration files on your local filel systems were automatically named after the export date; i.e., config082903.fsx, but can be changed when exporting.

Network information (the management IP, the device IP, default gateway, primary DNS, secondary DNS, NTP server, and other associated settings) are not passed along with the fsx file. After import, the system will retain its original network information (the management IP, the device IP, default gateway, primary DNS, secondary DNS, NTP server, and other associated settings).

The Import or Export Password

The password entered during the Import configuration operation is bound to that file.

Note: If running the Forum 1503, 2563, 3563, or 4563 platform or a software port, disregard all content that refers to HSM. For installation information on the HSM, refer to the Initialize HSM on the CLI for the First Time section of the *Forum Systems Sentry™ Version 8.1 HSM Quick Start Guide.*

Import on HSM-enabled Platform

On an HSM enabled platform, transferring Security Worlds between HSM-enabled systems is part of the configuration import/export procedure.

Import or Export Configurations with Various System Versions

The following graphic displays an overview of four scenarios for importing / exporting configuration files (.fsx) between two systems:

- HSM-enabled systems.
- non-HSM-enabled systems.
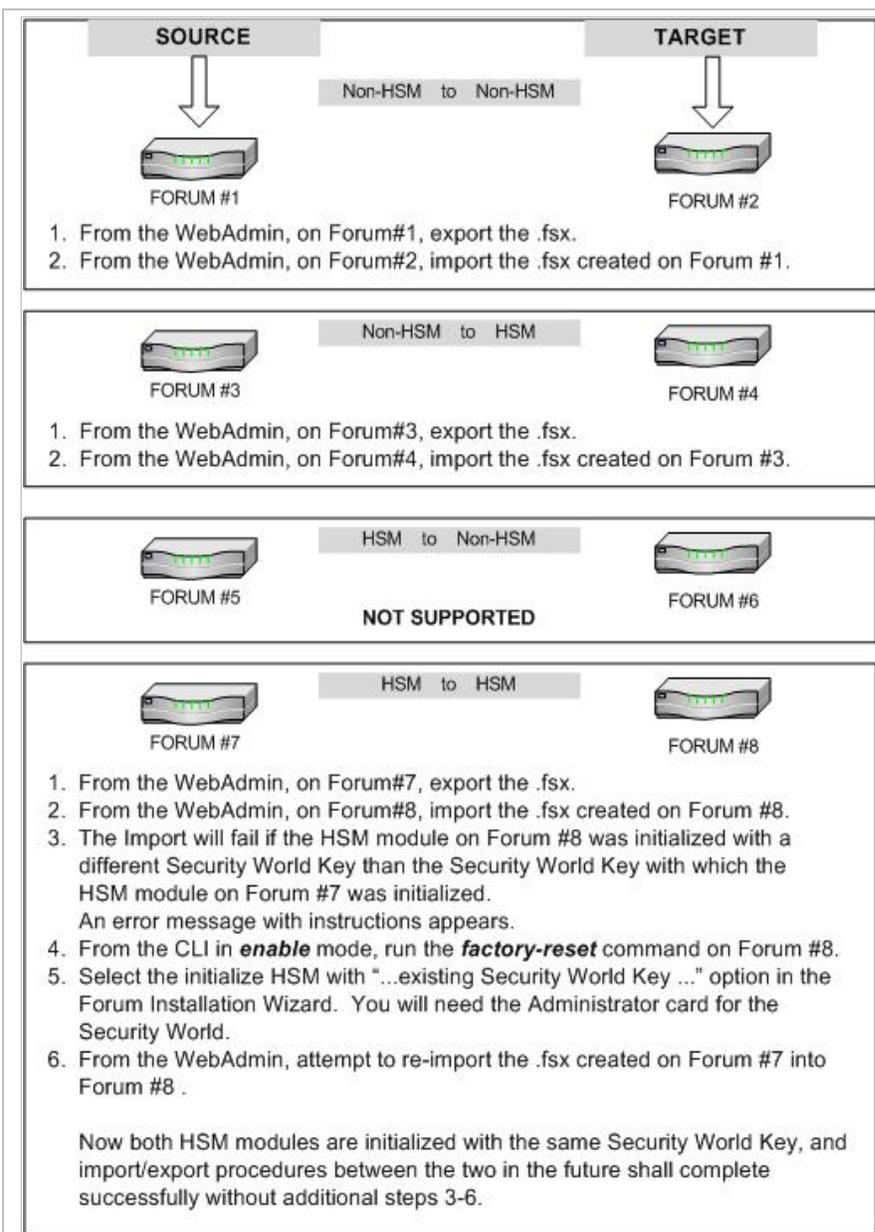
WebAdmin users may not import .fsx files from HSM-enabled systems (source) to non-HSM-enabled systems (target).

This is not possible because an HSM module stores information in a Security World which can only be shared with other HSM systems in the same Security World.

Figure 1: Import or Export Configurations with Systems Versions.

Import or Export Configurations with Various Appliance Versions

The following graphic displays an overview for exporting / importing configuration files (.fsx) between two Forum HSM-enabled systems:
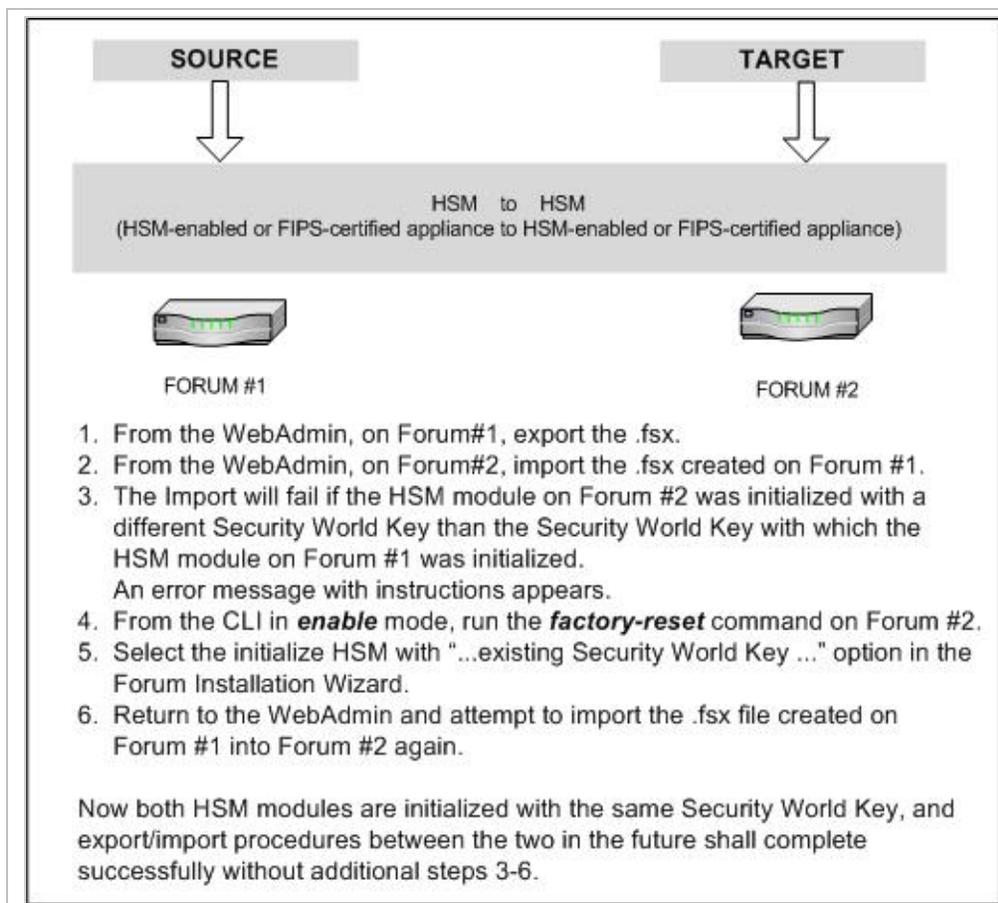
Figure 2: Import or Export Configurations with Various Appliance Versions.

The system supports importing configurations created on other systems up to one major version release behind the target system version.

> **Note:** When working on the system with Version 5.1.234 of the software, for example, Administrators may import any configuration version between 4.0.0 and 5.1.234. Likewise, Version 8.1.789 will be able to import any configuration between 7.0.0 and 8.1.789.
>
> Any exported configuration file built more than one major version prior will fail to import into the system.

GDM Full Configuration Import Examples

Examples for a GDM full configuration import include:

- Import System Configuration Without HSM.
- Import Configuration from HSM-enabled System to Another HSM-enabled System with Same Security World Key.
- Import Existing Configuration from HSM-enabled System to Another Initialized with Different Security World Key.

Note: If importing the same configuration on the product, the logged in User must be re-authenticated to the system with the new configuration. To accomplish this, the User password (not to be confused with the Import/Export password) that exists in the configuration being imported must have been created in clear text, displayed in the figure below:
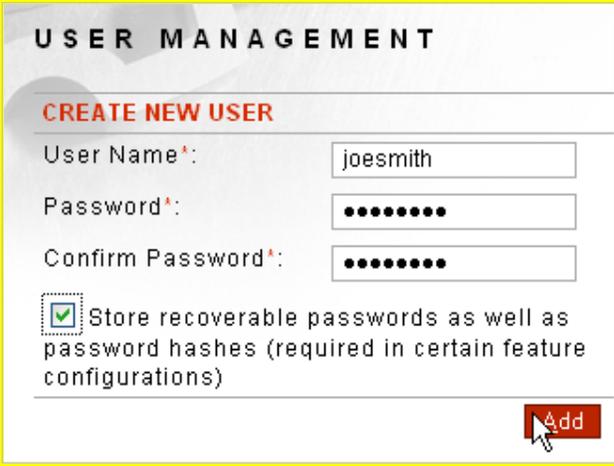
Import Configuration Without HSM

Importing a configuration file on a non-HSM platform is performed by entering the same password used earlier during the Export System Configuration Without HSM section.

IMPORT

IMPORT

Import completed successfully.
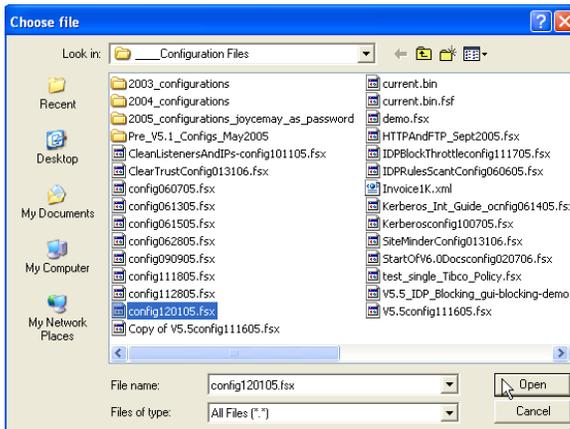
- From the Navigator, select **Import / Export** and the IMPORT / EXPORT screen appear.
- From the IMPORT section, aligned with the File field, click **Browse**. The Chose file screen appears.
- Click to select the **file** to import, click **Open** and the screen closes. The IMPORT / EXPORT screen refreshes.
- In the Password field, enter your **Import / Export Password**, and then click **Import**.
- The "Warning: Importing a configuration will overwrite all of your current system settings. Are you sure?" message appears. Click **OK,** and the IMPORT screen appears. The "Import in progress, please wait …" message, and then the "Import completed successfully" message appears.

Import Configuration with Same Security World Key

Administrators may import a configuration from an HSM-enabled system (source is HSM-enabled system to another HSM-enabled system (target also is HSM-enabled systems with the same Security World Key (SWK) by following the steps outlined in a previous section entitled Import Configuration Without HSM.

Note: To determine if two or more systems are on the same Security World, from the General Info screen, verify that each of the Security World ID names match. You may also determine this from the CLI start up screen, or by using the **show hsm security-world-id** command. For more information on Security Worlds, refer to the *Forum Systems Sentry™ Version 8.1 Guide to Security Worlds*. For users working with Luna HSM systems, refer to the *Forum Systems Sentry™ Version 8.1 SafeNet Luna® Integration Guide*.

Import Configuration with Different Security World Key

When attempting to import an existing configuration from one HSM-enabled system (source is HSM-enabled system) to another (target is HSM-enabled system and the target's HSM module was initialized with a different Security World Key (SWK) than the source's, the initial import will fail and the following message appears:

```
IMPORT / EXPORT

This appliance's HSM module is not initialized with the same security world key as that in the configuration file.

  ************************************************************
  *                                                        *
  *          Importing an HSM Security World Key           *
  *                                                        *
  * To import this configuration into this appliance,      *
  * you must first reinitialize the HSM module with the    *
  * same security world key contained in this              *
  * configuration file.  A copy of the security world      *
  * key from this configuration file has been saved on     *
  * this system.  You may now import the configuration     *
  * using the following procedure:                         *
  *                                                        *
  * 1. Access the command line interface and perform a     *
  * factory reset.  This must be done from enable mode     *
  * using the "factory-reset" command.                     *
  *                                                        *
  * 2. After the appliance reboots, the HSM portion of     *
  * the Install-Wizard will detect the existence of a      *
  * saved security world key.  It will then prompt you     *
  * to select whether to use the saved security world      *
  * key or to generate a new security world key to         *
  * initialize the HSM module.  Select to use the          *
  * existing key.                                          *
  *                                                        *
  * 3. The initialization procedure will then continue.    *
  * You must have an Administrator Card for the            *
  * security world key in the configuration file           *
  * available (as well as its passphrase) to complete      *
  * the HSM module initialization.                         *
  *                                                        *
  * 4. After the HSM module is initialized with the        *
  * saved security world key, return to this screen,       *
  * and perform the import of the configuration again.     *
  *                                                        *
  ************************************************************
```

Figure 3: HSM Import Error Message.

Note: After the import initially fails, the user must follow the above instructions to successfully import the configuration including the new Security World:

1. Run the system config factory-reset command from the CLI enable mode. When prompted, reply No to the "Do you want to save existing Security World?" message. The reason for replying No is because you want to reinitialize the HSM with the new Security Workd Key from the configuration file, and in doing so, discard the currently loaded Security World Key.

2. After the system reboots, enter the CLI and complete the installation wizard. When populating the HSM module section of the Installation Wizard, the CLI will prompt the user whether to generate a new Security World Key or to use a saved one (from the configuration file that previously failed to import). Choose to use the saved one.

3. The HSM module initialization procedure will then continue, during which the user must provide an Administrator card for the Security World Key in the configuration file (i.e. for the source system) and its passphrase.

4. The user should then return to the WebAdmin Import/Export screen and attempt to import the configuration file again.

Caution: The system config factory-reset command will delete all configuration data from the system including all policies, keys, users, groups and ACLs. The existing security world will also be removed from the system.

To review: the instructions are:

- From the **Import/Export** screen, on the HSM-enabled system (target), import the .fsx file created on the source system (this should fail initially with the error message shown above).
- From the CLI, switch to **enable** mode.
- Run the *system config factory-reset* command. When prompted, reply **No** to the "Do you want to save existing Security World?" message.

Note: When using the *system config factory-reset* command with Forum HSM-enabled system, the HSM security world will be deleted. The system will sense this during reboot and the user will be prompted to re-initialize the HSM on the CLI. With the serial connector attached to the system, cycle through the Forum System Installation Wizard once again to enter your network configuration.

- Confirm that the Smart Card Reader is attached to the target Forum HSM-enabled system.
- Access the CLI.
- The Forum Systems Installation Wizard starts.
- When presented with the choice: "Would you like to initialize the module with", reply by typing *1* for the option "The existing Security World Key using its corresponding Administrator Cards." and then press **<enter>**.
- Follow the on screen prompts to complete the Installation Wizard (You will need an Administrator Card and its associated password for the Security World Key in the configuration file you are attempting to load to complete initialization of the HSM module).
- Return to the **Import/Export** screen and attempt to import the configuration file again.

GDM PARTIAL CONFIGURATION IMPORTS

Through the Import / Export screen, users may import WSDL or XML policies with all their dependencies into the product.   This type of import is referred to as a GDM partial configuration import.

GDM Partial Configuration Import Examples

The example for a GDM partial configuration import is Import WSDL and Dependencies to an Agent Machine.

Import WSDL Policy and All Dependencies To an Agent Machine

When importing a WSDL or XML file, you are importing an .FSG file into the GDM IMPORT section of the Import / Export screen.   Follow these steps to import a WSDL policy from a file system to an Agent machine:
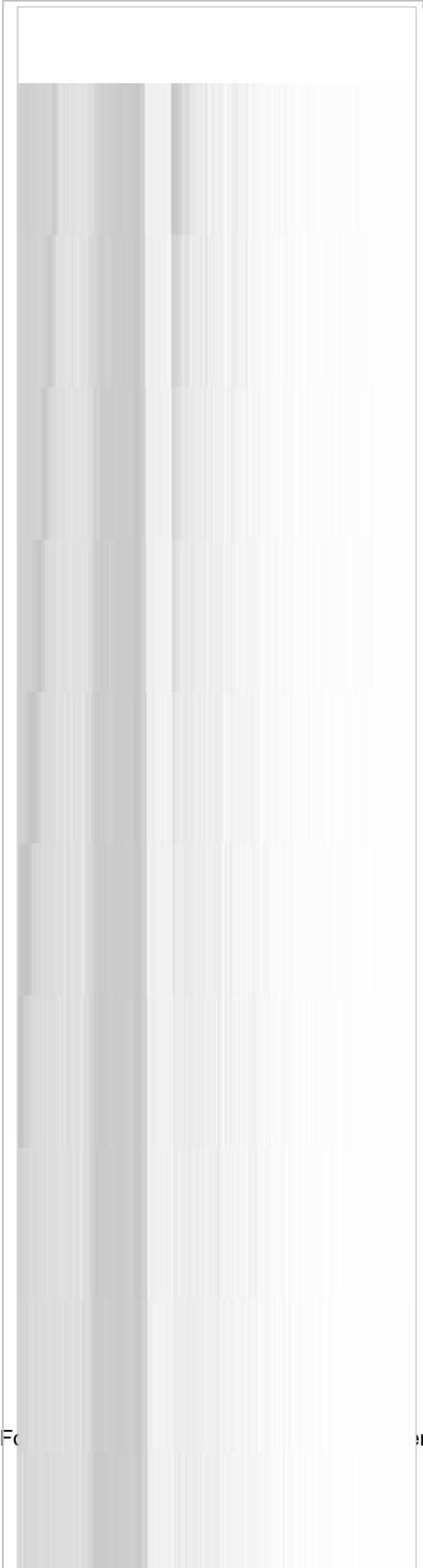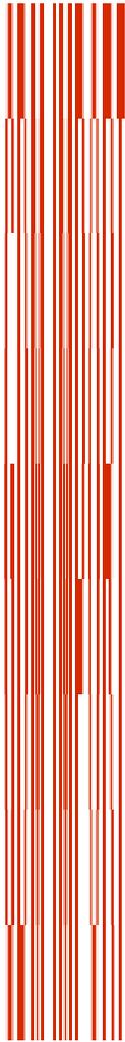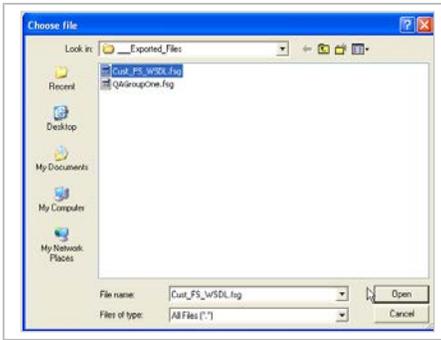
- From the Navigator, select **Import / Export**.
- From the GDM IMPORT section, aligned with the File field, click **Browse**. The Chose file screen appears.
- Navigate your file system, locate and click to select the **FSG file** to import, click **Open** and the screen closes. The File field on the GDM IMPORT section of the screen populates with the name of the selected file to download.
- Click **Import**. When finished downloading, the IMPORT / EXPORT screen refreshes with the "Import completed successfully" message visible at the top of the screen.

Note: Users may also import WSDL or XML policies from one Agent machine to another Agent machine by using the TRANSFER command, discussed earlier in the GDM Partial Configuration Transfer section.

GDM FULL CONFIGURATION EXPORTS

Export on Non-HSM-enabled and HSM-enabled Platforms

The system provides a method for exporting system configuration information, including policies, device setup, namespace and key data. The Import / Export screen provides a means of exporting system configuration information to import into other systems (for duplication or upgrade purposes) and also allows users to back up configuration information from their systems. Exported files are securely encrypted with a password provided when exporting.

From the Import / Export screen, users may export their full system configuration.

Only one configuration may be active on the system at one time. Exporting a configuration file will export a copy of the system's complete configuration information to a file. Configuration files are automatically named after the export date; i.e., config082903.fsx, but can be changed when exporting.

Network information (the management IP, the device IP, default gateway, primary DNS, secondary DNS, NTP server, and other associated settings) are not passed along with the fsx file.

The Export or Import Password

The password entered during the Export configuration operation is bound to that file. When exporting a file, the password provided is used to encrypt the .fsx file. Only by entering the same *password* while importing the .fsx file will the import process be successful.

Note: If running the Forum 1503, 2563, 3563, 4563 platform or a software port, disregard all content that refers to HSM. For installation information on the HSM, refer to the Initialize HSM on the CLI for the First Time section of the *Forum Systems Sentry™ Version 8.1 HSM Quick Start Guide.*

Export on HSM-enabled Platform

On an HSM enabled platform, transferring Security Worlds between HSM-enabled systems is part of the configuration import/export procedure.

GDM Full Configuration Export Examples

The example for a GDM full configuration export is Export System Configuration Without HSM.

Export Configuration

Exporting a configuration will result in a configuration file being generated and encrypted with the password that you supplied. Later, when you want to import this file, enter the same password in the IMPORT Password field to decrypt the file and import the configuration.
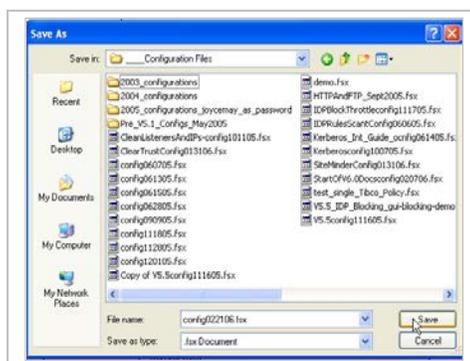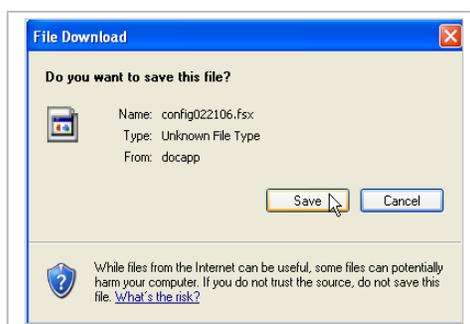
- From the Navigator, select **Import / Export** and the IMPORT / EXPORT screen appear.
- From the EXPORT section, in the Password field, enter your **Import / Export Password**.
- In the Confirm Password field, re-enter your **Import / Export Password**.
- Click **Export**. A system window appears.
- Click **Save** and the Save As screen appears. Navigate to an appropriate directory in your file system for saving the Exported configuration file, and then click **Save**.
- Click **Close**.

Note: Version 8.1 now has the ability to export the full configuration based on the policies configured for a particular agent. This is meant to ease moving configurations between non-interconnected network environments based on specific changes needed to move between environments..

GDM PARTIAL CONFIGURATION EXPORTS

Users may export one or more WSDL and / or XML policies to a local file system via an FSG file using the Export command visible on the WSDL POLICIES and XML POLICIES screens. This type of export is referred to as a GDM partial configuration export.

Note: Any exported configuration file built more than one major version prior will fail to import into the system.

GDM Partial Configuration Export Examples

The example for a GDM partial configuration export is Export WSDL Policy to Local File System.

Export WSDL Policy to Local File System

When exporting a WSDL or XML file, you are exporting an .FSG file. Follow these steps to export a WSDL policy to a local file system.
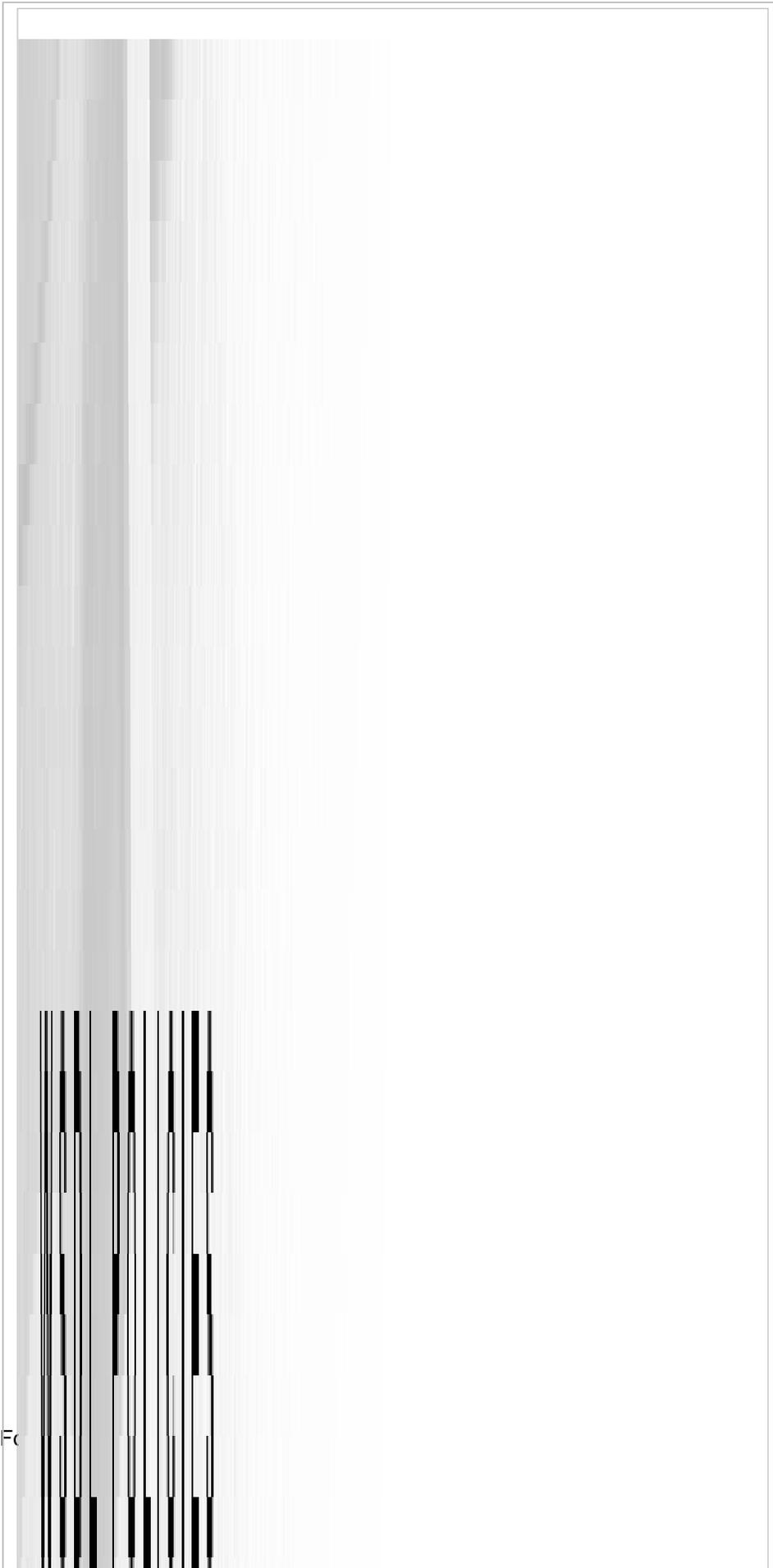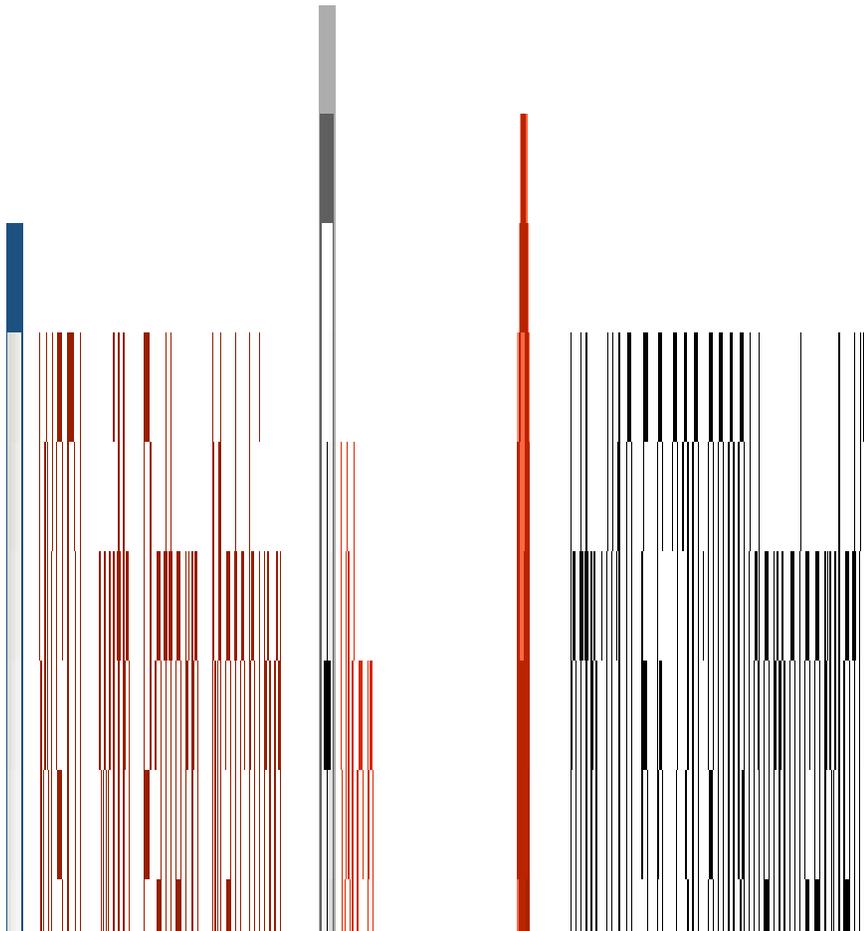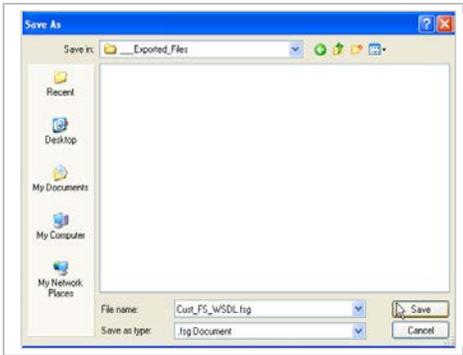
- Navigate to the **WSDL Policies** screen.
- Check the **checkbox** aligned with the WSDL policy to export.
- Select **Export**. The File Download screen appears. Select **Save** and the Save As screen appears.
- Navigate to a location in your file system. Select **Save**.

Note: For WSDL policies exclusively, do not confuse the **Export** command visible once a WSDL policy is opened with the **EXPORT** command on the WSDL POLICIES screen. Use the **Export** command visible once a WSDL policy is opened to export one or all operations of a WSDL policy based on an ACL.

SYSTEM

Under the Settings category of the Navigator, the System screen displays run-time configuration settings on the system.

System Settings Terms

While working with the System Settings screen, please consider the following:

FIELD NAME	DEFINITION
SYSTEM SETTINGS	
WebAdmin Port	The default port of the WebAdmin, 5050.
Global Device Management (GDM) Port	The default port for Global Device Management (GDM), 5070.
NTP Time Server	The IP address of your NTP time server. Server time is verified and synchronized with the NTP Time Server when this screen is saved. To resync, remove the IP address of your NTP time server, click **Save**, re-enter the IP address of your NTP time server and again, click **Save**.
Maximum Clock Skew (secs)	Setting to configure the clock skew or tolerance for tasks that consume WS-Security headers and SAML tokens. This value compensates for time differences between servers.
Session Timeout (in minutes)	Amount of time a session is allowed to be idle before the user is automatically logged out from the WebAdmin. Default is 8 minutes; however, minimum allowed is 1 minute and the maximum is 120.
SSL Termination Policy	The SSL Termination Policy used for the Web Admin and GDM listeners. By default it is set to the "factory ssl termination policy" which uses a self-signed certificate and key for authentication. This policy may not be deleted; however, it SHOULD be replaced on a production system with an SSL Termination Policy which provides proper authentication for the appliance.
SSL Initiation Policy	The SSL Initiation Policy used by any configuration screen which allows retrieval of a file via https (e.g. importing a WSDL file via https), or when browsing URLs. It is also used by any LDAP policy which initiates an LDAP connection over SSL. By default it is set to the "factory ssl initiation policy" which attempts to authenticate the remote server against the default signer group. This policy may not be deleted; however, it may be replaced by another SSL Initiation policy.
Web Admin IP ACL Policy	The IP ACL policy used as the system default. The factory system default IP ACL policy, **Unrestricted**, cannot be edited, and cannot be deleted. This IP ACL policy allows all IP ranges.
Block access to unprotected services	When checked, requires that some form of authentication must occur before a request has finished processing.

FIELD NAME	DEFINITION
EMAIL SETTINGS	
SMTP Mail Server	The IP address of your SMTP mail server. Used when sending Web Service reports, IDP alerts, failover alerts, and key expiration alerts.
From email address	The sender email address to use when sending Web Service reports, IDP alerts, failover alerts, and key expiration alerts.
Sends email alerts to	The recipient email address to use when sending failover alerts and key expiration alerts.
PROXY SETTINGS	
Use Proxy to connect to Remote Servers (HTTP only)	When checked, the Use Proxy to connect to Remote Servers (HTTP and HTTPS only) provides HTTP proxy requests for all outgoing HTTP Network policies. Used for deployment behind a proxy server where external HTTP requests require using a proxy.
HTTP Proxy Server	The IP address or host name of the HTTP proxy server. Used anytime an HTTP connection is made. For example, at run-time when connecting to an HTTP Remote policy or during configuration when importing a WSDL via HTTP URL.
HTTP Proxy Port	The port of the HTTP proxy server. Used anytime an HTTP connection is made. For example, at run-time when connecting to an HTTP Remote policy or during configuration when importing a WSDL via HTTP URL.
HTTPS Proxy Server	The IP address or host name of the HTTPS proxy server. Used anytime an HTTPS connection is made. For example, at run-time when connecting to an HTTPS Remote policy or during configuration when importing a WSDL via HTTPS URL.
HTTPS Proxy Port	The port of the HTTPS proxy server. Used anytime an HTTPS connection is made. For example, at run-time when connecting to an HTTPS Remote policy or during configuration when importing a WSDL via HTTPS URL.
Proxy Auth User	The user name to present for authentication when connecting to the proxy server. Used anytime an HTTP connection is made through a proxy.
Proxy Auth Password	The password of the user presenting credentials for authentication when connecting to the defined proxy server. Used anytime an HTTP connection is made through a proxy.

FIELD NAME	DEFINITION
Bypass Proxy for	A value or a list of values which represents an exception list of domain names that will be connected to directly without using the proxy server. The required format for this value is a list of hosts, each separated by a |. A wildcard character (*) can be used for matching. For example: "*.foo.com|*.moo.com|localhost" Used anytime an HTTP connection is made through a proxy.
Add X-Forwarded-For header to outgoing requests	When checked, adds X-Forwarded-For header and the IP of the client to outgoing requests. Used at run-time whenever a client request to a Listener policy is proxied to a remote server via a Remote policy. This applies to all requests to a WSDL policy and all requests to a proxy-mode Virtual Directory in an XML policy. When unchecked, nothing is added to outgoing requests.

Session Timeout

When accessing the WebAdmin for the first time, the session timeout default is 8 minutes; however, the minimum allowed is 1 minute, and the maximum allowed is 120 minutes. Any action that causes an interaction with the server resets the correct session time.

When the session timeout is adjusted, the adjustment does not affect the currently logged in users. These users are still subject to the previous session timeout value until they login again. Regain access to the WebAdmin by selecting the **LOGOUT** button, and then login again.

NTP Server Synchronization Overview

The system uses ntpd, Network Time Protocol NTP) daemon, for time synchronization and ntpdate to force a time synchronization. The **network utils ntp-validate** command, available in the CLI, performs three separate processes:
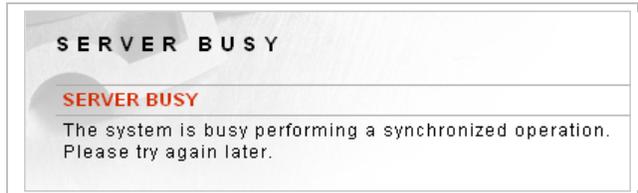
- Stops ntpd (which starts the NTP daemon)
- Runs ntpdate (which performs a synchronization by stopping the NTP daemon)
- Start ntpd (which turns the NTP daemon back on after synchronization)

Sync NTP Server from the WebAdmin UI

To verify the time and sync the NTP server from the WebAdmin UI:

- With the **Systems** screen open, enter the **IP address** of your NTP time server in the NTP Time Server field.
- Click **Save**.

The following message appears during synchronization.

Note: For more information on ntpd, refer to http://www.cis.udel.edu/~mills/ntp/html/ntpd.html.
For more information on ntpdate, refer to http://www.cis.udel.edu/~mills/ntp/html/ntpdate.html.

Resync NTP Server from the WebAdmin UI

To resync the NTP server from the WebAdmin UI:

- With the **Systems** screen open, remove the **IP address** of your NTP time server in the NTP Time Server field.
- Click **Save**.
- Re-enter the **IP address** of your NTP time server in the NTP Time Server field.
- Click **Save**.

System Settings Examples

The example for System settings is Reconfigure System Settings and Retain the Forum SSL Termination Policy.

Note: To reconfigure the System Settings with Your Corporate SSL Termination Policy, refer to the *Forum Systems Sentry™ Version 8.1 Web-based Administration Guide.*

Reconfigure System Settings and Retain Forum SSL Termination Policy

The SYSTEM SETTINGS screen is pre-populated with physical configuration data that were entered during initialization of the system from the Command Line Interface (CLI). When logging on to the WebAdmin UI, pre-loaded Forum SSL policies (factory ssl termination policy and factory ssl initiation policy) allow access to the WebAdmin.

The factory ssl termination policy secures the SSL connection between your web browser and the WebAdmin. The factory ssl initiation policy is used for outbound SSL LDAP connections or connecting to any HTTPS URLs (to pull in WSDLs over HTTPS. Follow these steps to reconfigure the system based on your network configuration:

Note: All HTTP headers are sent both in the clear to the proxy and encrypted via SSL to the remote server. As a result, if basic auth credentials are used, these credentials are protected between the proxy and the remote server but not between the client and the proxy.

- From the Navigator, under the Settings category, select **System**.
- Skip the WebAdmin and the Global Device Management (GDM) port fields.
- In the NTP Time Server field, enter an **IP address** for your NTP time server.
- Decide to accept the default value in the Maximum Clock Skew (secs) or change it.

Note: The value in the Maximum Clock Skew field is a tolerance setting which allows the system to compensate for time differences between servers. This setting affects tasks that include WS-Security headers and SAML Assertions. Increasing the default value of 0 by increasing it to 300 seconds will insure that tasks which might fail because the NotBefore SAML:Condition has not been met will, indeed, not fail.

Forum Systems recommends that customers working with WS-Security Headers and SAML Assertions increase the value of the Maximum Clock Skew to 300 seconds.

- Overwrite the Session Timeout (in minutes) field to **120**.
- Accept the default SSL Termination Policy (factory ssl termination policy).
- Accept the default SSL Initiation Policy (factory ssl initiation policy).
- From the Web Admin IP ACL Policy drop down list, skip Unrestricted to retain the system default IP ACL policy, or select another **IP ACL policy**.
- Decide to check the **Block access to unprotected services** checkbox or not.

Note: When checked, requires that some form of authentication must occur before a request has finished processing.

- In the SMTP mail server field, enter an **IP address** for your SMTP mail server.
- Enter a **user email address** in the From email address field.
- Enter a **user email address** in the Send system alerts to email address field.
- Skip the Use Proxy to connect to Remote servers (HTTP only) checkbox.

Note: This option is used for deployment behind a proxy server where external http requests require using a proxy.

- Skip the HTTP Proxy Server IP address field.
- Skip the HTTP Proxy Port field.
- Skip the HTTPS Proxy Server field.
- Skip the HTTPS Proxy Port field.
- Skip the Proxy Auth User field.
- Skip the Proxy Auth Password field.
- Skip the Bypass Proxy For field.
- Check the **Add X-Forwarded-For header to outgoing requests** checkbox, and then click **Save**.

CONTROL

From the navigator SYSTEM category, under Settings, select **Control**. The CONTROL SETTINGS screen appears.

> **Warning:** Forum Systems requires using the **Shutdown** command from the CLI or WebAdmin to turn the appliance off. If the appliance is not shutdown correctly, the system may perform a self diagnosis the next time the appliance is started. This routine may take several minutes, where the appliance appears unavailable.

Control Screen Examples
Examples for Control settings include:

- Reboot the Appliance.
- Shut down the Appliance.

Reboot the Appliance

> **Note:** If running the software product (non-appliance), the Reboot command is not visible.

- From the Navigator, select **Control**, and the CONTROL screen appears.
- Select **Reboot**. The "Are you sure you want to reboot the server?" message appears. Click **OK**.
- A confirmation message appears, notifying Administrators that a reboot is in progress.

Shutdown the Appliance

- From the Navigator, select **Control**, and the CONTROL screen appears.
- Select **Shutdown**. The "Are you sure you want to shutdown the server?" message appears. Click **OK**.
- A confirmation message appears, notifying Administrators that a shutdown is in progress.

PREFERENCES

The Preferences screen is used to set global user preferences that include:

- Default Process Response.
- Default HTTP Request Chunking.
- Default HTTP Response Chunking.
- Enable advanced XPath entry.
- Set a default Task List Group.

The following table details each user preference available from the Preferences screen:

OPTION	DETAIL
Default Process Response	Enabling this option will cause all newly created Remote policies to have Response Processing enabled. Disabling this option will cause all newly created Remote policies to have Response Processing disabled. The individual settings on Remote policies for response processing can be subsequently changed by editing the Remote policy directly. **Note:** For more information, refer to the *Forum Systems Sentry™ Version 8.1 HTTP Guide.*
Default HTTP Request Chunking	Enable HTTP 1.1 Chunking on new HTTP remote policies by default. This feature supports HTTP 1.1 chunk-encoding for customers that require large document transfers.
Default HTTP Response Chunking	Enable HTTP 1.1 Chunking on new HTTP listeners by default. This feature supports HTTP 1.1 chunk-encoding for customers that require large document transfers.
Enable advanced XPath entry	This options if for expert users only and should normally be disabled. Only expert XPath programmers should enable this option. Enabling this option exposes an extra blank row in the XPath expression tables for all tasks requiring XPath expressions. Normally, WebAdmin users compose XPath expressions by graphically selecting XML elements of the XML sample document specified for a Task List.

This advanced XPath option allows users to enter arbitrary raw XPath expressions that do not match the XML sample document. This option can be used to bypass the automatic XPath task validation features of the WebAdmin and may greatly increase the time and complexity involved in creating and debugging system Task Lists.

Default Task List Group	This feature provides the ability to set a default Task List Group. When this field is set, any: • XML policy created will automatically be associated with the Task List Group selected on the Preferences screen. On an XML policy, this default Task List Group is visible from the Task List tab. • WSDL policy created will automatically be associated with the Task List Group selected on the Preferences screen. On a WSDL policy, this default Task List Group is visible under the PROCESSING SETTINGS on the Settings tab. The individual settings on a WSDL or XML policy can be subsequently changed by editing the default Task List Group directly from the USER PREFERENCES screen or from the open WSDL or XML policy details screen. **Note:** For more information on editing a Task List Group, refer to the *Forum Systems Sentry™ Version 8.1 Tasks Management Guide.*

NETWORK

The Network screen is used for global network management of the system. The settings in this screen include the management interface IP and netmask, the device configuration IP and netmask, your default gateway, DNSs and topology (physical configuration - Inline or 1-port) mode, and all network routes. This screen also includes an option to allow communication between the device Management and Network interfaces. This option is usually used when deploying Management and Device IPs on the same subnet.

Although route information appears in the Network screen, routes are managed from the CLI. Only privileged users may change the System name. Privileged users are those users who have the Enable privileged access checkbox checked on the USER DETAILS screen

Network Screen Terms

When configuring your network from the Network Settings screen, please consider the following:

FIELD NAME	DEFINITION
MANAGEMENT NETWORK INTERFACE	
IP Address	The IP address of the Management Network Interface.
Netmask	The netmask for the Management Network Interface.
Management Interface	The Management Interface drop down list includes the three possible network interfaces; MGMT, WAN or LAN. Select the interface used by the WebAdmin and GDM listener to bind to, i.e. from which interfaces they listen for connections.
System Name	A unique name for this system. **Note:** Only privileged users may change the System name. Privileged users are those users who have the Enable privileged access checkbox checked on the USER DETAILS screen. The value entered in the System Name field will populate to the %sysname% tag found in the Default Template. If no value is entered in the System Name field, then the %sysname% tag appears as a blank in the Default Template. For more information about the Default Template and other error handling templates, refer to the *Forum Systems Sentry™ Version 8.1 HTTP Guide*.
DEVICE CONFIGURATION	
Topology Mode	Topology mode is a setting previously decided by your IT or Network Administrator. Check whichever setting your IT or Network Administrator has already decided upon. • With Inline (Single IP address) radio button selected, the system is configured in In-line mode with a LAN IP address and LAN netmask. • With Inline (Two IP addresses) radio button selected, the system is configured in In-line mode with a LAN IP address and LAN netmask as well as a WAN IP address and WAN netmask. • With One Port address radio button selected, the system is configured in one-port mode.

FIELD NAME	DEFINITION
DEVICE CONFIGURATION	
Device/WAN IP Address	The IP address for the WAN network interface.
Device/WAN Netmask	The netmask for the WAN network interface.
LAN IP Address	The IP address for the LAN network interface.
LAN Netmask	The netmask for the LAN network interface.
Default Gateway	Default Gateway for the system.
Gateway Interface	The default gateway interface options available on the system. • Select System Default to allow the system to choose an interface for you. • Select WAN to set the gateway interface to the WAN binding interface. • Select LAN to set the gateway interface to the LAN binding interface. • Select Management to set the gateway interface to the MGMT binding interface. • Select Virtual Interface to set the gateway interface that aggregates both the WAN and LAN binding interfaces. **Caution:** Available options for your Gateway Interfaces are not visible until you have previously selected the desired Topology Mode, selected Save, and the NETWORK SETTINGS screen has refreshed.
Allow communication between management and device networks	When checked, this option allows communications between the Network and Device Management interfaces. This setting is required when deploying Management and Device interfaces on the same subnet.
DNS SETTINGS	
Primary DNS	The address of your primary DNS.
Secondary DNS	The address of your secondary DNS.
NETWORK ROUTES	
Destination	The destination IP address or network address for the route.
Gateway	The gateway IP address for a route.
Netmask	The netmask of a route.
Type	The type of route. HOST specifies a specific IP address, and NET specifies a range of IP addresses.
Interface	The interface that the route will use: WAN, LAN, Management or Loopback.

Note: Whenever making changes to the Primary or Secondary DNS from the Network screen, you must subsequently run the **reboot** command from the Control screen in the WebAdmin for the new DNS

change(s) to be active. The only exception is when first configuring the system.

Network Screen Example

The example for Network settings is Reconfigure Network Settings.

> **Note:** Except when first configuring the system, when making changes to the Primary or Secondary DNS from the Network screen, you must then run the *reboot* command from the CLI in enable mode or from the Control screen in the WebAdmin for the new DNS change(s) to be active.

Reconfigure Network

This sample demonstrates changing the Topology mode, Primary and Secondary DNSes. Follow these steps to reconfigure network settings:

- From the Navigator, select **Network**.
- Accept the IP address value previously entered in the Installation Wizard.
- Accept the Netmark value previously entered in the Installation Wizard.
- From the Management Interface drop down list, select **MGMT**, **WAN** or **LAN** as the interface used by the WebAdmin and GDM listener to bind to, based on your network configuration (**MGMT**).
- In the System Name field, enter a unique **name** for this system (**Houston**).
- Change the Topology Mode radio button from One Port to **Inline (Single IP address)**. Note that the LAN IP Address and LAN Netmask are now grayed out.
- Click **Save**.

NETWORK SETTINGS

MANAGEMENT NETWORK INTERFACE

IP Address: 10.5.3.92
Netmask: 255.255.255.0
Management Interface*: MGMT
System Name: Houston

DEVICE CONFIGURATION

Topology Mode: ● Inline (Single IP address) ○ Inline (Two IP addresses) ○ One Port
Device/WAN IP Address*: 10.5.6.92
Device/WAN Netmask*: 255.255.255.0
LAN IP Address: 10.5.6.94
LAN Netmask: 255.255.255.0
Default Gateway: 10.5.6.1
Gateway Interface: ● System Default ○ Virtual Interface ○ Management
☑ Allow communication between management and device networks

DNS SETTINGS

Changes will not take effect until the system is rebooted
Primary DNS: 10.5.3.12
Secondary DNS: 10.5.3.11

[Save]

NETWORK ROUTES

Destination	Gateway	Netmask	Type	Interface
10.5.6.0	*	255.255.255.0	NET	WAN
10.5.3.0	*	255.255.255.0	NET	Management
127.0.0.0	*	255.0.0.0	NET	Loopback
0.0.0.0	10.5.6.1	0.0.0.0	NET	WAN

- Enter the **Device/WAN IP Address** in the Device/WAN IP Address field (**10.5.6.92**).
- Enter the **Device/WAN Netmask** in the Device/WAN Netmask field (**255.255.255.0**).
- Skip the disabled LAN IP Address field.
- Skip the disabled LAN Netmask field.
- Enter the **Default Gateway IP address** in the Default Gateway field **(10.5.6.1**.
- Aligned with Gateway Interface, select the **System Default, Virtual Interface** or **Management** radio button (**System Default**).
- Confirm that the **Allow communication between management and device networks** checkbox is checked. This setting is required when deploying Management and Device interface on the same subnet.
- Edit the **Primary DNS IP** in the Primary DNS field to **10.5.3.11**.
- Edit the **Secondary DNS IP** in the Secondary DNS field to **10.5.3.12**.
- Click **Save**.

UPGRADE SOFTWARE

From the Navigator, selecting **Upgrade** displays the Upgrade Software screen that is used for upgrading your Forum software directly on the system.

Note: When upgrading through major versions (i.e. 3.x -> 4.x -> 5.x), Administrators should export the configuration after completion of the upgrade to the final version.

The Forum software on the system may be upgrading by:

- Installing a local copy of the software onto the system.
- Installing in a copy of the software via a URL.

Upgrading software from the Upgrade screen is available only to users who have been granted privileged access (from the Users detail screen, check the Enable privileged access checkbox).
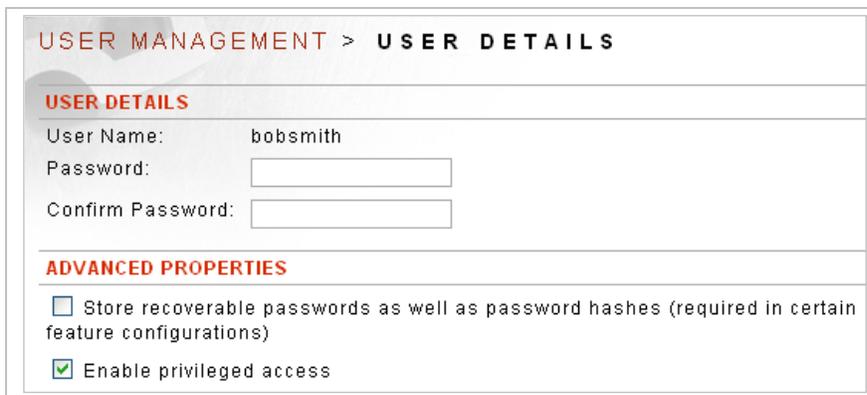
Upgrade Software Examples

The examples for the Upgrade Software screen include:

- Upgrade Forum Software from a Local Copy.
- Upgrade Forum Software from a URL.

Note: Every time you upgrade the product software, the database drivers are lost, and the new database drivers installed are whichever drivers are on the upgraded product software.

If subsequently upgrading database drivers, follow this action by running the **reboot** command from the CLI in enable mode or from the Control screen in the WebAdmin.

However, with DB2 databases, when upgrading the product software, the produce retains the most recent DB2 drivers.

Upgrade Forum Software from a Local Copy

If the Image File field, the Fingerprint File field and the URL field include values, the system gives preference to the URL field over the filename fields. Follow these steps to upgrade the Forum software from a local copy:
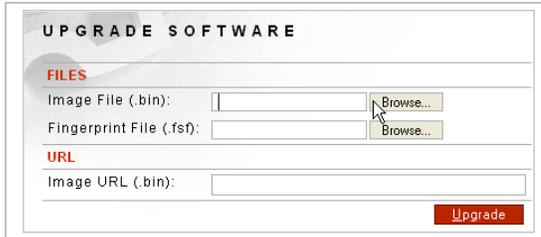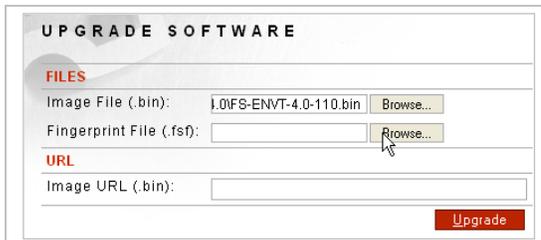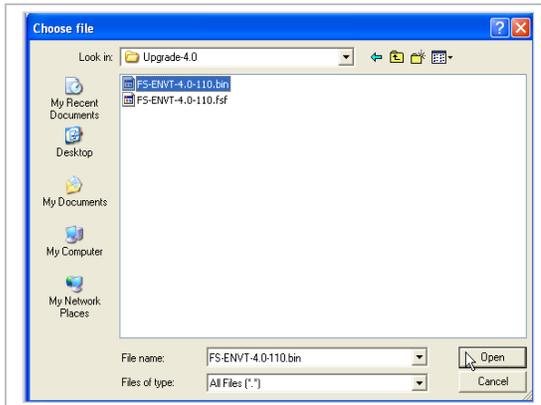
UPGRADE SOFTWARE

FILES

Image File (.bin):	.0\FS-ENVT-4.0-110.bin	Browse...
Fingerprint File (.fsf):	4.0\FS-ENVT-4.0-110.fsf	Browse...

URL

Image URL (.bin):

Upgrade

UPGRADE SOFTWARE

UPGRADE STATUS

Upgrade in progress, please wait...
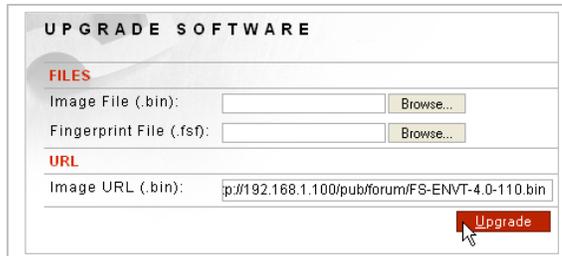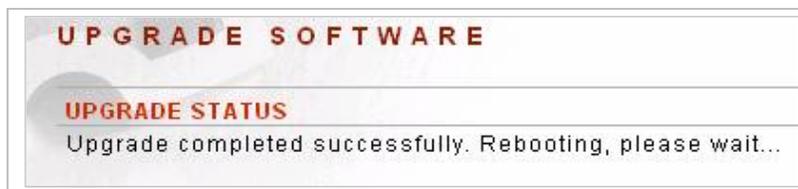

UPGRADE SOFTWARE

UPGRADE STATUS

Upgrade completed successfully. Rebooting, please wait...

- From the Navigator, select **Upgrade**.
- Aligned with the Image Image File (.bin) field, click **Browse** to navigate to and highlight a <**filename.bin**> file. The Chose file screen appears. Click the <**filename.bin>**, and then click **Open**. The UPGRADE SOFTWARE screen refreshes.
- Aligned with the Fingerprint File (.fsf) field, click **Browse** to navigate to and highlight a <**filename.fsf**> file. The Chose file screen appears. Click the <**filename.fsf>**, and then click **Open**. The UPGRADE SOFTWARE screen refreshes.
- Click **Upgrade**.
- The "Warning: Upgrade is not reversible. You may want to export a backup copy of your configuration before upgrading. Are you sure?" message appears. Click **OK**.
- The "Upgrade in progress, please wait" messages appear.
- The "completed successfully. Rebooting, please wait" messages appear.

Note: After upgrading the Forum software, the Administrator must log back into the WebAdmin.

Upgrade Forum Software from a URL

If the Image File field, the Fingerprint File field and the URL field include values, the system gives preference to the URL field over the filename fields. Follow these steps to upgrade the Forum software from a URL:

- From the Navigator, select **Upgrade**.
- In the Image URL (.bin) field, enter an **URL** (**ftp://<URL>/<path>/<filename.bin>**) for downloading the Forum software onto an system, and then click **Upgrade**.
- The "Warning: Upgrade is not reversible. You may want to export a backup copy of your configuration before upgrading. Are you sure?" message appears. Click **OK**.
- The "Upgrade in progress, please wait" messages appear.
- The "completed successfully. Rebooting, please wait" messages appear.

Note: After upgrading the Forum software, the Administrator must log back into the WebAdmin.

FAILOVER

Failover may be configured for one system (Standalone), or two; a Master and a Standby. For higher reliability, two systems can be connected together via a serial null-modem cable for redundancy. One system is designated as the Master system, while the second system becomes a Standby system.

Note: Failover is unavailable on the Forum Systems Type-PCI card product.

Failover Deployment Mode Scenarios

The following graphic displays three basic scenarios for Small/Medium class and Enterprise class failover deployment modes, followed by an overview of each deployment; two Forum System failover solutions and one generic:
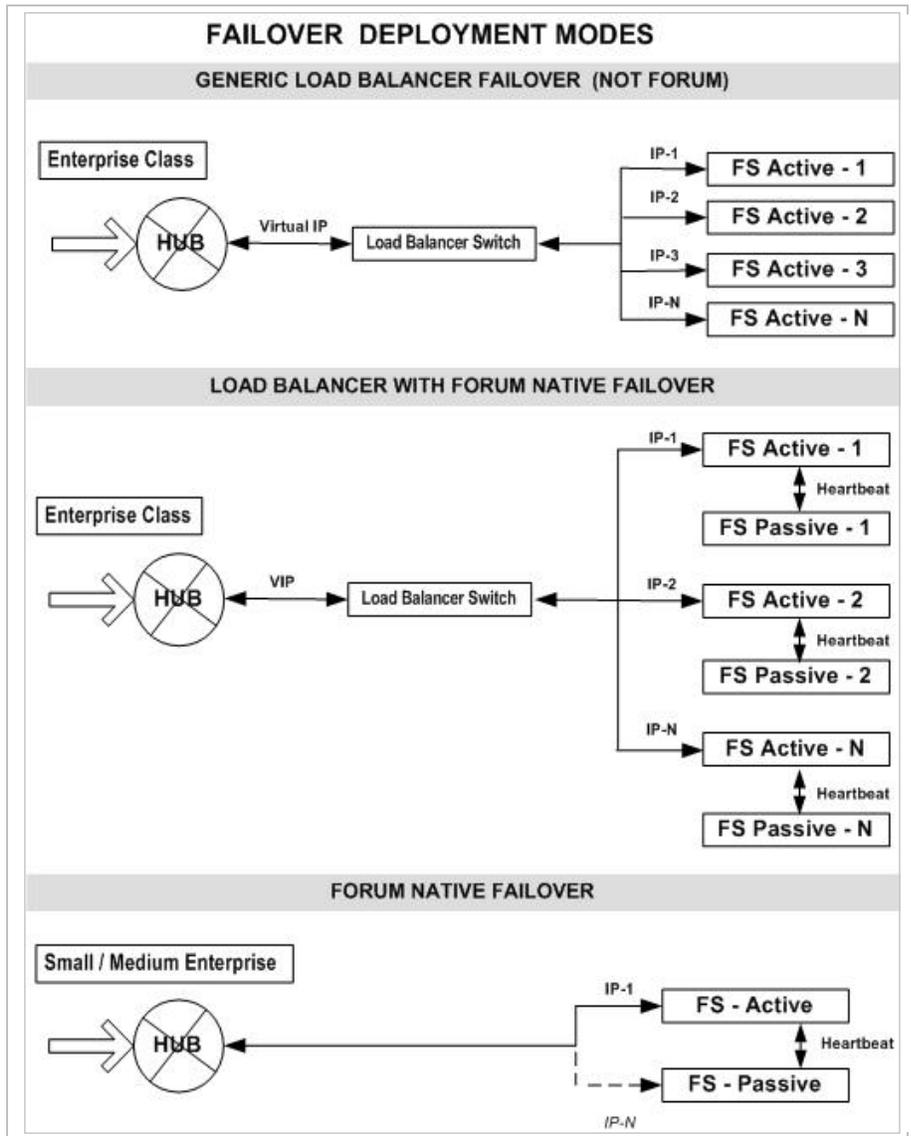

Figure 4: Failover Deployment Modes.

Generic Load Balancer Failover Scenario

In the Load Balancer Failover scenario presented in the Failover Deployment Mode Scenarios, failover is monitored by the load balancer switch with a number of standalone systems. This generic (not forum Systems' solution) scenario offers a solution with four standalone servers.

Load Balancer with Forum Native Failover Scenario

In the Load Balancer with Forum native Failover scenario presented in the Failover Deployment Mode Scenarios, failover is monitored first through the load balancer, and then through each Master and Standby pair. The Load Balancer provides a secondary level of redundancy control. This scenario offers a Load Balancer with Forum Failover.

Forum Native Failover Scenario

In the Forum Native Failover scenario presented in the Failover Deployment Mode Scenarios, basic failover is monitored with a Master system and a Standby system. This scenario offers basic Forum Failover.

Configure and Test Failover on a Master and Standby System

The following graphic displays the sequential steps to configure and test Failover on a Master and Standby system:
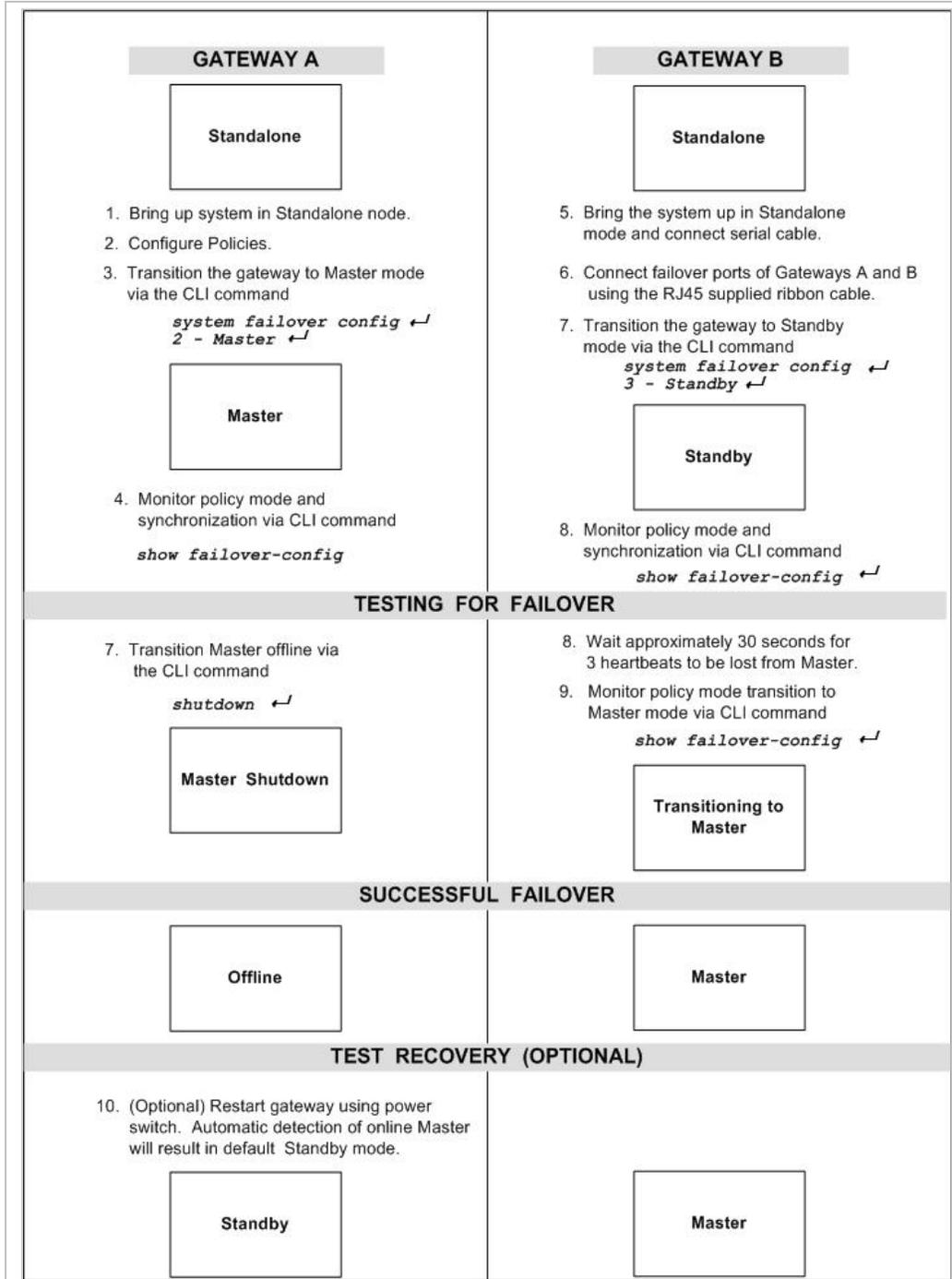

Figure 5: Configuring Failover on a Master System and Standby System.

Configuring Master and Standby Systems

During normal operation in a failover configuration, the Master system is active and the Standby system is not active, but is monitoring the Master system. Upon failure of the Master system, the Standby system becomes active. A failure is triggered by three missing heartbeat responses from the Master. Heartbeats are sent at ten second intervals.

Note: With two systems, always configure the Master before the Standby.

When the Standby system becomes Master, its configuration mirrors that of the failed Master system. All network services and addresses remain the same. The MAC address of the Master is reused in the Standby system.

Referring to the Failover Deployment Mode Scenarios, once configuration is established in Master and Standby mode (steps 1 through 7), the Standby continues to send heartbeats to the Master at ten second intervals.

Note: The CLI command show failover config, used in step 8 displays: 1.) the configuration mode of the Standalone, Master or standby system; 2.) the last synchronization timestamp; 3.) the % completion of the currently progressing synchronization.*

* 0% complete means that the CLI is not actively performing a synchronization.

If three subsequent heartbeats are not responded from the Master in approximately 30 seconds (step 8), the Standby will consider that the Master has failed, and subsequently it will transition itself to Master (step 9) while bringing up the synchronized policies. Subsequently, the Standby will become Master.

When the first Master becomes active again (step 10), it senses that there is a new Master, and automatically assumes the role of Standby.

Once the set of policies you wish to deploy operationally are established on the Master, go to the CLI and utilize the **system failover synchronize** command. At the next heartbeat (within the next 10 seconds), this command will schedule a synchronization between the Master and the Standby by which all new policies that were configured at the Master will be synchronized with the Standby. In this manner if Failover occurs, the Standby will have the latest policies.

When systems have been set in Master or Standby modes, the CLI **show failover-config** command will display the failover configuration mode for the system, the last synchronization timestamp and the synchronization % for completed or in progress policy synchronizations.

Upgrade Forum Systems Device when Using Forum Systems Native Failover

The following instructions are for upgrading Forum Systems™ device when using Forum Systems™ Native Failover feature and applies to all versions of Forum Systems™ devices.

Upgrade Overview

At the completion of the upgrade process the Forum Systems™ device will reboot automatically. When the "Master" system finishes upgrading and reboots, the "Standby" system will become the new "Master" system. When the first system comes back online, it will become the "Standby" system. When the upgrade of the second system, or the new "Master" system, completes it too, will automatically reboot causing the first system, or the original "Master" system, to again become the "Master". At this point, both systems will be upgraded and the Master / Standby scenario will be the same as it was when this upgrade process was started.

Upgrade Preparation

Please review the following information in preparation for upgrading the Forum Systems™ device.

Prior to upgrading the Forum Systems™ device, you will need to obtain the download site information from Forum Systems™ Technical Support. Please contact Forum Systems™ Technical Support for this information.

- Depending on the version you are upgrading from, you may require a new license key to use the latest version of the Forum Systems™ system. If you require a new license or if you are not sure, please contact Forum Systems™ Technical Support prior to beginning the upgrade process.
- Ensure that you have a backup of your current configuration. To accomplish this, log on to the WebAdmin and under the SYSTEM category, navigate to the Import/Export screen. The configuration file will be a .fsx file and, by default, it will be named in the configCURRENTDATE.fsx format. For example, a configuration file that was exported on December 5, 2004 would, by default, be named config120504.fsx.
- When exporting the configuration, be sure to enter a password that is familiar, as you will need to enter that same password if you ever need to import this configuration file.
- The system upgrade procedure is accomplished using the Forum Systems™ CLI (command line interface). You will need to access the CLI using either an SSH session or by connecting to the system via a serial cable and establishing a HyperTerminal session into the system.

Upgrade First System - the Master System

Access the CLI and enter *enable* mode. Verify the current failover status by typing the *show failover-config* command. This system should be in "Master" mode.

```
ForumOS# show failover-config <enter>

-----------------------------------
      Failover Configuration
-----------------------------------
Configuration Mode:  Master
Last synchronization:

Synchronization in progress:  0% completed

ForumOS#
```

Upgrade the "Master" system by typing the **management upgrade-software** command. Type the Transport Protocol to use for the upgrade and then **<enter>**. Normally this will be FTP.

Enter the Server name given to you by Forum Systems™ prior to upgrading. It will not be 10.10.10.10.
Enter the Package <*file*> name as given to you by Forum Systems™ Technical support.

```
ForumOS# management upgrade-software <enter>

# Please enter: Protocol
# The protocol for retrieving
   Available options: Http or FTP

> ftp <enter>
[Enter http or ftp, and then press <enter>]



# Please enter: Server name
# The name or address of the server where the package can be found

> 10.10.10.10 <enter>
[Enter Server Name or IP Address, and then press <enter>]



# Please enter: Package <file> name
# The name of the file to download

> config120504.fsx <enter>
[Enter the filename for the Forum upgrade package, and then press <enter>]
```

```
Upgrade successful.  Rebooting

ForumOS#
```

At this point your SSH session will be terminated as the system is being rebooted.

When the original "Master" finishes rebooting, it will become the new "Standby" system. At this point the two systems have swapped Failover modes and you should be able to SSH back into the CLI using the same management IP as before. You should also be able to access the WebAdmin using the same IP as before.

Note: the IP address is now active on the new "Master" machine which has not yet been upgraded.

Upgrade Second System - the New Master System

Run through the exact same procedures outlined in the Upgrade First System The New Master System section. When this is completed, this second system will reboot and the first system will transition itself back to Master Mode. When the second system comes back online it will be back to Standby Mode as it was before this process began.

Caution: If the failover scenario fails, it is possible that you could end up with two systems running in Master mode after the original "Master" finishes rebooting. This could cause an IP conflict on your network, so unplug the network cables on one of the systems immediately and contact Forum Systems Technical Support.

Note: If you have any questions or if you run into any issues with this procedure, please contact Forum Systems™ Technical Support either via email at support@forumsys.com or by calling 800-707-4590 Monday through Friday between 9am and 6pm EST.

SYSTEM TROUBLESHOOTING

The following table displays troubleshooting issues and solutions:

ISSUE TO TROUBLESHOOT	SOLUTION
How to move the system from one physical location to another.	Run the *shutdown* command from the CLI in enable mode or from the Control screen in the WebAdmin. Next, press the main power switch at the rear of the system and unplug from its wall outlet. Move the system to new location, re-plug the system into a wall outlet and restart the system by pressing the main power switch at the back of the system (and potentially, the front power switch as well).
How to trigger System DNS changes to take effect.	Run the *reboot* command from the CLI in enable mode or from the Control screen in the WebAdmin.
What to do after upgrading db drivers from the **Archiving** screen.	Run the *reboot* command from the CLI in enable mode or from the **Control** screen in the WebAdmin.
What to do after upgrading system software from the **Upgrade** screen.	Every time you upgrade the product software, the database drivers are lost, and the new database drivers installed are whichever drivers are on the upgraded product software. However, with DB2 databases, when upgrading the product software, the produce retains the most recent DB2 drivers.
How to reset WS Monitoring data back to zero on the **WS Monitoring** screen.	Selecting **Reset** resets WS Monitoring data back to zero without rebooting the appliance.
How to reset Statistics data back to zero on the **Statistics** screen.	Selecting **Reset** resets Statistics data back to zero without rebooting the appliance.

Warning: Forum Systems requires using the **Shutdown** command from the CLI or WebAdmin to turn the appliance off. If the appliance is not shutdown correctly, the system may perform a self diagnosis the next time the appliance is started. This routine may take several minutes, where the appliance appears unavailable.

If running the Forum Systems software product, the **Reboot** command is not visible.

APPENDIX

Appendix A - Contacting Forum Systems

If you need to contact Forum Systems, use the following telephone numbers or email addresses in the following table:

REASON FOR CONTACT	PHONE	FAX	EMAIL
Sales	[801] 313-4400	[801] 313-4401	sales@forumsys.com
Technical Support	[800] 707-4590	[781] 788-4201	support@forumsys.com
General Information	[781] 788-4200	[781] 788-4201	info@forumsys.com

Appendix B - Licensing Information

The following section includes licensing information for:

- Jetty License, Revision 3.5
- Apache Xerces and Xalan Software License
- ClamAV Software License
- Jaxen License
- jChart License
- The Legion of the Bouncy Castle License
- Common Public License – v1.0
- Cryptix General License
- Oracle License

Jetty License Revision 3.5

Preamble:
The intent of this document is to state the conditions under which the Jetty Package may be copied, such that the Copyright Holder maintains some semblance of control over the development of the package, while giving the users of the package the right to use, distribute and make reasonable modifications to the Package in accordance with the goals and ideals of the Open Source concept as described at http://www.opensource.org.

It is the intent of this license to allow commercial usage of the Jetty package, so long as the source code is distributed or suitable visible credit given or other arrangements made with the copyright holders.

Definitions:
- "Jetty" refers to the collection of Java classes that are distributed as a HTTP server with servlet capabilities and associated utilities.

- "Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification.

- "Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder.

- "Copyright Holder" is whoever is named in the copyright or copyrights for the package.
  Mort Bay Consulting Pty. Ltd. (Australia) is the "Copyright Holder" for the Jetty package.

- "You" is you, if you're thinking about copying or distributing this Package.

- "Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)

- "Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

0. The Jetty Package is Copyright (c) Mort Bay Consulting Pty. Ltd. (Australia) and others. Individual files in this package may contain additional copyright notices. The javax.servlet packages are copyright Sun Microsystems Inc.

1. The Standard Version of the Jetty package is available from http://jetty.mortbay.org.

2. You may make and distribute verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you include this license and all of the original copyright notices and associated disclaimers.

3. You may make and distribute verbatim copies of the compiled form of the Standard Version of this Package without restriction, provided that you include this license.

4. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.

5. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when you changed that file, and provided that you do at least ONE of the following:

   a) Place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as ftp.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.

   b) Use the modified Package only within your corporation or organization.

   c) Rename any non-standard classes so the names do not conflict with standard classes, which must also be provided, and provide a separate manual page for each non-standard class that clearly documents how it differs from the Standard Version.

   d) Make other arrangements with the Copyright Holder.

6. You may distribute modifications or subsets of this Package in source code or compiled form, provided that you do at least ONE of the following:

   a) Distribute this license and all original copyright messages, together with instructions (in the about dialog, manual page or equivalent) on where to get the complete Standard Version.

   b) Accompany the distribution with the machine-readable source of the Package with your modifications. The modified package must include this license and all of the original copyright notices and associated disclaimers, together with instructions on where to get the complete Standard Version.

   c) Make other arrangements with the Copyright Holder.

7. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. You may not charge a fee for this Package itself. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that you meet the other distribution requirements of this license.

8. Input to or the output produced from the programs of this Package do not automatically fall under the copyright of this Package, but belong to whomever generated them, and may be sold commercially, and may be aggregated with this Package.

9. Any program subroutines supplied by you and linked into this Package shall not be considered part of this Package.

10. The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.

11. This license may change with each release of a Standard Version of the Package. You may choose to use the license associated with version you are using or the license of the latest Standard Version.

12. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

13. If any superior law implies a warranty, the sole remedy under such shall be, at the Copyright Holders option either a) return of any price paid or b) use or reasonable endeavours to repair or replace the software. 14. This license shall be read under the laws of Australia.

The End
This license was derived from the *Artistic* license published on http://www.opensource.com

ClamAV Software License

ClamAV is distributed under the GNU public license, which is available here: http://www.gnu.org/licenses/

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

  The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

  When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

  To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

  For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

  Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

  For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

  Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those

products. If such problems arise substantially in other domains, we
stand ready to extend this provision to those domains in future versions
of the GPL, as needed to protect the freedom of users.

  Finally, every program is threatened constantly by software patents.
States should not allow patents to restrict development and use of
software on general-purpose computers, but in those that do, we wish to
avoid the special danger that patents applied to a free program could
make it effectively proprietary. To prevent this, the GPL assures that
patents cannot be used to render the program non-free.

  The precise terms and conditions for copying, distribution and
modification follow.

Apache Xerces and Xalan Software License

The Apache Software License, Version 1.1

Copyright (c) 1999 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided
that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the
following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the
following disclaimer in the documentation and/or other materials provided with the distribution.

3. The end-user documentation included with the redistribution, if any, must include the following
acknowledgment: "This product includes software developed by the Apache Software Foundation
(http://www.apache.org/)." Alternately, this acknowledgment may appear in the software itself, if and
wherever such third-party acknowledgments normally appear.

 4. The names "Axis" and "Apache Software Foundation" must not be used to endorse or promote
products derived from this software without prior written permission. For written permission, please
contact apache@apache.org.

5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their
name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND
FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE
SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF
THE POSSIBILITY OF SUCH DAMAGE.
==

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>.

Jaxen License

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE Jaxen AUTHORS OR THE PROJECT CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Jaxen Project and was originally created by bob mcwhirter <bob@werken.com> and James Strachan <jstrachan@apache.org>. For more information on the Jaxen Project, please see <http://www.jaxen.org/>.

jChart License

Copyright 2002 (C) Nathaniel G. Auvil. All Rights Reserved.

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain copyright statements and notices. Redistributions must also contain a copy of this document.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name "jCharts" or "Nathaniel G. Auvil" must not be used to endorse or promote products derived from this Software without prior written permission of Nathaniel G. Auvil. For written permission, please contact nathaniel_auvil@users.sourceforge.net.

4. Products derived from this Software may not be called "jCharts" nor may "jCharts" appear in their names without prior written permission of Nathaniel G. Auvil. jCharts is a registered trademark of Nathaniel G. Auvil.

5. Due credit should be given to the jCharts Project (http://jcharts.sourceforge.net/).

THIS SOFTWARE IS PROVIDED BY Nathaniel G. Auvil AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL jCharts OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Legion of the Bouncy Castle License

Copyright (c) 2000 The Legion Of The Bouncy Castle (http://www.bouncycastle.org)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Common Public License - v1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

  a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

  b) in the case of each subsequent Contributor:

  i) changes to the Program, and

  ii) additions to the Program;

  where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors.

Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

Cryptix General License

Copyright (c) 1995-2003 The Cryptix Foundation Limited. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

> 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
> 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE CRYPTIX FOUNDATION LIMITED AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE CRYPTIX FOUNDATION LIMITED OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Oracle License

ORACLE TECHNOLOGY NETWORK DEVELOPMENT AND DISTRIBUTION LICENSE AGREEMENT "We," "us," and "our" refers to Oracle Corporation. "You" and "your" refers to the individual or entity that has ordered the programs from Oracle. "Programs" refers to the software product which you have ordered and program documentation. "License" refers to your right to use the programs under the terms of this agreement. This agreement is governed by the substantive and procedural laws of California. You and Oracle agree to submit to the exclusive jurisdiction of, and venue in, the courts of San Francisco, San Mateo, or Santa Clara counties in California in any dispute arising out of or relating to this agreement.

We are willing to license the programs to you only upon the condition that you accept all of the terms contained in this agreement. Read the terms carefully and select the "Accept" button at the bottom of the page to confirm your acceptance. If you are not willing to be bound by these terms, select the "Do Not Accept" button and the registration process will not continue.

License Rights
We grant you a nonexclusive, nontransferable limited license to use the programs only for purposes of developing and prototyping your applications. You may also distribute the programs with your applications to your customers. If you want to use the programs for any purpose other than as expressly permitted under this agreement you must contact us, or an Oracle reseller, to obtain the appropriate license. We may audit your use of the programs. Program documentation is either shipped with the programs, or documentation may accessed online at http://otn.oracle.com/docs.

Ownership and Restrictions
We retain all ownership and intellectual property rights in the programs. You may make a sufficient number of copies of the programs for the licensed use and one copy of the programs for backup purposes.

You may not:

   ·use the programs for any purpose other than as provided above;
   ·distribute the programs unless accompanied with your applications;
   ·charge your end users for use of the programs;
   ·remove or modify any program markings or any notice of our proprietary rights;
   ·use the programs to provide third party training;
   ·assign this agreement or give the programs, program access or an interest in the programs to any individual or entity except as provided under this agreement;
   ·cause or permit reverse engineering or decompilation of the programs;
   ·disclose results of any program benchmark tests without our prior consent; or,
   ·use any Oracle name, trademark or logo.

Program Distribution
We grant you a nonexclusive, nontransferable right to copy and distribute the programs to your end users provided that you do not charge your end users for use of the programs and provided your end users may only use the programs to run your applications for their business operations. Prior to distributing the programs you shall require your end users to execute an agreement binding them to terms consistent with those contained in this section and the sections of this agreement entitled "License Rights," "Export," "Disclaimer of Warranties and Exclusive Remedies," "No Technical Support," "End of Agreement," "Relationship Between the Parties," and "Open Source." You must also include a provision stating that your end users shall have no right to distribute the programs, and a provision specifying us as a third party beneficiary of the agreement. You are responsible for obtaining these agreements with your end users.

You agree to: (a) defend and indemnify us against all claims and damages caused by your distribution of the programs in breach of this agreements and/or failure to include the required contractual provisions in your end user agreement as stated above; (b) keep executed end user agreements and records of end user information including name, address, date of distribution and identity of programs distributed; (c) allow us to inspect your end user agreements and records upon request; and, (d) enforce the terms of your end user agreements so as to effect a timely cure of any end user breach, and to notify us of any breach of the terms.

Export
You agree that U.S. export control laws and other applicable export and import laws govern your use of the programs, including technical data. You agree that neither the programs nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

Disclaimer of Warranty and Exclusive Remedies

THE PROGRAMS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. WE FURTHER DISCLAIM ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

IN NO EVENT SHALL WE BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR DATA USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR ENTIRE LIABILITY FOR DAMAGES HEREUNDER SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS (U.S. $1,000).

No Technical Support
Our technical support organization will not provide technical support, phone support, or updates to you for the programs licensed under this agreement.

Restricted Rights
If you distribute a license to the United States government, the programs, including documentation, shall be considered commercial computer software and you will place a legend, in addition to applicable copyright notices, on the documentation, and on the media label, substantially similar to the following:

NOTICE OF RESTRICTED RIGHTS
"Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065."

End of Agreement
You may terminate this agreement by destroying all copies of the programs. We have the right to terminate your right to use the programs if you fail to comply with any of the terms of this agreement, in which case you shall destroy all copies of the programs.

Relationship Between the Parties
The relationship between you and us is that of licensee/licensor. Neither party will represent that it has any authority to assume or create any obligation, express or implied, on behalf of the other party, nor to represent the other party as agent, employee, franchisee, or in any other capacity. Nothing in this agreement shall be construed to limit either party's right to independently develop or distribute software that is functionally similar to the other party's products, so long as proprietary information of the other party is not included in such software.

Open Source
"Open Source" software - software available without charge for use, modification and distribution - is often licensed under terms that require the user to make the user's modifications to the Open Source software or any software that the user 'combines' with the Open Source software freely available in source code form. If you use Open Source software in conjunction with the programs, you must ensure that your use does not: (i) create, or purport to create, obligations of us with respect to the Oracle programs; or (ii) grant, or purport to grant, to any third party any rights to or immunities under our intellectual property or proprietary rights in the Oracle programs. For example, you may not develop a software program using an Oracle program and an Open Source program where such use results in a program file(s) that contains code from both the Oracle program and the Open Source program (including without limitation libraries) if the Open Source program is licensed under a license that requires any "modifications" be made freely available. You also may not combine the Oracle program with programs licensed under the GNU General Public License ("GPL") in any manner that could cause, or could be interpreted or asserted to cause, the Oracle program or any modifications thereto to become subject to the terms of the GPL.

Entire Agreement
You agree that this agreement is the complete agreement for the programs and licenses, and this agreement supersedes all prior or contemporaneous agreements or representations. If any term of this agreement is found to be invalid or unenforceable, the remaining provisions will remain effective.

Appendix C - Constraints in System Management Guide

ELEMENT	CONSTRAINTS	CHAR COUNT
Import / Export Password	Unique & case sensitive Accepts the '@' character, underscores, dashes and spaces.	6-128
Agent Policy Name	Unique & case sensitive Accepts underscores and dashes.	5-32
Agent Group Policy Name	Unique & case sensitive Accepts underscores and dashes.	5-32
HSM Administrator Card Passphrase	Unique & case sensitive. Accepts the '@' character, underscores and dashes. Spaces are allowed, but leading and trailing whitespace is ignored.	6-128
Failover heartbeat interval	10 seconds	N/A

Appendix D - Specifications in System Management Guide

ELEMENT SUPPORTED	SPECIFICATIONS
Import / Export Configuration files	Only a single Appliance configuration (filename.fsx) file is active at any given time.
System Session Timeout	Default is 8 minutes; however minimum allowed is 1 minute and maximum allowed is 120 minutes.
Network Configuration	Only a single network configuration is allowed on each Appliance at one time.
Transport Protocols supported	- FTP / FTPS (FTP over SSL and FTP over TLS) - HTTP / HTTPS - SMTP - Tibco Rv - Tibco-EMS - IBM MQ
Agent Machine Policies supported	Unlimited *
Agent Group Policies supported	Unlimited *
Maximum clock skew	Default is 0 seconds. Maximum is 9999 seconds. Forum Systems recommends that customers working with WS-Security Headers and SAML Assertions increase the value of the Maximum Clock Skew to 300 seconds.

* Limited only by disk space.

INDEX