JUNIPER NETWORKS

Network and Security Manager

Configuring Infranet Controllers Guide

Release
2012.2

Published: 2013-01-03
Revision 01

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Network and Security Manager Infranet Controller Configuration Guide
2012.2

Revision History
January 2013 —01

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About this Guide

Objectives

Network and Security Manager (NSM) is a software application that centralizes control and management of your Juniper Networks devices. With NSM, Juniper Networks delivers integrated, policy-based security and network management for all security devices.

Unified Access Control (UAC) solution is an IP-based enterprise infrastructure that coordinates network, application, and endpoint security compliance and provides the control required to support network applications, manage network use, and reduce threats.

This guide provides the information you need to understand, configure, and maintain an Infranet Controller device using NSM. This guide explains how to use basic and advanced NSM functionality, including adding new devices, deploying new device configurations, updating device firmware, viewing log information, and monitoring the status of your Infranet Controller device.

Audience

This guide is intended for the system administrator responsible for configuring the Infranet Controller device.

Conventions

Table 1 on page x defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page x defines text conventions used in this guide.

Table 2: Text Conventions

Convention	Description	Examples
Bold typeface like this	• Represents commands and keywords in text. • Represents keywords • Represents UI elements	• Issue the **clock source** command. • Specify the keyword **exp-msg**. • Click **User Objects**
Bold typeface like this	Represents text that the user must type.	**user input**

`fixed-width font`	Represents information as displayed on the terminal screen.	`host1#`
		show ip ospf
		`Routing Process OSPF 2 with Router ID 5.5.0.250`
		`Router is an area Border Router (ABR)`

Key names linked with a plus (+) sign	Indicates that you must press two or more keys simultaneously.	Ctrl + d
Italics	• Emphasizes words • Identifies variables	• The product supports two levels of access, *user* and *privileged.* • *clusterID*, *ipAddress.*
The angle bracket (>)	Indicates navigation paths through the UI by clicking menu options and links.	**Object Manager > User Objects > Local Objects**

Table 3 on page xi defines syntax conventions used in this guide.

Table 3: Syntax Conventions

Convention	Description	Examples
Words in plain text	Represent keywords	terminal length
Words in italics	Represent variables	*mask, accessListName*
Words separated by the pipe (|) symbol	Represent a choice to select one keyword or variable to the left or right of this symbol. The keyword or variable can be optional or required.	diagnostic | line
Words enclosed in brackets ([ ])	Represent optional keywords or variables.	[internal | external]
Words enclosed in brackets followed by and asterisk ([ ]*)	Represent optional keywords or variables that can be entered more than once.	[level1 | level2 | l1]*
Words enclosed in braces ({ })	Represent required keywords or variables.	{ permit | deny } { in | out } { clusterId | ipAddress }

List of Technical Publications

Table 4: Network and Security Manager and Unified Access Control Solutions Publications

Network and Security Manager Installation Guide	Details the steps to install the NSM management system on a single server or on separate servers. It also includes information on how to install and run the NSM user interface. This guide is intended for IT administrators responsible for the installation and/or upgrade of NSM.
Network and Security Manager Administration Guide	Describes how to use and configure key management features in the NSM. It provides conceptual information, suggested workflows, and examples where applicable. This guide is best used in conjunction with the NSM Online Help, which provides step-by-step instructions for performing management tasks in the NSM UI. This guide is intended for application administrators or those individuals responsible for owning the server and security infrastructure and configuring the product for multi-user systems. It is also intended for device configuration administrators, firewall and VPN administrators, and network security operation center administrators.
Network and Security Manager Configuring Firewall/VPN Devices Guide	Describes NSM features that relate to device configuration and management. It also explains how to configure basic and advanced NSM functionality, including deploying new device configurations, managing Security Policies and VPNs, and general device administration.
Network and Security Manager Online Help	Provides task-oriented procedures describing how to perform basic tasks in the NSM user interface. It also includes a brief overview of the NSM system and a description of the GUI elements.
Unified Access Control Administration Guide	Provides comprehensive information about configuring the Unified Access Control solution and the Infranet Controller 4500 and 6500 appliances.
Unified Access Control Quick Start Guide	Provides an example of configuring the Unified Access Control solution for a front-end server deployment scenario.

Table 4: Network and Security Manager and Unified Access Control Solutions Publications *(continued)*

Unified Access Control Installation Guide	Details the steps to install the Infranet Controller and Infranet Enforcer Appliances. This guide is intended for IT administrators responsible for the installation and/or upgrade of Infranet Controller.

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

PART 1

Getting Started

CHAPTER 1

Understanding an Infranet Controller Configuration

NSM and Device Management Overview

NSM is the Juniper Networks network management tool that allows distributed administration of network appliances. You can use the NSM application to centralize status monitoring, logging, and reporting, and to administer Infranet Controller configurations.

With NSM you can manage the Infranet Enforcer and Intrusion Detection and Prevention (IDP) devices, and you can administer the complete Unified Access Control (UAC) solution from a single management interface.

In addition, NSM lets you manage most of the parameters that you can configure through the Infranet Controller admin console. The configuration screens rendered through NSM are similar to the screens in the Infranet Controller admin console.

NSM incorporates a broad configuration management framework that allows co-management using other methods. To manage the Infranet Controller configuration, you can also use the XML files import and export feature, or you can manage from the Infranet Controller admin console.

Related Documentation

- Communication Between an Infranet Controller and NSM Overview on page 3
- Infranet Controller Services and Device Configurations Supported in NSM on page 5

Communication Between an Infranet Controller and NSM Overview

The Infranet Controller and the NSM application communicate through the Device Management Interface (DMI). DMI is a collection of schema-driven protocols that run on a common transport (that is, TCP). DMI is designed to work with Juniper Networks platforms to make device management consistent across all administrative realms.

Supported DMI protocols include:

- NetConf (for inventory management, XML-based configuration, text-based configuration, alarm monitoring, and device specific commands)
- Structured syslog
- Threat flow for network profiling

DMI supports third-party network management systems that incorporate the DMI standard; however, only one DMI-based agent per device is supported.

The Infranet Controller's configuration is represented as a hierarchical tree of configuration items. This structure is expressed in XML and can be manipulated with NetConf. NetConf is a network management protocol that uses XML. DMI uses NetConf's generic configuration management capability to allow remote configuration of the device.

To allow NSM to manage the Infranet Controller using the DMI protocol, NSM must import the schema and metadata files from the Juniper Networks Schema Repository, a publicly accessible resource that is updated with each device release. In addition to downloading the Infranet Controller's current schema, NSM may also download upgraded software.

The Schema Repository enables access to XSD and XML files defined for each device, model, and software version.

Before attempting to communicate with NSM, you must first complete the initial configuration of the Infranet Controller. Initial configuration includes network interface settings, DNS settings, licensing, and password administration.

If you have several Infranet Controllers that will be configured in a clustering environment, the cluster abstraction must first be created in the NSM Cluster Manager. Then you can add individual nodes.

After you have completed the initial network configuration, you can configure the Infranet Controller to communicate with NSM using the appropriate network information. Once the Infranet Controller has been configured to communicate with NSM, the Infranet Controller contacts NSM and establishes a DMI session through an initial TCP handshake.

All communications between the Infranet Controller and NSM occur over SSH to ensure data integrity.

After the Infranet Controller initially contacts NSM and a TCP session is established, interaction between the Infranet Controller and NSM is driven from NSM, which issues commands to get hardware, software, and license details of the Infranet Controller. NSM connects to the Schema Repository to download the configuration schema that is specific to the Infranet Controller.

NSM then issues a command to retrieve configuration information from the Infranet Controller. If NSM is contacted by more than one Infranet Controller as a member of a cluster, information from only one of the cluster devices is gathered. NSM attempts to validate the configuration received from the Infranet Controller against the schema from Juniper Networks.

Once the Infranet Controller and NSM are communicating, the Infranet Controller delivers syslog and event information to NSM.

After NSM and the Infranet Controller are connected, you can make any configuration changes directly on the Infranet Controller, bypassing NSM. NSM automatically detects these changes and imports the new configuration data. Changes to Infranet Controller cluster members will similarly be detected by NSM.

When you make changes to the Infranet Controller configuration through NSM you must push the changes to the device by performing an Update Device operation.

When you double-click the Infranet Controller device icon in the Device Manager and select the **Configuration** tab, the configuration tree appears in the main display area in the same orientation as items appear on the Infranet Controller admin console.

Related Documentation

- NSM and Device Management Overview on page 3
- Infranet Controller Services and Device Configurations Supported in NSM on page 5

Infranet Controller Services and Device Configurations Supported in NSM

The Infranet Controller supports the following services in NSM:

- Inventory management service—Enables management of the Infranet Controllers software, hardware, and licensing details. Adding or deleting licenses and upgrading or downgrading software are not supported.
- Status monitoring service—Allows the Infranet Controller's status to be obtained, including name, domain, OS version, synchronization status, connection details, and current alarms.
- Logging service—Allows the Infranet Controller's logs to be obtained in a time-generated order. Logging configuration details that are set on the Infranet Controller will apply to NSM.
- XML-based configuration management service—Enables NSM to manage the configuration of the Infranet Controller. NSM uses the same XML schema as the Infranet Controller, so you can troubleshoot NSM using XML files downloaded from the Infranet Controller.

The following device configurations are not supported:

- Editing licensing information, although licenses can be viewed
- Packaging log files or debug files for remote analysis

Related Documentation

- NSM and Device Management Overview on page 3
- Communication Between an Infranet Controller and NSM Overview on page 3

CHAPTER 2

Infranet Controller and NSM Installation Overview

UAC Installation Overview

NOTE: For important safety information, read *Juniper Networks Security Products Safety Guide*.

The UAC components to be installed are the following:

1. Install Infranet Enforcer and/or 802.1X hardware and perform the basic setup. See the documentation that shipped with the system or visit the Juniper Networks Web site at http://www.juniper.net/techpubs/ to download the appropriate documentation.
2. Install Infranet Controller hardware and perform the basic setup using the serial console. See the *Juniper Networks Unified Access Control Installation Guide*.
3. License the Infranet Controller and verify user accessibility. Follow the initial configuration Task Guide instructions embedded in the Infranet Controller Web console.
4. Configure an SSL connection between the Infranet Controller appliance and your Infranet Enforcer appliances and/or 802.1X switches. See the *Juniper Networks Unified Access Control Quick Start Guide* or Part 1, "Getting Started," of the *Juniper Networks Unified Access Control Administration Guide*.

Related Documentation

- NSM Installation Overview on page 8
- NSM and Device Management Overview on page 3
- Communication Between an Infranet Controller and NSM Overview on page 3

NSM Installation Overview

NSM is a software application that enables you to integrate and centralize management of your Juniper Networks environment. You need to install two main software components to run NSM: the NSM management system and the NSM user interface (UI).

See the *Network Security Manager Installation Guide* for the steps to install the NSM management system on a single server or on separate servers. It also includes information on how to install and run the NSM user interface. The *Network Security Manager Installation Guide* is intended for IT administrators responsible for installing or upgrading NSM.

Related Documentation

- UAC Installation Overview on page 7
- NSM and Device Management Overview on page 3

PART 2

Integrating Infranet Controllers

CHAPTER 3

Adding Infranet Controllers

Importing an Infranet Controller Device Through Not Reachable Workflow

You can add an Infranet Controller to your existing network using NSM and import its configurations. Using the Add Device Wizard, you can configure a connection between the management system and the physical device, and then import all device parameters, policies, objects, VPNs, and so on.

Import an Infranet Controller through Not Reachable workflow into NSM by following these procedures:

1. Installing and Configuring the Infranet Controller Device on page 12
2. Adding the Infranet Controller Device Through NSM on page 12
3. Configuring and Enabling the DMI Agent on the Infranet Controller Device on page 13
4. Confirming Connectivity and Importing the Infranet Controller Device Configuration on page 14

Installing and Configuring the Infranet Controller Device

Before you can add the Infranet Controller to NSM, you must install and configure the Infranet Controller device to have logon credentials for an NSM administrator.

To install and configure the Infranet Controller:

1. Select **System** > **Network** > **Overview** on the device's admin console and ensure that basic connection information such as the following are configured on the Infranet Controller.
   - Network interface settings
   - DNS settings
   - Password
2. Select **Authentication** > **Auth Servers** and enter the username and password of the NSM administrator in the applicable authentication server.

   NOTE: **Only password-based authentication servers can be used. One-time password authentication is not supported.**
3. Select **Administrators** > **Admin Roles** and create a DMI agent role.
4. Select **Administrators** > **Admin Realms** and create a DMI agent administrator realm for the DMI agent on the device and use role mapping to associate the DMI agent role and realm.

   NOTE: **Ensure that the Host Checker, browser, and certificate restrictions are not applied for the DMI agent role or realms.**

For complete details on installing and configuring Infranet Controller devices, see the *Juniper Networks Unified Access Control Administration Guide*.

Adding the Infranet Controller Device Through NSM

To add the Infranet Controller device through the NSM UI:

1. From the left pane of the NSM UI, click **Configure**.
2. Expand **Device Manager** and select **Devices**. The Devices workspace appears on the right side of the screen.
3. Click the **Device Tree** tab, click the **New** button, and select **Device**. The New-Device dialog box appears.
4. Select **Device is Not Reachable** and click **Next**.
5. Enter the device name, and select the required color, OS name (IC), platform, and managed OS version from the drop-down lists.
6. From the Choose Device Server Connections Parameter area, select:

- **Use Default Device Server IP Address and Port**—Connects the device to the NSM device server IP address and port.
- **Use Device Server Through MIP**—Connects the NSM device server through a mapped IP address and port.

7. Click **Next**, and a unique external ID gets generated automatically. This ID represents the device within the management system.
8. Enter an admin username for the device admin.
9. Set the Admin User Password and the First Connection One-Time Password:
   a. Select **Set Password** and enter a new password.
   b. Confirm your new password and click **OK**.

NOTE:
- Make a note of the unique external ID. The device administrator will need it to configure connectivity with NSM. The wizard automatically enters this value for the device. This ID number represents the device within the management system.
- Specify the administrator username and password for the SSH connection. This name and password must match the name and password already configured on the device.
- Specify the First Connection One Time Password (OTP) that authenticates the device. Make a note of this password. The device administrator will need it to configure the connectivity with NSM.

10. Click **Finish** to add the device to the NSM UI. The Infranet Controller appears in the Devices workspace.

Configuring and Enabling the DMI Agent on the Infranet Controller Device

You must configure and activate the DMI agent on the Infranet Controller device. It helps to establish SSH communications with the NSM application and to control the Infranet Controller from the NSM application.

To configure and enable the DMI agent:

1. Select **System** > **Configuration** > **DMI Agent** to add the NSM management application.
2. Under DMI settings for outbound connections, enter the device server's IP address in the Primary Server box..
3. Enter **7804** in the Primary Port box.
4. Fill in the Backup Server and Backup Port boxes, if a device server is configured for high availability.
5. Enter the unique external ID provided by the NSM administrator in the Device ID box.

6. Enter the first connection one-time password provided by the NSM administrator in the HMAC Key box.
7. Click **Enable** to activate the DMI agent.
8. Click **Save Changes**, and the device attempts to establish a session with the NSM application.

The device software initiates the TCP connection to NSM and identifies itself using the specified device ID and HMAC. Both sides then engage in SSH Transport Layer interactions to set up an encrypted tunnel. The NSM application authenticates itself to the Infranet Controller based on the username and password.

Confirming Connectivity and Importing the Infranet Controller Device Configuration

In NSM, validate connectivity with the device, and then import the device configuration:

1. From the Devices workspace, select the **Device List** tab.
2. Check the newly added device in the Connection Status column. The connection status must change from Never Connected to Up.

If the connection status appears as Device Platform Mismatch or Device Firmware Mismatch, delete the device from the application and add it back using the correct device platform and managed OS, respectively.

To import the device configuration:

1. From the Devices workspace, select the **Device List** tab.
2. Right-click the newly added Infranet Controller device and select **Import Device**. The Save Changes dialog box appears.
3. If you are prompted to save policy or VPN changes, click **Yes**. The Device Import Option dialog box appears.
4. Select **Run Summarize Delta Config**, and click **OK** and **Yes**. The Job Information dialog box displays the progress of the delta config summary. You can also monitor the progress in Job Manager.

   The next step is to verify the imported configuration using either the Device Monitor or the Device Manager in NSM. See “Verifying Imported Device Configurations (NSM Procedure)” for details.

Related Documentation

- Importing an Infranet Controller Through Reachable Workflow on page 15
- Creating and Applying an Infranet Controller Template on page 29
- Verifying Imported Device Configurations on page 19

Requirements for Importing an Infranet Controller into NSM Through a Reachable Workflow

Adhere to the requirements to import an Infranet Controller into NSM through a reachable workflow:

- The inbound DMI connection must be enabled in the Infranet Controller.
- The SSH port must be configured in the Infranet Controller. The default SSH port is 22.
- The DMI agent admin realms must be configured and an admin user must be mapped to a role with full admin privileges.

Related Documentation

- Importing an Infranet Controller Through Reachable Workflow on page 15
- Importing an Infranet Controller Device Through Not Reachable Workflow on page 11
- Verifying Imported Device Configurations on page 19

Importing an Infranet Controller Through Reachable Workflow

To import an Infranet Controller through a reachable workflow into NSM:

1. From the left pane of the NSM UI, click **Configure**.
2. Expand **Device Manager** and select **Devices**. The Devices workspace appears on the right side of the screen.
3. Click the **Device Tree** tab, click the **New** button, and select **Device**. The New Device dialog box appears.
4. Select **Device is Reachable** and click **Next**.
5. Enter the following connection information:
   - Enter the IP address of the device.
   - Enter the username of the device administrator.
   - Enter the password for the device administrator.
   - Select **SSH V2** as the connection method.
   - Ensure that the TCP port number is 22 .
6. Click **Next**. The Verify Device Authenticity dialog box appears. The Add Device wizard displays the RSA Key FingerPrint information. To prevent man-in-the-middle attacks, you should verify the fingerprint using an out-of-band method.
7. Click **Next** to accept the fingerprint. The Detecting Device dialog box opens.
8. After the wizard displays the autodetected device information, verify that the device type, OS version, and the device serial number are correct. The wizard also detects the hostname configured on the device. You can either use the hostname as the NSM device name or you can enter a new name in the text box provided.

9. Click **Next** after verifying the auto detected device information.
10. Click **Finish** to add the device to the NSM UI. The Infranet Controller appears in the Devices workspace.

Related Documentation

- Importing an Infranet Controller Device Through Not Reachable Workflow on page 11
- Requirements for Importing an Infranet Controller into NSM Through a Reachable Workflow on page 15
- Verifying Imported Device Configurations on page 19

Importing Multiple Infranet Controllers

If your network includes a large number of devices, you can save time by adding multiple devices in a single workflow. You can add up to 4000 devices at a time to a single domain (but you cannot add multiple devices to different domains at one time).

Add multiple Infranet Controllers by following these procedures:

1. Creating the CSV File on page 16
2. Validating the CSV File on page 18
3. Adding and Importing Multiple Infranet Controllers on page 18

Creating the CSV File

The CSV file defines all the required and optional values for each Infranet Controller device. Within a .csv file, you define the Infranet Controller configuration values that you want to add. The required and optional values depend not only on how the Infranet Controllers are deployed on your network but also on the device family.

Juniper Networks provides CSV templates in Microsoft Excel format for each type of CSV file. These templates are located in the utils subdirectory where you have stored the program files for the UI client. For example:

C:\Program Files\Network and Security Manager\utils

For each CSV file, each row defines a single Infranet Controller's values for each parameter. For text files, columns are separated by commas.

Creating Infranet Controller Parameters in CSV File

For an Infranet Controller, Table 5 on page 16 lists the parameters to be set in the CSV file.

Table 5: CSV File Information for Infranet Controllers

Field	Type	Required	Acceptable Values
Name	String	yes	ic-6500, ic-4500

Table 5: CSV File Information for Infranet Controllers *(continued)*

Field	Type	Required	Acceptable Values
Color	String	yes	blue, red, green, yellow, cyan, magenta, orange, pink.
OS Name	String	yes	IC
Platform	String	yes	IC-4500, IC-6500
Device Subtype	String	yes	Set to “none”
Managed OS Version	String	yes	2.2
Device Admin Name	String	yes	<administrator>
Device Admin Password	String	yes	<password> Must be a minimum of nine characters.

Using an Excel File to Add Multiple Infranet Controllers

To edit the Excel file to add multiple Infranet Controllers:

1. Copy and open either the **bulkadd_nonreachable-sample.csv** file or the **bulkadd_nonreachable-DMI-sample.csv** file located in **C:/Program Files/Network and Security Manager/utils**.
2. Using one row for each Infranet Controller you want to add, enter the required values for each parameter that you wish to set for them. You can also provide optional values, if desired.
3. Save the file to a location on your local drive.

Using a Text File to Add Multiple Infranet Controllers

To add multiple Infranet Controllers using a text file, create a text file with the following text:

1. Open a text file and add the Infranet Controllers and its parameters as follows:

   Ic-6000, blue, ic, IC-6000, none, root, 2.2, netscreen

   Ic-6500, pink, ic, IC-6500, none, root, 2.2, netscreen

   Ic-4000, cyan, ic, IC-4000, none, root, 2.2, netscreen

   Ic-4500, pink, ic, IC-4500, none, root, 2.2, netscreen

2. Save the file as a .csv file.

Validating the CSV File

When you add the Infranet Controllers, NSM validates the configuration information in the .csv file and creates a validation report. The report lists any incorrect or duplicate configurations, and indicates the exact line that contains invalid data.

NOTE: The validation report displays only the first error in the line. If the line contains additional errors, those errors do not appear in the validation report.

Select **Cancel** to quit adding multiple Infranet Controllers, or select **Add Valid Devices** to begin adding the Infranet Controllers for which you have provided valid device configurations.

If the validation report listed incorrect configurations, you can still select **Add Valid Devices**; however, only the devices with correct configurations are added. If the .csv file contains duplicate configurations, NSM ignores the duplicates.

After you have added multiple Infranet Controllers, you cannot roll back or undo your changes. To edit or delete Infranet Controllers, select the Infranet Controller in the NSM UI and make the necessary changes.

Adding and Importing Multiple Infranet Controllers

To add and import multiple Infranet Controllers in the NSM UI:

1. From the left pane of the NSM UI, click **Configure**.
2. Expand **Device Manager** and select **Devices**. The Devices workspace appears on the right side of the screen.
3. Click the **Device Tree** tab, click the **New** button, and select **Many Devices**. The New-Device dialog box appears.
4. In the New-Device dialog box:
   - Select **Device is Not Reachable**.
   - Specify the location of the CSV file.
   - Specify the output directory for the .cli file. For each valid device configuration that uses a dynamic IP address, NSM creates a .cli output file. By default, the .cli file is saved to the following GUI server directory:

     /usr/netscreen/GuiSvr/var/ManyDevicesOutput/<inputFile_YYYYMMDDHHMM>/

     Before the Infranet Controllers can be managed by NSM, you must enter the CLI commands in the .cli file on the physical security device.
5. Click **Next**. The Add Device wizard validates the CSV file and provides a validation report.
   - Select **Cancel** to quit the Add Many Devices process.

- Select **Add Valid Devices** to begin adding the devices for which you have provided valid device configurations.

6. From the Choose Device Server Connections Parameter area select:
   - **Use Default Device Server IP Address and Port**—Connects the device to the NSM device server IP address and port.
   - **Use Device Server Through MIP**—Connects the NSM device server through a mapped IP address and port.
7. Click **Finish** to add the Infranet Controllers.

The time it takes for NSM to activate and import the Infranet Controllers depends on the number of Infranet Controllers and the management system configuration.

Related Documentation

- Importing an Infranet Controller Device Through Not Reachable Workflow on page 11
- Adding an Infranet Controller Cluster with Imported Cluster Members on page 24
- Creating and Applying an Infranet Controller Template on page 29
- Verifying Imported Device Configurations on page 19

Verifying Imported Device Configurations

After importing an Infranet Controller, you should verify whether all device information has been imported.

The imported device configurations can be verified in any of the following ways:

- Using Device Monitor on page 19
- Using Device Manager on page 20
- Using Job Manager on page 20
- Using Configuration Summaries on page 20

Using Device Monitor

The Device Monitor in NSM tracks the status of individual devices, systems, and their processes. To check the status of the imported device in the Device Monitor, from the left pane click **Investigate**, expand **Realtime Monitor**, and select **Device Monitor**. From the Device Monitor workspace, check the following parameters for your imported device:

- The Configured Status column says “Managed In Sync”.
- The Connection Status column says “Up”.

Using Device Manager

Using the Device Manager in NSM, you can verify the configuration settings of the imported device. To verify the configuration settings, click **Configure**, expand **Device Manager**, select **Devices** and click the **Device List** tab.

Ensure that the following parameters are indicated:

- Imported device serial number matches the serial number on the physical device
- Imported device IP address matches the IP address for the physical device

Using Job Manager

Job Manager tracks the status of major administrative tasks, such as importing or updating a device. After you import a device, view the report for the import task to ensure that the management system imported the device configuration as you expected. To track the status of the imported Infranet Controllers in NSM, from the left pane click **Administer** and select **Job Manager**.

Job Manager also tracks the status of configuration summaries, described in "Using Configuration Summaries."

Using Configuration Summaries

NSM provides three configuration summaries to help you manage device configurations and prevent accidental misconfigurations. Use configuration summaries after you import a device to ensure that the management system imported the physical device configuration as you expected.

Configuration summaries help with ongoing device maintenance, particularly for devices on which a local device administrator has been troubleshooting using CLI commands or the Web UI. Because the device object configuration in the NSM UI can overwrite the physical device configuration, you should always confirm the commands that are sent to the device.

The three configuration summaries that help you to manage device configurations are:

- Configuration Summary
- Delta Configuration Summary
- Running Configuration Summary

Configuration Summary

A configuration summary shows you the exact CLI commands that will be sent to the managed device during the next device update. To get a configuration summary in NSM, from the Devices menu, click **Configuration** and select **Summarize Config**. The Summarize Config dialog box appears. You see a list of security devices to which you have access. Select the device you just imported and click **OK**. NSM analyzes the UI device object configuration and generates a summary report that lists the CLI commands or XML messages to send to the physical device during the next device update.

For a just-imported device, the configuration summary report displays the device configuration that matches the configuration currently running on the physical device.

Delta Configuration Summary

A delta configuration summary shows you the differences between the configuration you see in the NSM UI and the configuration on the physical device. To get a delta configuration summary in NSM, from the Devices menu click **Configuration** and select **Get Summarize Delta Config**. The Get Delta Config Summary dialog box appears with a list of devices to which you have access. Select the device you just imported and click **OK**. NSM queries the physical device to obtain a list of all CLI commands or XML messages used in the device configuration, compares that list with the UI device configuration, and generates a summary report of all differences, or deltas, discovered.

Get Running Configuration

A running configuration summary shows you the exact CLI commands or XML messages that were used to create the current device configuration on the physical device. To get the running config summary in the NSM application, from the Devices menu click **Configuration** and select **Get Running Config**. The Get Running Config dialog box appears. You see a list of devices to which you have access. Select the device you just imported and click **OK**.

NSM queries the physical device to obtain a list of all CLI commands used in the device configuration and generates a summary report that lists those commands. For a just-imported device, the get running config summary report displays the device configuration currently running on the physical device.

Related Documentation

- Importing an Infranet Controller Device Through Not Reachable Workflow on page 11
- Importing an Infranet Controller Through Reachable Workflow on page 15

CHAPTER 4

Adding Infranet Controller Clusters

Infranet Controllers Clusters in NSM Overview

When you add an Infranet Controller cluster in NSM, you first add the cluster object and then add each member. Adding a member is similar to adding a standalone device.

Infranet Controller clusters can be configured by the device administrator to operate in active/passive mode or in active/active mode. Clusters in active/passive mode are made up of a primary member and a secondary member. All authentication requests are handled by the primary member. If a primary member fails, then the secondary member takes over.

In active/active mode, authentication requests are load-balanced across all cluster members. If one member fails, then load balancing takes place among the surviving members.

The number of members permitted in a cluster depends on the Infranet Controller platform and whether the cluster is configured in active/active mode or in active/passive mode. You can have no more than two cluster members in active/passive mode. In active/active mode you can have up to four members.

Before you can add a cluster member in NSM, the device administrator must have already created the cluster and added, configured, and enabled the physical cluster member. See the *Juniper Networks Unified Access Control Administration Guide* for details on creating and configuring clusters.

Infranet Controller devices configured in a cluster must have a cluster object and member objects defined in the NSM before the Infranet Controller Cluster nodes can be recognized by NSM. Nodes from this cluster that subsequently contact NSM will be represented by fully functional member icons in the Cluster Manager. Cluster members whose DMI agents do not contact NSM will be displayed in the NSM Device Monitor as unconnected devices.

Infranet Controller devices use member IDs to identify each cluster member object. When importing cluster members, the member ID is imported as part of the cluster, so the Add Cluster Member wizard does not prompt for the member ID.

To add an Infranet Controller cluster to NSM, first add the cluster object, and then add its members. You add cluster members one at a time, in a similar manner to adding standalone devices.

Once an Infranet Controller cluster is managed by NSM, subsequent changes applied to the cluster by NSM will be synchronized by the cluster across all cluster members. Similarly, changes to an Infranet Controller cluster membership that occur through administrator action on the native device UI will be reflected back to NSM, and NSM will display the modified cluster after the cluster configuration is imported to NSM.

You can add an Infranet Controller cluster from your existing network into NSM and import their configurations. Using the Add Device Wizard, you configure a connection between the management system and the physical device, and then import all device parameters.

Related Documentation

- Infranet Controller Services and Device Configurations Supported in NSM on page 5
- Adding an Infranet Controller Cluster with Imported Cluster Members on page 24

Adding an Infranet Controller Cluster with Imported Cluster Members

To add an Infranet Controller cluster to NSM, first add the cluster object, and then add its members. You add cluster members one at a time, in a similar manner to adding standalone devices.

Add and import an Infranet Controller cluster in NSM by following these procedures:

1. Installing and Configuring the Cluster on page 24
2. Adding the Cluster in NSM on page 24
3. Adding the Cluster Members in NSM on page 25
4. Configuring and Enabling the DMI Agent on the Cluster on page 27
5. Importing Cluster Configuration on page 27

Installing and Configuring the Cluster

You must install and configure the cluster to have logon credentials for an NSM administrator before you can add the cluster to NSM.

Adding the Cluster in NSM

Before you can add an Infranet Controller cluster to NSM, you must first add the cluster object, and then add its members.

To add a new cluster to NSM:

1. From the left pane of the NSM UI, click **Configure**.
2. Expand **Device Manager** and select **Devices**. The Devices workspace appears on the right side of the screen.

3. Click the **Device Tree** tab, click the **New** button, and select **Cluster**. The New - Cluster dialog box appears.
4. Enter the cluster name and select the required color, OS name (IC), platform, and managed OS version from the drop-down lists.
5. Click **OK**. The new cluster appears in the Device Manager.

Adding the Cluster Members in NSM

You add cluster members one at a time in a similar manner to adding standalone devices.

Adding Cluster Members through Not Reachable Workflow

To add a cluster member through the non-reachable workflow:

1. From the left pane of the NSM UI, click **Configure**.
2. Expand **Device Manager** and select **Devices**. The Devices workspace appears on the right side of the screen.
3. Click the **Device Tree** tab, and select the cluster to which you want to add the members.
4. Click the **New** button and select **Cluster Member**. The New–Cluster Member dialog box appears.
5. Enter the cluster member name, select **Device Is Not Reachable** and click **Next**.
6. From the Choose Device Server Connections Parameter area, select:
   - **Use Default Device Server IP Address and Port**—Connects the device to the NSM device server IP address and port.
   - **Use Device Server Through MIP**—Connects the NSM device server through a mapped IP address and port.
7. Click **Next**, and a unique external ID gets generated automatically. This ID represents the device within the management system.
8. Enter a admin user name for the device admin.
9. Set the admin user password and the first connection one-time password:
   a. Select the corresponding **Set Password** box and enter a new password.
   b. Confirm the new password and click **OK**.

NOTE:

- Make a note of the unique external ID. The device administrator will need it to configure connectivity with NSM. The wizard automatically enters this value for the device. This ID number represents the device within the management system.
- Specify the administrator username and password for the SSH connection. This name and password must match the name and password already configured on the device.
- Specify the first connection one time password (OTP) that authenticates the device. Make a note of this password. The device administrator will need it to configure the connectivity with NSM.

10. Click **Finish** to add the cluster member to the NSM GUI. The cluster member as a child of the Infranet Controller cluster in the Devices workspace.

Adding Cluster Members through Reachable Workflow

To add a cluster member:

1. From the left pane of the NSM UI, click **Configure**.
2. Expand **Device Manager** and select **Devices**. The Devices workspace appears on the right side of the screen.
3. Click the **Device Tree** tab, and select the cluster to which you want to add the members.
4. Click the **New** button and select **Cluster Member**. The New–Cluster Member dialog box appears.
5. Enter the cluster member name, select **Device Is Reachable** and click **Next**.
6. Specify the device connection settings:
   - **IP Address**—IP address of the Infranet Controller.
   - **Admin User Name**—Administrator user name created for the Infranet Controller.
   - **Password**—Administrator password created for the Infranet Controller.

NOTE: The ssh port number for cluster member is 22 by default and the port number cannot be modified.

7. Click **Next**, The Infranet Controller device is detected and the Infranet Controller details are displayed.
8. Enter a new name for the Infranet Controller device in **Device Name** to change the host name of the Infranet Controller device. An error message is displayed if the device name is not unique.
9. Click **Finish** to add the cluster member to the NSM GUI. The cluster member as a child of the Infranet Controller cluster in the Devices workspace.

Configuring and Enabling the DMI Agent on the Cluster

On each cluster member device, configure and activate the DMI agent and establish an SSH session with NSM.

Importing Cluster Configuration

After adding the cluster members, you must import the cluster configurations. You do this only once and for the entire cluster because the configuration is identical for all cluster members.

To import the cluster configuration:

1. From the left pane of the NSM UI, click **Configure**.
2. Expand **Device Manager** and select **Devices**. The Devices workspace appears on the right side of the screen.
3. Click the **Device Tree** tab. Right-click the cluster to which you want to import the configurations, and select **Import Device**.

NSM starts to import the configuration and a job window reports the progress of the job. When the job finishes, the configuration status for each cluster member in the Device List tab changes from Import Needed to Managed.

After importing, the configuration appears at the cluster level in NSM. To edit the configuration, open the cluster icon, not the individual cluster members.

Related Documentation

- Importing an Infranet Controller Device Through Not Reachable Workflow on page 11
- Importing an Infranet Controller Through Reachable Workflow on page 15
- Creating and Applying an Infranet Controller Template on page 29
- Verifying Imported Device Configurations on page 19
- Infranet Controllers Clusters in NSM Overview on page 23

CHAPTER 5

Using Templates

Creating and Applying an Infranet Controller Template

You can create and apply configuration templates for setting up new Infranet Controller devices through NSM.

Create and apply templates by following these procedures:

1. Creating the Template on page 29
2. Applying the Template on page 30

Creating the Template

To create an Infranet Controller template:

1. From the left pane of the NSM UI, click **Configure**.
2. Expand **Device Manager** and select **Device Templates**. The Device Templates workspace appears on the right side of the screen.
3. Click the **Device Template Tree** tab, click the **New** button, and select **IC Template**. The New Device Template dialog box appears.
4. Name the Infranet Controller template, and select a color for the template.
5. Enter the following basic information:
   - Device description
   - IP address
   - Admin user name
   - Admin user password
6. Click **OK** to save the template. The newly created templates will appear under the Device Template Tree.

7. Double-click the newly created template, to enter the configuration information. The Device Template screen appears.
8. Click the **Configuration** tab; select the required parameters on the left pane and specify the appropriate values.
9. Click **OK** to create an Infranet Controller template.

NOTE: In the new template, default values for the configuration parameters are displayed based on the default values from the schema. Default values are not displayed for configuration parameters that are based on match conditions such as device platform or release version.

You can now use this template when configuring Infranet Controllers.

NOTE: You can create a custom expression in a device template, but you cannot validate the custom expression. The Validate button is not enabled in the Custom Expressions editor for device templates.

Applying the Template

To apply a template to an Infranet Controller:

1. From the left pane of the NSM UI, click **Configure**.
2. Expand **Device Manager** and select **Devices**. The Devices workspace appears on the right side of the screen.
3. Double-click the Infranet Controller to open the device editor.
4. From the Device Info tab, select **Templates**. The templates configuration screen appears.
5. Click the **Edit** icon. The Edit Templates dialog box appears.
6. Select the required template from the list, and click **OK** in the Edit Templates dialog box.
7. In the templates configuration screen, select **Retain template values on removal** to retain template values if a template is removed from the device.
8. Click **Apply** to save your changes to the device configuration.

To apply the settings to the device itself, run the Update Device directive to push the configuration to the device.

Related Documentation

- Promoting an Infranet Controller Configuration to a Template on page 31
- Verifying Imported Device Configurations on page 19

Promoting an Infranet Controller Configuration to a Template

NSM allows you to import an Infranet Controller configuration and then convert, or promote, it to a template. You can then use that template to make identical configurations on other Infranet Controllers.

To promote an Infranet Controller configuration to a template:

1. From the Devices workspace in NSM, double-click the Infranet Controller whose configuration settings you want to promote to a template. The Infranet Controller Device dialog box appears.
2. Select the **Configuration** tab. The Device configuration tree appears.
3. From the Device configuration tree, select the configuration node that you want to promote to a template, and select **Promote Template**. The Select templates dialog box appears.
4. Select the template to which you want to apply the configuration settings and click **OK**. The Infranet Controller configuration is promoted to the selected template.

Related Documentation

- Creating and Applying an Infranet Controller Template on page 29
- Adding an Infranet Controller Cluster with Imported Cluster Members on page 24

Reverting an Infranet Controller Configuration to Default Values of a Template

NSM allows you to revert the device configuration values to that of the template default values. The default value is inherited from the template based on the order of priority in which the templates are applied to the device.

To revert an Infranet Controller configuration to the default values in a template:

1. From the Devices workspace in NSM, double-click the Infranet Controller whose configuration settings you want to revert. The Infranet Controller Device dialog box appears.
2. Select the **Configuration** tab. The Device configuration tree appears.
3. From the Device configuration tree, right-click the configuration node that you want to revert and select **Revert to template/default value**.
4. Click **OK**. The Infranet Controller configuration reverts to the template default values.

Related Documentation

- Creating and Applying an Infranet Controller Template on page 29
- Promoting an Infranet Controller Configuration to a Template on page 31

PART 3

Configuring an Infranet Controller

CHAPTER 6

Configuring User Roles and Administrator Roles

Configuring Infranet Controller User Roles (NSM Procedure)

A user role defines user session parameters and personalization settings. You can customize a user role by specifying access restrictions, enabling Host Enforcer (Windows) or agentless or Java agent access, and configuring session settings. You can create and configure user roles through the User Roles page from the Infranet Controller device configuration tree.

To configure a user role:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to configure the user roles.
3. Click the **Configuration** tab. In the configuration tree, select **Users > User Roles**. The corresponding workspace appears.
4. Click the **New** button, the New dialog box appears.
5. Add or modify settings on the General tab as specified in Table 6 on page 36.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 6: User Role Configuration Details

Option	Function	Your Action
General > Overview tab		
Name	Specifies a unique name for the user role.	Enter a name.
Description	Describes the user role.	Enter a brief description for the user role.
Session Options	Specifies the maximum session length, roaming capabilities, and session persistence.	Select **General > Session Options** to apply the settings to the role.
UI Options	Specifies customized settings for the Infranet Controller welcome page for Odyssey Access Client users mapped to this role.	Select **General > UI Options** to apply the settings to the role.
Odyssey Settings for IC Access	Specifies the Odyssey Access Client settings for Infranet Controller access.	Select this option to apply the Odyssey Access Client initial configuration settings.
Odyssey Settings for Preconfigured Installer	Specifies the Odyssey Access Client settings for the preconfigured installer.	Select this option to apply the Odyssey Access Client settings for the preconfigured installer.
General > Restrictions tab		
Source IP Restrictions	Specifies source IP restrictions.	See "Configuring Infranet Controller Source IP Access Restrictions (NSM Procedure)."
Browser Restrictions	Specifies browser restrictions.	See "Configuring Infranet Controller Browser Access Restrictions (NSM Procedure)."
Certificate Restrictions	Specifies certificate restrictions.	See "Configuring Infranet Controller Certificate Access Restrictions (NSM Procedure)."
Host Checker Restrictions	Specifies Host Checker restrictions.	See "Configuring Infranet Controller Host Checker Access Restrictions (NSM Procedure)."
General > Session Options tab		

Table 6: User Role Configuration Details *(continued)*

Option	Function	Your Action
Max. Session Length (minutes)	Specifies the number of minutes an active nonadministrative user session may remain open before ending. During an end-user session, prior to the expiration of the maximum session length, the Infranet Controller prompts the user to reenter authentication credentials, which avoids the problem of terminating the user session without warning.	Enter the session length in minutes. The default is five minutes, and the minimum is six minutes.
Heartbeat Interval (seconds)	Specifies the frequency at which the endpoint should send out a heartbeat to the Infranet Controller to keep the session alive. For agentless access, the browser refreshes the page with every heartbeat.	Enter the heartbeat interval in seconds. Users should not navigate away from the browser, as this interrupts the heartbeat and ends the session. The Odyssey Access Client and the Java agent respectively provide the heartbeat. You should ensure that the heartbeat interval of the agent is greater than the Host Checker interval, otherwise performance could be affected.
Heartbeat Timeout (seconds)	Specifies the amount of time that the Infranet Controller should “wait” before terminating a session when the endpoint does not send a heartbeat response.	Enter the heartbeat timeout in seconds.

Table 6: User Role Configuration Details *(continued)*

Option	Function	Your Action
Roaming session	• **Enabled**—Enables roaming user sessions for users mapped to this role. A roaming user session works across source IP addresses, which allows mobile users (laptop users) with dynamic IP addresses to sign in to the Infranet Controller from one location and continue working from another. Disable this feature to prevent users from accessing a previously established session from a new source IP address. This helps protect against an attack spoofing a user's session, provided the hacker was able to obtain a valid user's session cookie. • **Limit to subnet**—Limits the roaming session to the local subnet specified in the Netmask field. Users may sign in from one IP address and continue using their sessions with another IP address as long as the new IP address is within the same subnet. • **Disabled**—Disables roaming user sessions for users mapped to this role. Users who sign in from one IP address may not continue an active Infranet Controller session from another IP address; user sessions are tied to the initial source IP address.	Select this option to enable, limit, or disable the roaming session.
Roaming netmask	Displays the netmask for the local subnet.	Select this option to view the netmask for the local subnet.
Enable Session Extension	Allows users with a Layer 2 or Layer 3 connection to continue a session beyond the maximum session length.	Select this option to allow users with Odyssey Access Client and agentless access to reauthenticate and extend their current session without interruption.
General > UI Options tab		
Headers > Logo image	Displays the logo in the Infranet Controller welcome page.	Browse to your custom image file.
Headers > Background color	Displays the background color for the header area of the Infranet Controller welcome page.	Type the hexadecimal number for the background color, or click the Color Palette icon and pick the desired color.

Table 6: User Role Configuration Details *(continued)*

Option	Function	Your Action
Greeting > Show notification message	Enables the notification text box.	Select the **Show notification message** check box (optional).
Greeting > Notification Message	Displays the notification message at the top of the Infranet Controller welcome page.	Enter the message that you want to display. You may format text and add links using the following HTML tags: <i>, <b>, , <font>, and <a href>. However, the Infranet Controller does not rewrite links on the sign-in page (because the user has not yet authenticated), so you should only point to external sites. Links to sites behind a firewall will fail. You may also use Infranet Controller system variables and attributes in this field. NOTE: • The length of the personalized greeting cannot exceed 12K or 12288 characters. • If you use unsupported HTML tags in your custom message, the Infranet Controller may display the end user's Infranet Controller home page incorrectly.
Other > Show copyright notice and 'Secured by Juniper Networks' label in footer	Displays the copyright notice and label in the footer.	Select the **Show copyright notice and 'Secured by Juniper Networks' label in footers** check box (optional). This setting applies only to those users whose license permits disabling the copyright notice. For more information about this feature, call Juniper Networks Support.

Related Documentation

- Configuring Access Options on an Infranet Controller User Role (NSM Procedure) on page 40
- Configuring OAC Settings for a User Role (NSM Procedure) on page 42
- Creating and Configuring Infranet Controller Administrator Roles (NSM Procedure) on page 48
- Delegating Management Tasks to Infranet Controller Administrator Roles (NSM Procedure) on page 55
- Verifying Imported Device Configurations on page 19

Configuring Access Options on an Infranet Controller User Role (NSM Procedure)

To provide users access to protected resources, you can configure agent and agentless access for a user role.

To configure access options on a user role:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to configure the user- role access option.
3. Click the **Configuration** tab. In the configuration tree, select **Users > User Roles**. The corresponding workspace appears.
4. Add or open a user role. Click either the **Agent** or **Agentless** tab. Add or modify settings as specified in Table 7 on page 40.
5. Click one:
   - **OK** — Saves the changes.
   - **Cancel** — Cancels the modifications.

Table 7: User Role Access Configuration Details

Option	Function	Your Action
Agent tab		
Install Agent for this role	Allows the user to install the agent for this role.	Select this option to install the agent for this role.
Install Java Agent for this role	Allows the user to download and install the lightweight Java agent for Macintosh or Linux platforms.	Select this option to install Java agent for this role.

Table 7: User Role Access Configuration Details *(continued)*

Option	Function	Your Action
Enable Host Enforcer	Enables Host Enforcer on the endpoint and sends Host Enforcer policies to Odyssey Access Client for this role (Windows only).	Select this option to enable the Host Enforcer for this role. NOTE: • By default, after you enable the Host Enforcer option on a role, Odyssey Access Client denies all traffic on the endpoint except for the following allowed types: traffic to and from the Infranet Controller and Infranet Enforcer, WINS, DNS, IPsec, DHCP, ESP, IKE, outgoing TCP traffic, and some ICMP messages (for example, PING from the endpoint to other devices is allowed). Therefore, it's important that you configure Host Enforcer policies to specify the additional types of traffic you want to allow on each endpoint. For example, you must configure Host Enforcer policies to allow any incoming TCP traffic. See "Configuring Infranet Enforcer Resource Access Policies (NSM Procedure)". • To avoid blocking all traffic on endpoints and preventing users from accessing all network and Internet resources, we recommend that you configure Host Enforcer policies to allow the specific types of traffic on endpoints before you enable the Host Enforcer option on a role.
Session start script / Session stop script	Executes the script after the start or stop of the OAC session.	Specify the location of the session start scripts / session stop script you want to run on Windows endpoints after Odyssey Access Client connects or disconnects with the Infranet Controller. You can specify a fully qualified path. Scripts can be accessed locally or remotely by means of file share or other permanently available local network resource. You can also use environment variables, such as %USERNAME% in the script path name. For example: **\\abc\users\%USERNAME%\myscript.bat**
odyssey-settings	Specifies the IC Access and Preconfigured Installer settings	Click the **odyssey-settings** button. See "Configuring OAC Settings for a User Role (NSM Procedure)".
Agentless tab		

Table 7: User Role Access Configuration Details *(continued)*

Option	Function	Your Action
Enable Agentless Access for this role	Allows users to use agentless access to access protected resources.	Select this option to allow access to endpoints in addition to using Odyssey Access Client on Windows machines. If you don't select the agentless option, the Infranet Controller allows access to protected resources by means of Odyssey Access Client only. NOTE: To configure agentless access, you must also configure a permit infranet auth policy on the Infranet Enforcer to allow access for agentless endpoint platforms. For configuration instructions, see "Configuring Infranet Controller Source IP Access Restrictions (NSM Procedure)".
Disable use of AJAX for heartbeats	Disables use of AJAX for heartbeats.	Select this option to disable use of AJAX for heartbeats.

Related Documentation

- Delegating Management Tasks to Infranet Controller Administrator Roles (NSM Procedure) on page 55
- Configuring Infranet Controller User Roles (NSM Procedure) on page 35
- Creating and Configuring Infranet Controller Administrator Roles (NSM Procedure) on page 48

Configuring OAC Settings for a User Role (NSM Procedure)

Each time the user accesses a resource that is protected by the Infranet Controller, the Odyssey Access Client configuration settings you specify will be used.

NOTE: **Except for the login name in the profile, all of the other configuration settings you specify on the Infranet Controller overwrite any existing settings on the endpoint if Odyssey Access Client is already installed when the user accesses the Infranet Controller.**

To configure odyssey settings:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to configure the user-role access option.
3. Click the **Configuration** tab. In the configuration tree, select **Users** > **User Roles**.
4. Add or open a user role and click the **Agent** tab.
5. Click the **odyssey–settings** button and configure the settings as specified in Table 8 on page 43.

There are two tabs under Odyssey Settings. The first tab, IC Access, allows you to configure authentication and connection settings for the Odyssey Access Client. The second tab, Preconfigured Installer, provides an interface that allows you to upload a preconfigured version of Odyssey Access Client that you can deploy to users when they access a role.

6. Click one:
   - **OK** — Saves the changes.
   - **Cancel** — Cancels the modifications.

Table 8: OAC Configuration Details

Option	Function	Your Action
IC Access tab		
Name of Profile and Infranet Controller	Displays the hostname or the Infranet Controller URL.	Select the profile name. • **Use Infranet Controller's host name**—Specifies the name of the profile and the Infranet Controller instance in Odyssey Access Client. If the Infranet Controller does not have a hostname configured, the URL for the Infranet Controller or the redirect URL from a captive portal is used instead. • **Use this name:**—Specifies the name of the profile and the Infranet Controller instance in Odyssey Access Client.
Profile name	Specifies the profile name. The field is enabled only if the Use this name option is selected in Name of Profile and Infranet Controller box.	Enter the name for the profile and the Infranet Controller instance in Odyssey Access Client.
Require connection to this Infranet Controller	Requires Odyssey Access Client to always attempt to connect to this Infranet Controller and prevents the user from disconnecting from this Infranet Controller. The user also cannot delete the properties of this Infranet Controller from the Odyssey Access Client configuration.	Select this option to require connection to the Infranet Controller.

Table 8: OAC Configuration Details *(continued)*

Option	Function	Your Action
Login name	Specifies the settings that you want to configure in the Odyssey Access Client profile.	Select the login name. • **Use qualified Windows login name (domain name).**— Configures the login name with the user's Windows domain name and username in the format domain name\username. Use this option if you are using an Active Directory authentication server that requires a domain name in addition to a username for authentication. • **Use unqualified Windows login name**— Configures the login name with the user's Windows user name only. Use this option for authentication servers that require a user name only for authentication. • **Prompt for login name using the following Prompt:**— Displays a dialog box for the user to enter a name during the initial Odyssey Access Client installation only. The login name is then configured and the user is not prompted again. You can also configure the text string used for the prompt in the dialog box.
Login prompt to be displayed	Specifies the login prompt to be displayed.	Enter the login prompt if you have selected the **Prompt for login name using the following Prompt:** in the Login name box.
Permit login using password	Enables password authentication for how you want Odyssey Access Client to obtain the user's credentials to sign into the Infranet Controller.	Select to enable password authentication.
Select password type to use	Specifies the password type to use. This field appears only if you select **Permit login using password** field.	Select the option for how you want Odyssey Access Client to obtain the user's credentials. • **Use Windows password** — Enables Odyssey Access Client to automatically authenticate the user to the Infranet Controller by using the user's Windows password. During the initial Odyssey Access Client installation, the user must enter a password once, but then the Odyssey Access Client automatically uses the Windows password after that. • **Prompt for password**— Enables Odyssey Access Client to prompt the user to enter a password when the user is authenticated the first time after startup. Odyssey Access Client reuses the user's credentials for the duration of the Windows session. If you choose this option and if you have configured single sign-on, Odyssey Access Client does not prompt the user for the password.

Table 8: OAC Configuration Details *(continued)*

Option	Function	Your Action
Select protocol for outer authentication	Specifies whether the outer authentication protocol for traffic between Odyssey Access Client and the Infranet Controller are Tunneled TLS (TTLS) or Protected EAP (PEAP).	Select the protocol for outer authentication: • If you select **Use EAP-TTLS as outer authentication protocol** and you want to use a client certificate as part of the EAP-TTLS authentication, click the **eap-ttls** button and select **Use the user's certificate and perform inner authentication**. This option uses EAP-TTLS certificate-based authentication and tunnels password credentials with inner authentication. Note that the most typical use of EAP-TTLS authentication is without a client certificate. • If you select **Use EAP-PEAP as outer authentication protocol** and you want to use a client certificate as part of the EAP-PEAP authentication, click the **eap-peap** button and select **Inner authentication is required**. NOTE: • Only enable the personal client certificate option for either EAP-TTLS or EAPPEAP to use a client certificate if you also configure a realm or role to require a client certificate on the endpoint. If you enable the personal client certificate option and do not configure the realm or role certificate restriction, you will cause unnecessary restrictions on the use of this Odyssey Access Client profile. • If you enable the personal client certificate option, the Infranet Controller automatically selects **Permit login using my Certificate and Use automatic certificate selection** in the Odyssey Access Client profile.
Anonymous name	Enables users to appear to log in anonymously while passing the user's login name (called the inner identity) through an encrypted tunnel. As a result, the user's credentials are secure from eavesdropping and the user's inner identity is protected.	As a general rule enter **anonymous** in the Anonymous name box, which is the default value. In some cases, you may need to add additional text. For example, if the outer identity is used to route the user's authentication to the proper server, you may be required to use a format such as anonymous@acme.com. If you leave the Anonymous name box blank, Odyssey Access Client passes the user's login name (inner identity) as the outer identity.

Table 8: OAC Configuration Details *(continued)*

Option	Function	Your Action
Configure wired adapter	Configures a wired adapter to use for wired access to the Infranet Controller at a later time, if the user is accessing the Infranet Controller through a wireless adapter during Odyssey Access Client installation.	Select the option.
Configure wireless adapter	Specifies the network settings you want to configure in Odyssey Access Client for wireless adapters.	Select the wireless adapter option. The **Network name (SSID)** option, **Association mode** option and **Encryption method** option are enabled only if the wireless adapter option is selected.
Network name (SSID)	Specifies the network name.	Enter the network name, which can use up to 32 alphanumeric characters and is case-sensitive. You must enter the name correctly to connect successfully. For example: <MyCorpNet>.
Association mode	Specifies the association mode you want Odyssey Access Client to use when associating to the access point hardware on your network.	Select the association mode: • **open**—Connects to a network through an access point or switch that implements 802.1X authentication. Select this mode if users are not required to use shared mode or Wi-Fi Protected Access (WPA). • **WPA**—Connects to a network through an access point that implements WPA. • **WPA2**—Connects to a network through an access point that implements WPA2, the second generation of WPA that satisfies 802.11i.

Table 8: OAC Configuration Details *(continued)*

Option	Function	Your Action
Encryption method	Specifies the encryption method you want Odyssey Access Client to use. The available choices depend on the association mode you selected.	Select the encryption mode: • **none**—Uses 802.1X authentication without WEP keys. This option is available only if you configure access point association in open mode. This is a typical setting to use for wireless hotspots. • **WEP**—Uses WEP keys for data encryption. You can select this option if you selected open mode association. Select WEP encryption if the access points in your network require WEP encryption. Odyssey Access Client automatically generates the WEP keys. • **AES**—Uses the advanced encryption standard protocol. Select AES if the access points in your network require WPA or WPA2 association and are configured for AES data encryption. • **TKIP**—Uses the temporal key integrity protocol. Select TKIP if the access points in your network require WPA or WPA2 association and are configured for TKIP data encryption. NOTE: If you select WEP encryption, the Infranet Controller automatically selects the **Keys will be generated automatically for data privacy** option in the Odyssey Access Client Network properties for the wireless adapter on Odyssey Access Client.
Preconfigured Installer tab		
Current Preconfiguration file	Specifies the name of the zip containing the preconfigured installer file.	Enter the filename.
Preconfiguration file	Specifies the location containing the preconfigured installer file.	Browse to locate the preconfigured installer file.

Related Documentation

- Creating and Configuring Infranet Controller Administrator Roles (NSM Procedure) on page 48
- Configuring Infranet Controller User Roles (NSM Procedure) on page 35
- Configuring Access Options on an Infranet Controller User Role (NSM Procedure) on page 40
- Delegating Management Tasks to Infranet Controller Administrator Roles (NSM Procedure) on page 55

Creating and Configuring Infranet Controller Administrator Roles (NSM Procedure)

An administrator role defines administrator session and personalization settings. You can create and configure an administrator role from the Infranet Controller configuration tree.

To create an administrator role:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to configure administrator role.
3. Click the **Configuration** tab. In the configuration tree, select **Administrators** > **Admin Roles**.
4. Add or modify settings on the **Admin Role** tab as specified in Table 9 on page 48.
5. Click one:
   - **OK** — Saves the changes.
   - **Cancel** — Cancels the modifications.

NOTE: To create individual administrator accounts, you must add the users through the appropriate authentication server (not the role). For example, to create an individual administrator account, select **Authentication** > **Auth. Servers** > **Administrators** > **Users** from the NSM UI.

Table 9: Administrator Role Configuration Details

Option	Function	Your Action
Admin Role > General tab		
Name	Specifies a unique name for the administrator role.	Enter a name.
Admin Role > General > Overview tab		
Description	Describes the administrator role.	Enter a brief description for the administrator role.
Session Options	Specifies the maximum session length, roaming capabilities, and session persistence.	Select **General** > **Session Options** to apply the settings to the role.
UI Options	Specifies the logo, color, navigation menus and the copyright notice.	Select **General** > **UI Options** to apply the settings to the role.

Table 9: Administrator Role Configuration Details *(continued)*

Option	Function	Your Action
Admin Role > General > Restrictions > Source IP Restrictions tab		
Allow	Specifies from which IP addresses users can access an Infranet Controller sign-in page, be mapped to a role, or access a resource.	• Select **Users from any IP address** to enable users to sign into the Infranet Controller from any IP address in order to satisfy the access management requirement. • Select **Users from IP addresses which pass the specifies matching policies** to allow you to specify user access to the listed IP addresses.
Source IP Address	Specifies the source IP addresses.	Enter the IP address.
Source IP Netmask	Specifies the IP netmask.	Enter the IP netmask.
Access	Specifies whether to allow or deny access.	• Select **Allow** to allow the user to use the IP. • Select **Deny** to prevent users from using the IP.
Admin Role > General > Restrictions > Browser Restrictions tab		
Allow	Specifies from which web browsers users can access an Infranet Controller sign-in page or be mapped to a role.	• Select **Browsers with any user-agent** to allow users to access the Infranet Controller or resources using any of the supported Web browsers. • Select **Browsers whose user-agent pass the matching policies defined below** to allow you to define browser access control rules.
User agent pattern	Specifies the format.	Enter a string in the format *<browser_string>* where start (*) is an optional character used to match any character and <browser_string>is a case-sensitive pattern that must match a substring in the user-agent header sent by the browser. NOTE: You cannot include escape characters (\) in browser restrictions.
Action	Specifies whether to allow or deny access.	• Select **Allow access** to allow users to use a browser that has a user-agent header containing the<browser_string> substring. • Select **Deny access** to prevent users from using a browser that has a user-agent header containing the <browser_string> substring.
Admin Role > General > Restrictions >Certificate Restrictions tab		

Table 9: Administrator Role Configuration Details *(continued)*

Option	Function	Your Action
Allow	Restricts Infranet Controller and resource access by requiring client-side certificates	• Select **All users** to allow users to access the Infranet Controller or resources from any machine. • Select **Users with a trusted client certificate** to allow users to access the Infranet Controller from a machine with a trusted client certificate.
Certificate Field	Specifies the certificate field.	Enter the certificate field.
Expected Value	Specifies the expected value.	Enter the expected value.
Admin Role > General > Restrictions >Host Checker Restrictions tab		
Enforce	Specifies the Host Checker policy at the role level.	• Select **Allow all users** to restrict Host Checker to be installed in order for the user to meet the access requirement. • Select **Allow users whose workstations meet the requirements specified by the Host Checker policies** to requires that Host Checker is running the specified Host Checker policies in order for the user to meet the access requirement.
Host Checker policies	Specifies the Host Checker policies.	Select the required Host Checker policies.
Allow access to the role if	Specifies access to the role	• Select **All of the selected policies pass** to allow access only if all the policy requirements are met. • Select **Any ONE of the selected policies pass** to allow access even if one policy requirement is met.
Admin Role > General > Users > Roles > Delegate User Roles		
Administrators can manage ALL roles	Specifies whether the administrator can manage all roles	Select the user roles. If you only want to allow the administrator role to manage selected user roles, select those roles in the Non-members list and click **Add** to move it to the Members list.
Access	Specifies which user role pages the delegated administrator can manage.	• Select **Write All** to specify that members of the administrator role can modify all user role pages. • Select **Custom Settings** to allow you to pick and choose administrator privileges (Deny, Read, or Write) for the individual user role pages.

Table 9: Administrator Role Configuration Details *(continued)*

Option	Function	Your Action
Admin Role > General > Users > Role > Delegate As Read-Only Role		
Administrator can view (but not modify) ALL roles	Allows the administrator to view the user roles, but not manage.	Select the user role that you want to allow the administrator to view. NOTE: If you specify both write access and read-only access for a feature, the Infranet Controller grants the most permissive access. For example, if you select the **Administrators can manage ALL roles** check box under Delegate User Roles, and then select the Users role on the Delegate As Read-Only Roles page, then the Infranet Controller allows the delegated administrator role full management privileges to the Users role.
Admin Role > General > Users > Realms > Delegate User Realms		
Administrators can manage ALL realms	Specifies whether the administrator can manage all user authentication realms	Select the user realm. If you only want to allow the administrator role to manage selected realms, select those realms from theNon—members list and add to the Members list.
Access	Specifies which user authentication realms pages that the delegated administrator can manage.	• Select **Write All** to specify that members of the administrator role can modify all user authentication realm pages. • Select **Custom Settings** to allow you to pick and choose administrator privileges (Deny, Read, or Write) for the individual user authentication realm pages.
Admin Role > General > Users > Realms > Delegate As Read-Only Realms		
Administrator can view (but not modify) ALL realms	Allows the administrator to view the user authentication realms, but not modify.	Select the user authentication realms that you want to allow the administrator to view. NOTE: If you specify both write access and read-only access for an authentication realm page, the Infranet Controller grants the most permissive access. For example, if you select the **Administrators can manage ALL realms** check box under Delegate User Realms, and then select the Users role on the Delegate As Read-Only Realms page, then the Infranet Controller allows the delegated administrator role full management privileges to the Users realm.
Admin Role > General > Delegated Administrator Settings > Management of Admin roles		
Manage ALL admin roles	Manages all admin roles.	Select to manage all the admin roles.

Table 9: Administrator Role Configuration Details *(continued)*

Option	Function	Your Action
Allow Add/Delete admin roles	Allows the security administrator the ability to create administrator roles, even if the security administrator is not part of the Administrators role.	Select to allow the security administrator to add and delete admin roles.
Access	Indicates the level of access that you want to allow the security administrator role to set for system administrators.	• Select **Deny All** to specify that members of the security administrator role cannot see or modify any settings in the category. • Select **Read All** to specify that members of the security administrator role can view, but not modify, all settings in the category. • Select **Write All** to specify that members of the security administrator role can modify all settings in the category. • Select **Custom Settings** to allow you to pick and choose security administrator privileges (Deny, Read, or Write) for the individual features within the category.
Admin Role > General > Delegated Administrator Settings > Management of Admin realms		
Manage ALL admin realms	Manages all admin realms.	Select to manage all the admin realms.
Allow Add/Delete admin realms	Allows the security administrator to create and delete administrator realms, even if the security administrator is not part of the administrators role.	Select to allow the security administrator to add and delete admin realms.
Access	Indicates the level of realm access that you want to allow the security administrator role to set for system administrators for each major set of admin console pages.	• Select **Deny All** to specify that members of the security administrator role cannot see or modify any settings in the category. • Select **Read All** to specify that members of the security administrator role can view, but not modify, all settings in the category. • Select **Write All** to specify that members of the security administrator role can modify all settings in the category. • Select **Custom Settings** to allow you to pick and choose security administrator privileges (Deny, Read, or Write) for the individual features within the category. NOTE: All administrators that can manage admin roles and realms have at least read-only access to the admin role's Name and Description and to the realm's Name and Description, as displayed on the General page.

Table 9: Administrator Role Configuration Details *(continued)*

Option	Function	Your Action
Admin Role > General > Delegated Resource Policies > All tab		
Access	Indicates the level of access that you want to allow the administrator role for each Resource Policies submenu.	• Select **Deny All** to specify that members of the administrator role cannot see or modify any resource policies. • Select **Read All** to specify that members of the administrator role can view, but not modify, all resource policies. • Select **Write All** to specify that members of the administrator role can modify all resource policies. • Select **Custom Settings** to allow you to pick and choose administrator privileges (Deny, Read, or Write) for each type of resource policy or for individual resource policies.
Admin Role > General > Delegated Resource Policies > Custom Settings		
Additional Access Policies	Sets custom access levels for an individual policy	Select the access level for the policy (Deny, Read, or Write).
Policies	Provides custom access level.	Select the resource policy for which you want to provide a custom access level, and click **Add**.
Default Options for Delegated Admins > Session Options tab		
Idle Timeout (minutes)	Specifies the number of minutes an administrator session may remain idle before ending. The minimum is 5 minutes. The default idle session limit is ten minutes, which means that if an administrator's session is inactive for ten minutes, the Infranet Controller ends the session and logs the event in the system log (unless you enable session timeout warnings described below).	Enter the idle timeout duration in minutes.
Max. Session Length (minutes)	Specifies the number of minutes an active administrator session may remain open before ending. The minimum is 6 minutes. The default time limit for an administrator session is sixty minutes, after which the Infranet Controller ends the session and logs the event in the system log.	Enter the session length in minutes. The default is 300 seconds, and the minimum is six minutes.

Table 9: Administrator Role Configuration Details *(continued)*

Option	Function	Your Action
Roaming session	Roaming sessions allow users to work across source IP addresses. This is useful for mobile users with dynamically assigned IP addresses, as it allows them to sign in from their desk and continue working.	• Select **Enabled** to enable roaming user sessions for users mapped to this group. A roaming user session works across source IP addresses, which allows mobile administrators (laptop users) with dynamic IP addresses to sign in to the Infranet Controller from one location and continue working from another. Disable this feature to prevent users from accessing a previously established session from a new source IP address. This helps protect against an attack spoofing a user's session, provided the hacker was able to obtain a valid user's session cookie. • Select **Limit to subnet** to limit the roaming session to the local subnet specified in the Netmask field. Administrators may sign in from one IP address and continue using their sessions with another IP address as long as the new IP address is within the same subnet. • Select **Disabled** to disable roaming sessions for administrators mapped to this role. Administrators who sign in from one IP address may not continue an active Infranet Controller session from another IP address; administrator sessions are tied to the initial source IP address.
Default Options for Delegated Admins >UI Options tab		
Logo image	Displays the logo in the Current appearance box only after you save your changes.	Click the Browse button and locate your custom image file.
Background color	Updates the current appearance of the box.	Type the hexadecimal number for the background color or click the Color Palette icon and pick the desired color.
Navigation Menus	Displays hierarchical navigation menus.	• Select **Auto-enabled** to determine whether the administrator is signed in from a supported platform and enables or disables the hierarchical menus accordingly. • Select **Enabled** to enable hierarchical menus, regardless of your platform. If the administrator is signed in from an unsupported platform, they may not be able to use the hierarchical menus, even though they are enabled. • Select **Disabled** to disable hierarchical menus for all members of the role.

Table 9: Administrator Role Configuration Details *(continued)*

Option	Function	Your Action
Show copyright notice in footer	Specifies the copyright notice and label in the footer.	Select or clear the check box (optional). NOTE: If you do not want user roles to see the copyright notice, you can also deselect the option in the Default Settings for user roles, in general. That way, all subsequent roles you create do not allow the notice to appear on the end-user UI.

Related Documentation

- Delegating Management Tasks to Infranet Controller Administrator Roles (NSM Procedure) on page 55
- Configuring Infranet Controller User Roles (NSM Procedure) on page 35
- Configuring Access Options on an Infranet Controller User Role (NSM Procedure) on page 40
- Configuring OAC Settings for a User Role (NSM Procedure) on page 42

Delegating Management Tasks to Infranet Controller Administrator Roles (NSM Procedure)

You can delegate management tasks to various delegated administrator roles.

To delegate management tasks to administrator roles:

1. In the navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to configure administrator role.
3. Click the **Configuration** tab. In the configuration tree, select **Administrators** > **Admin Roles**.
4. Add or modify settings under **Admin Role** as specified in Table 10 on page 55.
5. Click one:
   - **OK** — Saves the changes.
   - **Cancel** — Cancels the modifications.

Table 10: Administrator Role Configuration for Delegation

Option	Function	Your Action
Users > Roles > Delegate User Roles		
Administrators can manage ALL roles	Specifies whether the administrator can manage all roles	Select the user roles. If you only want to allow the administrator role to manage selected user roles, select those roles in the Non-members list and click **Add** to move it to the Members list.

Table 10: Administrator Role Configuration for Delegation *(continued)*

Option	Function	Your Action
Access	Specifies which user role pages the delegated administrator can manage.	• Select **Write All** to specify that members of the administrator role can modify all user role pages. • Select **Custom Settings** to allow you to pick and choose administrator privileges (**Deny**, **Read**, or **Write**) for the individual user role pages.
Users > Role > Delegate As Read-Only Role		
Administrator can view (but not modify) ALL roles	Allows the administrator to view the user roles, but not manage.	Select the user roles that you want to allow the administrator to view. NOTE: If you specify both write access and read-only access for a feature, the Infranet Controller grants the most permissive access. For example, if you select the **Administrators can manage ALL roles** check box under Delegate User Roles, and then select the Users role on the Delegate As Read-Only Roles page then the Infranet Controller allows the delegated administrator role full management privileges to the Users role.
Users > Realms > Delegate User Realms		
Administrators can manage ALL realms	Specifies whether the administrator can manage all user authentication realms	Select the user realm. If you only want to allow the administrator role to manage selected realms, select those realms in the Non-members list and click **Add** to move it to the Members list.
Access	Specifies which user authentication realms pages that the delegated administrator can manage.	• Select **Write All** to specify that members of the administrator role can modify all user authentication realm pages. • Select **Custom Settings** to allow you to pick and choose administrator privileges (Deny, Read, or Write) for the individual user authentication realm pages.
Users > Realms > Delegate As Read-Only Realms		
Administrator can view (but not modify) ALL realms	Allows the administrator to view the user authentication realms, but not modify.	Select the user authentication realms that you want to allow the administrator to view. NOTE: If you specify both write access and read-only access for an authentication realm page, the Infranet Controller grants the most permissive access. For example, if you select the **Administrators can manage ALL realms** check box under Delegate User Realms, and then select the Users role on the Delegate As Read-Only Realms page, then the Infranet Controller allows the delegated administrator role full management privileges to the Users realm.

Table 10: Administrator Role Configuration for Delegation *(continued)*

Option	Function	Your Action
Delegated System Settings tab		
System Tasks	Indicates the level of access that you want to allow for system tasks.	• Select **Deny All** to specify that members of the administrator role cannot view or modify any settings. • Select **Read All** to specify that members of the administrator role can view, but not modify settings. • Select **Write All** to specify that members of the administrator role can modify all settings. • Select **Custom Settings** to allow you to pick and choose privileges (Deny, Read, or Write) for System, Archiving and Troubleshooting pages.
Log/Monitoring	Indicates the level of access that you want to allow for log/monitoring.	
Authentication	Indicates the level of access that you want to allow for authentication.	
Maintenance Tasks	Indicates the level of access that you want to allow for maintenance tasks.	
Delegated Administrator Settings > Management of Admin roles		
Manage ALL admin roles	Manages all admin roles.	Select to manage all the admin roles.
Allow Add/Delete admin roles	Allows the security administrator to create administrator roles, even if the security administrator is not part of the administrators role.	Select to allow the security administrator to add and delete admin roles.
Access	Indicates the level of access that you want to allow the security administrator role to set for system administrators.	• Select **Deny All** to specify that members of the security administrator role cannot see or modify any settings in the category. • Select **Read All** to specify that members of the security administrator role can view, but not modify, all settings in the category. • Select **Write All** to specify that members of the security administrator role can modify all settings in the category. • Select **Custom Settings** to allow you to pick and choose security administrator privileges (Deny, Read, or Write) for the individual features within the category.
Delegated Administrator Settings > Management of Admin realms		
Manage ALL admin realms	Manages all admin realms.	Select to manage all the admin realms.

Table 10: Administrator Role Configuration for Delegation *(continued)*

Option	Function	Your Action
Allow Add/Delete admin realms	Allows the security administrator to create and delete administrator realms, even if the security administrator is not part of the administrators role.	Select to allow the security administrator to add and delete admin realms.
Access	Indicates the level of realm access that you want to allow the security administrator role to set for system administrators for each major set of admin console pages (General, Authentication Policy, and Role Mapping.)	• Select **Deny All** to specify that members of the security administrator role cannot see or modify any settings in the category. • Select **Read All** to specify that members of the security administrator role can view, but not modify, all settings in the category. • Select **Write All** to specify that members of the security administrator role can modify all settings in the category. • Select **Custom Settings** to allow you to pick and choose security administrator privileges (Deny, Read, or Write) for the individual features within the category. NOTE: All administrators that can manage admin roles and realms have at least read-only access to the admin role's Name and Description and to the realm's Name and Description, as displayed on the General tab.
Delegated Resource Policies > All tab		
Access	Indicates the level of access that you want to allow the administrator role for each Resource Policies sub-menu	• Select **Deny All** to specify that members of the administrator role cannot see or modify any resource policies. • Select **Read All** to specify that members of the administrator role can view, but not modify, all resource policies. • Select **Write All** to specify that members of the administrator role can modify all resource policies. • Select **Custom Settings** to allow you to pick and choose administrator privileges (Deny, Read, or Write) for each type of resource policy or for individual resource policies.
Delegated Resource Policies > All (Custom Settings for Infranet Enforcer, Network Access, and Host Enforcer)		
Additional Access Policies	Sets custom access levels for an individual policy	Select the access level for the policy (Deny, Read, or Write.)
Policies	Provides custom access level.	Select the resource policy for which you want to provide a custom access level, and click **Add**.

Related Documentation

- Creating and Configuring Infranet Controller Administrator Roles (NSM Procedure) on page 48
- Configuring Infranet Controller User Roles (NSM Procedure) on page 35
- Configuring OAC Settings for a User Role (NSM Procedure) on page 42
- Configuring Access Options on an Infranet Controller User Role (NSM Procedure) on page 40

CHAPTER 7

Configuring Security Requirements for Administrators and Users

Configuring Infranet Controller Source IP Access Restrictions (NSM Procedure)

Source IP access restrictions control from which IP addresses users can access an Infranet Controller sign-in page, be mapped to a role, or access a resource.

To configure Infranet Controller source IP access restrictions:

1. In the navigation tree, select **Device Manager**> **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to configure source IP access restrictions.
3. Click the **Configuration** tab. In the Configuration tree, select:
   - **Administrators** > **Admin Roles** > *Select Role* > **General** > **Restrictions** > **Source IP Restrictions** to configure source IP access restrictions for admin roles.
   - **Administrators** > **Admin Realms** > *Select Realm* > **Authentication Policies** > **Source IP** to configure source IP access restrictions for admin realms.

- **Users** > **User Roles** > *Select Role* > **General** > **Restrictions** > **Source IP Restrictions** to configure source IP access restrictions for user roles.
- **Users** > **User Realms** > **Authentication Policies** > **Source IP** to configure source IP access restrictions for user realms.

4. Add or modify settings as specified in Table 11 on page 62.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 11: Source IP Access Restrictions Configuration Details

Option	Function	Your Action
Allow	Specifies from which IP addresses users can access an Infranet Controller sign-in page, be mapped to a role, or access a resource.	• Select **Users from any IP address** to enable users to sign into the Infranet Controller from any IP address. • Select **Users from IP addresses which pass the specified matching policies** to allow access only to the listed IP addresses.
Source IP Address	Specifies the source IP address.	Enter the IP address.
Source IP Netmask	Specifies the IP netmask.	Enter the IP netmask.
Access	Specifies whether to allow or deny access.	• Select **Allow** to allow the user to use the IP address. • Select **Deny** to prevent users from using the IP address.
Enable Administrators to sign in on the External Port	Specifies whether or not administrators can sign in from the external port	Select this option to enable administrators to sign in on the external port.. NOTE: This setting can be configured only for admin realms.
Enable Administrators to sign in on the Internal Port	Specifies whether or not administrators can sign in from the internal port.	Select this option. NOTE: This setting can be configured only for admin realms.

Related Documentation

- Configuring Infranet Controller Browser Access Restrictions (NSM Procedure) on page 63
- Configuring Infranet Controller Certificate Access Restrictions (NSM Procedure) on page 64
- Configuring Infranet Controller Password Access Restrictions (NSM Procedure) on page 66

- Configuring Infranet Controller Host Checker Access Restrictions (NSM Procedure) on page 67
- Configuring the Number of Concurrent Sessions and Concurrent Users for Infranet Controller Users (NSM Procedure) on page 70
- Configuring Infranet Controller User Roles (NSM Procedure) on page 35

Configuring Infranet Controller Browser Access Restrictions (NSM Procedure)

Browser restrictions control from which Web browsers users can access an Infranet Controller sign-in page or be mapped to a role. If a user tries to sign into the Infranet Controller using an unsupported browser, the sign-in attempt fails and a message displays stating that an unsupported browser is being used. This feature also ensures that users sign into the Infranet Controller from browsers that are compatible with corporate applications or are approved by corporate security policies.

To configure Infranet Controller browser access restrictions:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device tree** tab, and then double-click the Infranet Controller device for which you want to configure browser access restrictions.
3. Click the **Configuration** tab. In the configuration tree, select the level at which you want to implement browser access restrictions:
   - Realm level—Select:
     - **Administrators** > **Admin Realms** >*Select Realm* > **Authentication Policies** > **Browser** to configure browser access restrictions for admin realms.
     - **Users** > **User Realms** > *Select Realm* > **Authentication Policies** > **Browser** to configure browser access restrictions for user realms.
   - Role level—Select:
     - **Administrators** > **Admin Roles** > *Select Role* > **General** > **Restrictions** > **Browser Restrictions** to configure browser access restrictions for admin roles.
     - **Users** > **User Roles** > *Select Role* > **General** > **Restrictions** > **Browser Restrictions** to configure browser access restrictions for user roles.
4. Add or modify settings as specified in Table 12 on page 64.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 12: Browser Access Restrictions Configuring Details

Option	Function	Your Action
Allow	Specifies from which Web browsers users can access an Infranet Controller sign-in page or be mapped to a role.	• Select **Browsers with any user-agent** to allow users to access the Infranet Controller or resources using any of the supported Web browsers. • Select **Browsers whose user-agent pass the matching policies defined below** to allow you to define browser access control rules.
User—Agent pattern	Specifies the user agent string pattern.	Enter a string in the format *<browser_string>* where start (*) is an optional character used to match any character and <browser_string>is a case-sensitive pattern that must match a substring in the user-agent header sent by the browser. NOTE: You cannot include escape characters (\) in browser restrictions.
Action	Specifies whether to allow or deny browser access.	• Select **Allow access** to allow users to use a browser that has a user-agent header containing the<browser_string> substring. • Select **Deny access** to prevent users from using a browser that has a user-agent header containing the <browser_string> substring.

Related Documentation

- Configuring Infranet Controller Source IP Access Restrictions (NSM Procedure) on page 61
- Configuring Infranet Controller Certificate Access Restrictions (NSM Procedure) on page 64
- Configuring Infranet Controller Password Access Restrictions (NSM Procedure) on page 66
- Configuring Infranet Controller Host Checker Access Restrictions (NSM Procedure) on page 67
- Configuring the Number of Concurrent Sessions and Concurrent Users for Infranet Controller Users (NSM Procedure) on page 70
- Configuring Infranet Controller User Roles (NSM Procedure) on page 35
- Creating and Configuring Infranet Controller Administrator Roles (NSM Procedure) on page 48

Configuring Infranet Controller Certificate Access Restrictions (NSM Procedure)

Certificate access restrictions restrict Infranet Controller and resource access by requiring client side certificates.

To configure Infranet Controller certificate access restrictions:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device tree** tab, and then double-click the Infranet Controller device for which you want to configure certificate access restrictions.
3. Click the **Configuration** tab. In the configuration tree, select the level at which you want to implement certificate access restrictions:
   - Realm level—Select:
     - **Administrators** > **Admin Realms** >*Select Realm* > **Authentication Policies** > **Certificate** to configure certificate access restrictions for admin realms.
     - **Users** > **User Realms** >*Select Realm* > **Authentication Policies** > **Certificate** to configure certificate access restrictions for user realms.
   - Role level—Select:
     - **Administrators** > **Admin Roles** > *Select Role* > **General** > **Restrictions** > **Certificate Restrictions** to configure certificate access restrictions for admin roles.
     - **Users** > **User Roles** > *Select Role* > **General** > **Restrictions** > **Certificate Restrictions** to configure certificate access restrictions for user roles.
4. Add or modify settings as specified in Table 13 on page 65.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 13: Certificate Access Restrictions Configuring Details

Option	Function	Your Action
Allow	Restricts Infranet Controller and resource access by requiring client-side certificates.	• Select **All users** to allow users to access the Infranet Controller or resources from any machine. • Select **Users with a trusted client certificate** to allow users to access the Infranet Controller from a machine with a trusted client certificate. • Select **All users, remember certificate while user is signed in** to remember all the users' certificate while they are signed in. NOTE: This option is applicable for admin and user realms.
Certificate Field	Specifies the certificate field information for the field/value pair.	Enter the certificate field information.

Table 13: Certificate Access Restrictions Configuring Details *(continued)*

Option	Function	Your Action
Expected Value	Specifies the expected value information for the field/value pair.	Enter the expected value information.

Related Documentation

- Configuring Infranet Controller Source IP Access Restrictions (NSM Procedure) on page 61
- Configuring Infranet Controller Browser Access Restrictions (NSM Procedure) on page 63
- Configuring Infranet Controller Password Access Restrictions (NSM Procedure) on page 66
- Configuring Infranet Controller Host Checker Access Restrictions (NSM Procedure) on page 67
- Configuring the Number of Concurrent Sessions and Concurrent Users for Infranet Controller Users (NSM Procedure) on page 70
- Configuring Infranet Controller User Roles (NSM Procedure) on page 35
- Creating and Configuring Infranet Controller Administrator Roles (NSM Procedure) on page 48

Configuring Infranet Controller Password Access Restrictions (NSM Procedure)

You can restrict Infranet Controller and resource access by password-length when administrators or users try to sign in to an Infranet Controller. The user must enter a password whose length meets the minimum password-length requirement specified for the realm.

To configure Infranet Controller password access restrictions:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device tree** tab, and then double-click the Infranet Controller device for which you want to configure password access restrictions.
3. Click the **Configuration** tab. In the configuration tree, select the level at which you want to implement password access restrictions. Then select:
   - **Administrators** > **Admin Realms** >*Select Realm* > **Authentication Policies** > **Password** to configure password access restrictions for admin realms.
   - **Users** > **User Realms** >*Select Realm* > **Authentication Policies** > **Password** to configure password access restrictions for user realms.
4. Add or modify settings as specified in Table 14 on page 67.
5. Click one:
   - **OK**—Saves the changes.

- **Cancel**—Cancels the modifications.

Table 14: Password Access Restrictions Configuration Details

Option	Function	Your Action
Options for primary authentication server	Specifies the options for the primary authentication server.	• Select **Only allow users that have passwords of a minimum length** to restrict user access to only those who meet the Primary password minimum length requirement. • Select **Allow all users** to permit access to all the users.
Primary password minimum length	Specifies the minimum number of characters a password must have.	Select or enter the minimum number of characters that a password must have.

Related Documentation

- Configuring Infranet Controller Source IP Access Restrictions (NSM Procedure) on page 61
- Configuring Infranet Controller Browser Access Restrictions (NSM Procedure) on page 63
- Configuring Infranet Controller Certificate Access Restrictions (NSM Procedure) on page 64
- Configuring Infranet Controller Host Checker Access Restrictions (NSM Procedure) on page 67
- Configuring the Number of Concurrent Sessions and Concurrent Users for Infranet Controller Users (NSM Procedure) on page 70
- Configuring Infranet Controller User Roles (NSM Procedure) on page 35
- Creating and Configuring Infranet Controller Administrator Roles (NSM Procedure) on page 48

Configuring Infranet Controller Host Checker Access Restrictions (NSM Procedure)

A Host Checker restricts user's access to the Infranet Controller, a role, or a resource based on his Host Checker status.

To configure Infranet Controller Host Checker access restrictions:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device tree** tab, and then double-click the Infranet Controller device for which you want to configure Host Checker access restrictions.
3. Click the **Configuration** tab. In the configuration tree, select the level at which you want to implement Host Checker access restrictions:
   - Realm level—Select:

- **Administrators** > **Admin Realms** >*Select Realm* > **Authentication Policies** > **Host Checker** to configure Host Checker access restrictions for admin realms.
- **Users** > **User Realms** >*Select Realm* > **Authentication Policies** > **Host Checker** to configure Host Checker access restrictions for user realms.

- Role level—Select:
  - **Administrators** > **Admin Roles** > *Select Role* > **General** > **Restrictions** > **Host Checker Restrictions** to configure Host Checker access restrictions for admin roles.
  - **Users** > **User Roles** > *Select Role* > **General** > **Restrictions** > **Host Checker Restrictions** to configure Host Checker access restrictions for user roles.

4. Add or modify settings as specified in
   - Table 15 on page 68 to configure role level restrictions.
   - Table 16 on page 68 to configure realm level restrictions.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 15: Host Checker Access Restrictions for Role Level Configuration Details

Option	Function	Your Action
Enforce/Allow	Specifies the Host Checker policy at the role level.	• Select **Allow all users** to permit access to all users. • Select **Allow users whose workstations meet the requirements specified by the Host Checker policies** to require that Host Checker is running the specified Host Checker policies for the user to meet the access requirement.
Host Checker policies	Specifies the Host Checker policies.	Select the required Host Checker policies.
Allow access to the role if	Specifies access to the role.	• Select **All of the selected policies pass** to allow access only if all the policy requirements are met. • Select **Any ONE of the selected policies pass** to allow access even if one policy requirement is met.

Table 16: Host Checker Access Restrictions for Realm Level Configuration Details

Field	Function	Your Action
Evaluate ALL policies	Specifies if all policies must be evaluated.	Select to evaluate all policies.

Table 16: Host Checker Access Restrictions for Realm Level Configuration Details *(continued)*

Field	Function	Your Action
Evaluate selected policies	Specifies that the selected policies are to be evaluated.	Select the policies that must be evaluated and add them to the Members list.
Enforce ALL policies	Specifies if all policies must be enforced.	Select to enforce all policies.
Enforce selected policies	Specifies that the selected policies are to be enforced.	Select the policies that must be enforced and add them to the Members list.
Allow access to the realm if	Specifies access to the realm.	• Select **All of the enforced policies pass** to allow access only if all the enforced policy requirements are met. • Select **Any ONE of the enforced policies pass** to allow access even if one enforced policy requirement is met.

Related Documentation

- Configuring Infranet Controller Source IP Access Restrictions (NSM Procedure) on page 61
- Configuring Infranet Controller Browser Access Restrictions (NSM Procedure) on page 63
- Configuring Infranet Controller Certificate Access Restrictions (NSM Procedure) on page 64
- Configuring Infranet Controller Password Access Restrictions (NSM Procedure) on page 66
- Configuring the Number of Concurrent Sessions and Concurrent Users for Infranet Controller Users (NSM Procedure) on page 70
- Configuring Infranet Controller User Roles (NSM Procedure) on page 35
- Creating and Configuring Infranet Controller Administrator Roles (NSM Procedure) on page 48

Configuring Infranet Controller RADIUS Request Attribute Restrictions for User Realms (NSM Procedure)

You can create RADIUS request attribute policies to require authentication requests to contain specific RADIUS attribute values. If an endpoint attempts to access a realm with a RADIUS request attribute policy, the endpoint must meet the conditions specified in the policy.

To add a RADIUS request attribute policy to a realm:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device tree** tab, and then double-click the Infranet Controller device for which you want to configure RADIUS request attribute restrictions for user realms.
3. From the Configuration tab, select **Users** > **User Realms** >*Select Realm* > **Authentication Policies** > **RADIUS Request Attributes Policies** to configure RADIUS request attribute restrictions for user realms.
4. Select the RADIUS request attribute policies, which the endpoint must meet, from the Non-members area and click **Add** to move it to the Members area.
5. Select **Allow access to realm if any ONE of the selected policies are passed**.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Related Documentation

- Configuring RADIUS Request Attributes Policies (NSM Procedure) on page 83
- Configuring Infranet Controller Source IP Access Restrictions (NSM Procedure) on page 61
- Configuring Infranet Controller Browser Access Restrictions (NSM Procedure) on page 63
- Configuring Infranet Controller Password Access Restrictions (NSM Procedure) on page 66
- Configuring Infranet Controller Host Checker Access Restrictions (NSM Procedure) on page 67
- Configuring the Number of Concurrent Sessions and Concurrent Users for Infranet Controller Users (NSM Procedure) on page 70
- Configuring Infranet Controller User Roles (NSM Procedure) on page 35
- Creating and Configuring Infranet Controller Administrator Roles (NSM Procedure) on page 48

Configuring the Number of Concurrent Sessions and Concurrent Users for Infranet Controller Users (NSM Procedure)

You can limit the number of concurrent sessions and concurrent users for Infranet Controller users. A user who enters a URL to one of this realm's sign-in pages must meet any access management and concurrent user requirements specified for the authentication policy before the Infranet Controller presents the sign-in page to the user.

To configure the number of concurrent sessions and concurrent users for Infranet Controller users:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device tree** tab, and then double-click the Infranet Controller device for which you want to configure the number of concurrent sessions and concurrent users.
3. Click the **Configuration** tab. In the configuration tree, select the level at which you want to implement concurrent session restrictions. Then select:
   - **Administrators** > **Admin Realms** >*Select Realm* > **Authentication Policies** > **Limits** to configure the number of concurrent sessions for admin realms.
   - **Users** > **User Realms** >*Select Realm* > **Authentication Policies** > **Limits** to configure the number of concurrent sessions for user realms.

   NOTE: **The number of concurrent users can be configured only for user realms.**
4. Add or modify settings as specified in Table 17 on page 71.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 17: Number of Concurrent Sessions and Concurrent Users for Infranet Controller User Configuration Details

Option	Function	Your Action
Limit number of concurrent users	Limits the number of concurrent users on the realm.	Select this option to limit the number of concurrent users.
Guaranteed minimum	Specifies the number of users between zero (0) and the maximum number of concurrent users defined for the realm, or you can set the number to the maximum allowed by your license if there is no realm maximum.	Select or enter the number of users between zero (0) and the maximum number of concurrent users defined for the realm.
Limit the number of concurrent sessions per user	Specifies whether the number of concurrent sessions per user is limited.	Select this option to limit the number of concurrent sessions per user.
Session limit	Specifies the number of sessions permissible. NOTE: You can configure this option only for user realms.	Specify the number of sessions permitted. By default, the number is 1 if the realm maximum is greater than 0; otherwise, the default is 0. The maximum number must be no greater than the maximum number of concurrent users for the realm.

Table 17: Number of Concurrent Sessions and Concurrent Users for Infranet Controller User Configuration Details *(continued)*

Option	Function	Your Action
Maximum	Specifies the maximum number of concurrent users. NOTE: You can configure this option only for user realms.	Select or enter the maximum number of concurrent users permissible.

Related Documentation

- Configuring Infranet Controller Source IP Access Restrictions (NSM Procedure) on page 61
- Configuring Infranet Controller Browser Access Restrictions (NSM Procedure) on page 63
- Configuring Infranet Controller Certificate Access Restrictions (NSM Procedure) on page 64
- Configuring Infranet Controller Host Checker Access Restrictions (NSM Procedure) on page 67
- Configuring Infranet Controller User Roles (NSM Procedure) on page 35
- Creating and Configuring Infranet Controller Administrator Roles (NSM Procedure) on page 48

CHAPTER 8

Configuring the Infranet Controller RADIUS Server and Layer 2 Access

Configuring the Infranet Controller as a RADIUS Server (NSM Procedure)

The Infranet Controller contains an internal RADIUS server that can be configured to perform Extensible Authentication Protocol (EAP) inner and outer authentication, non-tunneled Web authentication without EAP, and MAC address authentication.

To configure the Infranet Controller as a RADIUS server, the following configurations must be performed:

1. Configuring Authentication Protocol Sets on page 73
2. Using RADIUS Proxy on page 75

Configuring Authentication Protocol Sets

To configure an authentication protocol set:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to configure authentication protocol sets.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication** > **Signing In** > **Authentication Protocols**.

NOTE: The default 802.1X protocol set is configured to work with either EAP-TTLS or EAP-PEAP as the primary outer authentication protocol, and EAP-JUAC or EAP-MSCHAP- V2 for inner authentication (if EAP-PEAP is used) and EAP-JUAC, PAP, MSCHAP- V2, EAP-MS-CHAP-V2, or EAP-GenericTokenCard (if EAP-TTLS is used).

4. Add or modify settings on the authentication protocol sets as specified in Table 18 on page 74.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 18: Authentication Protocol Sets Configuration Details

Option	Function	Your Action
Authentication Protocol		
Name	Specifies a unique name for the authentication protocol.	Enter a name for the authentication protocol.
Description	Describes the authentication protocol.	Enter a brief description for the authentication protocol.
Authentication Protocol > Authentication Protocol		
New Authentication Protocol	Specifies the main authentication protocol.	Select the authentication protocol from the list. NOTE: If you are using inner RADIUS proxy, do not select an inner protocol with EAP-PEAP or EAP-TTLS. See "Using RADIUS Proxy."
Authentication Protocol > PEAP		
New PEAP	Specifies the inner authentication protocol.	If you select EAP-PEAP as the main authentication protocol, under PEAP click **Add** and select an inner authentication protocol from the New PEAP list. NOTE: If you are configuring a protocol set to work with the Windows client and a Host Checker Statement of Health policy, you must choose the EAP-SOH protocol as the inner authentication method within a PEAP tunnel.
Authentication Protocol > TTLS		
New TTLS	Specifies the inner authentication protocol.	If you select EAP-TTLS as the main authentication protocol, under TTLS click **Add** and select an inner authentication protocol from the New TTLS list.

Using RADIUS Proxy

You can configure the Infranet Controller to proxy RADIUS inner or outer authentication to an external RADIUS server.

With RADIUS proxy, the Infranet Controller RADIUS server can forward authentication requests from a network access device to an external RADIUS server. The proxy target receives the request, performs the authentication, and returns the results. The Infranet Controller RADIUS server then passes the results to the network access device.

NOTE: **When RADIUS proxy is used, realm or role restrictions cannot be enforced. Host Checker policies, source IP restrictions, and any other limits that have been assigned are bypassed. RADIUS proxy should be used only if no restrictions have been applied. The exception is that session limitations can be enforced for inner proxy. With outer proxy, no session is established.**

You configure RADIUS proxy at the realm level. If the authentication server for the realm is a RADIUS server, option buttons on the page allow you to select inner proxy, outer proxy, or do not proxy. Do not proxy is selected by default. If the authentication server is not a RADIUS server, the proxy option buttons are hidden.

If the authentication server selected for a realm is a RADIUS server, the Proxy Outer Authentication option button controls whether outer authentication is proxied, and the Proxy Inner Authentication option button controls whether inner authentication is proxied.

You can also choose the Do not proxy option button if you do not want inner or outer authentication to be proxied. In this case, the Infranet Controller handles both inner and outer authentication. You must enable the JUAC protocol for this option.

Related Documentation

- Configuring Role Mapping Rules (NSM Procedure) on page 90
- Configuring RADIUS Clients (NSM Procedure) on page 77
- Using the Infranet Controller for 802.1X Network Access (NSM Procedure) on page 75

Using the Infranet Controller for 802.1X Network Access (NSM Procedure)

The IEEE 802.1X protocol provides authenticated access to a LAN. The Infranet Controller RADIUS server can fulfill RADIUS authentication requests from RADIUS clients that support 802.1X. (If you are using an external RADIUS server for authentication, you can use the Infranet Controller RADIUS proxy feature.)

To configure the Infranet Controller as a RADIUS server for an 802.1X network access device, perform these tasks:

- Configuring Location Groups (NSM Procedure)
- Configuring RADIUS Clients (NSM Procedure)
- Configuring a New RADIUS Vendor (NSM Procedure)

- Configuring RADIUS Attributes Policies (NSM Procedure)
- Configuring an Infranet Enforcer as a RADIUS Client of the Infranet Controller (NSM Procedure)
- Non-Juniper 802.1X Supplicant Configuration Overview

Related Documentation

- Configuring Location Groups (NSM Procedure) on page 76
- Configuring RADIUS Clients (NSM Procedure) on page 77
- Configuring a New RADIUS Vendor (NSM Procedure) on page 78

Configuring Location Groups (NSM Procedure)

You can use location groups to organize or logically group network access devices by associating the devices with specific sign-in policies. Location groups associate sign-in policies with network access devices.

To configure location groups:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to configure location groups.
3. Click the **Configuration** tab. In the configuration tree, select **UAC** > **Network Access** > **Location Groups**.
4. Add or modify **Location Groups** tab as specified in Table 19 on page 76.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 19: Location Groups Configuration Details

Option	Function	Your Action
Name	Specifies the location group name.	Enter a name for the location group.
Description	Describes the location group.	Enter a brief description for the location group.
Sign-in Policy	Specifies the sign-in policy you want to associate with the location group.	Select the sign-in policy.
MAC Authentication Realm	Specifies the MAC authentication realm.	Select the MAC authentication realm.

Related Documentation

- Configuring RADIUS Clients (NSM Procedure) on page 77

- Configuring a New RADIUS Vendor (NSM Procedure) on page 78
- Configuring RADIUS Return Attributes Policies (NSM Procedure) on page 80

Configuring RADIUS Clients (NSM Procedure)

To enable the Infranet Controller to respond to a network access device, you must configure a RADIUS client in the Infranet Controller.

Configure RADIUS clients by following these procedures:

1. Uploading a New RADIUS Client Dictionary on page 77
2. Creating a RADIUS Dictionary Based on an Existing Model on page 78
3. Configuring a New RADIUS Vendor (NSM Procedure) on page 78
4. Creating a RADIUS Client on page 79

Uploading a New RADIUS Client Dictionary

To upload a new RADIUS client dictionary to the Infranet Controller:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to upload the RADIUS client dictionary.
3. Click the **Configuration** tab. In the configuration tree, select **UAC** > **Network Access** > **RADIUS Dictionary**.
4. Add or modify settings on the RADIUS Dictionary tab as specified in Table 20 on page 77.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

NOTE:

- You can only remove dictionaries that are not associated with a vendor.
- You can download any dictionary from the list, including preinstalled dictionaries. You can modify the downloaded dictionary, and then upload it as a new make or model.

Table 20: RADIUS Dictionary Configuration Details

Option	Function	Your Action
Name	Specifies the RADIUS dictionary name.	Enter a name for the RADIUS dictionary.

Table 20: RADIUS Dictionary Configuration Details *(continued)*

Option	Function	Your Action
Description	Describes the RADIUS dictionary.	Enter a brief description for the RADIUS dictionary.
Dictionary	Specifies the dictionary file (.dct) path on a local or connected drive.	Select the dictionary file.
Dictionary filename	Specifies the dictionary filename.	Enter the filename.

Creating a RADIUS Dictionary Based on an Existing Model

To create a RADIUS dictionary based on an existing manufacturer's model:

1. Modify the existing dictionary.
   a. Select the existing dictionary that you would like to copy. See "Uploading a New RADIUS Client Dictionary" on page 77.
   b. Download the file, make the required modifications, and then rename and save the .dct file.
2. Browse for the file you have modified, and enter a new name and description for the new dictionary. See "Uploading a New RADIUS Client Dictionary" on page 77.

   NOTE: **There is no vendor associated with the new dictionary.**
3. Associate the dictionary to a new RADIUS vendor. See "Configuring a New RADIUS Vendor (NSM Procedure)" on page 78.

Configuring a New RADIUS Vendor (NSM Procedure)

To configure a new RADIUS vendor:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to configure a new RADIUS vendor.
3. Click the **Configuration** tab. In the configuration tree, select **UAC** > **Network Access** > **RADIUS Vendors**.
4. Add or modify RADIUS vendors on the **RADIUS Vendors** tab as specified in Table 21 on page 79.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 21: RADIUS Vendors Configuration Details

Option	Function	Your Action
Name	Specifies a name for the RADIUS vendor.	Enter a name for the RADIUS vendor.
Description	Describes the RADIUS vendors.	Enter a brief description for the RADIUS vendor.
Dictionary	Specifies the dictionary to be associated with the RADIUS vendor.	Select the dictionary.

Creating a RADIUS Client

To create a RADIUS client:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to create a RADIUS client.
3. Click the **Configuration** tab. In the configuration tree, select **UAC** > **Network Access** > **RADIUS Clients**.
4. Add or modify RADIUS clients on the RADIUS Clients tab as specified in Table 22 on page 79.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 22: RADIUS Clients Configuration Details

Option	Function	Your Action
Name	Specifies the RADIUS client's name.	Enter a name for the RADIUS clients.
Description	Describes the RADIUS clients.	Enter a brief description for the RADIUS clients.
IP Address	Specifies the IP address of the network access device.	Enter the IP address.
IP Address Range	Specifies the number of IP addresses in the IP address range for the network access devices, starting with the address specified for IP address.	Enter the IP address range. You can specify a range up to a maximum of 32,768 addresses.

Table 22: RADIUS Clients Configuration Details *(continued)*

Option	Function	Your Action
Shared Secret	Validates communications between the Infranet Controller and network access device.	Enter the shared secret. The Infranet Controller supports shared secrets of up to 127 alphanumeric characters, including spaces and the following special characters: ~!@#$%^&*()_+|\=-‘{}[]:”’;<>?/.,
Make/Model	Specifies the dictionary of RADIUS attributes to be used by the Infranet Controller when communicating with this client.	Select the make or model.
Location Group	Specifies the location group to use with this network access device.	Select the location group.
Support Disconnect Messages	Allows the Infranet Controller to send unsolicited disconnect requests to the network access device. When a user session is deleted on the Infranet Controller, the disconnect messages cause the user’s session to be terminated immediately, and all session information is removed.	Select this option to send terminate session requests to network access devices that support RFC 3576.
Enabled	Enables the RADIUS clients.	Select this option to enable RADIUS clients.

Related Documentation

- Configuring Location Groups (NSM Procedure) on page 76
- Configuring RADIUS Return Attributes Policies (NSM Procedure) on page 80
- Configuring RADIUS Request Attributes Policies (NSM Procedure) on page 83

Configuring RADIUS Return Attributes Policies (NSM Procedure)

You can configure RADIUS attributes policies on the Infranet Controller to send return list attributes to an 802.1X network access device. You can also configure other functions on a network access device's port based on the role assigned to the user who is currently using that port.

To configure RADIUS attributes policies:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to configure RADIUS return attributes policies.

3. Click the **Configuration** tab. In the configuration tree, select **UAC** > **Network Access** > **RADIUS Attributes** > **RADIUS Return Attributes Policies**.
4. Add or modify RADIUS return attributes policies as specified in Table 23 on page 81.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 23: RADIUS Return Attributes Policies Configuration Details

Option	Function	Your Action
Name	Specifies a name for the RADIUS return attribute policy.	Enter a name for the RADIUS return attribute policy.
Description	Describes the RADIUS return attribute policy.	Enter a brief description for the RADIUS return attribute policy.
Location Group	Specifies the location groups for the RADIUS attributes policies.	Select the location group from the Non-member list and click **Add** to move them to the Members list. NOTE: To apply the policy to all location groups, do not add any location groups and leave the default setting (all) listed in the Selected Location Groups list.
Enable Open port	Disables assigning endpoints to a VLAN or returning any RADIUS attributes.	Select this option to disable all other RADIUS attributes options.
Enable VLAN	Enables VLAN assignment according to RFC 3580 by returning the RADIUS tunnel attributes to the network access device.	Select this option to configure VLAN assignment. NOTE: Selecting this option is equivalent to manually specifying the three RFC 3580 RADIUS tunnel attributes in the Enable Return Attribute section.
VLAN	Specifies the existing VLAN ID on the network infrastructure that you want to use for the role(s) to which this policy applies.	Specify the existing VLAN ID.
Enable Return Attribute	Enables the **return-attribute** option.	Select this option to enable return attributes.

Table 23: RADIUS Return Attributes Policies Configuration Details *(continued)*

Option	Function	Your Action
return-attribute	Specifies the return attributes to be sent to the network access device.	Click **return-attribute** and add the return attribute. 1. From the Attribute drop-down list, select the return attribute you want to send. 2. For Value, enter the value for the selected attribute, and then click **OK**.
Enable addition of Session-Timeout attribute with value equal to the Session Lifetime	Sends the Infranet Controller a session timeout value equal to the timeout value of the configured session length on all RADIUS accepts.	Clear this check box to prevent the Infranet Controller from sending a session timeout value equal to the timeout value of the configured session length on all RADIUS accepts. This allows you to set the reauthentication timer statically on the switch port, if required
Interface	Specifies the Infranet Controller network interface for use by endpoints using RADIUS attributes policies to connect to the Infranet Controller.	• Select **Automatic** to use VLAN tagging . You must also connect the Infranet Controller internal interface to the trunk port on a VLAN-enabled switch that sees all of the VLAN traffic. • Select **Internal** if the endpoints using RADIUS attributes policies should use the IP address of the Infranet Controller's internal interface. • Select **External** if the endpoints on the configured VLAN should use the IP address of the Infranet Controller's external interface.

Table 23: RADIUS Return Attributes Policies Configuration Details *(continued)*

Option	Function	Your Action
Applies to Roles	Specifies the roles to which the policies apply.	• Select **Policy applies to ALL roles** to apply this policy to all users. • Select **Policy applies to SELECTED roles** to apply this policy only to users who are mapped to roles in the Members list. • Select **Policy applies to all roles OTHER those selected** to apply this policy to all users except for those who map to the roles in the Members list.
Role Selection	Lists the members and non—members for applying the policy.	Select the role from the Non-members list and click **Add** to move them to the Members list.

Related Documentation

- Configuring RADIUS Request Attributes Policies (NSM Procedure) on page 83
- Configuring RADIUS Attribute Logs (NSM Procedure) on page 211
- Configuring RADIUS Clients (NSM Procedure) on page 77
- Configuring a New RADIUS Vendor (NSM Procedure) on page 78

Configuring RADIUS Request Attributes Policies (NSM Procedure)

You can configure RADIUS request attributes policies to enforce restrictions on the processing of authentication requests, which are based on the RADIUS authentication requests, before a connection can be authenticated. Then you can assign RADIUS request attributes policies as a realm restriction.

To configure RADIUS request attributes policies:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to configure RADIUS request attributes policies.
3. Click the **Configuration** tab. In the configuration tree, select **UAC** > **Network Access** > **RADIUS Attributes** > **RADIUS Request Attributes Policies**.
4. Add or modify RADIUS request attributes policies as specified in Table 24 on page 84.
5. Click one:
   - **OK**—Saves the changes.

- **Cancel**—Cancels the modifications.

Table 24: RADIUS Request Attributes Policies Configuration Details

Option	Function	Your Action
Name	Specifies a name for the RADIUS request attributes policy.	Enter a name for the RADIUS request attributes policy. You select the RADIUS request attributes policy when you create a realm.
Description	Describes the RADIUS request attributes policy.	Enter a brief description for the RADIUS request attributes policy.
request-attributes	Specifies the request attributes. Any RADIUS authentication request must contain one of the values that you define.	Click **request-attributes** and add the request attribute. 1. Click **New** (+) to add a request attribute type. The New Request Attribute page appears. 2. From the Attribute Name drop-down list, select the request attribute name. 3. From the Attribute Type drop-down list, select the request attribute type. 4. Add values that are specific to the type and name of RADIUS attribute you have selected, and then click **OK**.

Related Documentation

- Configuring RADIUS Return Attributes Policies (NSM Procedure) on page 80
- Configuring RADIUS Attribute Logs (NSM Procedure) on page 211
- Configuring RADIUS Clients (NSM Procedure) on page 77
- Configuring a New RADIUS Vendor (NSM Procedure) on page 78

Configuring an Infranet Enforcer as a RADIUS Client of the Infranet Controller (NSM Procedure)

You can use an Infranet Enforcer as an 802.1X RADIUS client of the Infranet Controller. Unlike all other network access devices, you do not configure a RADIUS client for the Infranet Enforcer. When you use the following instructions, the Infranet Controller automatically creates an internal RADIUS client for the Infranet Enforcer that you cannot change. This RADIUS client for the Infranet Enforcer is not displayed in the Infranet Controller admin console.

To use an Infranet Enforcer as an 802.1X RADIUS client of the Infranet Controller:

1. Configure a location group policy for the Infranet Enforcer:
   a. Create a sign-in policy that you want to associate with the location group. See "Configuring Sign-In Policies (NSM Procedure)."
   b. Create a location group and select the sign-in policy you want to associate with the location group. See "Configuring Location Groups (NSM Procedure)."
2. Associate the location group with the Infranet Enforcer:
   a. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to use the Infranet Enforcer as a RADIUS Client.
   b. Click the **Configuration** tab. In the configuration tree, select **UAC** > **Infranet Enforcer** > **Connection**.
   c. Select an existing Infranet Enforcer connection and click the **Edit** button.
   d. Select the location group that you want to associate with the Infranet Enforcer.
   e. Click one:
      - **OK**—Saves the changes.
      - **Cancel**—Cancels the modifications.
3. Configure authenticated endpoints to connect to the Infranet Controller, and specify VLANs in RADIUS attributes policies. See "Configuring RADIUS Attributes Policies (NSM Procedure)."

Related Documentation

- Configuring Location Groups (NSM Procedure) on page 76
- Configuring RADIUS Clients (NSM Procedure) on page 77
- Configuring a New RADIUS Vendor (NSM Procedure) on page 78

Non-Juniper 802.1X Supplicant Configuration Overview

You can configure users to authenticate to the Infranet Controller using Odyssey Access Client, or you can use a non-Juniper 802.1X supplicant. Odyssey Access Client is preconfigured with standard protocols to work with the Infranet Controller. To use a non-Juniper supplicant, you must configure the authentication protocols manually. A non-Juniper supplicant is any client that is configured without the JUAC protocol.

To configure a non-Juniper supplicant:

1. Configure authentication protocols on the third-party supplicant per the instructions in the vendor's documentation.
2. Configure corresponding protocols on the Infranet Controller. See "Configuring Authentication Protocol Sets (NSM Procedure)."

3. Install the certificate from the CA that the Infranet Controller is using for trusted Client CAs.
4. Configure a Certificate Server. See “Configuring an Infranet Controller Certificate Server Instance (NSM Procedure).”
5. Create a role for the user(s) that will access the Infranet Controller using a non- Juniper supplicant. See “Configuring Infranet Controller User Roles (NSM Procedure).”
6. Create a realm for the endpoint. See “Creating an Authentication Realm (NSM Procedure).”
7. Create a new sign-in policy. See “Configuring Infranet Controller Sign-in Policies (NSM Procedure).”
8. Configure a new location group. See “Configuring Location Groups (NSM Procedure).”
9. Create a new RADIUS client. See “Configuring RADIUS Clients (NSM Procedure).”
10. Create a role for endpoints using the third-party supplicant. See “Configuring Infranet Controller User Roles (NSM Procedure).”
11. Configure a RADIUS attributes policy. See “Configuring RADIUS Attributes Policies (NSM Procedure).”
12. Complete the remaining steps in “Using the Infranet Controller for 802.1X Network Access (NSM Procedure).”

Related Documentation

- Configuring Location Groups (NSM Procedure) on page 76
- Configuring RADIUS Clients (NSM Procedure) on page 77
- Configuring a New RADIUS Vendor (NSM Procedure) on page 78

CHAPTER 9

Configuring Authentication Realms

Creating an Authentication Realm (NSM Procedure)

To create an authentication realm:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to create an authentication realm.
3. Click the **Configuration** tab. In the configuration tree, select **Administrators** > **Admin Realms** or **Users** > **User Realms**.
4. Add or modify settings on the General tab as specified in Table 25 on page 87.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 25: Authentication Realms Configuration Details

Option	Function	Your Action
Realm Name	Specifies a unique name for the authentication realm.	Enter the name.
Description	Describes the authentication realm.	Enter a brief description for the authentication protocol.
When editing, start on the Role Mapping page	Specifies whether the Role Mapping tab should be selected when you open the realm for editing.	Select this option to start editing on the Role Mapping page.

Table 25: Authentication Realms Configuration Details *(continued)*

Option	Function	Your Action
Authentication	Indicates the authentication server for authenticating the users who sign in to this realm.	Select the authentication. NOTE: The Infranet Controller supports RADIUS proxy for both inner and outer authentication. RADIUS proxy allows you to use an external RADIUS server for authentication. If the authentication server for a realm is a RADIUS server, three option buttons are visible: Proxy RADIUS Inner Authentication, Proxy RADIUS Outer Authentication, and Do not proxy. If the authentication server is not a RADIUS server, the proxy check boxes are hidden. See "Using RADIUS Proxy." When RADIUS proxy is used, realm or role restrictions cannot be enforced. Host Checker policies, source IP restrictions, and any other limits that have been assigned are bypassed. RADIUS proxy should be used only if no restrictions have been applied.
Directory/Attribute	Specifies the directory or attribute server to use.	Select this option to specify which directory or attribute server to use.
Accounting	Specifies the RADIUS accounting server to use.	Select this option to specify which RADIUS accounting server to use. NOTE: If the LDAP server is down, user authentication fails. You can find messages and warnings in the event log files. When an attribute server is down, user authentication does not fail. Instead, the groups or attributes list for role mapping and policy evaluation is empty.

Table 25: Authentication Realms Configuration Details *(continued)*

Option	Function	Your Action
Enable Dynamic policy evaluation	Enables an automatic timer for dynamic policy evaluation of this realm's authentication policy, role mapping rules, and role restrictions.	Select this option to enable dynamic policy evaluation. NOTE: If you select **Dynamic policy evaluation** and you do not select Refresh roles and Refresh resource policies, the Infranet Controller evaluates the realm's authentication policy, role mapping rules, and role restrictions only. Because dynamic policy evaluation can potentially impact system performance, keep these guidelines in mind: • Automatic (timer-based) refreshing of user roles and resource policies can affect system performance. You can improve performance by disabling either or both of the Refresh roles and Refresh resource policies options to reduce the scope of the refresh. • You can improve performance, by setting the Refresh interval option to a longer time period. • Use the Refresh Now button at times when users may not be affected.
Refresh roles	Refreshes the roles of all users in this realm. (This option does not control the scope of the Refresh Now button.)	Select this option to refresh roles.
Refresh policies	Refreshes the resource policies (not including Meeting and Email Client) for all users in this realm. (This option does not control the scope of the Refresh Now button.)	Select this option refresh policies.
Refresh interval (minutes)	Specifies how often you want the Infranet Controller to perform an automatic policy evaluation of all currently signed-in realm users. Specify the number of minutes (5 to 1440).	Enter the frequency in minutes.

Related Documentation

- Configuring Role Mapping Rules (NSM Procedure) on page 90
- Configuring Infranet Controller Source IP Access Restrictions (NSM Procedure) on page 61

- Configuring Infranet Controller RADIUS Request Attribute Restrictions for User Realms (NSM Procedure) on page 69

Configuring Role Mapping Rules (NSM Procedure)

You create a role mapping rule on the Role Mapping tab of an authentication realm. (For administrators, to create role mapping rules, select **Administrators** > **Admin Realms** > *Realm* > **Role Mapping** . For users, select **Users** > **User Realms** > *Realm* > **Role Mapping**.) When you click **New Rule** on the Role Mapping tab, the Role Mapping Rule page appears with an inline editor for defining the rule.

To specify role mapping rules for an authentication realm:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to configure role mapping rules.
3. Click the **Configuration** tab. In the configuration tree, select **Administrators** > **Admin Realms** or **Users** > **User Realms**.
4. Add or modify settings on the **Role Mapping Rules** tab as specified in Table 26 on page 90.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 26: Role Mapping Rules Configuration Details

Option	Function	Your Action
Name	Specifies the rule name.	Enter the name.
Assign these roles if the rule matches	Specifies the list of eligible roles that matches the rule.	Select the role from the Non-members list, and click **Add** to move them to the members list.
Stop processing rules when this rule matches	Stops evaluating role mapping rules if the user meets the conditions specified for this rule.	Select this option to stop evaluating role mapping rules when specific conditions are met.

Table 26: Role Mapping Rules Configuration Details *(continued)*

Option	Function	Your Action
Role mapping rule type	Specifies the parameters based on which the role mapping is created.	• Select **If user name** if the role mapping parameter must be based on the user name. Select **is/is not** conditional expressions for the rule, click the **Add** button, and enter the new user names. • Select **If certificate has any of the attributes** if the role mapping parameter must be based on the certificate attributes. Select **is/is not** conditional expressions for the rule, click the **Add** button, and enter the new values. • Select **If user has any of these custom expressions** if the role mapping parameter must be based on the custom expressions. The collection-of-expressions button appears. 1. Click the **collection-of-expressions** button to assign expressions. The expressions that were created for the selected authentication server appears. 2. Select an existing expression from the Non-members area and click **Add** to assign the expression to the role-mapping rule. 3. Click **New** (+) and create an expression to assign a new expression to the role-mapping rule. For information on creating custom expressions and using the Expression Dictionary, refer to "Creating a Custom Expression for an Authentication Server (NSM Procedure)." NOTE: You can create a custom expression in a device template, but you cannot validate the custom expression. The Validate button is not enabled in the Custom Expressions editor for device templates.
is/is not	Specifies the conditional expression used in the rule.	Select this option to specify conditional expression.
User must select from among assigned roles	Specifies that the rule is based on assigned roles.	Select this option to specify that the rule is based on assigned roles.
User must select the sets of merged roles assigned by each rule	Specifies that the rule is based on sets of merged roles.	Select this option to specify that the rule is based on sets of merged roles.

Related Documentation

- Creating an Authentication Realm (NSM Procedure) on page 87

- Configuring Infranet Controller Authentication Policies (NSM Procedure) on page 92
- Configuring Infranet Controller RADIUS Request Attribute Restrictions for User Realms (NSM Procedure) on page 69

Configuring Infranet Controller Authentication Policies (NSM Procedure)

An authentication policy is a set of rules that controls one aspect of access management—whether or not to present a realm's sign-in page to a user. An authentication policy is part of an authentication realm's configuration, specifying rules for the Infranet Controller to consider before presenting a sign-in page to a user. If a user meets the requirements specified by the realm's authentication policy, then the Infranet Controller presents the corresponding sign-in page to the user and forwards the user's credentials to the appropriate authentication server. If this server successfully authenticates the user, then the Infranet Controller moves on to the role evaluation process.

To configure an authentication realm policy:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to configure an authentication realm policy.
3. Click the **Configuration** tab. In the configuration tree, select **Administrators** > **Admin Realms** or **Users** > **User Realms**.
4. Add or modify authentication realm policy settings in the Authentication Policies tab for one or more of the access management options.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Related Documentation

- Configuring Infranet Controller Source IP Access Restrictions (NSM Procedure) on page 61
- Configuring Infranet Controller Browser Access Restrictions (NSM Procedure) on page 63
- Configuring Infranet Controller Certificate Access Restrictions (NSM Procedure) on page 64
- Configuring Infranet Controller Host Checker Access Restrictions (NSM Procedure) on page 67
- Configuring the Number of Concurrent Sessions and Concurrent Users for Infranet Controller Users (NSM Procedure) on page 70
- Configuring Infranet Controller RADIUS Request Attribute Restrictions for User Realms (NSM Procedure) on page 69

CHAPTER 10

Configuring Infranet Enforcer Policies

Configuring Infranet Enforcer Resource Access Policies (NSM Procedure)

An Infranet Enforcer resource access policy specifies which users are allowed or denied access to a set of protected resources.

To configure Infranet Enforcer resource access policies:

1. In the NSM navigation tree, select **Device Manager**> **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure Infranet Enforcer resource access policies.
3. Click the **Configuration** tab. In the configuration tree, select **UAC > Infranet Enforcer > Resource** tab.
4. Add or modify settings for resource access policies as specified in Table 27 on page 93.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 27: Resource Access Policies Configuration Details

Option	Function	Your Action
Name	Specifies the resource access policy name.	Enter a name for the resource access policy.

Table 27: Resource Access Policies Configuration Details *(continued)*

Option	Function	Your Action
Description	Describes the resource access policy.	Enter a brief description for the resource access policy.
Resources	Specifies the protocol, IP address, network mask, and port of each resource for which this Infranet Enforcer resource access policy applies.	Enter the protocol, IP address, network mask, and port of each resource (or range of addresses) for which this Infranet Enforcer resource access policy applies, one per line. Do not insert any spaces in your entries. If you insert spaces, the policy may not be applied correctly.
Applies to roles	Specifies the roles to which this policy is applicable.	• Select **Policy applies to ALL roles** to apply this Infranet Enforcer resource access policy to all users. • Select **Policy applies to SELECTED roles** to apply this Infranet Enforcer resource access policy only to users who are mapped to roles in the Selected roles list. • Select **Policy applies to all roles OTHER THAN those selected** to apply this Infranet Enforcer resource access policy to all users except those who map to the roles in the Selected roles list. NOTE: Select the policies from the Non-members list and click **Add** to move it to the Members list before applying the policies to the roles.
Action	Specifies whether this Infranet Enforcer resource access policy should allow or deny access to the specified resources.	• Select **Allow access** to allow access to the specified resources. • Select **Deny access** to deny access to the specified resources. NOTE: If you choose to deny access, a text box appears that allows you to customize the message for users. If you want to record deny actions in the User Access Log, select the **Enforcer Deny Messages** check box on the Log/monitoring > User Access > Settings page. The log records the user, source IP, destination IP, protocol, and destination port.

Table 27: Resource Access Policies Configuration Details *(continued)*

Option	Function	Your Action
Applies to Enforcer options	Specifies the Enforcer options to which the policy is applicable.	Select **Enforcer Option** to select the Enforcer policy options that you want to apply to selected roles. NOTE: By default, all policy options are enabled on the Infranet Controller. To enforce the policies, you must create corresponding policies on the Infranet Enforcer. If the Infranet Controller is upgraded from a previous version, all enforcer options are enabled for all of the resource access policies that were available prior to the upgrade. • Select **All Enforcer Options** to apply to all enforcer options in the Enforcer Option dialog box. • Select **SELECTED Enforcer Options** to apply only the selected enforcer options from the Enforcer Option dialog box. • Select **Enforcer options OTHER THAN those selected** to apply to the enforcer options that are not selected in the Enforcer Option dialog box.
ScreenOS VSYS	Specifies the name of the VSYS created on the ScreenOS enforcer.	Enter the name of the VSYS, if you had created a VSYS on a ScreenOS Enforcer.

Related Documentation

- Configuring Infranet Controller IPsec Routing Policies (NSM Procedure) on page 95
- Configuring Infranet Controller IP Address Pool Policies (NSM Procedure) on page 98

Configuring Infranet Controller IPsec Routing Policies (NSM Procedure)

An IPsec routing policy specifies the Infranet Enforcer device that endpoints must use to access resources when using IPsec. The IPsec routing policy also specifies that endpoints must use an IPsec tunnel to the Infranet Enforcer to access resources.

To configure an IPsec routing policy:

1. In the NSM navigation tree, select **Device Manager**> **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure IPsec routing policies.
3. Click the **Configuration** tab. In the configuration tree, select **UAC > Infranet Enforcer > IPsec Routing**.

4. Add or modify IPsec routing policy settings as specified in Table 28 on page 96.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 28: IPsec Routing Policies Configuration Details

Option	Function	Your Action
Name	Specifies the IPsec routing policy name.	Enter a name for the IPsec routing policy.
Description	Describes the IPsec routing policy.	Enter a brief description for the IPsec routing policy.
Resource Type	Specifies whether the Infranet Controller dynamically provisions or manually provisions the IPsec routing policy.	• Select **Manual**— if you are using ScreenOS version 6.1 or earlier. • Select **Dynamic**—if you are using ScreenOS version 6.1 or later.
Set Resources	Specifies the IP address and netmask of each resource that requires endpoints to use IPsec.	• Click **Set Resources**. The Set Resources dialog box appears. Select **Resources** and enter new resources one per line in the following format: <ip address>[/netmask] • Click **Set Resources > Exceptions** and enter new exceptions one per line in the following format: <ip address>[/netmask]
Enforcer	Specifies the Infranet Enforcer to which endpoints connect to access the resources specified in this IPsec routing policy.	Select the Infranet Enforcer.
Destination Zone	Specifies the destination zone where the protected resources specified in this IPsec routing policy are located. This destination zone is configured on the Infranet Controller.	Enter the destination zone that is configured on the Infranet Enforcer. For example: enter **trust**.

Table 28: IPsec Routing Policies Configuration Details *(continued)*

Option	Function	Your Action
Always use UDP Encapsulation	Allows the Odyssey Access Client and the Infranet Enforcer to create an IPsec tunnel inside a third-party IPsec tunnel by using UDP encapsulation even if a NAT device is not present.	Select this check box.
Always use a virtual adapter	Forces the use of a virtual adapter on the endpoint. If you select this option, you must also set up IP address pools even if a NAT device is not present.	Select this check box.
Persistent Tunnel Mode	Allows you to determine whether or not a tunnel is established when a user first connects to the Infranet Controller. If the check box is selected, an IPsec tunnel is established, and users can access protected resources behind the Infranet Enforcer. If the check box is not selected, the tunnel is not automatically set up: a tunnel will not be initiated until there is a request for traffic.	Select this check box.
Applies to roles	Specifies the policies that apply to the roles.	• Select **Policy applies to ALL roles** to apply this Infranet Controller IPsec routing policy to all users. • Select **Policy applies to SELECTED roles** to apply this Infranet Controller IPsec routing policy only to users who are mapped to roles in the Selected roles list. • Select **Policy applies to roles OTHER THAN those selected** to apply this Infranet Controller IPsec routing policy to all users except those who map to the roles in the Selected roles list. NOTE: Select the policies from the Non-members list and click **Add** to move it to the Members list before applying the policies to the roles.

Related Documentation

- Configuring Infranet Controller IP Address Pool Policies (NSM Procedure) on page 98
- Configuring Infranet Enforcer Resource Access Policies (NSM Procedure) on page 93

Configuring Infranet Controller IP Address Pool Policies (NSM Procedure)

You can configure a pool of virtual IP addresses that you want the Infranet Controller to automatically assign to endpoints by creating IP address pool policies. You can associate an IP address pool with one or more Infranet Enforcers.

To configure an IP address pool policy:

1. In the NSM navigation tree, select **Device Manager**> **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure an IP address pool policy.
3. Click the **Configuration** tab. In the configuration tree, select **UAC > Infranet Enforcer > IP Address Pools**.
4. Add or modify IP address pool policy settings as specified in Table 29 on page 98. Table 30 on page 99 gives the syntax for IP address pools.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 29: IP Address Pool Policy Configuration Details

Option	Function	Your Action
Name	Specifies the IP address pool policy name.	Enter a name for the IP address pool policy.
Description	Describes the IP address pool policy.	Enter a brief description for the IP address pool policy.
IP Address Pool	Specifies IP addresses or a range of IP addresses for the Infranet Controller to assign to endpoints.	Click the **Add** button and enter the IP address range as specified in Table 30 on page 99, where the last component of the IP address is a range delimited by a hyphen (-). No special characters are allowed. For example, to allocate all addresses in the range 172.20.0.0 through 172.20.3.255, enter **172.20.0.0-3.255**. To allocate all addresses in a class C network, specify 10.20.30.0/24. NOTE: Select the Infranet Enforcer(s) to which you want to apply this IP address pool policy from the Non-members list and click **Add** to move it to the Members list. To apply the policy to all Infranet Enforcers, do not add any Infranet Enforcers and leave the default setting **(all)**.

Table 29: IP Address Pool Policy Configuration Details *(continued)*

Option	Function	Your Action
Applies to roles	Specifies the policies that apply to the roles.	• Select **Policy applies to ALL roles** to apply this Infranet Controller IP address pool policy to all users. • Select **Policy applies to SELECTED roles** to apply this Infranet Controller IP address pool policy only to users who are mapped to roles in the Members list. • Select **Policy applies to roles OTHER THAN those selected** to apply this Infranet Controller IP address pool policy to all users except those who map to the roles in the Members list. NOTE: Select the policies from the Non-members list and click **Add** to move it to the Members list before applying the policies to the roles.

Table 30: Syntax for IP Address Pools

IP Address Range	Description
a.b.c.d	Specifies a single IP address.
a.b.c.d-e.f.g.h	Specifies all IP addresses from the first address to the last address, inclusive.
a.b.c.d-f.g.h	Specifies the range a.b.c.d through a.f.g.h.
a.b.c.d-g.h	Specifies the range a.b.c.d through a.b.g.h.
a.b.c.d-h	Specifies the range a.b.c.d through a.b.c.h.
a.b.c.d/mask	Specifies all addresses in a network.

Related Documentation

- Configuring Infranet Controller IPsec Routing Policies (NSM Procedure) on page 95
- Configuring Infranet Enforcer Resource Access Policies (NSM Procedure) on page 93

Configuring Infranet Controller Source Interface Policies (NSM Procedure)

A source interface policy specifies the source interface on the Infranet Enforcer that receives traffic from endpoints. The use cases for configuring source interface policies are limited.

You will need to use a source interface policy if you have multiple virtual routers, and you have an IPsec routing policy with destination zone DEST, and one of the following is true:

- There are multiple IPsec policies on the enforcer with a destination zone DEST and different source zones.
- There is an IPsec policy on the enforcer with a destination zone DEST whose source zone has multiple interfaces.

To configure a source interface policy:

1. In the NSM navigation tree, select **Device Manager**> **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure a source interface policy.
3. Click the **Configuration** tab. In the configuration tree, select **UAC > Infranet Enforcer > Source Interface**.
4. Add or modify source interface policy settings as specified in Table 31 on page 100.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 31: Source Interface Policy Configuration Details

Option	Function	Your Action
Name	Specifies the source interface policy name.	Enter a name for the source interface policy.
Description	Describes the source interface policy.	Enter a brief description for the source interface policy.
Enforcer	Specifies the Infranet Enforcer to which the endpoints connect.	Select the Infranet Enforcer.
Source Interface	Specifies the interface on the Infranet Enforcer to which traffic from endpoints connects.	Specify the interface. To view the zone table on the Infranet Enforcer, enter the following command: **get zone**

Table 31: Source Interface Policy Configuration Details *(continued)*

Option	Function	Your Action
Applies to roles	Specifies the policies that apply to the roles.	• Select **Policy applies to ALL roles** to apply this Source Interface policy to all users. • Select **Policy applies to SELECTED roles** to apply this Source Interface policy only to users who are mapped to roles in the Members list. • Select **Policy applies to roles OTHER THAN those selected** to apply this Source Interface policy to all users except those who map to the roles in the Members list. NOTE: Select the policies from the Non-members list and click **Add** to move it to the Members list before applying the policies to the roles.

Related Documentation

- Configuring Infranet Controller Source IP Access Restrictions (NSM Procedure) on page 61
- Configuring Infranet Controller Host Enforcer Policies (NSM Procedure) on page 105

Configuring an Infranet Controller to Connect to a ScreenOS Enforcer (NSM Procedure)

The ScreenOS Enforcer connects to the Infranet Controller over an SSH connection that uses the NetScreen Address Change Notification (NACN) protocol.

The Infranet Controller uses the NACN password and serial number for a connection from the ScreenOS Enforcer. When the ScreenOS Enforcer first turns on, it sends an NACN message containing the NACN password and serial number to the Infranet Controller. The Infranet Controller uses the serial number to determine which ScreenOS Enforcer is attempting to connect, and then the Infranet Controller uses the NACN password to authenticate the ScreenOS Enforcer. The Infranet Controller then begins communicating with the ScreenOS Enforcer using SSH.

To configure the Infranet Controller to accept a connection from the ScreenOS Enforcer:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller that you want to configure.
3. Click the **Configuration** tab. In the configuration tree, select **UAC > Infranet Enforcer > Connection**.
4. Click **New** (+). The New Infranet Enforcer dialog box appears.
5. Select the **ScreenOS** option button from the Platform area. The ScreenOS Enforcer page appears.

6. Enter a name for the ScreenOS Enforcer.
7. Enter an NACN password for this Infranet Enforcer in the NACN password box. You must enter this same NACN password when configuring the ScreenOS Enforcer.
8. Enter the administrator name and administrator password for signing into the ScreenOS Enforcer.
9. Enter the serial number(s) of the ScreenOS Enforcer. You can view the serial number on the home page of the Infranet Enforcer WebUI, or by entering the following Juniper Networks ScreenOS CLI command:

   get system

10. To configure ISG-IDP, select **Use IDP Module**.

NOTE: **For the Infranet Controller to interoperate with IDP, the ic-xxxx-ADD-tctrl coordinated threat control license is required.**

11. Select **No 802.1X** from the Location Group list if you are not using an Infranet Enforcer as an 802.1X RADIUS client of the Infranet Controller.
12. Click one:
    - **OK**—Saves the changes.
    - **Cancel**—Cancels the modifications.

Related Documentation

- Configuring an Infranet Enforcer as a RADIUS Client of the Infranet Controller (NSM Procedure) on page 84
- Configuring an Infranet Controller to Connect to a JUNOS Enforcer (NSM Procedure) on page 102
- Configuring Infranet Controller Source IP Access Restrictions (NSM Procedure) on page 61
- Configuring Infranet Controller Host Enforcer Policies (NSM Procedure) on page 105

Configuring an Infranet Controller to Connect to a JUNOS Enforcer (NSM Procedure)

You can use a JUNOS Enforcer with the UAC solution. A JUNOS Enforcer is a J Series Services Router or an SRX Series Services Gateway configured as a Layer 3 enforcement point. See the Unified Access Control Supported Platforms document for compatibility. The JUNOS Enforcer connects with the Infranet Enforcer over an SSL connection. To initiate the connection between the two appliances, you must specify the password and serial number of the JUNOS Enforcer.

To configure the Infranet Controller to accept a connection from the JUNOS Enforcer:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller that you want to configure.
3. Click the **Configuration** tab. In the configuration tree, select **UAC > Infranet Enforcer > Connection**.
4. Click **New** (+). The New Infranet Enforcer dialog box appears. By default, the ScreenOS Enforcer options are displayed.
5. Select the **JUNOS** option button. The JUNOS Enforcer page appears.
6. Enter the name and password of the Infranet Enforcer.
7. Enter the serial number(s) of the JUNOS Enforcer. You can view the serial number on the JUNOS Enforcer using the command:

   show chassis hardware

8. To configure IDP, select **Use IDP Module**. For more information on configuring ISG-IDP on a enforcer, refer to "Configuring ISG-IDP as a Sensor on the Infranet Controller (NSM Procedure)" on page 193.

   

   NOTE: **For the Infranet Controller to interoperate with IDP, the ic-xxxx-ADD-tctrl coordinated threat control license is required.**

9. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Related Documentation

- Configuring an Infranet Controller to Connect to a ScreenOS Enforcer (NSM Procedure) on page 101
- Configuring Infranet Controller Source IP Access Restrictions (NSM Procedure) on page 61
- Configuring Infranet Controller Host Enforcer Policies (NSM Procedure) on page 105

CHAPTER 11

Configuring Host Enforcer Policies

Configuring Infranet Controller Host Enforcer Policies (NSM Procedure)

Host Enforcer is a stateful packet filter that is built into the Odyssey Access Client. You configure Host Enforcer policies on the Infranet Controller.

To configure a Host Enforcer policy:

1. In the NSM navigation tree, select **Device Manager**> **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure a Host Enforcer policy.
3. Click the **Configuration** tab. In the configuration tree, select **UAC > Host Enforcer**.
4. Add or modify Host Enforcer policy settings as specified in Table 32 on page 105. Table 33 on page 106 gives examples of specifying for a Host Enforcer policy.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 32: Host Enforcer Policy Configuration Details

Option	Function	Your Action
Name	Specifies the Host Enforcer policy name.	Enter a name for the Host Enforcer policy.
Description	Describes the Host Enforcer policy.	Enter a brief description for the Host Enforcer policy.
collection-of-resources	Specifies the traffic you want to allow or deny on the endpoints.	Click **collection-of-resources** and add or modify resources, one rule per line using the following syntax: [<protocol>'://']<host>['/'<net-mask>]':'<DestinationPorts>[{{':'<SourcePorts>]

Table 32: Host Enforcer Policy Configuration Details *(continued)*

Option	Function	Your Action
Applies to roles	Specifies the roles to which this policy is applicable.	• Select **Policy applies to ALL roles** to apply the Host Enforcer policy to all users. • Select **Policy applies to SELECTED roles** to apply the Host Enforcer policy only to users who are mapped to roles in the Members list. • Select **Policy applies to roles OTHER THAN those selected** to apply the Host Enforcer policy to all users except those who map to the roles in the Members list. NOTE: Select the policies from the Non-members list and click **Add** to move it to the Members list before applying the policies to the roles.
Action	Specifies whether you want this policy to allow or deny the traffic you specified for resources. For example, you can create a policy that denies outgoing TCP traffic for a particular role.	Select this option.

Table 33: Examples of Specifying Resources in a Host Enforcer Policy

Specify This Protocol	To Allow
tcp_out://*:21,80,443	Outgoing TCP traffic on ports 21, 80, and 443 only.
tcp_in://10.11.0.0/255.255.0.0:*:20	Incoming FTP traffic from 10.11.0.0/255.255.0.0 on FTP server port 20 to all ports on the endpoint.
udp_in://*:*	Incoming UDP traffic from all IP addresses to all ports on the endpoint.
icmp://*:*	Incoming and outgoing ICMP traffic from all IP addresses to all ports on the endpoint.

Related Documentation

- Configuring Infranet Enforcer Resource Access Policies (NSM Procedure) on page 93
- Configuring Infranet Controller IP Address Pool Policies (NSM Procedure) on page 98
- Configuring Infranet Controller IPsec Routing Policies (NSM Procedure) on page 95

CHAPTER 12

Configuring IF-MAP Federation Settings

Configuring IF-MAP Server Settings on the Infranet Controller (NSM Procedure)

You must add all IF-MAP clients to the Infranet Controller IF-MAP server to permit the server to communicate with its clients. To add clients, you must specify the IP address and the security mechanism and credentials for each client.

An IF-MAP server certificate must also be installed on the IF-MAP server. The client verifies the server certificate when it connects to the server. The server certificate must be signed by a certificate authority (CA), the client must be configured to trust certificates signed by that CA, and the hostname in the server certificate must match the hostname in the IF-MAP URL on the client.

To configure IF-MAP server settings on the Infranet Controller that will be the IF-MAP server:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure IF-MAP server settings.
3. Click the **Configuration** tab. In the configuration tree, select **System > IF–MAP Federation > Overview**.
4. From the IF-MAP Configuration list, select **IF-MAP Server**.
5. Click the **OK** button to save the changes.
6. From the This Server tab, select **Clients and Replicas** and click the **New** button.

7. Enter a name and an optional description for this client.
8. From the Type list, select **Client**.
9. Type one or more IP addresses of the client. If the client is multihomed, for best results list all of its physical network interfaces. If the client is an Infranet Controller or Secure Access cluster, list the internal and external network interfaces of all nodes. It is necessary to enter all of the IP addresses for all of the interfaces because equipment failures may cause traffic between the IF-MAP client and the IF-MAP server to be rerouted through a different network interface. Listing all of the IP addresses maximizes the probability that IF-MAP Federation still works in the event of a failure.
10. Under Authentication Type, select the Client Authentication Method: **Basic** or **Certificate**.
    - If you select **Basic**, enter a username and password. The same information should be added to the IF-MAP server.
    - If you select **Certificate**, choose which CA to use to verify the certificate for this client. Optionally, specify certificate attributes or restrictions to require values for certain client certificate attributes.
11. Click **OK** to save the IF-MAP client instance on the IF-MAP server.

Related Documentation

- Configuring IF-MAP Client Settings on the Infranet Controller (NSM Procedure) on page 108
- Configuring IF-MAP Session Export Policy on the Infranet Controller (NSM Procedure) on page 109
- Configuring IF-MAP Session Import Policy on the Infranet Controller (NSM Procedure) on page 112
- Configuring IF-MAP Server Replicas (NSM Procedure) on page 114

Configuring IF-MAP Client Settings on the Infranet Controller (NSM Procedure)

You must identify the IF-MAP server to each Infranet Controller and SA appliance IF-MAP client. To add the server, you specify the IF-MAP URL of the server and how to authenticate to the server. Match the URL and security settings to equal those on the IF-MAP server(s) to which the IF-MAP client will connect.

To configure IF-MAP client settings on the Infranet Controllers or SA appliances that will be IF-MAP clients:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure IF-MAP client settings.
3. Click the **Configuration** tab. In the configuration tree, select **System > IF–MAP Federation > Overview**.
4. From the IF-MAP Configuration list, select **IF-MAP Client**.

5. Type the server URL for the IF-MAP Web service on the IF-MAP server. For a Juniper IF-MAP server, use:

   https://<FQDN>/dana-ws/soap/dsifmap

   FQDN is the fully qualified domain name of the replica's internal or external interface; for a cluster, the FQDN of the internal or external VIP should be used.

6. Under Authentication Type, select the Client Authentication Method: **Basic** or **Certificate**.

   - If you select **Basic**, enter a username and password. The same information should be added to the IF-MAP server.
   - If you select **Certificate**, select the device certificate to use.
   - Ensure that the certificate of the CA that signed the IF-MAP server certificate is added from the System > Configuration > Certificates > Trusted Server CAs page.

     The IF-MAP client validates the IF-MAP server certificate: if validation fails, the connection fails. Ensure that the hostname in the IF-MAP URL on the client machine matches the hostname of the server certificate on the IF-MAP server, and that the CA that signed the server certificate is configured as a trusted server CA on the IF-MAP client.

7. Click **OK** to save the changes.

Related Documentation

- Configuring IF-MAP Server Settings on the Infranet Controller (NSM Procedure) on page 107
- Configuring IF-MAP Session Export Policy on the Infranet Controller (NSM Procedure) on page 109
- Configuring IF-MAP Session Import Policy on the Infranet Controller (NSM Procedure) on page 112
- Configuring IF-MAP Server Replicas (NSM Procedure) on page 114

Configuring IF-MAP Session Export Policy on the Infranet Controller (NSM Procedure)

Session-export policies determine how users are identified on the IF-MAP server when their session is published through IF-MAP. The session-export policy sets the IF-MAP identity.

To configure a session-export policy:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure a session-export policy.
3. Click the **Configuration** tab. In the configuration tree, select **System > IF–MAP Federation > Session-Export Policies**.

4. Add or modify settings as specified in Table 34 on page 110.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

You must create corresponding session-import policies that allow IF-MAP client Infranet Controllers that are connected to an Infranet Enforcer in front of protected resources to collect IF-MAP data from the IF-MAP server.

Table 34: IF–MAP Session-Export Policy Configuration Details

Option	Function	Your Action
Name	Specifies a unique name for the policy.	Enter a name for the policy.
Description	Describes the policy.	Enter a brief description for the policy.
Administrative Domain	Identifies the IP address, username, or MAC address data. In a large network environment with several domains, a username, an IP address, or a MAC address could be duplicated. By entering the domain, you ensure that the correct user is identified.	Type the administrative domain for the session export policy. If you want different aspects of a user session to be exported with different administrative domains, you then create several export rules.
Roles	Determines the roles for which this policy should apply.	Select roles from the Non-members area and add the roles to the Members area.
Stop on match	Stops matching the roles when an IF-MAP client has successfully matched the roles selected for this policy to roles based on session-import policies configured on the target device.	Select this option to stop matching roles after a successful match is found.
Identity tab		

Table 34: IF–MAP Session-Export Policy Configuration Details *(continued)*

Option	Function	Your Action
Set IF-MAP Identity	Specifies the applicable identity.	Select this action and the identity options appear. • **Identity**—Enter the identity name. Identity is normally specified as <Name>, which assigns the user's login name. Any combination of literal text and context variables may be specified. • **Identity Type**—Select the identity type. If you choose **Other** for Identity Type, enter a unique identity type in the text box.
Roles tab		
Set IF-MAP Roles	Specifies the applicable roles.	Select this action and the following role options appear. • **Copy matching roles**—Select this option to copy all of the user roles that match the roles specified in the Roles section of this policy into the IF-MAP roles data. • **Copy ALL roles**—Select this option to copy all of the roles from the user session to the IF-MAP capabilities data. • **Set roles specified below**—Select this option to set the specified roles. The Roles option appears. From Roles, click **New** and enter a specified role.
Capabilities tab		
Set IF-MAP Capabilities	Specifies the applicable roles.	Select this action. When you select this action and the following role options appear. • **Copy matching roles**—Select this option to copy all of the user roles that match the roles specified in the Roles section of this policy into the IF-MAP capabilities data. • **Copy ALL roles**—Select this option to copy all of the roles from the user session to the IF-MAP roles data. • **Set capabilities specified below**—Select this option to set the specified capabilities. The Capabilities option appears. From Capabilities, click **New** and enter a specified capability.
Device Attributes tab		

Table 34: IF–MAP Session-Export Policy Configuration Details *(continued)*

Option	Function	Your Action
Set IF-MAP Device Attributes	Specifies a passed Host Checker policy on the Infranet Controller or SA appliance.	Select this action and the following options appear. • **Copy Host Checker policy names**—Select this option to copy the name of each Host Checker policy that passed for the session to a device attribute. • **Set device attributes specified below**—Select this option to set the specified device attributes. The Device Attributes option appears. From Device Attributes, click **New** and enter a specified device attribute.

Related Documentation

- Configuring IF-MAP Client Settings on the Infranet Controller (NSM Procedure) on page 108
- Configuring IF-MAP Server Settings on the Infranet Controller (NSM Procedure) on page 107
- Configuring IF-MAP Session Import Policy on the Infranet Controller (NSM Procedure) on page 112
- Configuring IF-MAP Server Replicas (NSM Procedure) on page 114

Configuring IF-MAP Session Import Policy on the Infranet Controller (NSM Procedure)

The session-export policies that you create allow IF-MAP data that represents a session to be stored on the IF-MAP server. Session-import policies specify how the Infranet Controller derives a set of roles and a username from the IF-MAP data in the IF-MAP server. Session-import policies establish rules for importing user sessions from a different Infranet Controller or SA appliance. Import policies allow you to match authenticated users with corresponding roles on the target device. For example, you might configure an import policy to specify that when IF-MAP data for a session includes the “Contractor” capability, the imported session should have the “limited” role. Session-import policies allow the Infranet Controller to properly assign roles based on information that the IF-MAP server provides.

You configure session-import policies on IF-MAP client Infranet Controllers that are connected to an Infranet Enforcer in front of protected resources.

To configure a session-import policy:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure a session-import policy.
3. Click the **Configuration** tab. In the configuration tree, select **System > IF–MAP Federation > Session-Import Policies**.

4. Add or modify settings as specified in Table 35 on page 113.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 35: IF–MAP Session-Import Policy Configuration Details

Option	Function	Your Action
Name	Specifies a unique name for the session-import policy.	Enter a name for the session-import policy.
Description	Describes the policy.	Enter a brief description for the policy.
Stop on match	Stops matching the roles when an IF-MAP client has successfully matched the roles.	Select this option to stop matching roles after a successful match is found.
Match Criteria > Identity tab		
Match IF-MAP Identity	Specifies that identity should be used as the criteria for assigning roles.	Select this action and the following identity options appear. • **Identity**—Enter the identity name. For example, for a regular employee named Bob Smith you might enter the Identity as **username bsmith** and select **username** for the identity type. • **Identity Type**—Select the identity type. If you choose **Other** for identity type, enter a unique identity type in the text box. • **Administrative Domain**—Type the administrative domain for the session-import policy. All aspects of the IF-MAP identity (name, type, and administrative domain) must exactly match the session-import policy.
Match Criteria > Roles tab		
Match IF-MAP Roles	Specifies that role match should be used as the criteria for assigning roles.	Select this action and the following role option appears. • **Roles**— From Roles, click **New** and enter a specified role.
Match Criteria > Capabilities tab		
Match IF-MAP Capabilities	Specifies that capability match should be used as the criteria for assigning roles.	Select this action and the following option appears. • **Capabilities**—From Capabilities, click **New** and enter a specified capability.

Table 35: IF–MAP Session-Import Policy Configuration Details *(continued)*

Option	Function	Your Action
Match Criteria > Device Attributes tab		
Match IF-MAP Device Attributes	Specifies that device attribute match should be used as the criteria for assigning roles.	Select this action and the following option appears. • **Device Attributes**—From Device Attributes, click **New** and enter a specified device attribute.
Actions > Assign Roles tab		
Use these roles	Assigns roles from the available list.	Select Infranet Controller roles from the Non-members area and move it to the Members area.
Actions > Copy IF-MAP Roles tab		
Copy IF-MAP Roles	Copies the specified roles.	Select **Copy IF-MAP roles** and select **All roles**, **Specified roles**, or **All roles other than those specified below**, and then list the IF-MAP roles.
Actions > Copy IF-MAP Capabilities tab		
Copy IF-MAP Capabilities	Copies the IF-MAP capabilities.	Select **Copy IF-MAP capabilities** and select **All capabilities**, **Specified capabilities** or **All capabilities other than those specified below**, and then list the IF-MAP capabilities.

Related Documentation

- Configuring IF-MAP Session Export Policy on the Infranet Controller (NSM Procedure) on page 109
- Configuring IF-MAP Server Replicas (NSM Procedure) on page 114
- Configuring IF-MAP Server Settings on the Infranet Controller (NSM Procedure) on page 107
- Configuring IF-MAP Client Settings on the Infranet Controller (NSM Procedure) on page 108

Configuring IF-MAP Server Replicas (NSM Procedure)

You can configure an IF-MAP server to replicate all of its IF-MAP data to other IF-MAP servers. For example, if you have a network in Boston and a network in London, you can run IF-MAP servers in both places and configure the IF-MAP servers in both locations to replicate data to one another. These connected IF-MAP servers are known as replicas.

To configure IF-MAP server replicas to communicate with each other:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure IF-MAP server replicas.
3. Click the **Configuration** tab. In the configuration tree, select **System > IF–MAP Federation > This Server**.
4. Add or modify settings as specified in Table 36 on page 115.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 36: Replica IF–MAP Server Configuration Details

Option	Function	Your Action
Name	Specifies a unique name for the replica IF-MAP server.	Enter a name for the replica IF-MAP server.
Description	Describes the replica or replica network.	Enter a brief description for the replica or replica network.
Type	Specifies whether the configuration is for an IF-MAP client or for a replica IF-MAP server.	From the Type list, select **Replica**.
Hostname	Specifies the hostname that exactly matches the replica's device certificate.	Enter the hostname of the replica's device certificate. The hostname is used when this IF-MAP server initiates a connection to the replica. The fully qualified domain name (FQDN) of the replica's internal or external interface should be used; for a cluster, the FQDN of the internal or external VIP should be used.
IP Address(es)	Specifies the IP addresses from which the replica may initiate connections to this server.	Enter one or more IP addresses from which the replica may initiate connections to this server. If the replica is standalone, for survivability list both the internal and external network interfaces. If the replica is a cluster, for survivability list the internal and external network interfaces of both cluster nodes.

Table 36: Replica IF–MAP Server Configuration Details *(continued)*

Option	Function	Your Action
Authentication Type	Specifies the authentication type.	Select the authentication method: • **Basic**—If you select **Basic**, enter a username and password. • **Certificate**—If you select **Certificate**, select the certificate authority that issued the IF-MAP replica's certificate. Enter any restrictions, one per line. If any restrictions match, for example CN=ic.example.com, the certificate is accepted.

Related Documentation

- Configuring IF-MAP Session Export Policy on the Infranet Controller (NSM Procedure) on page 109
- Configuring IF-MAP Session Import Policy on the Infranet Controller (NSM Procedure) on page 112
- Configuring IF-MAP Server Settings on the Infranet Controller (NSM Procedure) on page 107
- Configuring IF-MAP Client Settings on the Infranet Controller (NSM Procedure) on page 108

CHAPTER 13

Configuring Authentication Servers

Configuring an Infranet Controller Anonymous Server Instance (NSM Procedure)

An anonymous server instance allows users to access the Infranet Controller without providing a username or password.

To configure an anonymous server instance:

1. In the NSM navigation tree, select **Device Manager**> **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure an anonymous server instance.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Auth Servers**.

4. Add or modify anonymous server settings as specified in Table 37 on page 118.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 37: Anonymous Server Instance Configuration Details

Option	Function	Your Action
Auth Server Name	Specifies a name for the auth server.	Enter a name for the auth server.
Auth Server Type	Specifies the auth server type.	Select **Anonymous Server**.

Related Documentation

- Configuring an Infranet Controller RSA ACE/Server Instance (NSM Procedure) on page 119
- Configuring an Infranet Controller Active Directory or NT Domain Server Instance (NSM Procedure) on page 121
- Creating an Authentication Realm (NSM Procedure) on page 87

Creating a Custom Expression for an Authentication Server (NSM Procedure)

Custom expressions are strings that are made up of variables, operators, and subexpressions all concatenated together. These operators and variables are provided through an expressions dictionary.

To create a custom expression for an authentication server:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure a server catalog.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Auth Servers**.
4. Add or modify an auth server instance and then select **Server Catalog**. The Expressions tab appears.
5. Click **New** (+) to create a custom expression. The Custom Expression editor appears. On the left side of the editor is the Expression Dictionary, which includes the following custom expression building blocks:
   - Logical Operators: This node consists of logical operators that are used to build expressions. Select a logical operator and click the **Insert Expression** button to insert logical operators in expressions.
   - Prebuilt Expressions: This node consists of expressions that function as templates for custom expressions. Select a prebuilt expression and click the **Insert Expression**

button. The prebuilt expression is displayed in the Expression area. Modify the values to create your own custom expression.

- Variables: This node consists of variables. When a variable is selected, the conditional operators that can be applied to this variable are listed in the center of the Custom Expressions editor. Also, some variables have extensions that are displayed in the drop-down list next to the variable. Double-click a variable to display its description and example usage. Click the example variable to insert it in the Expression area.
- Your Expressions: This node consists of expressions that you created for a particular server catalog. To reuse an existing expression, select the expression and click the **Insert Expression** button.

NOTE: Refer to the *Juniper Networks Unified Access Control Administration Guide* for more information on variables and writing custom expressions.

6. Enter a name for the custom expression.
7. Select a variable or prebuilt expression from the Custom Dictionary, and click **Insert Expression**. The expression is displayed in the Expression area on the right side of the Custom Expression editor. The conditional operators can be selected only after a leaf node is selected.
8. Click the **Validate** button to validate the expression. The expression is validated by the device and the validation status appears.

NOTE: You can create a custom expression in a device template, but you cannot validate the custom expression. The Validate button is not enabled in the Custom Expressions editor of device templates.

9. Click **OK** to save the custom expression. The new custom expression is displayed under the Expressions tab of the server catalog.
10. Click **OK** to save the auth server settings.

Related Documentation

- Creating a Custom Expression for Sensor Settings (NSM Procedure) on page 198

Configuring an Infranet Controller RSA ACE/Server Instance (NSM Procedure)

The RSA ACE/Server, which is supported by the Infranet Controller, is used to authenticate users. If the ACE/Server positively authenticates the user, the user gains access to the Infranet Controller.

To configure an ACE/Server instance:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure an ACE server instance.

3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Auth Servers**.
4. Add or modify ACE/Server settings as specified in Table 38 on page 120.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 38: ACE Server Instance Configuration Details

Option	Function	Your Action
Auth Server Name	Specifies a name for the auth server.	Enter a name for the auth server.
Auth Server Type	Specifies the auth server type.	Select **ACE Server**.
ACE Settings		
ACE Port	Specifies the default port of the ACE/Server.	Enter a default port number. NOTE: If no port is specified in the sdconf.rec file, then the Infranet Controller uses this setting.
Config File Name	Specifies the RSA ACE/agent configuration file.	Enter the config file name. NOTE: You must update this file on the device anytime you make changes to the source file.
Imported on	Specifies the date on which the config file is imported.	For information only. View the date on which the config file was imported.
Import Config File	Specifies the configuration file for importing.	Select the configuration file to be imported by using the browse button.
Users authenticate using tokens or one-time passwords	Prompts the user for a token instead of a password.	Select this option if users submit tokens or one-time passwords to the Infranet Controller.
Server Catalog > Expressions tab		
name	Specifies a name for the user expression in the ACE/Server user directory.	Enter a name for the user expression.
value	Specifies a value for the user expression in the ACE/Server user directory.	Enter a value for the user expression.

Related Documentation

- Configuring an Infranet Controller Active Directory or NT Domain Server Instance (NSM Procedure) on page 121

- Configuring an Infranet Controller Certificate Server Instance (NSM Procedure) on page 124

Configuring an Infranet Controller Active Directory or NT Domain Server Instance (NSM Procedure)

The Infranet Controller supports Windows NT authentication and Active Directory using NTLM or Kerberos authentication. When authenticating users with an NT Primary Domain Controller (PDC) or Active Directory, users sign into the Infranet Controller using the same username and password they use to access their Windows desktops.

To configure an Active Directory or Windows NT domain server instance:

1. In the NSM navigation tree, select **Device Manager**> **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure an Active Directory or NT domain server instance.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Auth Servers**.
4. Add or modify an Active Directory or NT domain server instance as specified in Table 39 on page 121.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 39: Active Directory or NT Domain Instance Configuration Details

Option	Function	Your Action
Auth Server Name	Specifies a name for the auth server.	Enter a name for the auth server.
Auth Server Type	Specifies the auth server type.	Select **AD/NT Server**.
AD/NT Settings > General tab		
Primary Domain Controller or Active Directory	Specifies the name or IP address for the primary domain controller or Active Directory server.	Enter the name or IP address.
Secondary Domain Controller or Active Directory	Specifies the name or IP address for the backup domain controller or Active Directory server.	Enter the name or IP address.

Table 39: Active Directory or NT Domain Instance Configuration Details *(continued)*

Option	Function	Your Action
Domain	Specifies the domain name of the Active Directory or Windows NT server.	Enter the domain name of the Active Directory or Windows NT domain. NOTE: For example, if the Active Directory domain name is us.amr.asgqa.net and you want to authenticate users who belong to the **US** domain, enter **US** as the domain.
Allow domain to be specified as part of username	Allows users to sign in by entering a domain name in the Username box in the format: "domain\username."	Select **AD/NT Settings > General > Allow domain to be specified as part of username** to enable this feature.
Allow trusted domains	Allows users to get group information from all trusted domains within a forest.	Select **AD/NT Settings > General >Allow trusted domains** to enable this feature.
Admin Username	Specifies an administrator username for the Active Directory or NT server.	Enter an administrator username for the Active Directory or NT server.
Admin Password	Specifies an administrator password for the Active Directory or NT server.	Enter an administrator password for the Active Directory or NT server.
Kerberos (most secure)	Allows the Infranet Controller to send user credentials to Kerberos.	Select **AD/NT Settings > General >Kerberos (most secure)** to enable this feature.
NTLMV2 (moderately secure)	Allows the Infranet Controller to send user credentials to NTLMv2.	Select **AD/NT Settings > General >NTLMV2 (moderately secure)** to enable this feature.
NTLMV1 (least secure)	Allows the Infranet Controller to send user credentials to NTLMv1.	Select **AD/NT Settings > General >NTLMV1 (least secure)** to enable this feature.
Use LDAP to get Kerberos realm name	Allows the Infranet Controller to retrieve the Kerberos realm name from the Active Directory server using the specified administrator credentials.	Select **AD/NT Settings > General >Specify Kerberos realm name** to enable this feature.
Specify Kerberos realm name	Specifies Kerberos realm name.	Enter the name.

AD/NT Settings > Advanced tab

Table 39: Active Directory or NT Domain Instance Configuration Details *(continued)*

Option	Function	Your Action
User may belong to Domain Local Groups across trust boundaries	Specifies that the selected user belongs to the Domain Local Groups who honor trust relationships in Active Directory.	Select **AD/NT Settings > Advanced > User may belong to Domain Local Groups across trust boundaries** to enable this feature.
Container Name	Specifies the name that the Infranet Controller uses to join the specified Active Directory domain as a computer.	Enter the computer name.
Server Catalog > Expressions tab		
Name	Allows you to enter a name for the user expression in the Active Directory or NT Domain server user directory.	Enter a name for the user expression.
Value	Allows you to enter a value for the user expression in the Active Directory or NT domain server user directory.	Enter the value for the user expression.
Server Catalog > Groups tab		
Name	Specifies the name of the group.	Enter the name for the user group.
Group	Specifies the admin domain local groups information.	Enter the name for the admin domain local group.
AD Group	Specifies the group that contains the administrators to enable centralized administration in an Active Directory domain.	Enter the name for the administrators Active Directory group.

Related Documentation

- Configuring an Infranet Controller NIS Server Instance (NSM Procedure) on page 133
- Creating an Authentication Realm (NSM Procedure) on page 87

Configuring an Infranet Controller Certificate Server Instance (NSM Procedure)

The certificate server feature allows users to authenticate based on attributes contained in client-side certificates. You may use certificate server by itself or in conjunction with another server to authenticate users and map them to roles.

Import the CA certificate used to sign the client-side certificates.

To configure certificate server instance:

1. In the NSM navigation tree, select **Device Manager**> **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure a certificate server instance.
3. Click the **Configuration** tab. In the configuration tree, use settings in the **System > Configuration > Certificates > CA Certificates** tab to import the CA certificate used to sign the client-side certificates.
4. Configure the certificate server instance, by selecting **Authentication > Auth Servers**. Then add or modify certificate server settings as specified in Table 40 on page 124.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 40: Certificate Server Instance Configuration Details

Option	Function	Your Action
Auth Server Name	Specifies a name for the auth server.	Enter a name for the auth server.
Auth Server Type	Specifies the auth server type.	Select **Certificate Server**.
Certificate Settings		
User Name Template	Specifies how the Infranet Controller should construct a username.	Enter any combination of certificate variables contained in angle brackets and plain text.
Server Catalog > Expressions tab		
Name	Specifies a name for the user expression in the certificate server user directory.	Enter a name for the user expression.
Value	Specifies a value for the user expression in the certificate server user directory.	Enter a value for the user expression.

Related Documentation

- Configuring an Infranet Controller Active Directory or NT Domain Server Instance (NSM Procedure) on page 121
- Configuring Infranet Controller Certificate Access Restrictions (NSM Procedure) on page 64

Configuring an Infranet Controller LDAP Server Instance (NSM Procedure)

The Infranet Controller supports two LDAP-specific authentication options:

- **Unencrypted** — The Infranet Controller sends the username and password to the LDAP Directory Service in clear, simple text.
- **LDAPS** — The Infranet Controller encrypts the data in the LDAP authentication session using the Secure Socket Layer (SSL) protocol before sending it to the LDAP Directory Service.

To define an LDAP server instance:

1. In the NSM navigation tree, select **Device Manager**> **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure an LDAP server instance.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Auth Servers**.
4. Add or modify an LDAP server instance as specified in Table 41 on page 125.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 41: LDAP Server Instance Configuration Details

Option	Function	Your Action
Auth Server Name	Specifies a name for the auth server.	Enter a name for the auth server.
Auth Server Type	Specifies the auth server type.	Select **LDAP server**.
LDAP Settings > Basic Settings tab		
LDAP Server	Specifies the name or IP address of the LDAP server that the Infranet Controller uses to validate your users.	Enter the name or IP address of the LDAP server.

Table 41: LDAP Server Instance Configuration Details *(continued)*

Option	Function	Your Action
LDAP Port	Specifies the port on which the LDAP server responds. NOTE: This port is 389 when using an unencrypted connection and 636 when using SSL.	Set the port for the LDAP server.
Backup LDAP Server1	Specifies the parameters for backup LDAP server1 (optional). NOTE: The Infranet Controller uses this type of server for failover processing. Also, backup LDAP servers must be the same version as the primary LDAP server.	Enter the IP address of the backup LDAP server1. NOTE: We do not recommend entering hostname as it may accelerate failover processing by eliminating the need to resolve the hostname to an IP address.
Backup LDAP Port1	Specifies the parameters for backup LDAP port1.	Enter the port number for the backup LDAP port1.
Backup LDAP Server2	Specifies the parameters for backup LDAP server2 (optional).	Enter the IP address of the backup LDAP server2.
Backup LDAP Port2	Specifies the parameters for backup LDAP port2.	Enter the port number for the backup LDAP port2.
LDAP Server Type	Specifies the type of LDAP server that you want to authenticate users against.	Select the type of LDAP server from the drop-down list.
Connection	Specifies whether or not the connection between the Infranet Controller and the LDAP Directory Service should be unencrypted, use SSL (LDAPs), or use TLS.	Select the type of connection from the drop-down list.
Connection Timeout (seconds)	Specifies how long you want the Infranet Controller to wait for a connection to the primary LDAP server first, and then each backup LDAP server in turn.	Set the time required for the connection to time out.
Search Timeout (seconds)	Specifies how long you want the Infranet Controller to wait for search results from a connected LDAP server.	Set the time required for the search to time out.

Table 41: LDAP Server Instance Configuration Details *(continued)*

Option	Function	Your Action
LDAP Settings > Authentication tab		
Authentication required to search LDAP	Specifies if the Infranet Controller needs to authenticate against the LDAP directory to perform a search or to change passwords using the password management feature.	Select **LDAP Settings >Authentication>Authentication required to search LDAP** to enable this option.
Admin DN	Specifies the administrator DN.	Enter the admin DN name.
Password	Specifies the password for the admin DN name.	Enter the password.
Strip domain from Windows user names	Removes the domain from a domain\username pair. This feature allows the Infranet Controller to pass the username without the domain to the LDAP server.	Select the check box.
Enable Challenge-Response open protocols	Specifies challenge-response protocol for authentication, if you are configuring this LDAP server instance for noninteractive endpoints.	Select the check box. NOTE: If the LDAP server is configured to limit the rate of password-guessing attacks, and you select the **Enable Challenge-Response open protocols** check box, the LDAP server's rate-limiting feature is bypassed.
LDAP Settings > Finding User Entries tab		
Base DN	Searches for user entries.	Enter a base DN name. For example, enter **DC=eng, DC=Juniper, DC=com**.
Filter	Fine tunes the search.	Enter a filter value. For example, enter **samAccountname= <username>** or **cn= <username>** NOTE: • Include **<username>** in the filter to use the username entered on the sign-in page for the search. • Specify a filter that returns 0 or 1 user DNs per user; the Infranet Controller uses the first DN returned if more than one DN is returned.
LDAP Settings > Determining Group Membership tab		
Base DN	Searches for user groups.	Enter a base DN name.

Table 41: LDAP Server Instance Configuration Details *(continued)*

Option	Function	Your Action
Filter	Fine tunes the search for a user group.	Enter a filter value.
Member Attribute	Specifies members of a static group.	Enter a name if you want to identify all the members of a static group. For example, enter **member uniquemember (iPlanet-specific)**.
Reverse group search	Specifies that the search starts from the member instead of the group.	Select **LDAP Settings**>**Determining Group Membership** > **Reverse group search**.
Query Attribute	Specifies an LDAP query that returns the members of a dynamic group.	Enter a name for the query attribute. For example, enter **memberURL**.
Nested Group Level	Specifies how many levels within a group to search for the user. NOTE: Because the higher the number, the longer the query time, we recommend that you specify to perform the search no more than two levels deep.	Set the number for the search query time.
Nested Group Search	Specifies the types of nested group search available. They are: • Nested groups in Server Catalog — This option is faster because it can search within the implicit boundaries of the nested group. • Search all nested groups — With this option, the Infranet Controller searches the Server Catalog first. If the Infranet Controller finds no match in the catalog, then it queries LDAP to determine if a group member is a subgroup.	Select one type of nested group search from the drop-down list.
LDAP Settings > Meetings tab		
User Name	Specifies the username attribute for the LDAP server.	Enter the username for the server. For example, enter **SamAccountName** for an Active Directory server or **uid** for an iPlanet server.

Table 41: LDAP Server Instance Configuration Details *(continued)*

Option	Function	Your Action
Email Address	Specifies the e-mail attribute for the LDAP server.	Enter the e-mail address for the server.
Display Name, Attributes	Specifies if there are any additional LDAP attributes whose contents you want to allow meeting creators to view (optional).	Enter a name. For example, to help the meeting creator easily distinguish between multiple invitees with the same name, you may want to expose an attribute that identifies the departments of individual users. NOTE: Enter the additional attributes one per line using the format: **DisplayName,AttributeName**. You may enter up to 10 attributes.
Server Catalog > Expressions tab		
Name	Specifies the name that is used to show a list of common LDAP expressions.	Enter a name. For example, enter **cn**, **uid**, **uniquemember**, and **memberof**.
Value	Specifies the custom value of the LDAP server.	Enter a value for the LDAP server.
Server Catalog > Attributes tab		
Name	Specifies the name that is used to show a list of common LDAP attributes	Enter a name for the LDAP attributes.
Server Catalog > Groups tab		
Name	Specifies the name that is used to easily retrieve group information from an LDAP server and add it to the server's device server catalog.	Enter a name.
DN	Specifies the base DN name of the group.	Enter a base DN name. NOTE: If you do not know the exact container of your groups, you can specify the domain root as the BaseDN, such as **dc=juniper**, **dc=com**. The search page returns a list of groups from your server, from which you can choose groups to enter into the Groups list
Group Type	Specifies the group type.	Select any one group type from the drop-down list.

Related Documentation

- Configuring an Infranet Controller RADIUS Server Instance (NSM Procedure) on page 134
- Configuring an Infranet Controller Anonymous Server Instance (NSM Procedure) on page 117
- Configuring an Infranet Controller Local Authentication Server Instance (NSM Procedure) on page 130

Configuring an Infranet Controller Local Authentication Server Instance (NSM Procedure)

The Infranet Controller enables you to create one or more local databases of users who are authenticated by the Infranet Controller. You might want either to create local user records for users who are normally verified by an external authentication server that you plan to disable or to create a group of temporary users.

To configure a local authentication server instance:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure a local authentication server instance.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Auth Servers**.
4. Add or modify local authentication server instance settings as specified in Table 42 on page 130.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 42: Local Authentication Server Instance Configuration Details

Option	Function	Your Action
Auth Server Name	Specifies the local auth server instance name.	Enter a name for the local authentication server instance.
Auth Server Type	Specifies the auth server type.	Select **Local Authentication**.
Local Auth Settings		
Minimum password length (characters)	Specifies the minimum number of characters that a password must have.	Enter the minimum password length.
Maximum password length	Specifies the maximum number of characters that a password can consist of.	Enter the maximum length of the password.

Table 42: Local Authentication Server Instance Configuration Details *(continued)*

Option	Function	Your Action
Minimum number of digits required in the password (digits)	Specifies the minimum number of digits that must be present in the password.	Enter the minimum number of digits that must be present in the password.
Minimum number of letters required in the password (letters)	Specifies the minimum number of letters that must be present in the password.	Enter the minimum number of digits that must be present in the password.
Require passwords to have a mix of UPPER and LOWER CASE letters	Specifies that the password contain both upper- and lowercase letters.	Select **Local Auth Settings** > **Require passwords to have a mix of UPPER and LOWER CASE letters** to enable this option.
Require password to be different from username	Specifies that the password must be different from the username.	Select **Local Auth Settings** > **Require password to be different from username** to enable this option.
Require new passwords to be different from previous password	Specifies that the new password must be different from the previous password.	Select **Local Auth Settings** >**Require new passwords to be different from previous password** to enable this option.
Allow users to change their passwords	Specifies that users can change their passwords.	Select **Local Auth Settings**> **Allow users to change their passwords** to enable this option.
Force user to change password (days)	Specifies the days after which the user would be forced to change the password.	Enter the number of days after which the password expires.
Prompt user to change password (days)	Specifies the number of days after which users are prompted to change their password.	Enter the number of days after which users are prompted to change their password.
Password stored as clear text	Enables CHAP and EAP-MD5-Challenge to work with local auth servers.	Select the check box. NOTE: Be aware of the security implications of storing passwords as clear text.
Users		
Username	Specifies the username.	Enter the username.
Full name	Specifies the user's full name.	Enter the user's full name.
Password	Specifies the password.	Enter the password.
One-time user	Specifies that the user is limited to one login.	Select **Users** > **One-time user** to enable this option.

Table 42: Local Authentication Server Instance Configuration Details *(continued)*

Option	Function	Your Action
Enabled	Allows the administrator to selectively enable or disable any user (one time or permanent).	Select **Users** > **Enabled** to enable this option.
Require user to change password at next sign in	Specifies that users must change their password at the next login.	Select **Users** > **Require users to change password at next sign in** to enable this option.
Admin Users		
	You can create user administrators to give individuals with user-level permissions some administrative capabilities on the Infranet Controller. A user administrator can add new users, change passwords, delete existing users, specify an expiration time, and specify one-time privileges for guest accounts. NOTE: User administrators can only administer local authentication servers.	
Username	Specifies the username of the user who you want to manage accounts for the selected authentication server. This user does not need to be added as a local user on the server.	Enter the username.
Realm name	Specifies the authentication realm that the user administrator maps to when signing in to the Infranet Controller.	Select the authentication realm.
Server Catalog > Expressions tab		
name	Specifies the name of the expression.	Enter a name for the expression.
value	Specifies the value(s) of the expression.	Enter a value for the expression.

Related Documentation

- Configuring an Infranet Controller LDAP Server Instance (NSM Procedure) on page 125
- Configuring an Infranet Controller RADIUS Server Instance (NSM Procedure) on page 134
- Configuring an Infranet Controller RSA ACE/Server Instance (NSM Procedure) on page 119

Configuring an Infranet Controller NIS Server Instance (NSM Procedure)

When authenticating users with a UNIX/NIS server, the Infranet Controller verifies that the username and password entered through the sign-in page corresponds to a valid user ID and password pair in the NIS server.

To configure an NIS server instance:

1. In the NSM navigation tree, select **Device Manager**> **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure an NIS server instance.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Auth Servers**.
4. Add or modify NIS server settings as specified in Table 43 on page 133.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 43: Infranet Controller NIS Server Instance Configuration Details

Option	Function	Your Action
Auth Server Name	Specifies a name for the auth server.	Enter a name for the auth server.
Auth Server Type	Specifies the auth server type.	Select **NIS Server**.
NIS Settings		
NIS Server	Specifies the name or IP address of the NIS server.	Enter the name or IP address.
NIS Domain	Specifies the domain name for the NIS server.	Enter the domain name.
Server Catalog > Expressions tab		
Name	Specifies a name for the user expression in the NIS server user directory.	Enter the name for the user expression.
Value	Specifies a value for the user expression in the NIS server user directory.	Enter the value for the user expression.

Related Documentation

- Configuring an Infranet Controller RADIUS Server Instance (NSM Procedure) on page 134
- Configuring an Infranet Controller Local Authentication Server Instance (NSM Procedure) on page 130

Configuring an Infranet Controller RADIUS Server Instance (NSM Procedure)

A Remote Authentication Dial-In User Service (RADIUS) server allows you to centralize authentication and accounting for remote users. When using a RADIUS server to authenticate Infranet Controller users, you need to configure it to recognize the Infranet Controller as a client and specify a shared secret for the RADIUS server.

To configure a connection to the RADIUS server on the Infranet Controller:

1. In the NSM navigation tree, select **Device Manager**> **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure a RADIUS server instance.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Auth Servers**.
4. Add or modify RADIUS server settings as specified in Table 44 on page 134.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 44: RADIUS Server Configuration Details

Option	Function	Your Action
Auth Server Name	Specifies a name for the auth server.	Enter a name for the auth server.
Auth Server Type	Specifies the auth server type.	Select **Radius Server**.
Radius Settings > Primary Server tab		
Radius Server	Specifies a unique name or IP address for the RAIDUS server.	Enter the name or IP address.
NAS-Identifier	Specifies a name for the network access server (NAS) client, which communicates with the RADIUS server.	Enter the name for the NAS client.
Authentication Port	Specifies the authentication port value for the RADIUS server.	Enter the port value. NOTE: Typically this port is 1812, but some legacy servers might use 1645.
Shared Secret	Specifies the shared secret.	Enter the shared secret.

Table 44: RADIUS Server Configuration Details *(continued)*

Option	Function	Your Action
Accounting Port	Specifies the accounting port value for the RADIUS server.	Enter the port value. NOTE: Typically this port is 1813, but some legacy servers might use 1646.
NAS-IP-Address	Specifies the NAS IP address value passed to RADIUS requests.	Enter the NAS IP address.
Timeout (minutes)	Specifies the time interval for the Infranet Controller to wait for a response from the RADIUS server before timing out the connection.	Enter the timeout interval in minutes.
Retries	Specifies the number of retries an Infranet Controller can make after the first connection attempt fails.	Enter the number of retries.
Users authenticate using tokens or one-time passwords	Specifies that the password entered by the user cannot be submitted to other SSO enabled applications.	Select the **Users authenticate using tokens or one-time passwords** check box.
Radius Settings > Backup Server tab		
Backup Radius Server	Specifies a secondary RADIUS server for the Infranet Controller to use if the primary server (the one defined in this instance) is unreachable.	Enter a secondary RADIUS server name or IP address.
Backup Authentication Port	Specifies the authentication port for the backup RADIUS server.	Enter the port value.
Backup Shared Secret	Specifies the string for the shared secret.	Enter a string for the shared secret.
Backup Accounting Port	Specifies the accounting port for the backup RADIUS server.	Enter the port value.
Radius Settings > Radius Accounting tab		

Table 44: RADIUS Server Configuration Details *(continued)*

Option	Function	Your Action
User-Name	Specifies the user information that the Infranet Controller should send to the RADIUS accounting server.	Enter the user information. The default variables for this field are: • **<username>**—Logs the user's Infranet Controller username to the accounting server. • **<REALM>**— Logs the user's Infranet Controller realm to the accounting server. • **<ROLE>**— Logs the user's Infranet Controller role to the accounting server. If the user is assigned to more than one role, the Infranet Controller comma separates them.
Interim Update Interval (minutes)	Specifies an interim update interval that enables precise billing for long-lived session clients and in case of a network failure.	Enter the time.
Use NC assigned IP Address for FRAMED-IP-ADDRESS attribute	Specifies that the IP address returned from the Infranet Controller is used for the framed-IP-address attribute.	Select the **Use NC assigned IP Address for FRAMED-IP-ADDRESS attribute** check box.
Server Catalog > Expressions tab		
Name	Specifies a name for the user expression in the RADIUS server user directory.	Enter a name for the user expression.
Value	Specifies a value for the user expression in the RADIUS server user directory.	Enter a value for the user expression.
Server Catalog > Attributes tab		
Name	Specifies a name for the user attribute in the RADIUS server user directory.	Enter a name for the user attribute.

Related Documentation

- Configuring an Infranet Controller Anonymous Server Instance (NSM Procedure) on page 117
- Configuring an Infranet Controller eTrust SiteMinder Server Instance (NSM Procedure) on page 137
- Configuring an Infranet Controller LDAP Server Instance (NSM Procedure) on page 125

Configuring an Infranet Controller eTrust SiteMinder Server Instance (NSM Procedure)

Within the Infranet Controller, an eTrust SiteMinder instance is a set of configuration settings that defines how the Infranet Controller interacts with the eTrust SiteMinder policy server.

To configure an eTrust SiteMinder server instance:

1. In the NSM navigation tree, select **Device Manager**> **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure an eTrust SiteMinder server instance.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Auth Servers**.
4. Add or modify eTrust SiteMinder server settings as specified in Table 45 on page 137.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 45: Infranet Controller eTrust SiteMinder Configuration Details

Option	Function	Your Action
Auth Server Name	Specifies a name for the auth server.	Enter a name for the auth server.
Auth Server Type	Specifies the auth server type.	Select **Siteminder Server**.
Siteminder Settings > Basic Settings tab		
Policy Server	Specifies the name or IP address of the SiteMinder policy server.	Enter a name or IP address.
Backup Server(s)	Specifies a list of backup policy servers (optional).	Enter a comma-delimited list of backup policy servers (optional).
Failover Mode?	Specifies that the Infranet Controller can use the main policy server unless it fails.	• Select **Yes** — Infranet Controller uses the main policy server unless it fails. • Select **No**— Infranet Controller load balances among all the specified policy servers.
Agent Name	Specifies the SiteMinder agent name.	Enter an agent name. NOTE: Shared secret and agent name are case-sensitive.

Table 45: Infranet Controller eTrust SiteMinder Configuration Details *(continued)*

Option	Function	Your Action
Secret	Specifies the shared secret.	Enter a shared secret name. NOTE: Shared secret and agent name are case-sensitive.
Compatible with	Specifies a SiteMinder server version. Version 5.5 supports versions 5.5 and 6.0. Version 6.0 supports only version 6.0 of the SiteMinder server API. The default value is 5.5 policy servers.	Select the server version from the drop-down list.
On logout, redirect to	Specifies a URL to which users are redirected when they sign out of the Infranet Controller (optional). If you leave this box empty, users see the default Infranet Controller sign-in page.	Enter a URL.
Protected Resource	Specifies a default protected resource. If you do not create sign-in policies for SiteMinder, the Infranet Controller uses this default URL to set the user's protection level for the session. The Infranet Controller also uses this default URL if you select the Automatic Sign-In option.	Enter a URL. NOTE: You must enter a forward slash (/) at the beginning of the resource (for example, "/ive-authentication").
Users authenticate using tokens or one-time passwords	Specifies that the user authentication is done using tokens or one-time passwords.	Select the check box.
Siteminder Settings > SMSESSION Cookie Settings tab		

Table 45: Infranet Controller eTrust SiteMinder Configuration Details *(continued)*

Option	Function	Your Action
Cookie Domain	Specifies the cookie domain of the Infranet Controller.	Enter a URL for the cookie domain. NOTE: • Multiple domains should use a leading period and be comma separated. For example: .sales.myorg.com, .marketing.myorg.com. • Domain names are case-sensitive. • You cannot use wildcard characters. For example, if you define ".juniper.net", the user must access the Infranet Controller as "http://Infranet Controller.juniper.net" to ensure that the **SMSESSION** cookie is sent back to the Infranet Controller.
IVE Cookie Domain	Specifies the internet domain(s) to which the Infranet Controller sends the SMSESSION cookie using the same guidelines outlined for the Cookie Domain box.	Enter a URL.
Protocol	Specifies that you to send cookies either securely or nonsecurely.	Select the Protocol from the drop down list: • **HTTPS**— Sends cookies securely if other Web agents are set up to accept secure cookies. • **HTTP**—Sends cookies nonsecurely.
Siteminder Settings > Authentication tab		
Automatic Sign-In	Specifies that users with a valid SMSESSION automatically sign in to the Infranet Controller.	Select the **Automatic Sign-In** check box to enable this feature.
Automatic Sign In realm to use	Specifies an authentication realm for automatically signed-in users. The Infranet Controller maps the user to a role based on the role mapping rules defined in the selected realm.	Select an authentication realm from the drop-down list.

Table 45: Infranet Controller eTrust SiteMinder Configuration Details *(continued)*

Option	Function	Your Action
If Automatic Sign In fails, redirect to	Specifies an alternate URL for users who sign into the Infranet Controller through the Automatic Sign-In mechanism. The Infranet Controller redirects users to the specified URL if the Infranet Controller fails to authenticate and no redirect response is received from the SiteMinder policy server. If you leave this box empty, users are prompted to sign back in to the Infranet Controller. NOTE: • Users who sign in through the sign-in page are always redirected back to the Infranet Controller sign-in page if authentication fails.	Enter a URL.
Authentication Type > Custom Agent	Specifies that authentication can be done using the Infranet Controller custom Web agent.	Select **Siteminder Settings > Authentication > Authentication Type > Custom Agent**.
Authentication Type > Form POST	Specifies to post user credentials to a standard Web agent that you have already configured rather than contacting the SiteMinder policy server directly.	Select **Siteminder Settings > Authentication > Authentication Type > Form POST** to contact the policy server to determine the appropriate sign-in page to display to the user.
Form POST Target	Specifies the target URL. NOTE: The form post target, form post protocol, form post Webagent, form post port, form post path, and form post parameters boxes are displayed only when you select the **Form POST** option from the Authentication Type drop-down list.	Enter the target URL.

Table 45: Infranet Controller eTrust SiteMinder Configuration Details *(continued)*

Option	Function	Your Action
Form POST Protocol	Specifies the protocol for communication between the IVE and the specified Web agent. NOTE: This box is displayed only when you select the **Form POST** option from the Authentication Type drop-down list.	Select the protocol from the drop-down list: • **HTTP**—For nonsecure communication. • **HTTPS**—For secure communication.
Form POST Webagent	Specifies the name of the Web agent from which the Infranet Controller is to obtain **SMSESSION** cookies. NOTE: This box is displayed only when you select the **Form POST** option from the Authentication Type drop-down list.	Enter the name of the Web agent.
Form POST Port	Specifies the port for the protocol. NOTE: This box is displayed only when you select the **Form POST** option from the Authentication Type drop-down list.	Enter port 80 for HTTP or port 443 for HTTPS.
Form POST Path	Specifies the path of the sign-in page. NOTE: This box is displayed only when you select the **Form POST** option from the Authentication Type drop-down list.	Enter the path of the Web agent's sign-in page. NOTE: The path must start with a backslash (/) character. In the Web agent sign-in page URL, the path appears after the Web agent.

Table 45: Infranet Controller eTrust SiteMinder Configuration Details *(continued)*

Option	Function	Your Action
Form POST Parameters	Specifies the post parameters to be sent when a user signs in. NOTE: This box is displayed only when you select the **Form POST** option from the Authentication Type drop-down list.	Enter the post parameters. Common SiteMinder variables that you can use include USER PASS and Target. These variables are replaced by the username and password entered by the user on the Web agent's sign-in page and by the value specified in the Target box. These are the default parameters for login.fcc—if you have made customizations, you may need to change these parameters.
Authentication Type > Delegate to a Standard Agent	Specifies that you can delegate authentication to a standard agent. When the user accesses the Infranet Controller sign-in page, the Infranet Controller determines the FCC URL associated with the protected resource's authentication scheme. The Infranet Controller redirects the user to that URL, setting the Infranet Controller sign-in URL as the target. After successfully authenticating with the standard agent, an SMSESSION cookie is set in the user's browser and the user is redirected back to the Infranet Controller. The Infranet Controller then automatically signs in the user and establishes an Infranet Controller session.	Select **Siteminder Settings > Authentication > Authentication Type > Delegate to a Standard Agent**.
Siteminder Settings > Advanced tab		
Poll Interval (seconds)	Specifies the interval at which Infranet Controller polls the SiteMinder policy server to check for a new key.	Enter the poll interval in seconds.

Table 45: Infranet Controller eTrust SiteMinder Configuration Details *(continued)*

Option	Function	Your Action
Maximum Agents	Specifies the maximum number of simultaneous connections that the Infranet Controller is allowed to make to the policy server. NOTE: The default setting is 20.	Enter a number.
Maximum Requests/Agent	Specifies the maximum number of requests that the policy server connection handles before the Infranet Controller ends the connection. If necessary, tune to increase performance. NOTE: The default setting is 1000.	Enter a number.
Idle Timeout (minutes)	Specifies the maximum number of minutes a connection to the policy server may remain idle (the connection is not handling requests) before the Infranet Controller ends the connection. The default setting of “none” indicates no time limit.	Enter the Idle timeout in minutes.
Authorize while Authenticating	Specifies that the Infranet Controller should look up user attributes on the policy server immediately after authentication to determine if the user is truly authenticated.	Select **Siteminder Settings > Advanced > Authorize while Authenticating**.

Table 45: Infranet Controller eTrust SiteMinder Configuration Details *(continued)*

Option	Function	Your Action
Enable Session Grace Period	Specifies that users can eliminate the overhead of verifying a user's SMSESSION cookie each time the user requests the same resource by indicating that the Infranet Controller should consider the cookie valid for a certain period of time. If you do not select this option, the Infranet Controller checks the user's SMSESSION cookie on each request.	Select **Siteminder Settings > Advanced > Enable Session Grace Period** to enable this feature. You can eliminate the overhead of verifying a user's SMSESSION cookie each time the user requests the same resource by indicating that the Infranet Controller should consider the cookie valid for a certain period of time. During that period, the Infranet Controller assumes that its cached cookie is valid rather than revalidating it against the policy server. Note that the value entered here does not affect session or idle timeout checking.
Validate cookie every (seconds)	Specifies the time period for the Infranet Controller to eliminate the overhead of verifying a user's SMSESSION cookie each time the user requests the same resource by indicating that the Infranet Controller should consider the cookie valid for a certain period of time.	Enter the time period in seconds.
Ignore Query Data	Specifies the query parameter in the URL as specified in the cached URL. The Infranet Controller does not cache the query parameter in its URLs. Therefore, if a user requests the same resource as is specified in the cached URL, the request should not fail. For example, if you enable the **Ignore Query Data** option, both of the following URLs are considered the same resource: http://foo/bar?param=value1 http://foo/bar?param=value2	Select the **Ignore Query Data** option to enable this feature.

Table 45: Infranet Controller eTrust SiteMinder Configuration Details *(continued)*

Option	Function	Your Action
Accounting Port	Specifies that the value entered in this box matches the accounting port value entered through the Policy Server Management Console. By default, this box matches the policy server's default setting of 44441.	Enter the value for the accounting port.
Authentication Port	Specifies that the value entered in this box matches the authentication port value entered through the Policy Server Management Console. By default, this box matches the policy server's default setting of 44442.	Enter a value for the authentication port.
Authorization Port	Specifies that the value entered in this box matches the authorization port value entered through the Policy Server Management Console. By default, this box matches the policy server's default setting of 44443.	Enter a value for the authorization port.
Server Catalog > Expressions tab		
Name	Specifies a name for the user expression in the SiteMinder user directory.	Enter a name.
Value	Specifies a value for the user expression in the SiteMinder user directory.	Enter a value.
Server Catalog > Attributes tab		
Name	Specifies a name for the user attribute cookie in the SiteMinder user directory.	Enter a name.

Related Documentation

- Configuring an Infranet Controller Certificate Server Instance (NSM Procedure) on page 124
- Configuring an Infranet Controller Anonymous Server Instance (NSM Procedure) on page 117

Configuring an Infranet Controller MAC Address Authentication Server for Unmanageable Devices (NSM Procedure)

To configure a MAC address authentication server for unmanageable devices:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure MAC address authentication.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Auth Servers**.
4. Add or modify MAC address authentication settings as specified in Table 46 on page 146.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 46: MAC Address Authentication Server Configuration Details

Option	Function	Your Action
Auth Server Name	Specifies a name for the auth server.	Enter a name for the auth server.
Auth Server Type	Specifies the auth server type.	Select **MAC Address Authentication**.
MAC Address Authentication Server > Optional LDAP Server		
Optional LDAP Server	Specifies the list of optional LDAP servers.	Select the optional LDAP servers from the Non-members list and click **Add** to move it to the Members list.
MAC Address Authentication Server > MAC Adresses > MAC Addresses		
MAC Address	Specifies the MAC address.	Enter MAC address entries in the format: 00:11:85:bb:8c:66 To enter wildcards, use the format 00:11:22*:*:* (a single asterisk represents two characters).
Action	Specifies if the MAC address is authenticated.	• Select **Allow** to grant authentication. • Select **Deny** to refuse authentication.
MAC Address Authentication Server > MAC Adresses > Attributes		
Name	Allows you to enter the name of the user attribute cookie in the MAC address authentication user directory.	Enter a name.

Table 46: MAC Address Authentication Server Configuration Details *(continued)*

Option	Function	Your Action
Value	Associates the MAC address with a particular group or organization. For example: dept=eng represents that this MAC address belongs to engineering.	Enter a value.

Related Documentation

- Configuring an Infranet Controller LDAP Server Instance (NSM Procedure) on page 125

CHAPTER 14

Configuring Sign-In Policies

Configuring Infranet Controller Sign-in Policies (NSM Procedure)

Sign-in policies define the URLs that users and administrators use to access the Infranet Controller and the sign-in pages that they see. The Infranet Controller has two types of sign-in policies—one for administrators and one for users. When configuring sign-in policies, you associate realms, sign-in pages, and URLs.

This topic contains the following information about sign-in policies:

Configuring Administrator Sign-In Policies

To define an administrator sign-in policies:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to define the administrator sign-in policies.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Signing In > Sign-in Policies > User/Administrator URLs**.
4. Add or modify the settings for the User/Administrator URLs as specified in Table 47 on page 150.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 47: Administrator Sign–in Policies Configuration Details

Option	Function	Your Action
Sign-in URL	Specifies the URL that you want to associate with the policy.	Enter the URL. Use the format <host>/<path>, where <host> is the hostname of the Infranet Controller and <path> is any string you want users to enter. For example, enter: **users1.yourcompany.com/ic.** To specify multiple hosts, use the * wildcard character. To specify that all administrator URLs should use the sign-in page, enter ***/admin**. NOTE: You may only use wildcard characters (*) in the beginning of the hostname portion of the URL. The Infranet Controller does not recognize wildcards in the URL path.
Description	Specifies the description for the policy.	Enter a brief description for the administrator sign-in policy.
Enable	Enables the sign-in policy option.	Select this option.
Sign-in Page	Specifies the page that you want to associate with the sign-in policy.	Select the sign-in page.
User Type	Specifies the user type.	Select **Administrator**, and click **Add** to move the required Admin Realms from the Non-members list to the Members list.

Table 47: Administrator Sign–in Policies Configuration Details *(continued)*

Option	Function	Your Action
Realm Select	Specifies which realm(s) map to the policy, and how users and administrators should pick from among realms.	• Select **User types the realm name** for the Infranet Controller to map the sign-in policy to all authentication realms, but do not provide a list of realms from which the administrator can choose. Instead, the administrator must manually enter the realm name into the sign-in page. • Select **User picks from a list of authentication realms** for the Infranet Controller to map only the sign-in policy to the authentication realms that you choose. The Infranet Controller presents this list of realms when the administrator signs-in to the Infranet Controller and allows a realm to be chosen from the list. NOTE: The Infranet Controller does not display a drop-down list of authentication realms if the URL is only mapped to one realm. Instead, only the realm you specify is displayed.

Configuring User Sign-in Policies

To define user sign-in policies:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to define the user sign-in policies.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Signing In > Sign-in Policies > User/Administrator URLs**.
4. Add or modify the settings for the User/Administrator URLs as specified in Table 48 on page 152.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 48: User Sign–in Policies Configuration Details

Option	Function	Your Action
Sign-in URL	Specifies the URL that you want to associate with the policy.	Enter the URL.Use the format <host>/<path>, where <host> is the hostname of the Infranet Controller and <path> is any string you want users to enter. For example, enter: **users1.yourcompany.com/ic**. To specify multiple hosts, use the * wildcard character. To specify that all end–user URLs should use the sign-in page, enter ***/.**
Description	Describes the user sign-in policies.	Enter a brief description for the user sign-in policies.
Enable	Enables the sign-in policy option.	Select this option.
Sign-in Page	Specifies the page that you want to associate with the sign–in policy.	Select the default page that comes with the Infranet Controller, a variation of the standard sign-in page, or a custom page that you create using the customizable UI feature. For more information, see "Configuring Standard Sign-In Pages."
User Type	Specifies the user type.	Select **User**.
authentication-realms	Specifies the realm(s) that should be mapped to the sign-in policy.	1. Click **authentication-realms**. The Authentication dialog box appears. 2. Select the **Realm** and **Authentication Protocol**. 3. Click **OK**.
User may specify the realm name as a username suffix	Allows non-UAC endpoints to access the Infranet Controller by entering their credentials in the format user@realm.	Select this option.
Remove realm suffix before passing to authentication server	Allows users who enter their credentials with a suffix to send the user name without the suffix. Most authentication servers are not compatible with a realm suffix or decorated username.	Select this option.

Related Documentation

- Configuring Infranet Controller Standard Sign-in Pages (NSM Procedure) on page 153

Configuring Infranet Controller Standard Sign-in Pages (NSM Procedure)

A sign-in page defines the customized properties in the enduser's welcome page such as the welcome text, Help text, logo, header, footer, and error message.

To configure a standard sign-in page:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to configure the standard sign-in page.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication** > **Signing In** > **Sign-in Pages** > **User/Administrator Sign-in Pages**.
4. Add or modify the settings of the User/Administrator Sign-in Page as specified in Table 49 on page 153.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 49: Administrator Sign–in Pages Configuration Details

Option	Function	Your Action
Name	Specifies the sign-in page name.	Enter a name for the sign-in page.
Sign-in Page Type	Specifies the type of sign-in page to present to the users and administrators.	Select **Standard**.
Custom Text tab	Specifies the text to be used for the various screen labels.	Enter the required information. NOTE: If you use unsupported HTML tags in your custom message, the Infranet Controller may display the enduser's Infranet Controller home page incorrectly. When adding text to the Instructions box, format text and add links using the following HTML tags: <i>, <b>, , <font> and <a href>.
Header Appearance tab	Specifies the logo and background color in the screen header	Browse and select the logo image and select the background color.

Table 49: Administrator Sign–in Pages Configuration Details *(continued)*

Option	Function	Your Action
Custom Error Messages tab	Specifies the default text that is displayed to users if they encounter certificate errors.	Enter the missing certificate and invalid certificate error message. You can include <host>, <port>, <protocol>, and <request> variables and user attribute variables, such as <UserAttr.cn>, in the custom error messages. NOTE: The variables must follow the format <varible> to distinguish them from HTML tags, which have the format <tag>.
Help tab	Provides custom Help or additional instructions for users.	Select the **Show Help Button**, enter the Help label to display on the button and specify an HTML file to upload to the Infranet Controller.

NOTE: For information on customized sign-in pages, see the *Custom Sign-In Pages Solution Guide*.

Related Documentation

- Configuring Infranet Controller Sign-in Policies (NSM Procedure) on page 149

CHAPTER 15

Configuring Host Checker Policies

Creating Infranet Controller Global Host Checker Policies Overview

Host Checker is a client-side agent that performs endpoint health and security checks for hosts that attempt to connect to the Infranet Controller. To use Host Checker as a policy enforcement tool for managing endpoints, you must create global Host Checker policies through the NSM UI, and then implement the policies at the realm or role levels.

The Infranet Controller provides several mechanisms that you can use to enable, create, and configure Host Checker policies:

- **Predefined rules (check for third party applications)**—Host Checker contains a wide array of predefined rules that check for antivirus software, firewalls, malware, spyware, and specific operating systems from a wide variety of industry leaders. You can enable one or more of these rules within a Host Checker client-side policy to ensure that the integrated third-party applications that you specify are running on your computers in accordance with your specifications.
- **Custom rules (check for additional requirements)**—In addition to the predefined rules, you can create custom rules within a Host Checker policy to define requirements that your computers must meet. Using custom rules, you can:
  - Configure Host Checker to check for custom third-party DLLs that perform customized client-side checks.
  - Verify that certain ports are open or closed on the user's computer.
  - Confirm that certain processes are or are not running on the user's computer.
  - Check that certain files are or are not present on the client machine.
  - Evaluate the age and content of required files through MD5 checksums.
  - Confirm that registry keys are set on the client machine.
  - Check the NetBIOS name, MAC addresses, or certificate of the client machine.
  - Assess the client operating system and application service packs to ensure they are up to date.
  - Perform application and version checks to ensure that endpoints are running the correct software.
- **Custom integrated applications (implement through server API)**—For Windows clients, you can upload a third-party J.E.D.I. DLL to the Infranet Controller.
- Within a single policy, you can create different Host Checker requirements for Windows, Macintosh, Linux, and Solaris, checking for different files, processes, and products on each operating system. You can also combine any number of host check types within a single policy and check for alternative sets of rules.

NOTE: **To use Host Checker with Linux or Solaris, you must use the Firefox browser.**

Related Documentation

- Configuring Advanced Endpoint Defense Policy (NSM Procedure) on page 157
- Specifying Customized Requirements Using Custom Rules (NSM Procedure) on page 161
- Enabling Customized Server-Side Policies (NSM Procedure) on page 168

Configuring Advanced Endpoint Defense Policy (NSM Procedure)

Host Checker includes integrated antispyware functionality that can detect and remediate Windows endpoints with spyware and keyloggers. Advanced endpoint defense (AED) ensures that malware, spyware, viruses or worms are not present on endpoints that attempt to connect to the Infranet Controller, and you can restrict or quarantine these endpoints depending on your Host Checker policy configuration.

AED antispyware functionality is available on Windows platforms (including Vista) with Odyssey Access Client or with the agentless Host Checker component.

To enable and use AED antispyware:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure an AED policy.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Endpoint Security > Host Checker**.
4. Under Policies, click the **Add** button.
5. Enter a policy name and select **Advanced Endpoint Defense Policy**.
6. From the Policy Info tab, select **Enable Signature definitions check**.
7. In the Check that Signature definitions are update in (days) box, enter the frequency in days of the signature definitions database update.
8. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

When you create or configure realm or role Host Checker restrictions, you can select the AED policy to apply to that role or realm.

Related Documentation

- Configuring New Client-Side Policies (NSM Procedure) on page 157
- Configuring Infranet Controller Host Checker Access Restrictions (NSM Procedure) on page 67
- Creating Infranet Controller Global Host Checker Policies Overview on page 155

Configuring New Client-Side Policies (NSM Procedure)

You can create a variety of policies through the Host Checker client that check for antivirus software, firewalls, malware, spyware, and specific operating systems from a wide variety of industry leaders. You can also create Host Checker policies that use third-party integrity measurement verifiers (IMVs) and third-party DLLs, or check for ports, processes, files, registry keys, and the NetBIOS name, MAC addresses, or certificate of the client machine.

When creating the policies, you must define the policy name, and either enable predefined rules or create custom rules that run the specified checks. Optionally, you can specify how Host Checker should evaluate multiple rules within a single policy.

To create a standard client-side policy:

1. In the NSM navigation tree, select **Device Manager**> **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to create a standard client-side policy.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Endpoint Security > Host Checker**.
4. Under Policies, click the **Add** button.
5. Enter a policy name and select a policy type.
6. Create one or more rules to associate with the policy.
7. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Related Documentation

- Configuring Advanced Endpoint Defense Policy (NSM Procedure) on page 157
- Specifying Customized Requirements Using Custom Rules (NSM Procedure) on page 161
- Remediating Infranet Controller Host Checker Policies on page 174
- Configuring Infranet Controller Host Checker Access Restrictions (NSM Procedure) on page 67

Configuring Virus Signature Version Monitoring and Patch Assessment (NSM Procedure)

You can configure Host Checker to monitor and verify that the virus signatures, operating systems, software versions, and patches installed on client computers are up to date, and remediate those endpoints that do not meet the specified criteria.

To configure the Infranet Controller to automatically import the current virus signature version monitoring and patch management version from the Juniper Networks staging site:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure virus signature version monitoring and patch assessment.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Endpoint Security > Host Checker > Live Update Settings**.
4. Add or modify settings as specified in Table 50 on page 159.
5. Click one:

- **OK**—Saves the changes.
- **Cancel**—Cancels the modifications.

Table 50: Virus Signatures and Patch Management Info Configuration Details

Option	Function	Your Action
Virus signature version monitoring		
Virus signatures list last updated	Specifies when the virus signatures list was last updated.	Displays the date on which the virus signature list was last updated.
Auto-update virus signatures list	Specifies that the virus signatures list is automatically updated.	Select this option to automatically update the virus signatures list.
Download Path	Specifies the URL of the staging sites.	The default url of the Juniper Networks staging site is displayed.
Download Interval	Specifies how often you want the Infranet Controller to automatically import the current lists.	Select the interval.
Portal Username	Specifies the Juniper Networks portal username.	Enter the Juniper Networks portal username.
Portal Password	Specifies the Juniper Networks portal password.	Enter the Juniper Networks portal password.
Use Proxy Server	Specifies that a proxy server is used.	Select this option to use a proxy server.
Address	Specifies the IP address of the proxy server.	Enter the IP address.
Port	Specifies the port that the Juniper Networks support site will use to communicate with your proxy server.	Enter the port.
Proxy Username	Specifies the username of the proxy server.	Enter the username.
Proxy Password	Specifies the password of the proxy server.	Enter the password.
Manually import virus signature list	Specifies that the virus signatures list is manually imported.	Select from the drop-down list or click the (+) button to browse and select the list.

Table 50: Virus Signatures and Patch Management Info Configuration Details *(continued)*

Option	Function	Your Action
Patch Management Info monitoring		
Patch Management data last updated	Specifies when the patch management data was last updated.	Displays the date on which the patch management data was last updated.
Auto-update Patch Management data	Patch management data is automatically updated.	Select this option to automatically update the patch management data.
Download Path	Specifies the URL of the staging sites.	The default url of the Juniper Networks staging site is displayed.
Download Interval	Specifies how often you want the Infranet Controller to automatically import the current lists.	Select the interval.
Portal Username	Specifies the Juniper Networks portal username.	Enter the Juniper Networks portal username.
Portal Password	Specifies the Juniper Networks portal password.	Enter the Juniper Networks portal password.
Use Proxy Server	Specifies that proxy server is used.	Select this option.
Address	Specifies the IP address of the proxy server.	Enter the IP address.
Port	Specifies the port that the Juniper Networks support site will use to communicate with your proxy server.	Enter the port.
Proxy Username	Specifies the username of the proxy server.	Enter the username.
Proxy Password	Specifies the password of the proxy server.	Enter the password.
Manually import patch management data	Specifies that the patch management list is manually imported.	Select from the drop-down list or click the (+) button to browse and select the list.

Related Documentation

- Specifying Customized Requirements Using Custom Rules (NSM Procedure) on page 161
- Configuring New Client-Side Policies (NSM Procedure) on page 157

Specifying Customized Requirements Using Custom Rules (NSM Procedure)

If the predefined client-side policies and rules that come with the Infranet Controller do not meet your needs, you can create custom rules within a Host Checker policy to define requirements that your users' computers must meet.

NOTE: You can only check for registry keys, third-party DLLs, NeTBIOS names, MAC addresses, and machine certificates on Windows computers.

To create a client-side Host Checker policy:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to create a client-side Host Checker policy.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Endpoint Security > Host Checker**.
4. Create a new policy or click an existing policy in the Policies area of the page.
5. Click the tab that corresponds to the operating system for which you want to specify Host Checker options—**Windows**, **Mac**, **Linux** or **Solaris**. In the same policy, you can specify different Host Checker requirements for each operating system.
6. Under Rule Settings, click **Add**. The Add Custom Rule page appears.
7. Add or modify settings as shown in Table 51 on page 161.
8. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 51: Custom Rules Configuration Details

Rule	Usage	Your Action
Remote IMV Rule	Configures integrity measurement software that a client must run to verify a particular aspect of the client's integrity, such as the client's operating system, patch level, or virus protection.	1. Enter the rule name. 2. Select the **IMV** option. 3. Click **OK**.

Table 51: Custom Rules Configuration Details *(continued)*

Rule	Usage	Your Action
NHC Rule	(Windows only)—Specifies the location of a custom DLL. Host Checker calls the DLL to perform customized client-side checks. If the DLL returns a success value to Host Checker, then the Infranet Controller considers the rule met.	1. Enter the rule name, vendor name and the path to NHC DLL on client machines. 2. Select the **Monitor this rule for change in result** check box to continuously monitor the policy compliance of endpoints. 3. Click **OK**.
Ports Rule	Controls the network connections that a client can generate during a session. This rule type ensures that certain ports are open or closed on the client machine before the user can access the Infranet Controller.	1. Enter the rule name. 2. Select the **Required** option to specify that these ports are open or closed. 3. Enter a comma delimited port list (without spaces) of ports or port ranges, such as: 1234,11000-11999,1235. 4. Click **OK**.
Process Rule	Controls the software that a client may run during a session. This rule type ensures that certain processes are running or not running on the client machine before the user can access resources protected by the Infranet Controller.	1. Enter the rule name. 2. Select the **Required** option to specify that these ports are open or closed. 3. Enter the process name (executable file), such as: good-app.exe. 4. Enter the MD5 checksums value of each executable file to which you want the policy to apply (optional). 5. Select the **Monitor this rule for change in result** check box to continuously monitor the policy compliance of endpoints. 6. Click **OK**.

Table 51: Custom Rules Configuration Details *(continued)*

Rule	Usage	Your Action
File Rule	Ensures that certain files are present or not present on the client machine before the user can access the Infranet Controller. You may also use file checks to evaluate the age and content (through MD5 checksums) of required files and allow or deny access accordingly.	1. Enter the rule name. 2. Enter the file name such as: c:\temp\bad-file.txt or /temp/bad-file.txt. 3. Select the **Required** option to specify that these ports are open or closed. 4. Enter the minimum version of the file (optional). For example, if you require notepad.exe to be present on the client, you can enter **5.0** in the box. Host Checker accepts version 5.0 and later of notepad.exe. 5. Enter the maximum age of files in the File modified less than (days ago) box. 6. Enter the MD5 checksums value of each executable file to which you want the policy to apply (optional). 7. Select the **Monitor this rule for change in result** check box to continuously monitor the policy compliance of endpoints. 8. Click **OK**.

Table 51: Custom Rules Configuration Details *(continued)*

Rule	Usage	Your Action
Registry Setting Rule	(Windows only)—Controls the corporate PC images, system configurations, and software settings that a client must have to access the Infranet Controller. This rule type ensures that certain registry keys are set on the client machine before the user can access the Infranet Controller. You may also use registry checks to evaluate the age of required files and allow or deny access accordingly.	1. Enter the rule name. 2. Select **Registry root key** from the drop-down list. 3. Enter the path to the application folder for the registry subkey. 4. Enter the name of the key's value 5. Select the key value's type (**String, Binary**, or **DWORD**) from the drop-down list (optional). 6. Enter the registry value. 7. Select the **Set Registry value specified in the criteria** check box. 8. Select **Minimum Version** to allow the specified version or newer versions of the application. For example, you can use this option to specify version information for an antivirus application to make sure that the client antivirus software is current. The Infranet Controller uses lexical sorting to determine if the client contains the specified version or later. 9. Select the **Monitor this rule for change in result** check box to continuously monitor the policy compliance of endpoints. 10. Click **OK**.
NetBIOS Rule	(Windows only, does not include Windows Mobile)—Checks the NetBIOS name of the client machine before the user can access the Infranet Controller.	1. Enter the rule name. 2. Select the **Required** option to require that NetBIOS name of the client machine matches or does not match any one of the names you specify. 3. Enter a comma-delimited list (without spaces) of NetBIOS names. The name can be up to 15 characters in length. You can use wildcard characters in the name and it is not case-sensitive. For example: md*, m*xp and *xp all match MDXP. 4. Click **OK**.

Table 51: Custom Rules Configuration Details *(continued)*

Rule	Usage	Your Action
MAC Address Rule	(Windows only)—Checks the MAC addresses of the client machine before the user can access the Infranet Controller.	1. Enter the rule name. 2. Select the **Required** option to require that a MAC address of the client machine matches or does not match any of the addresses you specify. 3. Enter a comma-delimited list (without spaces) of MAC addresses in the form XX:XX:XX:XX:XX:XX where the X's are hexadecimal numbers. For example: 00:0e:1b:04:40:29. 4. Click **OK**.
Machine Certificate Rule	(Windows only)— Checks that the client machine is permitted access by validating the machine certificate stored on the client machine.	1. Enter the rule name. 2. From the Select Issuer Certificate list, select the certificate that you want to retrieve from the user's machine and validate. Or, select **Any Certificate** to skip the issuer check and only validate the machine certificate based on the optional criteria that you specify below. 3. Enter **Certificate field and Expected value** to specify any additional criteria that Host Checker should use when verifying the machine certificate. 4. Click **OK**.

Related Documentation

- Configuring New Client-Side Policies (NSM Procedure) on page 157
- Remediating Infranet Controller Host Checker Policies on page 174

Configuring a Patch Assessment Custom Rule (NSM Procedure)

For Windows clients, you can use the system management server (SMS) remediation feature to provide automatic updates to noncompliant software. By using a patch assessment custom rule, you can force the client to initiate the software update immediately after the patch assessment check.

To configure a patch assessment custom rule:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure a patch assessment custom rule.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Endpoint Security > Host Checker**.
4. Under Policies, select an existing policy or click the **Add** button to create a policy.
5. Under Platforms, select **Windows**.
6. Select the **Settings** tab, and then select **Patch Assessment Rules**.
7. Click **Add**. The New Custom: Patch Assessment page appears.
8. Enter a name for the integrity measurement rule.
9. Select either **Scan for specific products** or **Scan for specific patches**.
10. Select either **Scan for specific products > All products** or **Scan for specific products > Specific products**. The Host Checker checks for all of the exposed patches on the endpoint.
    a. If you select **All Products**, then the Host Checker scans for all of the exposed patches on the endpoint.
        - Click the **Ignore these patches** button to select specific patches that you wish to ignore for all products. Then click the **Add** button.
        - Click the **OK** button to save information on specific patches that you wish to ignore.
        - For Microsoft products, clear the check boxes to determine the severity level of the patches that you wish to ignore. For example, if you wanted to check for only critical patches for the selections, clear the check boxes for **Severity Important**, **Severity Moderate**, **Severity Low**, and **Severity Unspecified**.
    b. If you select **Specific Products**, then the Host Checker scans for specific product versions and ignores specific patches of those products.
        - Select software products from the Non-members area and add then to the Members area.
        - Click the **Ignore these products** button to ignore specific patches pertaining to products.
        - From the Non-members area, select the patches you wish to ignore, and click the **Add** button to move it to the Members area
        - Click the **OK** button to save information on specific patches that you wish to ignore.
11. Select **Scan for specific patches** to scan for specific patches from the list of available patches.

- Select patches from the Non-members area and click **Add** to move the patches to the Members area.

12. Select **Enable SMS patch update** to direct the Infranet Controller to notify the SMS server to update the client in the event of a failed patch assessment rule. SMS remediation is triggered each time Host Checker detects that an endpoint is not compliant.
13. Click the **OK** button to save the changes.
14. Click the **Remediation** tab on the main Host Checker Policy page, and then select the **Send reason strings** option to display remediation information to users.

Related Documentation

- Specifying Customized Requirements Using Custom Rules (NSM Procedure) on page 161
- Configuring the Remote IMV Server (NSM Procedure) on page 167
- Configuring Infranet Controller Host Checker Access Restrictions (NSM Procedure) on page 67

Configuring the Remote IMV Server (NSM Procedure)

The server-side components of Trusted Network Computing (TNC) are: the TNC-server (TNCS) and the integrity measurement verifiers (IMVs). You can configure the remote IMV server to communicate with the Infranet Controller.

To configure a remote IMV server to communicate with the Infranet Controller:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure the remote IMV server.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Endpoint Security > Host Checker**.
4. Add or modify settings as specified in Table 52 on page 167.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 52: IMV Server Configuration Details

Option	Function	Your Action
Remote IMV > Remote IMV Servers		
Name	Specifies a name for the remote IMV server.	Enter a name for the remote IMV server.
Description	Describes the server.	Enter a brief description about the server.

Table 52: IMV Server Configuration Details *(continued)*

Option	Function	Your Action
Host	Specifies the host.	Enter either the IP address or hostname as defined in the server certificate.
Port	Specifies the port number used by the Infranet Controller to communicate with the remote IMV server.	Enter a unique port number. Ensure that no other service is using this port number. The default port number is the same as the default HTTPS port number.
Shared secret	Specifies the shared secret information.	Enter the same shared secret used in the client information entry on the remote IMV server.
Remote IMV > Remote IMVs		
Name	Specifies a name for the remote IMV.	Enter a name for the remote IMVs.
Description	Describes the IMV.	Enter a brief description about the IMV.
IMV Name	Specifies the IMV name that matches the “human readable name” in the IMV’s well-known registry key on the remote IMV server.	Enter a name for the IMV.
Primary Server	Specifies the primary remote IMV server where the IMV is installed.	Select the primary remote IMV server.
Secondary Server	Specifies the secondary remote IMV server where the IMV is installed. The secondary server acts as a failover in case the primary server becomes unavailable.	Select the secondary remote IMV server.

Related Documentation

- Remediating Infranet Controller Host Checker Policies on page 174
- Configuring Infranet Controller Host Checker Access Restrictions (NSM Procedure) on page 67

Enabling Customized Server-Side Policies (NSM Procedure)

For Windows clients, you can create global Host Checker policies that take a third-party J.E.D.I. DLL that you upload to the Infranet Controller and run on client machines.

NOTE: This feature is primarily provided for backwards compatibility. We recommend that you use integrity measurement collectors (IMCs) and integrity measurement verifiers (IMVs) instead.

To enable a customized server-side Host Checker policy:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to enable a customized server-side Host Checker policy.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Endpoint Security > Host Checker > Settings**.
4. Under Policies, create a new policy and select **3rd Party Policy**.
5. Add or modify settings as specified in Table 53 on page 169.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 53: Customized Server-Side Policies Configuration Details

Option	Function	Your Action
Package	Specifies the 3rd party policy package.	Select the package from the drop-down or browse for the package using the browse (+) button.
File Name	Specifies the filename.	Enter a filename.
Enable Custom Instructions	Specifies that custom instructions can be displayed to the user on the Host Checker remediation page.	Select this option and enter the custom instructions you want to display to the user on the Host Checker remediation page. You can use the following HTML tags to format text and add links to resources such as policy servers or Web sites: <i>, <b>, , <font>, and <a href>.
Remediate	Specifies that remediation actions are enabled.	Select this option.
Kill Processes	Specifies the processes you want to kill if the user's computer does not meet the policy requirements. You can include an optional MD5 checksum for the process.	Select this option and on each line enter the name of one or more processes you want to kill. NOTE: You cannot use wildcards in the process name.

Table 53: Customized Server-Side Policies Configuration Details *(continued)*

Option	Function	Your Action
Delete Files	Specifies the filenames to be deleted if the user's computer does not meet the policy requirements.	Select this option and add or modify files to be deleted. NOTE: You cannot use wildcards in the filename.
Send reason strings	Displays a message to users (called a reason string) that is returned by Host Checker or IMV and explains why the client machine does not meet the Host Checker policy requirements. This option applies to predefined rules, custom rules, and to third-party IMVs that use extensions in the Juniper Networks TNC SDK.	Select this option.

Related Documentation

- Remediating Infranet Controller Host Checker Policies on page 174
- Configuring Infranet Controller Host Checker Access Restrictions (NSM Procedure) on page 67

Executing Host Checker Policies

When the user tries to access the Infranet Controller, Host Checker evaluates its policies in the following order:

1. **Initial evaluation**—When a user first tries to access the Infranet Controller sign-in page, Host Checker performs an initial evaluation. Using the rules you specify in your policies, Host Checker verifies that the client meets your endpoint requirements and returns its results to the Infranet Controller. Host Checker performs an initial evaluation regardless of whether you have implemented Host Checker policies at the realm, role, or resource policy level.

   For agentless access deployments, if the user navigates away from the Infranet Controller sign-in page after Host Checker starts running but before signing in to the Infranet Controller, Host Checker continues to run on the user's machine until the Host Checker process times out. If the Infranet Controller does not receive a result from Host Checker for any reason (including because the user manually terminated Odyssey Access Client or Host Checker), the Infranet Controller displays the remediation instructions if they are enabled, or else displays an error and directs the user back to the sign-in page.

   Otherwise, if the Host Checker process returns a result, the Infranet Controller goes on to evaluate the realm-level policies.

2. **Realm-level policies**—The Infranet Controller uses the results from Host Checker's initial evaluation to determine which realms the user may access. Then, the Infranet Controller displays or hides realms from the user, only allowing him to sign into those realms that you enable for the sign-in page, and if he meets the Host Checker requirements for each realm. If the user cannot meet the Host Checker conditions required by any of the available realms, the Infranet Controller does not display the sign-in page. Instead, it displays an error stating the user has no access unless you configure remediation actions to help the user bring his computer into compliance.

   

   NOTE: **The Host Checker performs realm-level checks when the user first signs into the Infranet Controller and during the user's session.**

3. **Role-level policies**—After the user signs into a realm, the Infranet Controller evaluates role-level policies and maps the user to the role or roles if he meets the Host Checker requirements for those role(s). Then, the Infranet Controller pushes the role and policy information to the Infranet Enforcer and Odyssey Access Client.

   If Host Checker returns a different status during a periodic evaluation, the Infranet Controller dynamically remaps the user to roles based on the new results. If the user loses rights to all available roles during one of the periodic evaluations, the Infranet Controller disconnects the user's session unless you configure remediation actions to help the user bring his computer into compliance.

4. **Infranet Enforcer resource access policies and Host Enforcer policies**—After the Infranet Controller pushes the role and policy information to the Infranet Enforcer and Odyssey Access Client, the user may try to access a protected resource that is controlled by an Infranet Enforcer resource access policy or Host Enforcer policy. When he does, the Infranet Enforcer or Odyssey Access Client determines whether or not to allow or deny the user access to the protected resource based on the user's assigned role.

   If Host Checker returns a different status during a periodic evaluation, the new status can change the assigned roles. The Infranet Controller then pushes the role and policy

information to the Infranet Enforcer and Odyssey Access Client, which could prevent the user from accessing the protected resource.

With either a success or failure, Odyssey Access Client or Host Checker remains on the client. Windows users can manually uninstall Odyssey Access Client from the control panel.

If you enable client-side logging through the Infranet Controller, then the directory where Odyssey Access Client is installed contains a log file, which the Infranet Controller appends each time Odyssey Access Client or Host Checker runs.

You may specify that the Infranet Controller evaluate your Host Checker policies only when the user first tries to access the realm or role that references the Host Checker policy. Or, you may specify that the Infranet Controller periodically reevaluate the policies throughout the user's session. If you choose to periodically evaluate Host Checker policies, the Infranet Controller dynamically maps users to roles and instructs the Infranet Enforcer or Odyssey Access Client to allow users access to new resources based on the most recent evaluation.

Use a Host Checker restriction to require client machines to meet the specified Host Checker policies to access an Infranet Controller sign-in page or be mapped to a role.

Related Documentation

- Implementing Infranet Controller Host Checker Policies (NSM Procedure) on page 172
- Remediating Infranet Controller Host Checker Policies on page 174

Implementing Infranet Controller Host Checker Policies (NSM Procedure)

Implementing Infranet Controller Host Checker policies involves:

- Restricting Infranet Controller and Resource Access Through Host Checker on page 172
- Configuring Host Checker Restrictions on page 173

Restricting Infranet Controller and Resource Access Through Host Checker

After you create global policies, you can restrict Infranet Controller and resource access through the Host Checker in a policy or role:

Realm authentication policy—When administrators or users try to sign in to the Infranet Controller, the Infranet Controller evaluates the specified realm's authentication policy to determine if the preauthentication requirements include Host Checker. You can configure a realm authentication policy to download Host Checker, launch Host Checker, and enforce Host Checker policies specified for the realm, or not require Host Checker. The user must sign in using a computer that adheres to the Host Checker requirements specified for the realm. If the user's computer does not meet the requirements, then the Infranet Controller denies access to the user unless you configure remediation actions to help the user bring his computer into compliance.

To configure realm-level restrictions:

1. In the NSM navigation tree, select **Device Manager> Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to realm-level restrictions.
3. Click the **Configuration** tab. In the configuration tree,
   - select **Administrators > Admin Realms > Select Realm > Authentication Policy > Host Checker** to configure administrator realm-level restrictions.
   - select **Users > User Realms > Select Realm > Authentication Policy > Host Checker** to configure user realm-level restrictions.
4. Configure realm-level restrictions.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Role—When the Infranet Controller determines the list of eligible roles to which it can map an administrator or user, it evaluates each role's restrictions to determine if the role requires that the user's computer adheres to certain Host Checker policies. If it does and the user's computer does not follow the specified Host Checker policies, then the Infranet Controller does not map the user to that role unless you configure remediation actions to help the user bring his computer into compliance.

To configure role-level restrictions:

1. In the NSM navigation tree, select **Device Manager> Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to role-level restrictions.
3. Click the **Configuration** tab. In the configuration tree,
   - select **Administrators > Admin Roles > Select Role > General > Restrictions** to configure administrator role-level restrictions.
   - select **Users > User Roles > Select Role > General > Restriction** to configure user role-level restrictions.
4. Configure role-level restrictions.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Configuring Host Checker Restrictions

To configure Host Checker restrictions:

1. Specify global Host Checker restrictions. See “Creating Infranet Controller Global Host Checker Policies (NSM Procedure).”
2. If you want to implement Host Checker at the *realm* level and *role* level, see “Configuring Infranet Controller Host Checker Access Restrictions (NSM Procedure).”
3. If you want to create role-mapping rules based on a user’s Host Checker status, see “Configuring Role Mapping Rules (NSM Procedure).”

Related Documentation

- Remediating Infranet Controller Host Checker Policies on page 174
- Executing Host Checker Policies on page 170

Remediating Infranet Controller Host Checker Policies

You can specify general remediation actions that you want Host Checker to take if an endpoint does not meet the requirements of a policy. For example, you can display a remediation page to the user that contains specific instructions and links to resources to help the user bring their endpoint into compliance with Host Checker policy requirements.

You can also choose to include a message to users (called a reason string) that is returned by Host Checker or an integrity measurement verifier (IMV) that explains why the client machine does not meet the Host Checker policy requirements.

General Host Checker Remediation User Experience

Users may see the remediation page in the following situations:

- Before the user signs in:
  - If you enable custom instructions or reason strings for a policy that fails, the Infranet Controller displays the remediation page to the user. The user has two choices:
    - Take the appropriate actions to make his computer conform to the policy and then click the **Try Again** button on the remediation page. Host Checker checks the user’s computer again for compliance with the policy.
    - Leave his computer in its current state and click the **Continue** button to sign in to the Infranet Controller. He cannot access the realm, role, or resource that requires compliance with the failed policy.

      NOTE: If you do not configure the Infranet Controller with at least one realm that allows access without enforcing a Host Checker policy, the user must bring his computer into compliance before signing into the Infranet Controller.

  - If you do not enable custom instructions or reason strings for a policy that fails, Host Checker does not display the remediation page to the user. Instead, a message appears telling the user that no additional information has been provided and to

contact the system administrator. The Infranet Controller does not assign the user a role that allows access to protected resources.

- After the user signs in:
  - (**Odyssey Access Client only**) During a session, if a user's computer becomes noncompliant with the requirements of a Host Checker policy, a pop-up message appears briefly in the system tray that informs the user of the noncompliance. The user can display the remediation page by right-clicking the **Odyssey Access Client** icon in the system tray, choosing Odyssey Access Client Manager from the context menu, and then clicking the **How do I resolve this problem** link in the status section of the Odyssey Access Client window.
  - (**Agentless—Windows, Macintosh, Linux and Solaris**) During a session, if a user's agentless computer becomes noncompliant with the requirements of a Host Checker policy, the Infranet Controller displays the remediation page to inform the user of the noncompliance. On Windows agentless computers, Host Checker displays a bubble and tray icon if the endpoint becomes noncompliant. The user must click the bubble or tray icon to open a browser window that contains the remediation instructions. On Macintosh, Linux, or Solaris agentless computers, Host Checker automatically opens a browser window that contains the remediation instructions as soon as the endpoint is noncompliant.

Related Documentation

- Creating Infranet Controller Global Host Checker Policies Overview on page 155
- Executing Host Checker Policies on page 170
- Configuring New Client-Side Policies (NSM Procedure) on page 157
- Enabling Customized Server-Side Policies (NSM Procedure) on page 168
- Implementing Infranet Controller Host Checker Policies (NSM Procedure) on page 172

Configuring Infranet Controller General Host Checker Options (NSM Procedure)

You can configure global options for Host Checker that apply to any user for whom Host Checker is required in an authentication policy or a role mapping rule.

To configure general Host Checker options:

1. In the NSM navigation tree, select **Device Manager**> **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure general Host Checker options.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Endpoint Security > Host Checker > Settings** tab.
4. Add or modify Host Checker settings as specified in Table 54 on page 176.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 54: Host Checker Options Configuration Details

Option	Function	Your Action
Perform check every (minutes)	Specifies the interval at which you want Host Checker to perform policy evaluation on a client machine.	Enter the interval in minutes. NOTE: If you enter a value of zero, Host Checker runs on the client machine only when the user signs into the Infranet Controller for the first time.
Client-side process, login inactivity timeout (minutes)	Specifies the time-out interval, if the user navigates from the sign-in page or if the user downloads the Host Checker over a slow connection.	Enter the time-out interval in minutes.

Related Documentation

- Configuring Infranet Controller Host Checker Access Restrictions (NSM Procedure) on page 67

Configuring Host Checker Automatic Installation (NSM Procedure)

You can configure the Infranet Controller to automatically install Host Checker on client computers only for agentless access deployments.

NOTE: To install Host Checker, users must have appropriate privileges, as described in the *Client-Side Changes Guide* on the Juniper Networks Support site.

To automatically install Host Checker on client computers:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to automatically install Host Checker.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Endpoint Security > Host Checker**.
4. From the Settings tab, select the **Auto-upgrade Host Checker** check box.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Related Documentation

- Configuring Infranet Controller Host Checker Access Restrictions (NSM Procedure) on page 67

Configuring Infranet Controller Host Checker Logs (NSM Procedure)

The Infranet Controller writes a client-side log to endpoints, when client-side logging for the Host Checker and Odyssey Access Client is enabled.

NOTE: Because these settings are global, the Infranet Controller writes a log file to all clients that use the feature for which you enable client-side logging. Also, the Infranet Controller does not remove client-side logs. Users need to manually delete log files from their clients. For information about where the Infranet Controller installs log files, see the *Client-Side Changes Guide* on the Juniper Networks Customer Support Center.

To configure global client-side log settings:

1. In the NSM navigation tree, select **Device Manager**> **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to specify global client-side log settings.
3. Click the **Configuration** tab. In the configuration tree, select **System > Log/Monitoring > Client Log > Settings**.
4. Select the **Host Checker** check box.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Related Documentation

- Configuring Infranet Controller Host Checker Access Restrictions (NSM Procedure) on page 67
- Creating Infranet Controller Global Host Checker Policies Overview on page 155

PART 4

Managing an Infranet Controller

CHAPTER 16

Unified Access Control Manager

UAC Manager in NSM Overview

Opening the UAC Manager in the Configure module of the NSM UI allows you to view UAC policy attributes from the perspective of Infranet Controllers and enforcement points.

The Infranet Controller View

The NSM main display area is horizontally divided into two tables. When you select the Infranet Controller view, the upper table lists all the Infranet Controllers managed by NSM's current domain. If the Infranet Controllers are in cluster mode, the table also displays whether they are Active-Active or Active-Passive clusters. Selecting an Infranet Controller causes NSM to list all the enforcement points and their location groups that are associated with the selected Infranet Controller in the lower table. If the association is created with a load balancer option, then the load balancer is also displayed. In Active-Active cluster mode, the Infranet Controller cluster member name is displayed but not in the case of Stand Alone and Active-Passive cluster modes. From the Infranet Controller table, you can edit the configuration of a selected Infranet Controller using the edit button provided above the Infranet Controller table. The edit dialog is similar to the edit device action in the Device Manager.

The Enforcement Point View

When you select the enforcement point view, the NSM main display area is horizontally divided into the enforcement point table at the top and tab views of associated Infranet Controllers and port details. NSM displays only EX-series switches managed by a current domain in the enforcement point table. Selecting an enforcement point causes NSM to populate relevant information in the tab views. From the Infranet Controller tab view,

you can view the associated Infranet Controller and its location group information. From the Port details tab, you can see the 802.1X enabled port names and their details.

Related Documentation

- Associating Enforcement Points with an Infranet Controller Using the UAC Manager on page 182
- Enabling Dot1x Ports on the Enforcement Points Using the UAC Manager on page 184
- Disassociating the Configuration Between an Enforcement Point and an Infranet Controller on page 183
- Disabling the Dot1x Ports on an Enforcement Point Using the UAC Manager on page 185

Associating Enforcement Points with an Infranet Controller Using the UAC Manager

NOTE:

Before you begin associating enforcement points with an Infranet Controller, ensure the following:

- **The administrator must have proper privileges for associating enforcement points with an Infranet Controller in the current domain.**
- **The Infranet Controller and the enforcement points should be managed by NSM in the current domain.**
- **The connection status of the devices to be associated should be "up" in NSM.**

To associate enforcement points with an Infranet Controller:

1. In the NSM navigation tree, select **UAC Manager > Infranet Controller**. The Infranet Controller workspace appears.
2. Select the stand-alone Infranet Controller or the Infranet Controller cluster to which you need to associate enforcement points.

NOTE: **The Infranet Controller is deployed either as a standalone device or as a cluster (active-active cluster mode or active-passive cluster mode).**

3. Click the **Add Enforcement Point** button. The Select Enforcement Points dialog box appears with the list of enforcement points managed by NSM but not yet associated with the Ex-series switch.
4. If the Infranet Controller is deployed as a active-active cluster, select the cluster member.
5. Select the Ex-series switch to which the association has to be made, and move it to the Selected Enforcement Points list.
6. Enter the RADIUS secret shared between the Infranet Controller and enforcement points.

7. Select the Location Group the enforcement points must belong to in the selected Infranet Controller. Each enforcement point can be associated with only one Location Group available in the Infranet Controller.
8. Enter the Infranet Controller port number to which the enforcement point should communicate. The default port is 1812.
9. Enter the IP address that should be used for RADIUS communication. If you do not specify an address, the enforcement point's management IP address is used by default. You have the option to select the IP address of the RADIUS communication server only if you select a single enforcement point because the IP address to communicate with an Infranet Controller is unique.
10. Select **Use Load Balancer with IP Address** if the Infranet Controller is load balancer administered. The IP address of the Load Balancer is then used as the Radius Server in the EX-series switch configuration.
11. Select **Run "Update Device" task** to push configuration changes on both the Infranet Controller and enforcement points. The configuration status of the enforcement points changes to Managed, InSync.
12. Select **Run "Summarize Delta Config" task** to ensure the association between the Infranet Controller and enforcement point in the application database. The configuration status of these devices becomes Managed, NSM Changed.
13. Click **OK**. The selected enforcement points are listed under the associated Infranet Controller.

Related Documentation

- Enabling Dot1x Ports on the Enforcement Points Using the UAC Manager on page 184
- Disassociating the Configuration Between an Enforcement Point and an Infranet Controller on page 183
- Disabling the Dot1x Ports on an Enforcement Point Using the UAC Manager on page 185
- UAC Manager in NSM Overview on page 181

Disassociating the Configuration Between an Enforcement Point and an Infranet Controller

To disassociate enforcement points from an Infranet Controller:

1. In the NSM navigation tree, select **UAC Manager > Infranet Controller**. The Infranet Controller workspace appears.
2. Select the Infranet Controller and the Ex-series switch that needs to be disassociated.
3. Click the **Delete Enforcement Point** button. The Disassociate Enforcement Points dialog box appears with the list of enforcement points to be deleted.
4. Select **Run "Update Device" task** to push configuration changes on both the Infranet Controller and enforcement points. The configuration status of the enforcement points changes to Managed, InSync.

5. Select the check box to run a Summarize Delta Config task that ensures the association between the Infranet Controller and enforcement point in the application database. The configuration status of these devices becomes Managed, NSM Changed.
6. Click **OK**. The selected enforcement points are removed from the Infranet Controller. Resolving Configuration Conflicts with the Infranet Controller in

Related Documentation

- Enabling Dot1x Ports on the Enforcement Points Using the UAC Manager on page 184
- Associating Enforcement Points with an Infranet Controller Using the UAC Manager on page 182
- Disabling the Dot1x Ports on an Enforcement Point Using the UAC Manager on page 185
- UAC Manager in NSM Overview on page 181

Enabling Dot1x Ports on the Enforcement Points Using the UAC Manager

NOTE:

Before you begin enabling dot1x ports on the enforcement points, ensure the following:

- The administrator must have proper privileges for associating enforcement points with an Infranet Controller in the current domain.
- The connection status of the devices to be associated should be “up” in NSM.

To enable dot1x ports on the enforcement points:

1. In the NSM navigation tree, select **UAC Manager > Enforcement Point**. The Enforcement Point workspace appears. The Infranet Controller associated with an enforcement point and the dot1x ports enabled for the enforcement point are displayed in the workspace.
2. Select the Ex-series switch in which you need to enable dot1x ports.
3. Click the **Enable Dot1x on Port(s)** button. The Select ports to enable Dot1x dialog box appears with the list of ports on which dot1x can be enabled.
4. Select one or more ports from the list, and select one of the following supplicant modes:
   - Single Secure—A single dedicated host is authenticated.
   - Multiple—Multiple hosts are individually authenticated.
   - Single—Only the first host is authenticated. All the remaining hosts use the same authentication made by the first host.
5. Select **Enable reauthentication** to allow reauthentication in case of authentication failures.

6. Specify the action to be taken in case of authentication failure:
   - Deny access—Denies access to the client.
   - Move to VLan—Moves the client to VLANs available in the switch.
7. Select **Run "Update Device" task** to apply the device configuration.
8. Select **Run "Summarize Delta Config" task** to view the difference in the configuration.
9. Click **OK** to enable the dot1x ports on the enforcement points. The delta configuration that was pushed to the device is displayed.

Related Documentation

- Disabling the Dot1x Ports on an Enforcement Point Using the UAC Manager on page 185
- Associating Enforcement Points with an Infranet Controller Using the UAC Manager on page 182
- Disassociating the Configuration Between an Enforcement Point and an Infranet Controller on page 183
- UAC Manager in NSM Overview on page 181

Disabling the Dot1x Ports on an Enforcement Point Using the UAC Manager

To disable dot1x ports on an enforcement point:

1. In the NSM navigation tree, select **UAC Manager > Enforcement Point**. The Enforcement Point workspace appears.
2. Select the Ex-series switch on which the dot1x port needs to be disabled.
3. Select the **Dot1x Enabled Ports** tab. The dot1x enabled ports on the enforcement point is displayed.
4. Select the port on which dot1x needs to be disabled, and click the **Delete Dot1x Port** button. The Remove Dot1x on Selected ports dialog box appears with the list of ports to be deleted.
5. Select **Run "Update Device" task** to push configuration changes on the enforcement point. The configuration status of the enforcement points changes to Managed, InSync. Ports on which 802.1X is disabled are removed from the enforcement point.
6. Select the check box to run a Summarize Delta Config task that ensures the association between the enforcement point and the ports in the application database. The configuration status of these devices become Managed, NSM Changed.
7. Click **OK** to disable the selected dot1x ports. The delta configuration that was pushed to the device is displayed.

Related Documentation

- Enabling Dot1x Ports on the Enforcement Points Using the UAC Manager on page 184
- Associating Enforcement Points with an Infranet Controller Using the UAC Manager on page 182

- Disassociating the Configuration Between an Enforcement Point and an Infranet Controller on page 183
- UAC Manager in NSM Overview on page 181

CHAPTER 17

Using System Management Features in an Infranet Controller

Managing Large Binary Data Files

Large binary data files that form a part of the configuration of Secure Access and Infranet Controller devices are handled differently from the remainder of the configuration in NSM. The size of some of these binary files could make configurations large enough to overload resources on the NSM server. Consequently, only the large binary files you specify are imported into NSM, and those files are configured as shared objects, which avoids duplication if they are applied to multiple devices.

To download a large binary data file and link that file into the Secure Access or Infranet Controller device configuration tree:

1. In the Device Manager, right-click the device icon and select **Import Device** from the list to import the Secure Access or Infranet Controller device configuration. When the import job is finished, the device object configuration contains the MD5 stubs for each of the large binary data files.
2. Upload each required large binary data file onto the NSM client workstation. Use the device Web UI to upload binary files form the Secure Access or Infranet Controller device. Other files, such as ESAP configuration files, should be downloaded from the site of origin.
3. Create a shared object in the NSM Object Manager for the binary file:
   a. In the NSM navigation tree, select **Object Manager > Binary data**, and then click the **Add** icon.
   b. In the Binary Data dialog box, enter a name for the object, select a color for the object icon, add a comment if desired, and select the file you uploaded in Step 2.

c. Click **OK**.

4. Link the shared object to the corresponding node in the device configuration tree:

   a. In the Device Manager, double-click the Secure Access or Infranet Controller device to open the device editor, and then select the **Configuration** tab.

   b. Navigate to the node in the configuration where you want to load the binary file. For example, to load an ESAP package, expand **Authentication** and then select **Endpoint Security**. In the Host Checker tab, select **Endpoint Security Assessment Plug-Ins**, and then click the **Add** icon.

   c. Select the shared object. To continue the ESAP example, in the New Endpoint Security Assessment Plug-Ins dialog box, enter a version number, and select a shared binary data object from the Path to Package list.

   d. Click **OK**. If the object you want is not in the list, you can add it to the shared binary data list by clicking the **Add** icon. The Binary Data dialog box appears as in Step 3.

   e. Click **OK** to save the newly configured links.

Related Documentation

- Importing an Infranet Controller Device Through Not Reachable Workflow on page 11
- Adding an Infranet Controller Cluster with Imported Cluster Members on page 24

Configuring Infranet Controller System Options (NSM Procedure)

You can configure the following Infranet Controller system options through NSM:

- Version monitoring
- GNU zip (gzip) compression
- Kernel watchdog
- File system auto-clean
- Enable automatic upgrade
- End-user localization

To configure the Infranet Controller system options:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure system options.
3. Click the **Configuration** tab. In the configuration tree, select **System > Maintenance > System Maintenance Options**.
4. Add or modify settings as specified in Table 55 on page 189.
5. Click one:
   - **OK**—Saves the changes.

- **Cancel**—Cancels the modifications.

Table 55: System Maintenance Options Configuration Details

Option	Function	Your Action
Enable automatic upgrade of UAC Agents	Allows you to more effectively manage Odyssey Access Client endpoints and roll out features at your discretion. By default, the Infranet Controller automatically upgrades UAC agents of users who connected if the agent is not current.	Select this option to disable automatic upgrade of the UAC agent.
Automatic Version Monitoring	Keeps your system current and secure by having the Infranet Controller notify you about critical software patches and updates. To do this, it reports to Juniper Networks the following data: your company name, an MD5 hash of your license settings, and information describing the current software version.	Select this option to automatically receive notifications of critical software patches and updates.
Enable gzip compression	Reduces download speeds when using HTTP compression-enabled browsers.	Select this option to reduce the amount of data sent to browsers that support HTTP compression.
Enable Kernel Watchdog	Enables the kernel watchdog that automatically restarts the system under kernel lock down or when the kernel runs low on some key resource. CAUTION: Changing this setting will reboot the system.	Select this option to allow the Infranet Controller to automatically shut down in the event of an issue with the kernel.
Enable File System Auto-clean Feature	Enables the system to automatically clean up the file system when disk utilization reaches 90%. CAUTION: When enabled, this feature might result in loss of data that might be relevant in debugging system problems that occurred a week ago or earlier. (That is, old debug logs, core files, and snapshots might be removed.)	Select this option to allow the system to automatically clean up the file system when disk utilization reaches 90%.
End-user localization	Enables the language version for the Odyssey Access Client end user.	Select the language version for the Odyssey Access Client end user or accept the default.

Related Documentation

- Infranet Controller Services and Device Configurations Supported in NSM on page 5

Removing an Infranet Controller from NSM Management (NSM Procedure)

Deleting a device removes all device configuration information from the management system, but might be the best solution if you need to perform extensive troubleshooting or reconfigure the device locally.

To remove an Infranet Controller from NSM management:

1. In the NSM navigation tree, select **Device Manager**> **Devices**.
2. Click the **Device Tree** tab.
3. From the device tree, select the Infranet Controller device that you would like to remove from NSM management.
4. Right-click and select **Delete**, or click the **Delete** button. The Delete dialog box appears. If the device is referenced in a firewall rule, this dialog box displays the rules that reference it. You can click the links that appear to display the security policies to view or edit those references.
5. Remove the device by clicking **Next**. The Delete dialog box displays the progress of the deletion.
6. After NSM finishes, click **Finish** to close the dialog box.

Related Documentation

- Deactivating a DMI Agent in an Infranet Controller (NSM Procedure) on page 190
- Importing an Infranet Controller Device Through Not Reachable Workflow on page 11
- Adding an Infranet Controller Cluster with Imported Cluster Members on page 24

Deactivating a DMI Agent in an Infranet Controller (NSM Procedure)

To deactivate the DMI Agent in an Infranet Controller:

1. In the NSM navigation tree, select **Device Manager**> **Devices**.
2. Click the **Device Tree** tab.
3. From the device tree, select the Infranet Controller device in which you would like to deactivate the DMI agent.
4. Click the **Configuration** tab. In the configuration tree, select **System > Configuration > DMI Agent**.
5. In the DMI Agent page, clear the **Enabled** check box.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Related Documentation

- Removing an Infranet Controller from NSM Management (NSM Procedure) on page 190

- Adding an Infranet Controller Cluster with Imported Cluster Members on page 24

CHAPTER 18

Configuring the Infranet Controller to Interoperate with IDP

NOTE: For the Infranet Controller to interoperate with IDP, the ic-xxxx-ADD-tctrl coordinated threat control license is required.

Configuring ISG-IDP as a Sensor on the Infranet Controller (NSM Procedure)

When ISG-IDP is configured, ISG-IDP notifies the Infranet Controller when an attack event is detected from any endpoint. To avoid overwhelming the SSH connection between the Infranet Controller and the Infranet Enforcer, the number of attack notifications is limited to 10 per second. If additional attacks are detected, the Infranet Enforcer holds an additional 10 notifications in a queue.

To configure ISG-IDP on the Infranet Controller:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device on which you want to configure ISG-IDP.
3. Click the **Configuration** tab. In the configuration tree, select **UAC > Infranet Enforcer**. The corresponding workspace appears.
4. Select the name of the Enforcer on which you want to configure IDP.
5. Select the **Use IDP Module** check box.
6. Select **IDP for this IC's sessions only** to restrict ISG-IDP to report attacks from end points whose authentication table entries are present on ISG-IDP.

   Do not select this option, if you want attack alerts for attacks generated by unknown users to be published to IF-MAP.

7. Select **1-Info** through **5-Critical** from the IDP Severity Filter drop-down list. The severity filter allows you to specify the level of attacks that the Infranet Enforcer reports to the Infranet Controller. For example, if you select **3**, only level 3 attacks or greater is reported.
8. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Related Documentation

- Configuring Infranet Controller Sensor Settings for Connecting to a Standalone IDP Device (NSM Procedure) on page 194
- Configuring Sensor Event Policies (NSM Procedure) on page 196

Configuring Infranet Controller Sensor Settings for Connecting to a Standalone IDP Device (NSM Procedure)

You can specify system settings that the Infranet Controller uses to establish a connection to a Juniper Networks Intrusion Detection and Prevention (IDP) device. The sensor settings allow you to perform a number of tasks related to configuring and managing interaction between the Infranet Controller and an IDP device.

1. Creating an IDP Device Entry on page 194
2. Enabling or Disabling the Connection to an Existing IDP Device on page 195

Creating an IDP Device Entry

In IDP versions prior to 5.0, the Infranet Controller sends only the user IP address. With version 5.0, the Infranet Controller sends session information including the user, role, and IP address. This allows you to configure more granulated IDP policies based on roles in IDP.

To create an IDP device entry:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device on which you want to configure a new IDP device entry.
3. Click the **Configuration** tab. In the configuration tree, select **System > Configuration > Sensors**.
4. Select the **Sensors** tab. The corresponding workspace appears.
5. Add or modify settings as specified in Table 56 on page 195.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 56: New IDP Device Entry Configuration Details

Option	Function	Your Action
Name	Specifies the name used to identify the new connection entry.	Enter a name for the new connection entry.
Hostname	Specifies the hostname or IP address of the IDP device to which the Infranet Controller connects to receive application and resource attack alert messages.	Enter the hostname or IP address.
TCP Port	Specifies the TCP port on the IDP device to which the Infranet Controller listens when receiving application and resource attack alert messages.	Enter the TCP port number.
One Time Password	Specifies the encrypted password the Infranet Controller uses when conducting the initial Transport Layer Security (TLS) handshake with the IDP device.	Enter the encrypted Infranet Controller OTP password as displayed on the IDP ACM configuration summary screen. NOTE: The hostname, TCP port, and one-time password must already be configured on the IDP device before this configuration can be successful.
Addresses to monitor	Reports attack information only for the specified IP addresses.	Enter the individual IP addresses and address ranges, one entry per line. Enter the subnet address in network format **0.0.0.0/0**.
Severity Filter	Specifies the severity level, which is a number on a scale from 1 to 5, where 1 is informational and 5 is critical.	Select a severity level between 1 and 5.

Enabling or Disabling the Connection to an Existing IDP Device

To enable or disable existing IDP device entries on the Infranet Controller:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device on which you want to enable or disable the IDP device.
3. Click the **Configuration** tab. In the configuration tree, select **System > Configuration > Sensors**.
4. Select the **Sensors** tab. The corresponding workspace appears.
5. Click the IDP device entry you want to enable or disable.
6. From the IDP device workspace, select the **Enable/Disable Sensor** option.
7. Click one:
   - **OK**—Saves the changes.

- **Cancel**—Cancels the modifications.

Related Documentation

- Configuring ISG-IDP as a Sensor on the Infranet Controller (NSM Procedure) on page 193
- Configuring Sensor Event Policies (NSM Procedure) on page 196

Configuring Sensor Event Policies (NSM Procedure)

You can specify one or more rules that specify the actions the Infranet Controller takes when it receives attack alert messages from an IDP device.

To create an IDP rule:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to specify sensor event policies.
3. Click the **Configuration** tab. In the configuration tree, select **System > Configuration > Sensors > Sensor Event Policies**.
4. Add or modify settings as specified in Table 57 on page 196.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 57: Sensor Event Policies Configuration Details

Option	Function	Your Action
Name	Specifies a unique name for the event.	Enter a name for the event.
Event	Specifies an existing event.	Select an existing event.
Event Count	Determines the number of times an event must occur before action is taken.	Enter a number between 1 and 256.

Table 57: Sensor Event Policies Configuration Details *(continued)*

Option	Function	Your Action
Action to be taken	Specifies the action to be taken when an event has occurred.	Select one of the following actions: • **Ignore (just log the event)**—Specifies that the Infranet Controller should log the event, but take no further action against the user profile to which this rule applies. This option is best used to deal with very minor "informational" attack alert messages that come from the IDP device. • **Terminate user session**—Specifies that the Infranet Controller should immediately terminate the user session and require the user to sign in to the Infranet Controller again. • **Disable user account**—Specifies that the Infranet Controller should disable the user profile associated with this attack alert message, thus rendering the client unable to sign in to the Infranet Controller until the administrator reenables the user account. (This option is only applicable for users who have a local Infranet Controller user account.) • **Replace user's role with this one**—Specifies that the role applied to this user's profile should change to the role you select from the associated drop-down list. This new role remains assigned to the user profile until the session terminates. This feature allows you to assign a user to a specific controlled role of your choice, based on specific IDP events. For example, if the user performs attacks, you might assign the user to a restricted role that limits the user's access and activities.
Replace user role with this role	Specifies that the role applied to the user's profile should change to the role selected from this list.	Select a role from this list.
Replace user role	Specifies whether the role assignment is permanent or only for a session.	Select a role assignment option: • **Permanent**—User remains in the quarantined state across subsequent logins until the administrator releases the user from the quarantined state. • **For this session only**—Default. User can log in to another session.
Applies to role	Specifies the roles to which the policy is applicable.	Select one of the following options: • **All**—To apply this policy to all users. • **Selected**—To apply this policy only to users who are mapped to roles in the Members list. Make sure to add roles to this list from the Non-members list. • **Except for those selected**—To apply this policy to all users except for those who are mapped to the roles in the Members list. Make sure to add roles to this list from the Non-members list.

Table 57: Sensor Event Policies Configuration Details *(continued)*

Option	Function	Your Action
Role Selection	Specifies the selected roles.	Select roles from the Non-members list and click **Add** to move them to the Members list.

Related Documentation

- Configuring ISG-IDP as a Sensor on the Infranet Controller (NSM Procedure) on page 193
- Configuring Infranet Controller Sensor Settings for Connecting to a Standalone IDP Device (NSM Procedure) on page 194
- Configuring an Infranet Controller to Connect to a ScreenOS Enforcer (NSM Procedure) on page 101

Creating a Custom Expression for Sensor Settings (NSM Procedure)

Custom expressions are strings that are made up of variables, operators, and subexpressions all concatenated together. These operators and variables are provided through an expressions dictionary.

To create a custom expression for sensor settings:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure sensor settings.
3. Click the **Configuration** tab. In the configuration tree, select **System** > **Configuration** > **Sensors**.
4. Select the **Sensor Events** tab.
5. Click **New** (+) to create a custom expression. The Custom Expression editor appears. On the left side of the editor is the Expression Dictionary, which includes the following custom expression building blocks:
   - Logical Operators: This node consists of logical operators that are used to build expressions. Select a logical operator and click the **Insert Expression** button to insert logical operators in expressions.
   - Prebuilt Expressions: This node consists of expressions that function as templates for custom expressions. Select a prebuilt expression and click the **Insert Expression** button. The prebuilt expression is displayed in the Expression area. Modify the values to create your own custom expression.
   - Variables: This node consists of variables. When a variable is selected, the conditional operators that can be applied to this variable are listed in the center of the Custom Expressions editor. Also, some variables have extensions that are displayed in the drop-down list next to the variable. Double-click a variable to display its description and example usage. Click the example variable to insert it in the Expression area.

- IF-MAP Variables: This node consists of IF-MAP variables. Double-click a IF-MAP variable to display its description and example usage. Click the IF-MAP variable example to insert it in the Expression area.
- Juniper IDP Variables: This node consists of Juniper IDP variables. Double-click a Juniper IDP variable to display its description and example usage. Click the Juniper IDP variable example displayed to insert it in the Expression area.

NOTE: Refer to the *Juniper Networks Unified Access Control Administration Guide* for more information on variables and writing custom expressions.

6. Enter a name for the custom expression.
7. Select a variable or prebuilt expression from the Custom Dictionary, and click **Insert Expression**. The expression is displayed in the Expression area on the right side of the Custom Expression editor. The conditional operators can be selected only after a leaf node is selected.
8. Click the **Validate** button to validate the expression. The expression is validated by the device and the validation status appears.

NOTE: You can create a custom expression in a device template, but you cannot validate the custom expression. The Validate button is not enabled in the Custom Expressions editor of device templates.

9. Click **OK** to save the custom expression. The new custom expression is displayed under the Sensor Events tab.
10. Click **OK** to save the sensor events settings.

Related Documentation

- Configuring Sensor Event Policies (NSM Procedure) on page 196
- Configuring ISG-IDP as a Sensor on the Infranet Controller (NSM Procedure) on page 193
- Configuring Infranet Controller Sensor Settings for Connecting to a Standalone IDP Device (NSM Procedure) on page 194

CHAPTER 19

Troubleshooting an Infranet Controller

Troubleshooting the IF-MAP Federation Network (NSM Procedure)

Diagnostic tools on the Infranet Controller can assist you with troubleshooting a federated network. You can obtain an IF-MAP client log and an IF-MAP server trace log from the diagnostic tools.

On the IF-MAP client, the IF-MAP Client User Messages option logs information that is published and removed from the IF-MAP server. On the IF-MAP server, the IF-MAP Server Trace option logs the XML for all IF-MAP requests and responses.

To enable IF-MAP Client User Messages and IF-MAP Server Trace option logs:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to enable IF-MAP Client User Messages.
3. Click the **Configuration** tab. In the configuration tree, select **System > Log/Monitoring**.
4. From the User Access tab, select **IFMAP Client User Messages** to enable IF-MAP Client User Messages.
5. From the Events tab, select **IFMAP Server Trace** to enable IF-MAP Server Trace.

NOTE: **IF-MAP Server Trace should only be enabled for troubleshooting purposes, as running this diagnostic impacts performance.**

6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Related Documentation

- Configuring IF-MAP Client Settings on the Infranet Controller (NSM Procedure) on page 108
- Configuring IF-MAP Server Settings on the Infranet Controller (NSM Procedure) on page 107

PART 5

Monitoring and Configuring Logs in an Infranet Controller

CHAPTER 20

Monitoring an Infranet Controller

Realtime Monitor Overview

The Realtime Monitor module in NSM includes views that you can use to monitor real-time status and statistics about all the managed security devices, VPN tunnels, NSRP clusters, IDP sensors, and IDP clusters in your network. You can also use the Realtime Monitor to identify problems, track security events, and discover trends across multiple geographic regions and functional areas from a central management location.

The Realtime Monitor can also help you quickly identify potential device, network, and system-level problems, such as:

- Configuration status—At the device level, you can monitor the changing status of one or more security devices in real time.
- Connection status—At the network level, you can monitor problems that could lead to failed devices.

The Realtime Monitor does the work of a management expert by first gathering information about specific processes and network activity, and then color-coding each event to organize problems.

Related Documentation

- Viewing Device Status on page 205
- Viewing Device Monitor Alarm Status on page 208

Viewing Device Status

Table 58 on page 206 lists and describes device information that you can view through the Device Monitor.

Table 58: Device Status Information

Column	Description
Name	Unique name assigned to the device in NSM.
Domain	Domain in NSM in which the device is managed.
Platform	Model number of the device.
OS Version	Operating system firmware version running on the device.
Config Status	Current configuration status of the device in NSM: • None—No state has been set (does not show in Device Monitor). • Modeled—The device exists in NSM, but a connection to the device has not yet been established. • RMA—Equivalent to bringing the device into the Modeled state. RMA results from an administrator selection in the UI when a device goes down. • Waiting for 1st connect—NSM is waiting for the device to connect. You must enter a command on the device to make it connect to NSM. • Import Needed—You must import the configuration of the device into NSM. When you add a device for the first time, verify that your status indicates "Import Needed" before you attempt to import the device. During migration, this state indicates that importation of the security device configuration is still required. • OS Version Adjustment Needed—The firmware version detected running on the device is different than what was previously detected in NSM. This could happen in the event that the automatic adjustment option was cleared during a change device firmware directive or an Update Device directive was issued to an IDP device with a firmware version mismatch. • Platform Mismatch—The device platform selected when adding the DMI device in NSM does not match the device itself. A device in this state cannot connect to NSM. • Device Firmware Mismatch—The OS version selected when adding a DMI device does not match the OS version running on the device itself. • Device Type Mismatch—The type of device specified when adding the device in NSM does not match the device itself. The device type might indicate whether the device is part of a vsys device, part of a cluster, or part of a virtual chassis. A device in this state cannot connect to NSM. • Detected duplicate serial number—The device has the same sequence number as another managed device. A device in this state cannot connect to NSM. • Update Needed—An update to this device is required. • Managed—The device is currently being managed by NSM. • Managed, In Sync—The physical device configuration is synced with the modeled configuration in NSM.

Table 58: Device Status Information *(continued)*

Column	Description
Config Status (continued)	• Managed, Device Changed—The physical device configuration is out of sync with the modeled configuration in NSM. Changes were made to the physical device configuration (the configuration on the physical device is newer than the modeled configuration). • Managed, NSM Changed—The modeled device configuration is out of sync with the physical device configuration. Changes were made to the modeled configuration (the configuration on the NSM is newer than the physical device configuration). • Managed, NSM and Device Changed—Both device configurations (physical and modeled) are out of sync with each other. Changes were made to the physical device configuration and to the modeled configuration. • Managed, Sync Pending—Completion of the Update Device directive is suspended and waiting for the device to reconnect. This state occurs only for ScreenOS devices that have the Update When Device Connects option selected during the device update.
Connection Status	Connection status of the device in NSM: • Up—Device is currently connected to NSM. • Down—Device is not currently connected to NSM but has connected in the past. • Never Connected—Device has never connected to NSM. The Device Server checks the connection status of each device every 120 seconds by default. You can change this behavior by editing the value for the **devDaemon.deviceHeartbeatTimeout** parameter in the Device Server configuration file. Refer to the *Network and Security Manager Installation Guide* for more information on editing configuration files. NOTE: If the network connection goes down for a period longer than six to eight minutes, the device connection will permanently time out. If this occurs and the device goes down for any reason, the device still appears as Up in the Device Monitor.
Alarm	Displays the current alarm status for each device in NSM: • If the device has any alarms, the most severe alarm severity is displayed (either Major or Minor). • None—The device has no alarms. • Unknown—The device status is unknown. For example, the device might not be connected. • N/A—The device's alarm is not pollable or discoverable, for example, this column shows N/A for ScreenOS and IDP devices. • Alarm is color-coded: ◦ Red for Major. ◦ Orange for Minor. ◦ Green for Ignore, None, Unknown, or N/A.

Table 58: Device Status Information *(continued)*

Column	Description
H/W Inventory Status	Displays the inventory status for hardware on the device: • In Sync—The inventory information in the NSM database is synchronized with the information on the device. • Out Of Sync—The inventory information in the NSM database is not synchronized with the information on the device. • N/A—The connected device is a ScreenOS or IDP device, or the device is not connected and imported.
S/W Inventory Status	Displays the inventory status for software on the device: • In Sync—The inventory information in the NSM database is synchronized with the software on the device. • Out Of Sync—The inventory information in the NSM database is not synchronized with the software on the device. • N/A—The connected device is a ScreenOS or IDP device, or the device is not connected and imported.
License Inventory Status	Displays the inventory status for software on the device: • In Sync—The inventory information in the NSM database is synchronized with the licenses on the device. • Out Of Sync—The inventory information in the NSM database is not synchronized with the licenses on the device. • N/A—The connected device is a ScreenOS or IDP device, or the device is not connected and imported.
First Connect	The first time the security device connected to the NSM device server.
Latest Connect	The last time the security device connected to the NSM device server.
Latest Disconnect	The last time the security device disconnected from the NSM device server.

Related Documentation

- Viewing Device Monitor Alarm Status on page 208
- Realtime Monitor Overview on page 205

Viewing Device Monitor Alarm Status

Alarms refresh automatically through periodic polling.

To view the Alarm status and time:

1. From Device Monitor, right-click the device row entry and select the **View Alarm** option.

   The device Alarm Status dialog box displays the alarm list and polling time for the device.

2. Retrieve the current alarm status in the device by clicking the **Refresh** button.

The poll time is derived from the device server time.

Related Documentation

- Viewing Device Status on page 205
- Realtime Monitor Overview on page 205

CHAPTER 21

Configuring Logs in an Infranet Controller

Configuring RADIUS Attribute Logs (NSM Procedure)

You can configure the Infranet Controller to enable or disable RADIUS attribute logging and obtain a granular record of RADIUS authentication attempts using configurable, detailed authentication logs.

To configure RADIUS attribute logging:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller device for which you want to configure RADIUS attribute logging.
3. Click the **Configuration** tab. In the configuration tree, select **UAC** > **Network Access** > **RADIUS Attributes** > **RADIUS Attribute Logging**.
4. Select **Authentication Success Log Message** to record events with successful authentication attempts.
5. From the Non-members area, select the attribute for which successful authentication attempts should be recorded and then move it to the Members area.
6. Select **Authentication Reject Log Message** to record events with unsuccessful authentication attempts.
7. From the Non-members area, select the attribute for which unsuccessful authentication attempts should be recorded and then move it to the Members area.
8. Click one:
   - **OK**—Saves the changes.

- **Cancel**—Cancels the modifications.

Related Documentation

- Configuring RADIUS Return Attributes Policies (NSM Procedure) on page 80
- Configuring RADIUS Request Attributes Policies (NSM Procedure) on page 83

Configuring Event Logs (NSM Procedure)

The events log file contains a variety of system events, such as session timeouts (including idle and maximum length session timeouts), system errors and warnings, requests to check server connectivity, and Infranet Controller service restart notifications.

To configure event logs:

1. In the NSM navigation tree, select **Device Manager**> **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure event logs.
3. Click the **Configuration** tab. In the configuration tree, select **System > Log/Monitoring > Events**.
4. Add or modify settings as specified in Table 59 on page 212.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 59: Event Logs Configuration Details

Option	Function	Your Action
Settings		
Max Log Size	Specifies the maximum file size for the local log file. The limit is 500 MB.	Enter the maximum log file size.
Connection Requests	Logs the connection requests.	Select this option to log connection requests.
System Status	Logs the system status.	Select this option to log system status information.
System Errors	Logs the system errors.	Select this option to log system error details.
Statistics	Logs the statistical information.	Select this option to log statistical details.
Performance	Logs the performance information.	Select this option to log performance details.

Table 59: Event Logs Configuration Details *(continued)*

Option	Function	Your Action
Enforcer Events	Logs the enforcer events.	Select this option to log enforcer event details.
Enforcer Command Trace	Logs the enforcer command trace events.	Select this option to log enforcer command trace events.
Syslog Servers		
Server name/IP	Specifies the name or IP address of the syslog server.	Enter the server name or the IP address.
Facility	Specifies the facility for the server. The Infranet Controller provides eight facilities (LOCAL0-LOCAL7) that you can map to facilities on your syslog server.	Select the facility.
Filter	Specifies the filter that you want to apply to the log file.	Select the filter to be applied to the log file.

Related Documentation

- Configuring Client-Side Logs (NSM Procedure) on page 216
- Configuring User Access Logs (NSM Procedure) on page 213
- Configuring Administrator Access Logs (NSM Procedure) on page 215
- Configuring the Infranet Controller as an SNMP Agent (NSM Procedure) on page 217

Configuring User Access Logs (NSM Procedure)

The user access log file contains information about when users access the appliance, including the number of simultaneous users at each one-hour interval (logged on the hour) and user sign-ins and sign-outs.

To configure user access logs:

1. In the NSM navigation tree, select **Device Manager**> **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure user access logs.
3. Click the **Configuration** tab. In the configuration tree, select **System > Log/Monitoring > User Access**.
4. Add or modify settings as specified in Table 60 on page 214.
5. Click one:

- **OK**—Saves the changes.
- **Cancel**—Cancels the modifications.

Table 60: User Access Logs Configuration Details

Option	Function	Your Action
Settings		
Max Log Size	Specifies the maximum file size for the local log file. The limit is 500 MB.	Enter the maximum log file size.
Select Event to Log		
Login/Logout	Logs the user login and logout information.	Select this option to log login and logout information.
User Settings	Logs the user settings.	Select this option to log user setting information.
Client Certificate	Logs the client certificate messages for the user.	Select this option to log client certificate messages for the user.
IFMAP Client User Message	Logs the IFMAP client user messages.	Select this option to log IFMAP client user messages.
Outlook Anywhere	Logs the RPC over http messages.	Select this option to log RPC over http messages.
Enforcer Deny Messages	Logs the enforcer deny messages.	Select this option to log enforcer deny messages.
Radius Accounting Messages	Logs the radius accounting messages.	Select this option to log radius accounting messages
User Connection Messages	Logs the user connection messages.	Select this option to log the user connection messages.
Endpoint Heartbeat Messages	Logs heartbeat messages from the endpoints.	Select this option to log heartbeat messages from the endpoints.
Pulse Client Messages	Logs pulse client messages.	Select this option to log pulse client messages.
Syslog Servers		

Table 60: User Access Logs Configuration Details *(continued)*

Option	Function	Your Action
Server name/IP	Specifies the name or IP address of the syslog server.	Enter the server name or the IP address.
Facility	Specifies the facility for the server. The Infranet Controller provides eight facilities (LOCAL0-LOCAL7) that you can map to facilities on your syslog server.	Select the facility.
Filter	Specifies the filter that you want to apply to the log file.	Select the filter.

Related Documentation

- Configuring Administrator Access Logs (NSM Procedure) on page 215
- Configuring Client-Side Logs (NSM Procedure) on page 216
- Configuring the Infranet Controller as an SNMP Agent (NSM Procedure) on page 217
- Configuring Event Logs (NSM Procedure) on page 212

Configuring Administrator Access Logs (NSM Procedure)

The administrator access log file contains administration information, including administrator changes to user, system, and network settings, such as changes to session timeouts and machine and server information. It also creates a log entry whenever an administrator signs in, signs out, or changes licenses on the appliance.

To configure administrator access logs:

1. In the NSM navigation tree, select **Device Manager**> **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure administrator access logs.
3. Click the **Configuration** tab. In the configuration tree, select **System > Log/Monitoring > Admin Access**.
4. Add or modify settings as specified in Table 61 on page 216.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 61: Administrator Access Logs Configuration Details

Option	Function	Your Action
Settings		
Max Log Size	Specifies the maximum file size for the local log file. The limit is 500 MB.	Enter the maximum log file size.
Administrator Changes	Logs the administrator changes.	Select this option to log administrator changes.
Administrator Logins	Logs the administrator login information.	Select this option to log administrator login information.
License Changes	Logs the license change information.	Select this option to log license change information.
Syslog Servers		
Server name/IP	Specifies the name or IP address of the syslog server.	Enter the server name of the IP address.
Facility	Specifies the facility for the server. The Infranet Controller provides eight facilities (LOCAL0-LOCAL7) that you can map to facilities on your syslog server.	Select the facility.
Filter	Specifies the filter that you want to apply to the log file.	Select the filter.

Related Documentation

- Configuring Client-Side Logs (NSM Procedure) on page 216
- Configuring User Access Logs (NSM Procedure) on page 213
- Configuring Event Logs (NSM Procedure) on page 212
- Configuring the Infranet Controller as an SNMP Agent (NSM Procedure) on page 217

Configuring Client-Side Logs (NSM Procedure)

You can enable client-side logging for the Host Checker and Odyssey Access Client. When you enable this option, the Infranet Controller writes a client-side log to endpoints that use the feature. The Infranet Controller appends to the log file each time the feature is invoked during subsequent user sessions. This feature is useful when working with the support team to debug problems with the respective feature.

To configure client-side logs:

1. In the NSM navigation tree, select **Device Manager**> **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to specify global client-side logging settings.
3. Click the **Configuration** tab. In the configuration tree, select **System > Log/Monitoring > Client Logs > Settings**.
4. Select the features for which you want the Infranet Controller to write client-side logs.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Related Documentation

- Configuring the Infranet Controller as an SNMP Agent (NSM Procedure) on page 217
- Configuring User Access Logs (NSM Procedure) on page 213
- Configuring Administrator Access Logs (NSM Procedure) on page 215
- Configuring Event Logs (NSM Procedure) on page 212

Configuring the Infranet Controller as an SNMP Agent (NSM Procedure)

The Infranet Controller supports Simple Network Management Protocol version 2 (SNMPv2), implements a private MIB, and defines its own traps. To enable your network management station to process these traps, you need to download the Juniper Networks MIB file and specify the appropriate information to receive the traps.

To specify SNMP settings:

1. In the NSM navigation tree, select **Device Manager**> **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to specify SNMP settings.
3. Click the **Configuration** tab. In the configuration tree, select **System > Log/Monitoring > SNMP**.
4. Add or modify settings as specified in Table 62 on page 217.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 62: SNMP Agent Configuration Details

Option	Function	Your Action
Trap Settings		

Table 62: SNMP Agent Configuration Details *(continued)*

Option	Function	Your Action
Check Frequency	Specifies the check frequency trap threshold .	Enter the check frequency trap threshold in seconds.
Log Capacity	Specifies the log capacity trap threshold .	Enter a percentage for the log capacity trap threshold.
Users	Specifies the users trap threshold.	Enter a percentage for the users trap threshold.
Memory	Specifies the memory trap threshold.	Enter a percentage for the memory trap threshold.
Swap Memory	Specifies the swap memory trap threshold.	Enter a percentage for the swap memory trap threshold.
Disk	Specifies the disk trap threshold.	Enter a percentage for the disk trap threshold.
CPU	Specifies the CPU trap threshold.	Enter a percentage for the CPU trap threshold.
Send Traps for Critical Log Events	Specifies that SNMP traps will be sent for critical log events.	Select this option to send SNMP traps for critical log events.
Send Traps for Major Log Events	Specifies that SNMP traps will be sent for major log events.	Select this option to send SNMP traps for major log events.
SNMP Servers	Specifies the servers to which you want the Infranet Controller to send the traps that it generates.	Enter the hostname or IP address, port number, and community.
Settings		
SNMP Queries	Specifies the SNMP queries for the Infranet Controller.	Select this option.
SNMP Traps	Specifies the SNMP traps for the Infranet Controller.	Select this option.
System Name	Specifies the agent name.	Enter the system name.
System Location	Specifies the agent location.	Enter the system location.
System Contact	Specifies the agent contact information.	Enter the system contact information.

Table 62: SNMP Agent Configuration Details *(continued)*

Option	Function	Your Action
Community	Specifies the agent community.	Enter a string.

Related Documentation

- Configuring Event Logs (NSM Procedure) on page 212
- Configuring User Access Logs (NSM Procedure) on page 213
- Configuring Administrator Access Logs (NSM Procedure) on page 215
- Configuring Client-Side Logs (NSM Procedure) on page 216

Configuring Custom Log Filters (NSM Procedure)

You can create custom log filters or edit the set of predefined log filters to specify which data is written to your log files as well as its format.

To configure the log filters:

1. In the NSM navigation tree, select **Device Manager** > **Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure log filter.
3. Click the **Configuration** tab. In the configuration tree, select **System > Log/Monitoring > Filters**.
4. Add or modify settings as specified in Table 63 on page 219.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 63: Log Filter Configuration Details

Option	Function	Your Action
Filter Name	Specifies a name for the filter.	Enter a name for the filter.
Start Date	Specifies the date from which logs have to be written.	Enter a start date.
End Date	Specifies the date up to which logs have to be written.	Enter an end date.

Table 63: Log Filter Configuration Details *(continued)*

Option	Function	Your Action
Query	Specifies the custom expression language to control which subset of data the Infranet Controller writes to the log.	To use the Infranet Controller custom expression language: 1. Click the **New Expression** button. The Custom Expression editor is displayed. 2. Select the variable from the Expression Dictionary and click the **Insert Expression** button. 3. Click the **Validate** button to validate the expression. 4. Click **OK** to save the custom expression.
Format Type	Specifies the format of the data in the log.	Select one of the following format types: • Standard: This log filter format logs the date, time, node, source IP address, user, realm, and the Infranet Controller event ID and message. • WELF: This customized WebTrends Enhanced Log Format (WELF) filter combines the standard WELF format with information about the Infranet Controller appliance's realms, roles, and messages. • W3C: The World Wide Web Consortium's extended log file format is a customizable ASCII format with a variety of different fields. Visit http://www.w3.org for more information about this format. Only the User Access log offers this filter as an option. • Custom: Enter the format you want to use in Custom Format. When entering a format, surround variables with percentage symbols (for example %user%). All other characters in the field are treated as literals.

Related Documentation

- Configuring Client-Side Logs (NSM Procedure) on page 216
- Configuring User Access Logs (NSM Procedure) on page 213
- Configuring Administrator Access Logs (NSM Procedure) on page 215
- Configuring the Infranet Controller as an SNMP Agent (NSM Procedure) on page 217

PART 6

Index

Index