Ivanti Neurons for Secure Access

ICS Tenant Administration Guide

v22.3R4

Published	Feb 13, 2023
Document Version	1.0
Document Build	release/zta-22.3R4 a6d92401

Ivanti
10377 South Jordan Gateway
Suite 110
South Jordan, Utah 84095
https://www.ivanti.com

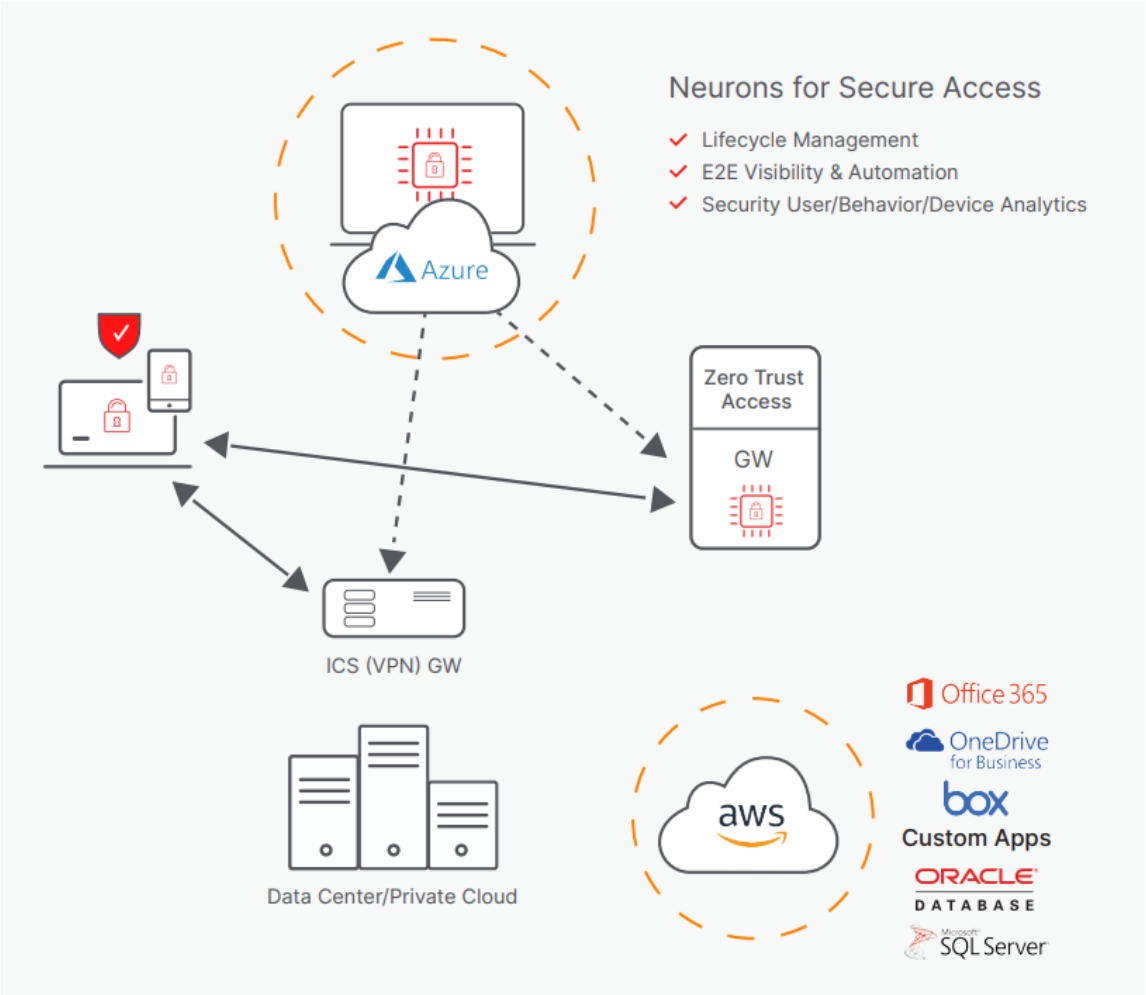
END USER LICENSE AGREEMENT

Contents

Ivanti Neurons for Secure Access Overview

Neurons for Secure Access (nSA) is a SaaS-delivered, centralized management and reporting platform designed to work with both Ivanti Connect Secure (ICS) and Neurons for Zero Trust Access (nZTA).

- nSA provides a unified interface allowing security admins to manage multiple gateways and/or locations quickly and efficiently.
- nSA simplifies workflows by consolidating all logging, reporting and activity data to a single pane of glass.
- Administrators gain powerful analytics tools to review the health status of their deployments as part of their daily routine.
- Proprietary risk scores identify non-compliant or anomalous user activity, enabling admins to identify risky user activity and react accordingly.
- Scheduled reports let admins design, customize and schedule reports to arrive in their inbox with the exact data they want to see.



nSA works with existing ICS deployments and does not require additional hardware to be implemented, nor must any network or connectivity changes be made in order to integrate nSA into an ICS deployment. Registering an ICS Gateway with nSA will initiate secure WebSocket communications between the ICS Gateway and nSA. Once connected, the ICS Gateway logs and analytics are uploaded to nSA and can be viewed and reported on from the nSA portal. Gateway-management duties allowing for the ability to upgrade, roll back and restart — as well as provide troubleshooting tools — are all enabled once ICS is connected to nSA.

The following list shows the supported features and benefits.

- **Secure Access Foundation**:
  - Manages Connect Secure Gateways and/or Zero Trust.
  - Access Gateways in all aspects.
  - Supports both existing and next-gen VPN gateways.
- **Gateway Lifecycle Management**: Enables centralized upgrades, downgrades and restarts.
- **Configuration Management**:
  - Supports gateway configurations.

  - Configuration groups for multi-node configuration management.

- **Single-Pane-of-Glass Visibility**: Holistic visibility and compliance reporting of users, devices, applications and infrastructure across the enterprise.
- **User Entity Behavior Analytics (UEBA)**: Leverages analytical data to reduce security risks, detect anomalies, optimize user experience and adapt to a mobile workforce.
- **Local (Gateway) and Central Debugging**: Enables getting back to business faster.
- **Hybrid Configuration Support**: Gateways can be deployed in a variety of configurations including the cloud.

Logging in to Ivanti Neurons for Secure Access

Preparing to Log in

To log in to Ivanti Neurons for Secure Access (nSA), you require a Tenant Admin login.

All Tenant Admin accounts are set up by the Ivanti DevOps team. Once your Tenant Admin account has been created, you will receive an email which describes how to log in to the nSA as a Tenant Admin.

You can then proceed to log in to nSA. See *Logging in to the Ivanti Neurons for Secure Access as a Tenant Admin* (page 5).

Logging in to the Ivanti Neurons for Secure Access as a Tenant Admin

Before you can log in as a Tenant Admin, you will receive an email from the Ivanti DevOps team. This email contains:

- Your Tenant Admin user name.
- Your password.
- The nSA domain. That is, the FQDN of Ivanti Neurons for Secure Access.
- An Admin hyperlink to start the login process. Example: https://<tenant FQDN>/login/admin

To log in to your Tenant Admin account:

1. Click the hyperlink in your email.

   The administrator login page appears.

FIGURE 2.1 : Tenant Admin Login Page

2. Log in using your supplied Tenant Admin credentials. If you are logging in for the first time, system prompts for a password reset.

   The following timeouts are used for all Admin sessions:

   - The idle timeout is 10 minutes.
   - The session timeout is 60 minutes.

   Note: If you have forgotten your password, click the **Forgot Password** link, provide “User name” and “Email address”, and click **Reset Password**. You will receive an email with the new password.

3. If nSA requests it, specify a new password for your account.

   Once this procedure is complete, you can access the nSA graphical interface as an admin user.

   The **Secure Access Setup** page appears.

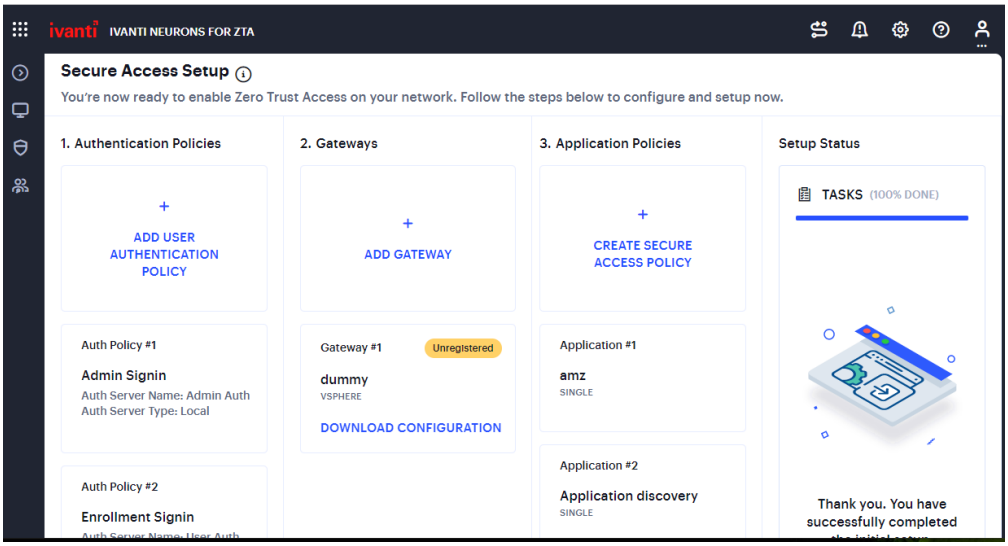


FIGURE 2.2 : The Secure Access Setup page

4. Click '9 dots' on extreme left corner. Choose **Ivanti Connect Secure**. These two steps are required for every login.

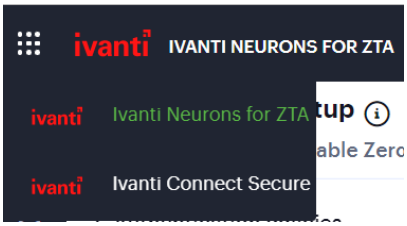


FIGURE 2.3 : Gateway Switcher

From this page, you can view and configure all functions and capabilities allowed through your subscription and role. Using the Ivanti Connect Secure menu at the left-hand side, choose from:

- The **Show/Hide** menu icon, providing the ability to show or collapse the Ivanti Connect Secure menu tree:

FIGURE 2.4 : Showing or hiding the nSA menu system

- The **Insights** menu icon, providing access to the analytics and monitoring components of the nSA portal:

FIGURE 2.5 : Accessing the Insight menu

To learn more about the functionality offered by this menu, see *Ivanti Connect Secure Gateway Analytics* (page 29).

- The **Gateways** menu icon, providing access to register and manage the Gateways:

FIGURE 2.6 : Accessing the Secure Access menu

- The **Administration** menu icon, providing access to administrative functions related to your ICS subscription:

FIGURE 2.7 : Accessing the Administration menu

The chapters in this guide cover each of these functions in detail.

Changing the UI Theme

nSA offers two themes for your UI display:

To change the current theme, which remains in place through subsequent logins, use the **Settings** menu located on the top-right-corner of the page:

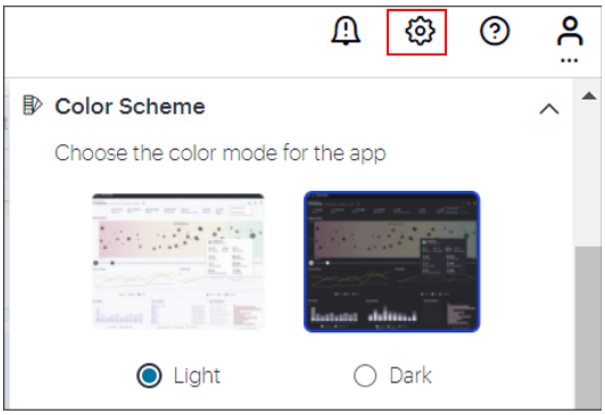


FIGURE 2.8 : Changing the UI theme

Through the **Color Scheme** panel (indicated), click **Light** or **Dark** to switch between themes.

Setting the Timezone

To configure the default timezone for this admin login account, use the **Settings** menu located on the top-right-corner of the page:

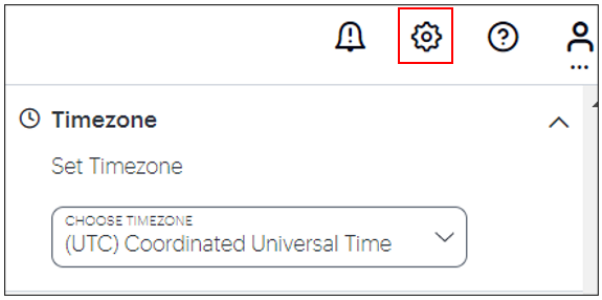


FIGURE 2.9 : Configuring the default timezone

Choose a timezone in the provided drop-down selector, then click **Apply**.

The configured timezone affects the display of data on all **Insights** pages, and each admin login account within a tenant deployment has their own specific timezone configuration. Changes to the timezone persist across login sessions, and the default setting is *UTC (Coordinated Universal Time)*.

Note: Changing the timezone can affect the data displayed in each chart or graph. For example, a recently-observed non-compliance event involving a client device in

the GMT timezone that appears in the *Last Hour* view (when using GMT (UTC + 00:00) as your configured timezone) might then only appear in the *Last X Hours* view when you switch your timezone to IST (UTC+05:30).

Configuring Session Timeouts

To configure timeout values for admin and user sessions, use the **Settings** menu located on the top-right-corner of the page:

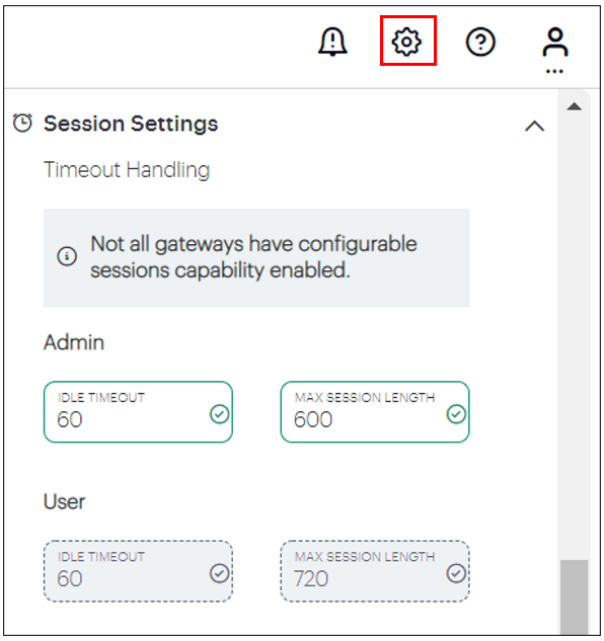


FIGURE 2.10 : Configuring timeout values for admin and user sessions

Through the **Session Settings** panel (indicated), you can set the following timeout values:

- **Admin Idle Timeout**: the time, in minutes, after which the admin login session to the Tenant Admin Portal times out due to inactivity. (default: 10)
- **Admin Max Session Length**: the time, in minutes, after which the admin login session to the Tenant Admin Portal ends and must be re-authenticated. (default: 60)
- **User Idle Timeout**: the time, in minutes, after which the user login session to nSA times out due to inactivity. (default: 60)
- **User Max Session Length**: the time, in minutes, after which the login session to nSA ends and must be re-authenticated. (default: 720)

To apply your changes, click **APPLY**.

Note: To use these settings, your configured Gateways must all meet minimum version requirements for session control. nSA disables the panel and displays a

warning message if this is not the case.

Logging out of the Ivanti Neurons for Secure Access

To log out of the nSA and end the current session, click the *Profile* icon and select **Logout**.

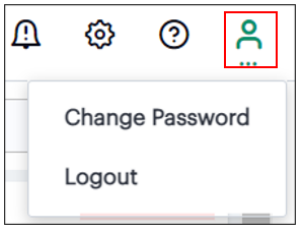


FIGURE 2.11 : Logging Out of the Portal

Managing Existing Ivanti Connect Secure 9.x Appliance

The existing Ivanti Connect Secure 9.x appliance can be managed by Ivanti Neurons for Secure Access (nSA), by upgrading the appliance to the nSA managed 9.1R11.5 version. Note that the fresh installation is not available for this release.

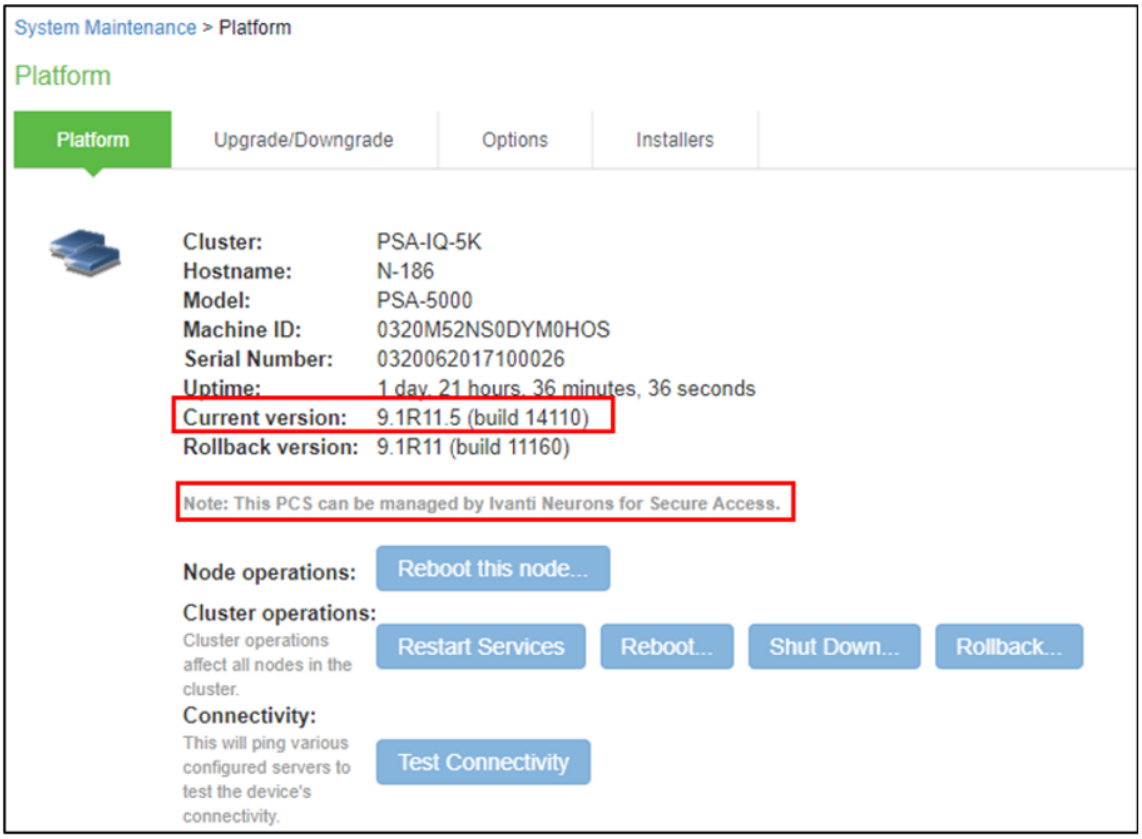


FIGURE 3.1 : nSA Managed Ivanti Connect Secure 9.x

The note “This Ivanti Connect Secure can be managed by Ivanti Neurons for Secure Access” confirms that the appliance is upgraded to the correct version.

Registering Ivanti Connect Secure Gateway

Once you have logged into the Ivanti Neurons for Secure Access, the next step is to launch Ivanti Connect Secure Gateway UI, then register one or more ICS.

To launch ICS Gateway UI

1. In the Ivanti Neurons for Secure Access UI, select the Gateway Switcher icon located on the top left corner.

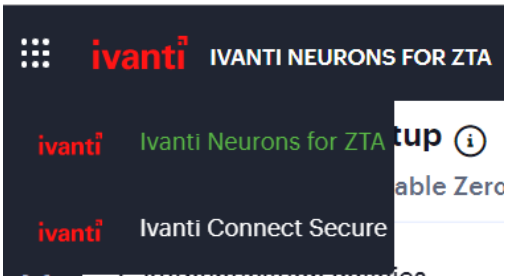


FIGURE 4.1 : Gateway Switcher

2. From the list, select **Ivanti Connect Secure**.

   The Ivanti Connect Secure UI page is displayed.

To register ICS Gateway:

1. From the Ivanti Connect Secure menu, click the **Gateways** icon, then select **Gateways > Gateways List**.

   The All Gateways page is displayed.

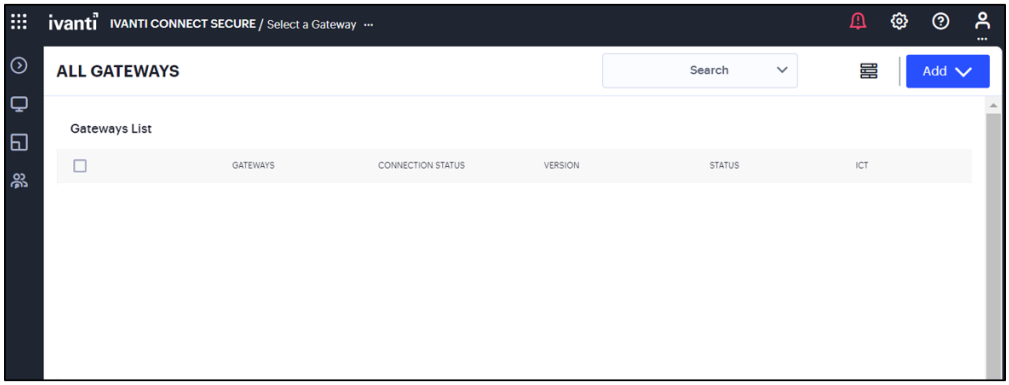


FIGURE 4.2 : Gateways list option

2. In the All Gateways page, click the **Add** drop-down list.

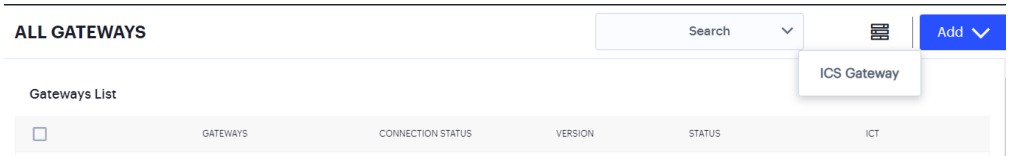


FIGURE 4.3 : Add Gateway Selection

3. From the Gateway types list, select **ICS Gateway**.

   The Register ICS Gateway page is displayed.

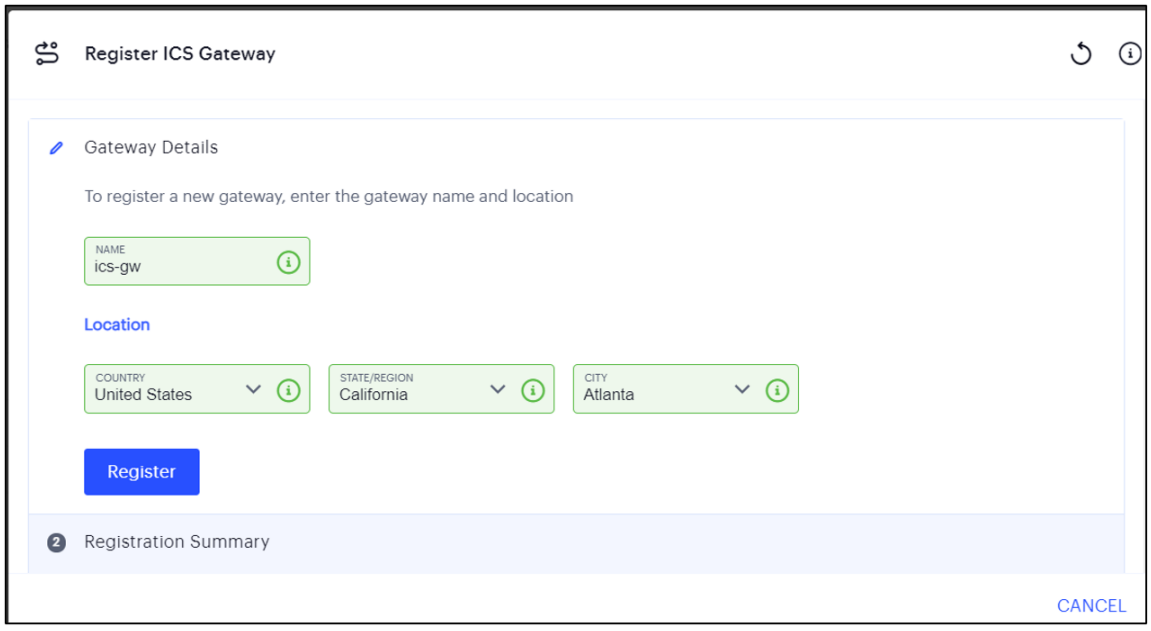


FIGURE 4.4 : ICS Gateway Registration

4. Enter a unique name for ICS gateway.

Note: The name should be maximum 15 characters, only alphanumeric,

underscores, and hyphens are allowed between characters, and **must start with a letter**.

5. Enter your Location details such as Country, State/Region, City, and then click **Register**.

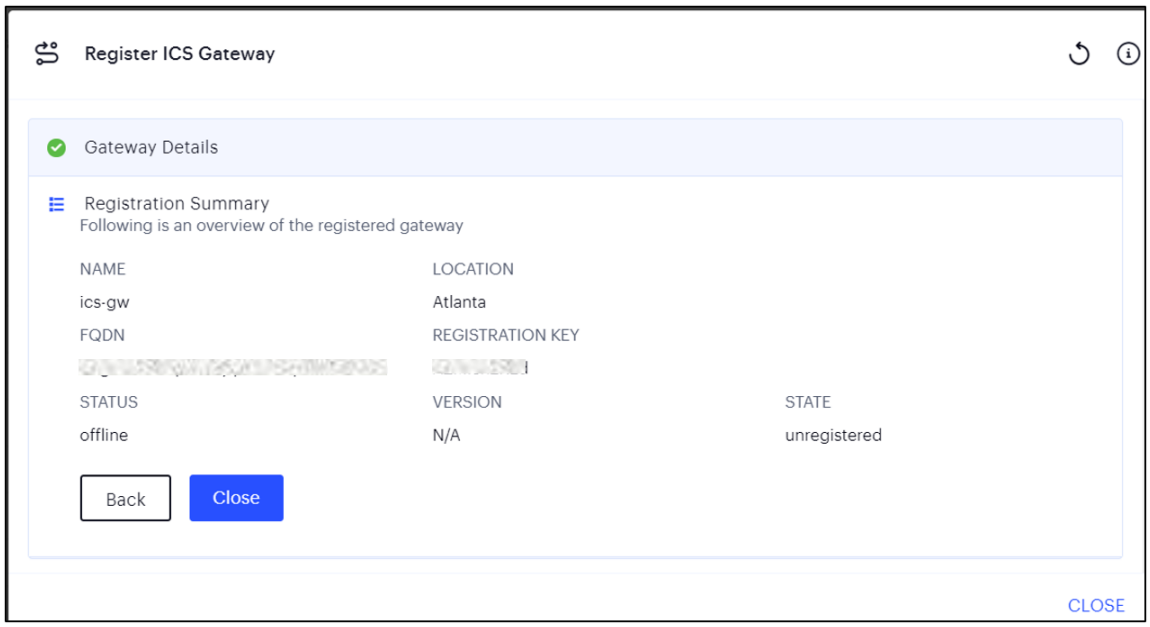


FIGURE 4.5 : ICS Gateway Registration Summary

The Registration Summary page contains the FQDN URL and Registration Key, which you need to enter in the ICS Gateway to complete the registration. See *Completing Registration of a ICS Appliance* (page 17).

6. Click **Close**.

   The newly added ICS Gateway gets listed as “Unregistered” under ICS Gateways list.

Completing Registration of a ICS Appliance

For all platforms, make sure the firewall rules for the Public Subnet in which your ICS Gateway External Interface resides is configured to accept inbound client connections on TCP port 443.

Furthermore, make sure you configure the Network Gateway serving your Private Subnet to allow outbound traffic to the nSA Controller in the following ways:

- Allow outbound TCP traffic on port 443 to the Controller service
- Allow outbound UDP traffic to the following Network Time Protocol (NTP) services:
  - time.windows.com (port 123)

- time.nist.gov (port 123)

Note: We recommend you use NTP server to ensure the clocks are synchronized and features on Ivanti Neurons for Secure Access work properly.

To complete registration of a ICS appliance:

1. Log in to the ICS appliance as an Admin.
2. Select the **System > Configuration > Ivanti Neurons for Secure Access > Settings** tab.
3. Enter the Registration FQDN and Registration Code.

   Note: The Registration FQDN and Registration Code were displayed during ICS Registration with nSA" .

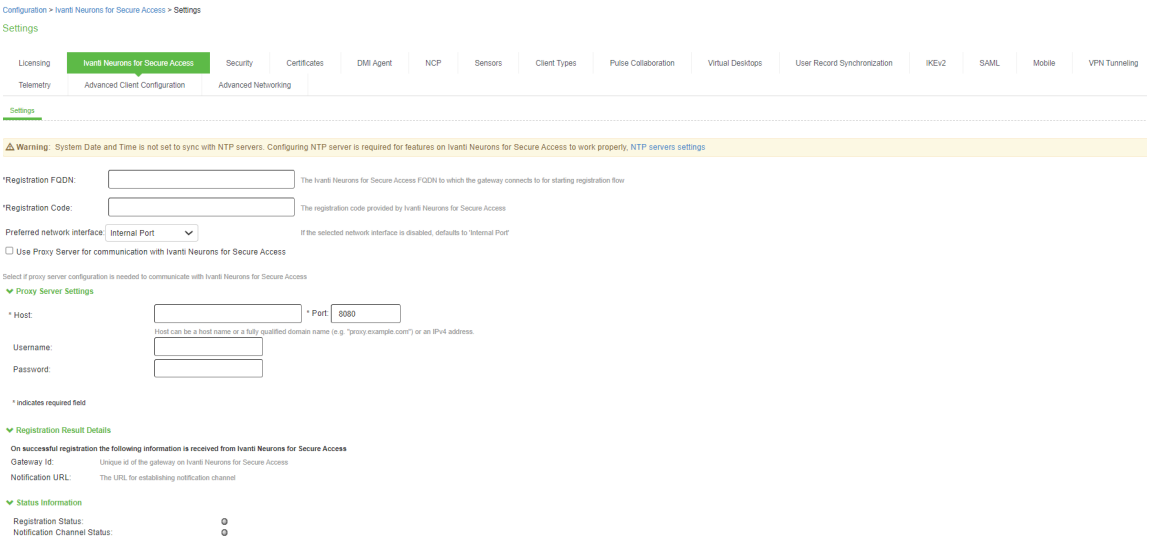


FIGURE 4.6 : ICS: Ivanti Neurons for Secure Access Settings

4. Click **Save Changes**.

   The Status Information displays the Registration Status in green.

Ivanti Connect Secure Gateway Deployment

The following sections describe the new parameters that are added for the deployment of Ivanti Connect Secure VA on VMware, Amazon Web Services cloud and Microsoft Azure cloud.

Deploying on VMware

For a detailed ICS VA deployment procedure, refer to *Virtual Appliance Deployment Guide* at https://www.ivanti.com/support/product-documentation.

This below table describes the new parameters that are added in the script file **create-va.pl**, which is included in your PSA-V package.

TABLE 5.1 : Sample Script Parameters - New Parameters

Parameter	Description
New Parameters	
registrationCode	The registration code, which is generated during the ICS gateway registration on nSA. Example, KyZR6YDL8
registrationFQDN	The registration FQDN name, which is generated during the ICS gateway registration on nSA. Example, auto.lark.pzt.dev.perfsec.com
enableproxy	Default is set to n.
proxyHost	The proxy server name.
proxyPort	The port number of the proxy server. Example, 8080
proxyUsername	The username of the proxy server. Example, usr
proxyPassword	The password of the proxy server. Example, pxx124
registerNetworkInterface	The interface through which the gateway registers with nSA. Example, external

Deploying on Hyper-V

For a detailed ICS on Hyper-V deployment procedure, refer to *ICS Gateway Deployment on Hyper-V Platform* at https://www.ivanti.com/support/product-documentation.

Deploying on KVM

For a detailed ICS on KVM deployment procedure, refer to *ICS Gateway Deployment on KVM Platform* at https://www.ivanti.com/support/product-documentation.

Deploying on AWS Cloud

For a detailed ICS VA on AWS Cloud deployment procedure, refer to *Virtual Appliance on Amazon Web Services Deployment Guide* at https://www.ivanti.com/support/product-documentation.

Ivanti Connect Secure accepts the following parameters as provisioning parameters in the XML format.

```
<pulse-config>
  <primary-dns><value></primary-dns>
  <secondary-dns><value></secondary-dns>
  <wins-server><value></wins-server>
  <dns-domain><value></dns-domain>
  <admin-username><value></admin-username>
  <admin-password><value></admin-password>
  <cert-common-name><value></cert-common-name>
  <cert-random-text><value></cert-random-text>
  <cert-organisation><value></cert-organisation>
  <config-download-url><value></config-download-url>
  <config-data><value></config-data>
  <auth-code-license><value></auth-code-license>
  <enable-license-server><value></enable-license-server>
  <accept-license-agreement><value></accept-license-agreement >
  <enable-rest><value></enable-rest>
  <registration-code> 1grkL2Xbr </registration-code>
  <registration-fqdn>auto.toad.pzt.dev.perfsec.com</registration-fqdn>
  <enable-proxy>n</enable-proxy>
  <proxy-host></proxy-host>
  <proxy-port></proxy-port>
  <proxy-username></proxy-username>
  <proxy-password></proxy-password>
  <register-network-interface>external</register-network-interface>
</pulse-config>
```

The below table describes the new parameters that are added in the XML file.

TABLE 5.2 : XML File Details - New Parameters

Parameter	Type	Description
New Parameters		
registrationCode	string	The registration code, which is generated during the ICS gateway registration on nSA. Example, KyZR6YDL8
registrationFQDN	string	The registration FQDN name, which is generated during the ICS gateway registration on nSA. Example, sample.domain.com
enableproxy	string	Default is set to n.
proxyHost	string	The proxy server name.
proxyPort	integer	The port number of the proxy server. Example, 8080
proxyUsername	string	The username of the proxy server. Example, usr
proxyPassword	string	The password of the proxy server. Example, pxx124
registerNetworkInterface	string	The interface through which the gateway registers with nSA. Example, external

Note: The XML parsing fails if the following characters are used in the strings:

- “”””
- “‘”
- “<”
- “>”
- “&”

System Operations

The AWS portal provides Start, Restart Stop and Terminate operations to control the Virtual Appliance connection.

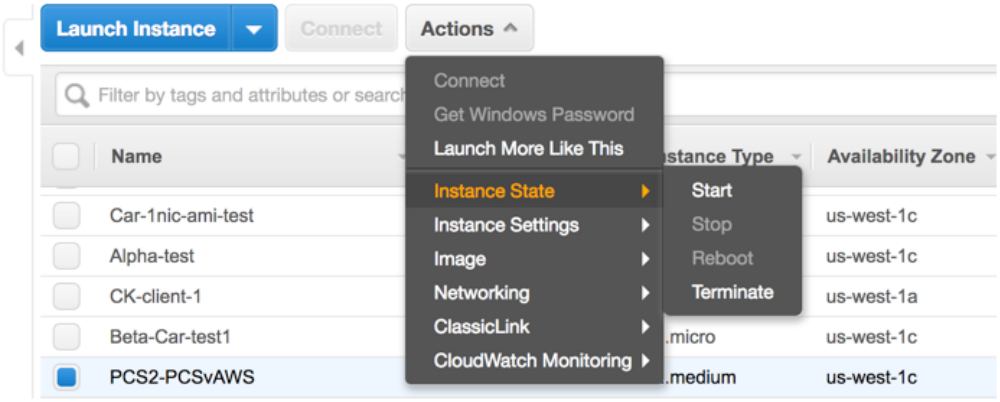


FIGURE 5.1 : System Operations

On the AWS portal, select **AWS Services > Launch Instance**. From the Actions menu, select **Instance State**.

- Click **Start** to start a VM
- Click **Stop** to stop the VM
- Click **Restart** to restart the VM
- Click **Terminate** to terminate the VM

Troubleshooting

Ivanti Connect Secure emits booting logs at a specified storage. You can check the storage details of the boot diagnostic logs as shown below:

1. Select **AWS Services > Instances > Launch Instance**.
2. From the list displayed, select **Instance Settings > Get System Log**.

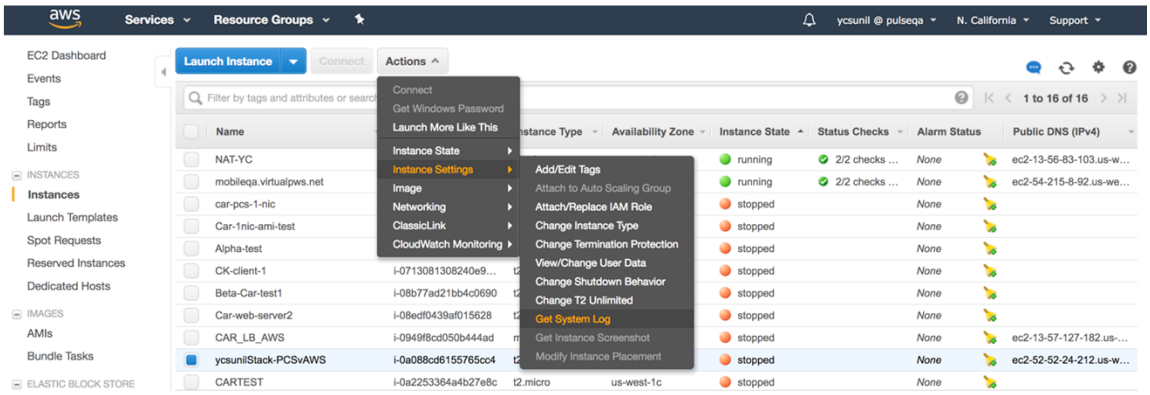


FIGURE 5.2 : Boot Diagnostics

The system logs window is displayed.

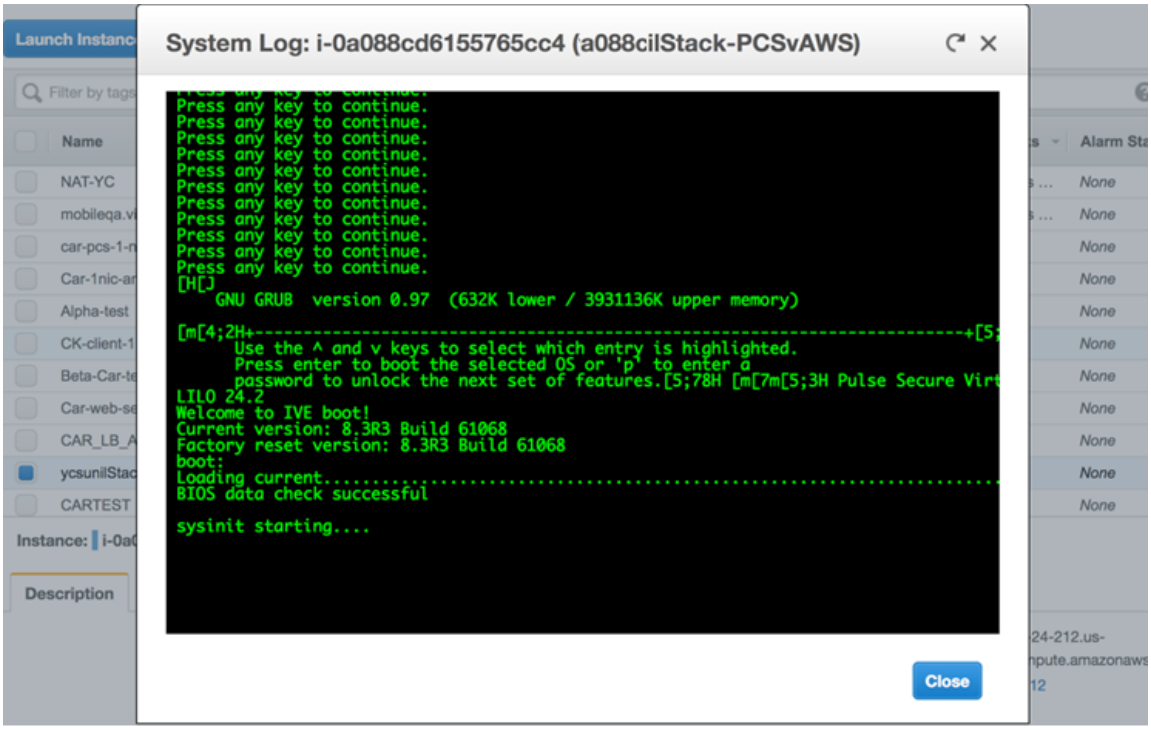


FIGURE 5.3 : System Logs

Frequently Asked Questions

FAQ1: Packets transmitted from ICS Internal Interface are getting dropped by AWS Virtual Gateway in L3 traffic.

Cause: The packets are dropped because the source IP and MAC address are not matching and the transit routing is not supported.

Solution: Ivanti Connect Secure must be able to SNAT these packets to the Internal interface IP which belongs to a subnet within the VPC.

To NAT endpoint tunnel IP to Internal interface IP, do the following:

1. Log in to Ivanti Connect Secure admin console.
2. Navigate to **System > Network > VPN Tunneling**.
3. Enable **Source NATTING**. By default, Source NATTING is disabled.

Deploying on Azure Cloud

For a detailed deployment procedure, refer to *Virtual Appliance on Microsoft Azure Deployment Guide* at https://www.ivanti.com/support/product-documentation.

Ivanti Connect Secure accepts the following parameters as provisioning parameters in the XML format.

```
"<pulse-config>

 <primary-dns>8.8.8.8</primary-dns>

 <secondary-dns>8.8.8.9</secondary-dns>

 <wins-server>1.1.1.1</wins-server>

 <dns-domain>psecure.net</dns-domain>

 <admin-username>admin</admin-username>

 <admin-password>password</admin-password>

 <cert-common-name>va1.psecure.net</cert-common-name>

 <cert-random-text>fdsfpisonvsfnms</cert-random-text>

 <cert-organisation>Psecure Org</cert-organisation>

 <config-download-url><value></config-download-url>

 <config-data><value></config-data>

 <auth-code-license><value></auth-code-license>

 <enable-license-server>n</enable-license-server>

 <accept-license-agreement>n</accept-license-agreement>

 <enable-rest>n</enable-rest>

 <registration-code> 1grkL2Xbr </registration-code>

 <registration-fqdn>auto.toad.pzt.dev.perfsec.com</
↪registration-fqdn>

 <enable-proxy>n</enable-proxy>

 <proxy-host></proxy-host>

 <proxy-port></proxy-port>

 <proxy-username></proxy-username>

 <proxy-password></proxy-password>
```

(continues on next page)

(continued from previous page)

```
  <register-network-interface>external</register-network-
↪interface>

</pulse-config>"
```

The below table describes the new parameters that are added in the XML file.

TABLE 5.3 : XML File Details

Parameter	Type	Description
New Parameters		
registrationCode	string	The registration code, which is generated during the ICS gateway registration on nSA. Example, KyZR6YDL8
registrationFQDN	string	The registration FQDN name, which is generated during the ICS gateway registration on nSA. Example, sample.domain.com
enableproxy	string	Default is set to n.
proxyHost	string	The proxy server name.
proxyPort	integer	The port number of the proxy server. Example, 8080
proxyUsername	string	The username of the proxy server. Example, usr
proxyPassword	string	The password of the proxy server. Example, pxx124
registerNetworkInterface	string	The interface through which the gateway registers with nSA. Example, external

Note: The XML parsing fails if the following characters are used in the strings:

- “”””
- “”’
- “<”
- “>”
- “&”

System Operations

The Azure VA portal provides Start, Restart and Stop operations to control the Virtual Appliance connection.

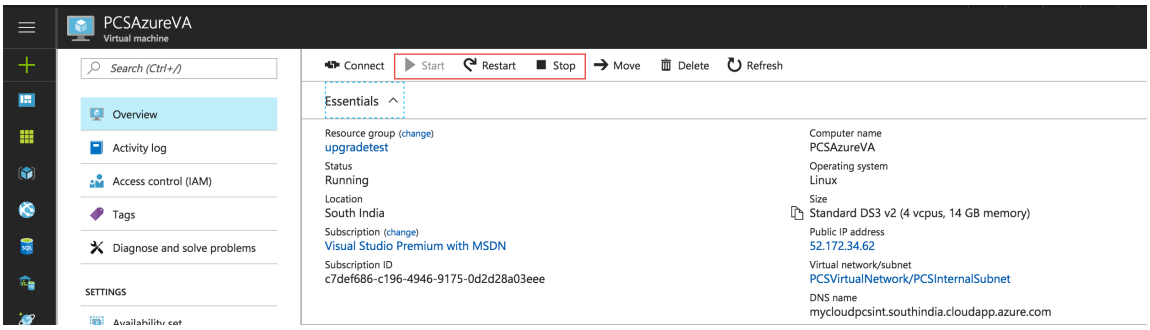


FIGURE 5.4 : System Operations

On the Azure portal top menu bar:

- Click **Start** to start a VM
- Click **Stop** to stop the VM
- Click **Restart** to restart the VM

The corresponding CLI commands are:

- Start a VM

```
az vm start --resource-group myResourceGroup --name myVM
```

- Stop a VM

```
az vm stop --resource-group myResourceGroup --name myVM
```

- Restart a VM

```
az vm restart --resource-group myResourceGroup --name myVM
```

Deploying on Google Cloud Platform

For a detailed ICS on GCP deployment procedure, refer to *ICS Gateway Deployment on Google Cloud Platform* at https://www.ivanti.com/support/product-documentation.

Ivanti Connect Secure Gateway Analytics

Introduction

Ivanti Neurons for Secure Access Admin portal provides visibility of user activity and service usage across your Ivanti Connect Secure Gateways in your enterprise through network activity analytics, gateway performance graphs, application usage metrics, and stored activity logs.

After you log in to the Ivanti Neurons for Secure Access Admin portal and select Ivanti Connect Secure from the Gateway Switcher (Ivanti Connect Secure, Ivanti Neurons for Secure Access), Ivanti Connect Secure displays the **Network Overview** page. This page presents a top-down overview of your application infrastructure, providing an opportunity to monitor user and Gateway activity, and to identify

problems and compliance issues as they occur. For more information, see *Reviewing Your Network Activity* (page 30).

Through the Ivanti Connect Secure menu, use the **Insights** menu icon to:

- View graphs, metrics, and logs concerning all users activities, see *Reviewing Users Activity* (page 55).
- View graphs, metrics, and logs concerning to individual user activities, see *Reviewing Individual User Activity* (page 78).
- See details and usage of applications configured in your Ivanti Connect Secure service, see *Reviewing Application Usage* (page 66).
- View graphs, metrics, and logs concerning to all gateways status and versions, see *Reviewing Gateways Status and Versions* (page 82).
- Configure certain actions based on different types of Insights, see *Configuring Actionable Insights* (page 102).

Note: Ivanti Connect Secure provides both a light theme and a dark theme for the UI display.

Reviewing Your Network Activity

The *Network Overview* page shows real-time analytics data for your application infrastructure, providing a one-page dashboard of activity across your organization.

To access the **Network Overview** page:

1. Log in to the Ivanti Neurons for Secure Access Admin portal as a Tenant Admin, and select Ivanti Connect Secure from the Gateway Switcher. See *Logging in to Ivanti Neurons for Secure Access* (page 5).

   The *Network Overview* page appears by default.

2. To return to the *Network Overview* page at any time, click the **Insights** menu icon and then click **Overview**. Alternatively, click the "Ivanti Neurons for Secure Access" banner at the top.

Ivanti Connect Secure provides bread-crumb navigation for all *Insights* pages at the top.

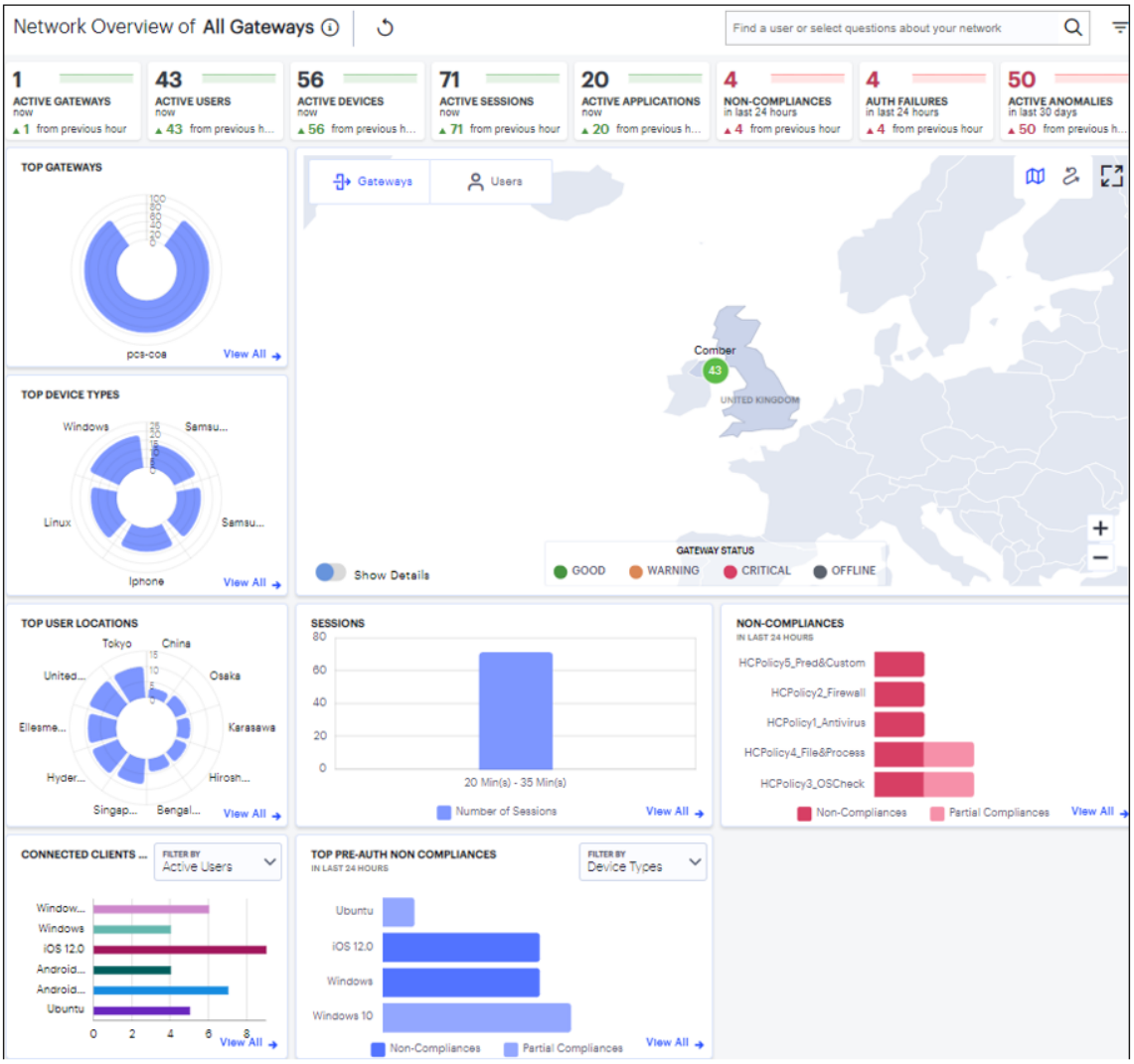


FIGURE 6.1 : An overview of Network activity across your enterprise

Understanding the Display

The primary components of the **Network Overview** page are the following:

- **Filter bar**, allowing the selection of any individual Ivanti Connect Secure Gateway. For details, see *Using the Filter Bar* (page 32).
- **Summary ribbon**, showing totals for active **Gateways**, **Users**, **Devices**, **Sessions**, **Applications**, **Non-Compliances**, **Auth Failures**, and **Anomalies**. For more details, see *Viewing the Network Summary Ribbon* (page 33).
- **Switchable World Map and Sankey chart**, showing active Gateways locations and Users locations:
  - In the world map view, each Gateway location and User location provides a summary of the activity observed there. For more details, see *Using the World Map* (page 39).
  - In the Sankey chart view, you can view the relationships between user

groups, device types, and Gateways. For more details, see *Using the Sankey Chart View* (page 47).

- **Radar charts**, providing top usage data for **Gateways**, **Device Types**, and **User Locations**. For more details, see *Using the Top Active Breakdown Charts* (page 51).
- **Bar chart** breakdowns showing **Sessions**, **Non-compliances**, **Connected Clients Version** and **Pre-auth Non-Compliances** activity. For more details, see *Using the Sessions, Non-Compliances, Connected Clients Version and Pre-Auth Non-Compliances Charts* (page 48).

Note: The data in this page refreshes automatically every 5 minutes.

With each chart, click the **View all** link to view detailed log records for that category.

The following principles apply to all elements of the page:

- A user can have one or more devices.
- Each device can have one or more active secure access sessions on multiple gateways.
- One session can connect to multiple applications.
- One session can be associated with multiple Gateways.
- One Gateway can have multiple applications registered with it.

Using the Filter Bar

Ivanti Connect Secure uses the top part of the display on all **Insights** data analysis pages to show the current page title, the default time period, and options to:

- Manually refresh the data
- Set a filter for a specific Ivanti Connect Secure gateway
- Ask a predefined question (Intent):
  - Search for a specific user in the tenant by typing the username
  - Show me users connected in last one hour
  - Show me non-compliant users
  - Show me users connected more than one days
  - Show me users from most busy gateway
  - Show me users from least busy gateway

By default, analytics data on this page and others is shown for the last hour or current day. To manually refresh the data, click the circular arrow:

FIGURE 6.2 : Refreshing the data

Ivanti Connect Secure provides the ability to show focused metrics for a specific Ivanti Connect Secure Gateway. To select a specific gateway, use the filter icon:

FIGURE 6.3 : The Filter icon

In the Filter panel, from the drop-down list select the required gateway and click **Apply**. To clear the selection, click **Clear All**.

Viewing the Network Summary Ribbon

The Summary ribbon at the top of the page shows data totals for the selected time filter:

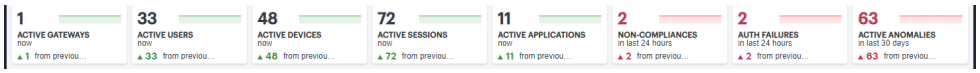


FIGURE 6.4 : Viewing the Summary Ribbon

The ribbon indicates the totals accrued for each category during the displayed time period, as indicated adjacent to the category name.

The following categories are provided in the ribbon:

- The number of **Active Gateways**.
- The number of **Active Users**.
- The number of **Active Devices**.
- The number of **Active Sessions**.
- The number of **Active Applications**.
- The number of **Non-compliances**. In other words, non-compliant attempts to access your applications. For the default time period filter, non-compliance totals shown here are for 24 hours. For other selected time periods, the number reflect the total for that period.
- For the default time period filter, **Auth Failures** totals shown here are for 24 hours. For other selected time periods, the number reflect the total for that period.
- The number of **Anomalies** detected by Ivanti Connect Secure. That is, the total number of geographic anomalies. For the default time period filter, anomaly totals shown here are for the previous 30 days, and include only

unacknowledged anomalies. For other selected time periods, this total includes both acknowledged and unacknowledged anomalies.

If you are currently viewing data for the *last hour*, each category in the ribbon includes a trend graph (highlighted, top) showing the changes in data during the hour. Also included is a change value (highlighted, bottom) based on the previous hour:

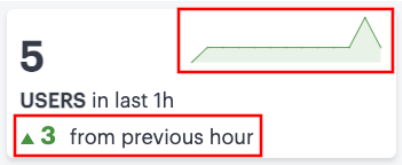


FIGURE 6.5 : Data trends for this hour versus the previous hour

Note: In the default *last hour* view, while data for Active Gateways, Users, Devices, Sessions and Applications is shown as such, Non-Compliances and Auth Failures are shown for the previous 24 hours, and anomalies are shown for the previous 30 days. This is as indicated against the Category name.

Additional trend indicators are present for the *last hour* time period only. Trends are not applicable when any filter is applied (intent or gateway).

If you click on any of the categories in the ribbon, Ivanti Connect Secure displays a sliding info-panel dialog showing more details for that category. For example, if you click on the **Active Gateways** category, a panel appears showing the list of active Gateways. In this case, a summary box is displayed for each Gateway showing statistics relevant to that instance, such as the number of active users, active sessions, active devices, non-compliance events, system status such as the system uptime, last config update, session counts such as current SSL sessions count, auth-only sessions, ActiveSync device count.

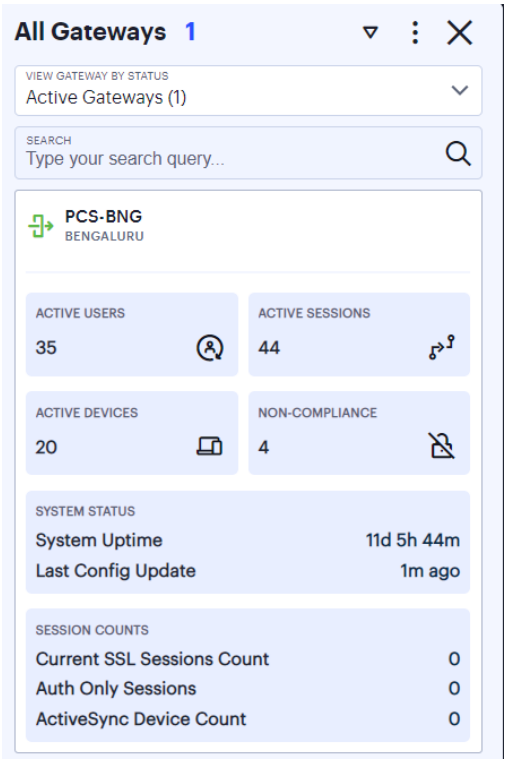


FIGURE 6.6 : Viewing the Gateways info-panel

Note: This version of the info-panel shows details for *all Gateway locations*. To view an info-panel for a single Gateway location, click the Gateway location bubble in the world map. For more details, see *Using the World Map* (page 39).

For the *Active Gateways* info-panel, use the **View Gateway by Status** drop-down list to change the type of Gateways displayed in the panel. Choose from:

- **All Gateways**: All Gateways regardless of status.
- **Active Gateways**: All active Gateways. That is, only Gateways that have active sessions. This is the default view.
- **Offline Gateways**: All offline or unregistered Gateways. That is, only Gateways that are unresponsive or not yet registered with the Ivanti Neurons for Secure Access.
- **Online Gateways**: All online Gateways. That is, all Gateways that are registered with the Ivanti Neurons for Secure Access.

Note: The number of instances of each type is given in brackets.

For example, by selecting *Offline Gateways*, the panel updates as follows:

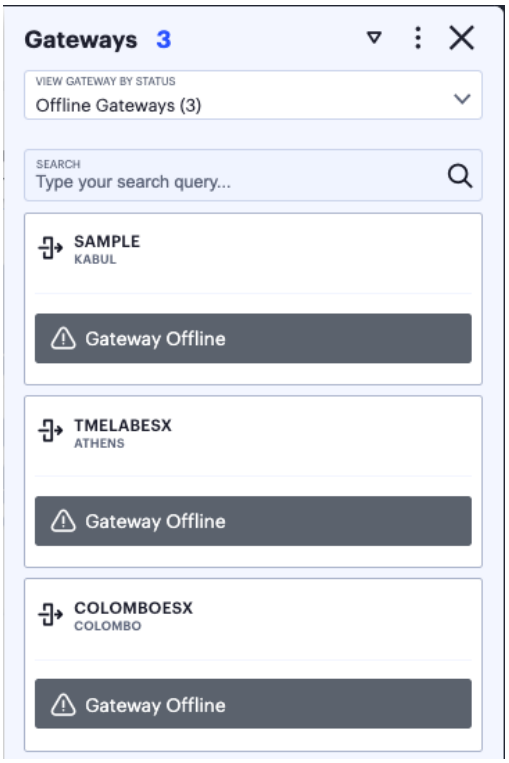


FIGURE 6.7 : Viewing all offline/unregistered Gateways in the Gateways info-panel

Use the **Search** bar at the top to filter the results list. For example, to show only those Gateways that match a search string. To clear your search, click **CLEAR SEARCH RESULTS**.

To learn more about the meaning of the different indicator colors used in the info-panel, see *Understanding Gateway Status Indicator Colors* (page 43). Hover your pointer over the instance health indicators to display a tooltip showing more specific details and values.

Click on any Critical or Warning notification banner to display a drop-down summary of the issues:

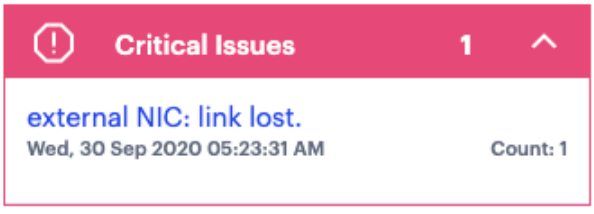


FIGURE 6.8 : Viewing critical issues

You can click on each entry to obtain more details and logs concerning the issue.

Note: For the Active Users info-panel, Ivanti Connect Secure displays an *average UEBA threat score*. To learn more about UEBA threat scores, see *Reviewing Users*

Activity (page 55).

Note: For Non-Compliance and Anomalies info-panels, summaries are displayed on a per-user basis, with the reason for the event shown.

To change the sort order of the items displayed in the info-panel, use the *Sorting* controls at the top:

FIGURE 6.9 : Changing the info-panel sort order

Use the *dots* icon to select the sort criteria, then use the *arrow* icon to toggle between ascending and descending order. The sort criteria varies depending on the category chosen, and is based on the statistics shown for each item. For example, by selecting the **Gateways** info-panel, you can choose the display order for your Gateways based on the following statistics:

- Active Users
- Non-Compliances
- Active Devices
- Number of Issues
- Gateway Name
- City Name

A tick identifies the currently chosen criteria.

For **Anomalies**, the info-panel lists Unacknowledged and Acknowledged anomalies, and provides additional functionality to enable you to *Acknowledge* individual Unacknowledged anomalies.

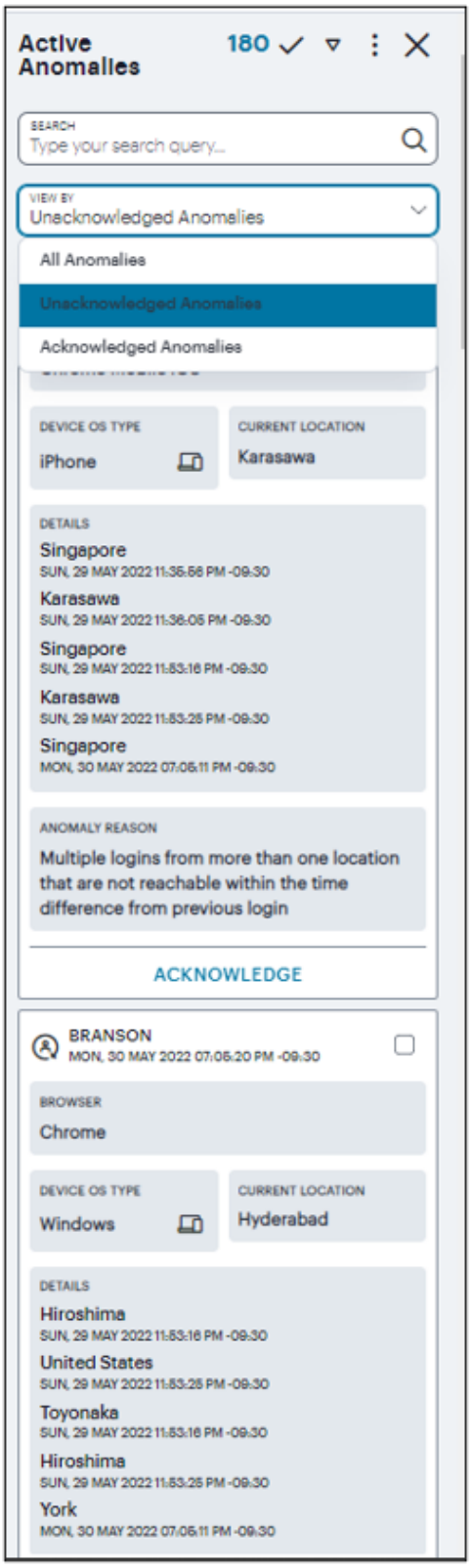


FIGURE 6.10 : Viewing the Anomalies info panel

Each box in the info-panel lists a user and the active anomalies connected to them. For each user, from the Unacknowledged anomalies list, click **ACKNOWLEDGE** to

remove this anomaly from the list.

Alternatively, use the *tick* icon and check boxes adjacent to each user name to acknowledge multiple, or all, anomalies in a single action. Note that when the default "active" time period filter is selected, the anomalies count in the Summary ribbon decreases by 1 for each acknowledgment.

For the **Gateways** info-panel, click a Gateway name to access the corresponding *Gateways Overview* page that provide usage metrics or configuration details for that item.

Using the World Map

The Map view contains Gateways and Users tabs. Your Gateways locations are presented on the map as a series of geographically-placed counters, with each counter depicting a location, the status of the services held there, and the number of Gateways. To learn more about the colors used to indicate service status, see *Understanding Gateway Status Indicator Colors* (page 43).

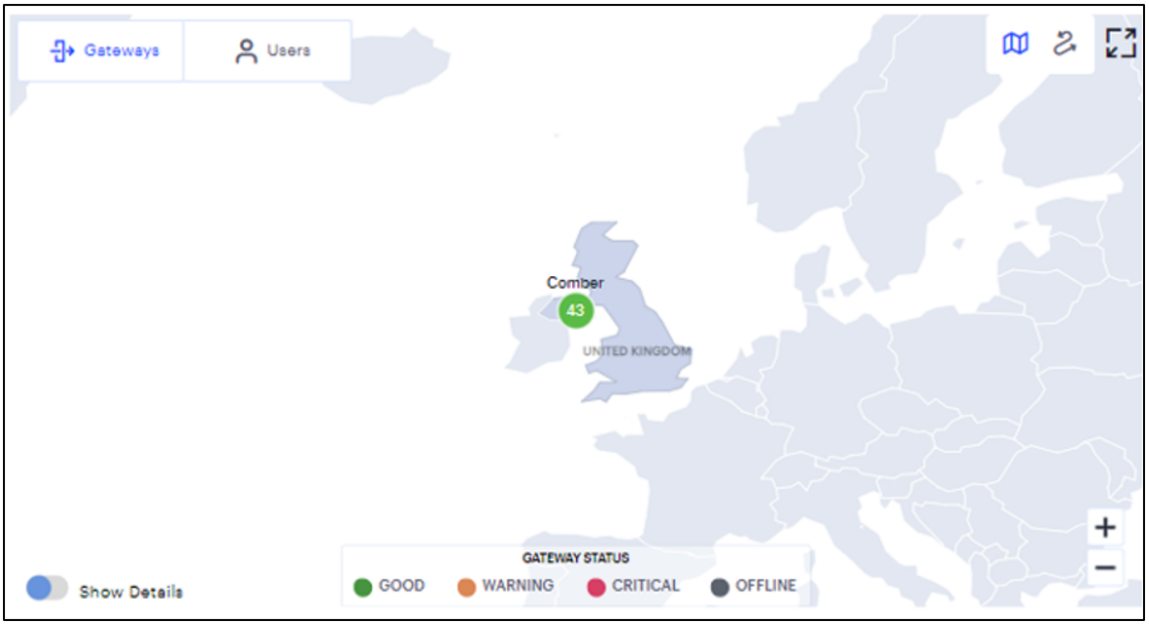


FIGURE 6.11 : Viewing the world map - Gateways

Use the Plus (+) and Minus (-) controls to zoom in and out of the world map, allowing you to select the desired level of detail. Alternatively, use your pointer to manipulate the map display. Double-click/tap an open area of the map to zoom in, or reposition the map display through drag and drop.

To toggle between the Map view and Sankey chart view, use the icons at the top-right:

FIGURE 6.12 : Toggle between Map view and Sankey chart view

The data shown is representative of the currently-selected time period, and by default shows *active* data (for the previous 1 hour). To learn more about setting time periods for the displayed data, see *Using the Filter Bar* (page 32).

To learn more about network usage or alerts at a particular location, hover your pointer over the location identifier. It shows the active user sessions established from that Gateway location to other Gateway locations.

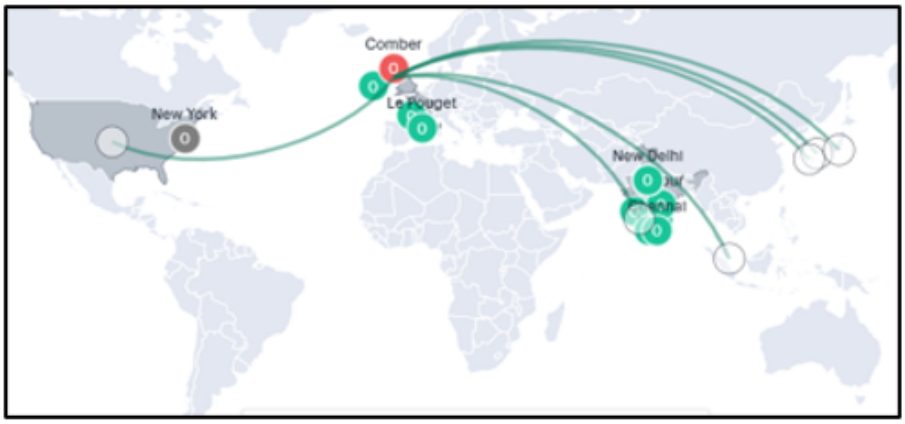


FIGURE 6.13 : Sessions from the Gateway location

By turning on the **Show Details** switch located at the bottom-left of the map, and by hovering on a Gateway location, the current Gateway status is indicated by the color scheme shown in the legend.

Note: To learn more about the meaning of the different indicator colors used in the map and panels, see *Understanding Gateway Status Indicator Colors* (page 43).

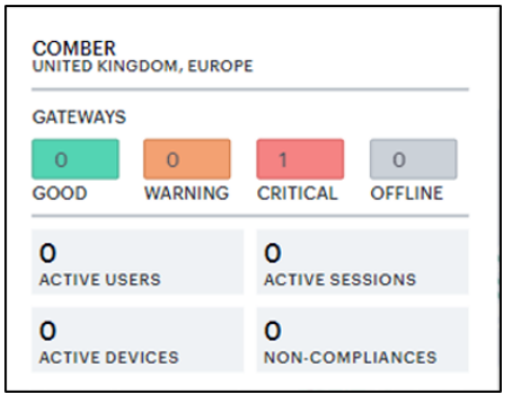


FIGURE 6.14 : Viewing an extended location status

To expand the current view, click the Full Screen icon:

FIGURE 6.15 : Expand the current view

In the expanded view, the Gateway Status pop-up summary panel is expanded to include more details concerning usage at that location:

In addition to the status indicator, this version of the summary panel shows the following statistics:

- **Active Users**: The number of unique users that have sessions through Gateways at the location (as also indicated in the location bubble)
- **Active Sessions**: The number of sessions accessed through Gateways at the location
- **Active Devices**: The number of unique devices that have sessions through Gateways at the location
- **Non-Compliances**: The number of active non-compliant sessions (full/partial non-compliant) in this location

Note: Click the Full Screen icon again to return to the standard view.

In both views, click a location bubble to display a sliding info-panel dialog for the Gateways at that location.

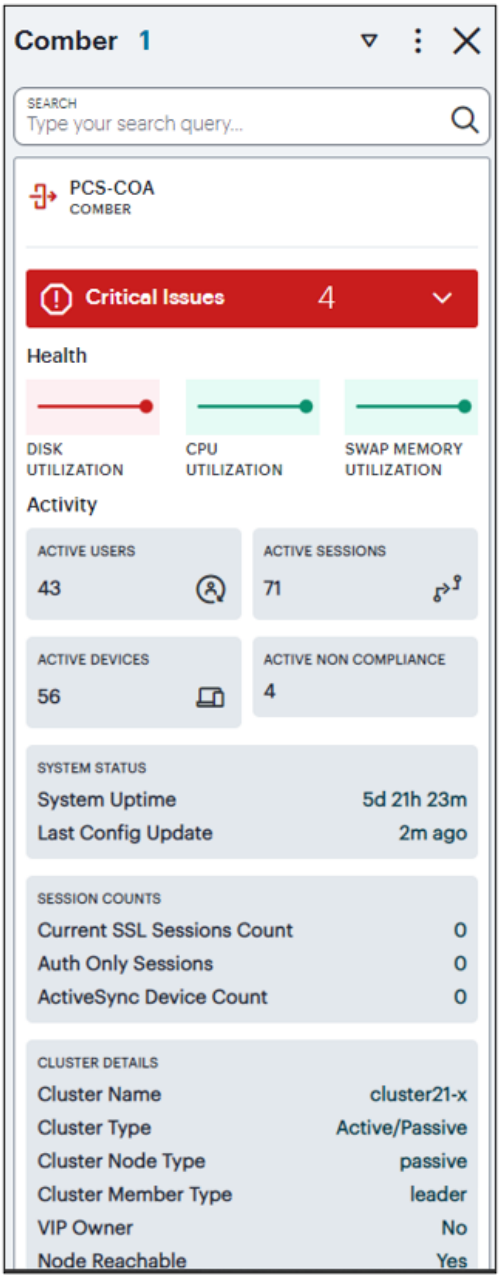


FIGURE 6.16 : Viewing the Gateway info-panel for a single location

Use this info-panel to view health and usage statistics for the location, with further details concerning any reported problems with the deployed Gateways. The panel displays the following details:

- **Location name and number of Gateways**: The descriptor for this location and the number of Gateway instances deployed there.
- **Active Users**: The number of unique users that have sessions through Gateways at the location (as also indicated in the location bubble).
- **Active Sessions**: The number of sessions accessed through Gateways at the location.
- **Active Devices**: The number of unique that have sessions through Gateways

at the location.

- **Non-Compliance**: The number of active non-compliant sessions (full/partial non-compliant) in this location.
- **System Status**: The system uptime and the time since the last config update.
- **Session Counts**: The number of current SSL sessions, number of auth only sessions, and the number of ActiveSync devices.
- **Cluster Details**: The cluster name, type, and node details.

This view of the info-panel displays data for a *single* Gateway location. To view an info-panel showing data for *all* Gateway locations, click the Gateways category in the Summary ribbon. To learn more, see *Viewing the Network Summary Ribbon* (page 33).

Note: When displaying active data, all non-compliance and unacknowledged anomaly totals are displayed for the previous 24 hours.

To learn more about the information and controls contained in the info-panel, see *Viewing the Network Summary Ribbon* (page 33).

Understanding Gateway Status Indicator Colors

In the world map view, your current Gateway status is indicated by the color scheme shown in the legend:

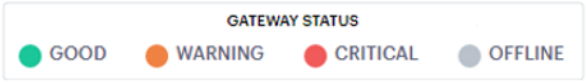


FIGURE 6.17 : Map legend showing Gateway status meanings

- **Good (Green)**: All Gateways are functioning normally.
- **Warning (Amber)**: One or more of the Gateways at that location is experiencing a *warning* scenario. This status is triggered by the occurrence of any one of the following conditions:
  - Gateway device CPU usage is within the range 80% - 90%
  - Gateway device swap memory usage is within 10% - 50%
  - Gateway device disk usage is within the range 80% - 90%
- **Critical (Red)**: One or more of the Gateways at that location is experiencing an *critical* alert scenario. This status is triggered by the occurrence of any one of the following conditions:
  - Gateway device swap memory usage is greater than 50%
  - Gateway device disk usage is greater than 90%
  - At least 1 critical error has been reported

- **Offline (Grey)**: All offline or unregistered Gateways. That is, only Gateways that are unresponsive or not yet registered with the Ivanti Neurons for Secure Access.

Furthermore, counters in the *Summary ribbon* use the following color scheme to reflect status:

- **Red**:
  - **Users**: at least one user has anomalies in the selected duration
  - **Devices**: at least one active device is non-compliant in the selected duration
  - **Gateways**: as described above
  - **Non-compliance**: if the count is non-zero
  - **Anomalies**: if the count is non-zero

Users Map View

In the world map **Users** tab, each location shows the number of active users in that location.

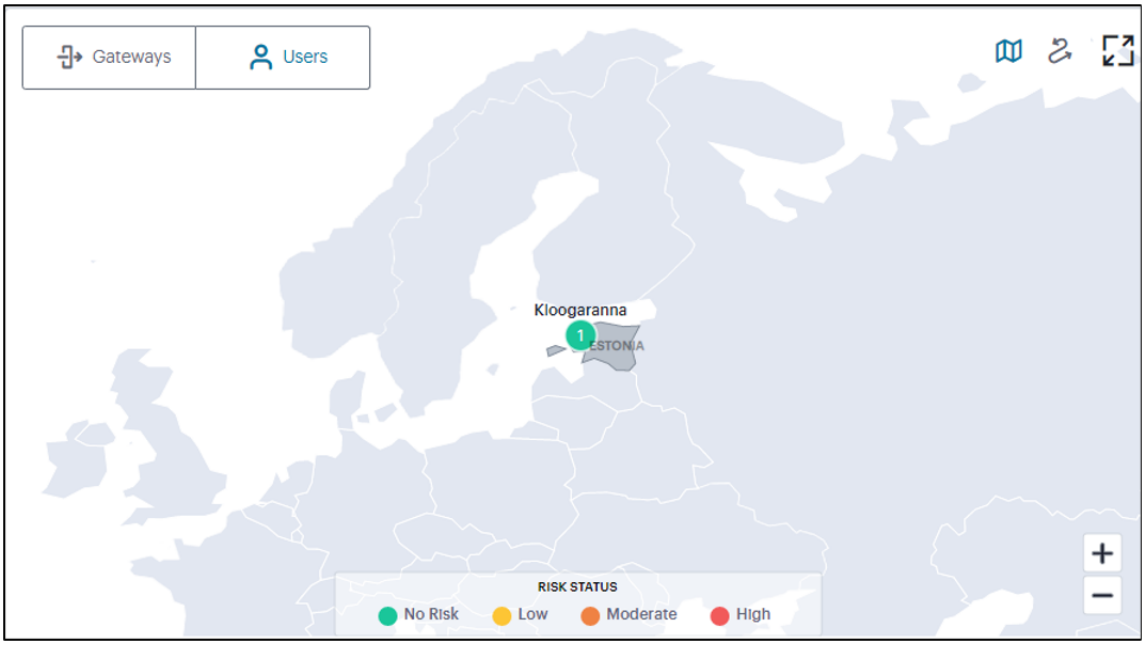


FIGURE 6.18 : Viewing the world map - Users

Use the Plus (+) and Minus (-) controls to zoom in and out of the world map, allowing you to select the desired level of detail. Alternatively, use your pointer to manipulate the map display. Double-click/tap an open area of the map to zoom in, or reposition the map display through drag and drop.

To toggle between the Map view and Sankey chart view, use the icons at the top-right:

FIGURE 6.19 : Toggle between Map view and Sankey chart view

The color of the location shows the average UEBA Threat scores of the active users in that location:

- **Green (No Risk)** - UEBA Threat score < 10
- **Yellow (Low)** - UEBA Threat score > 10 < 20
- **Orange (Medium)** - UEBA Threat score > 20 < 30
- **Red (High)** - UEBA Threat score > 30
- Hover on a user location to view detailed UEBA Threat scores of the users in that users location.

By hovering on a User location, the current Users' status is indicated by the color scheme shown in the legend.

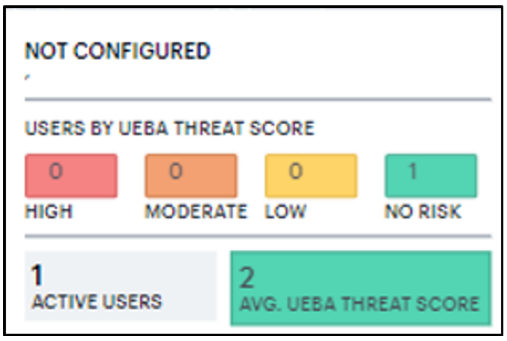


FIGURE 6.20 : Viewing current users status

Click a location bubble to display a sliding info-panel dialog for the Users at that location.

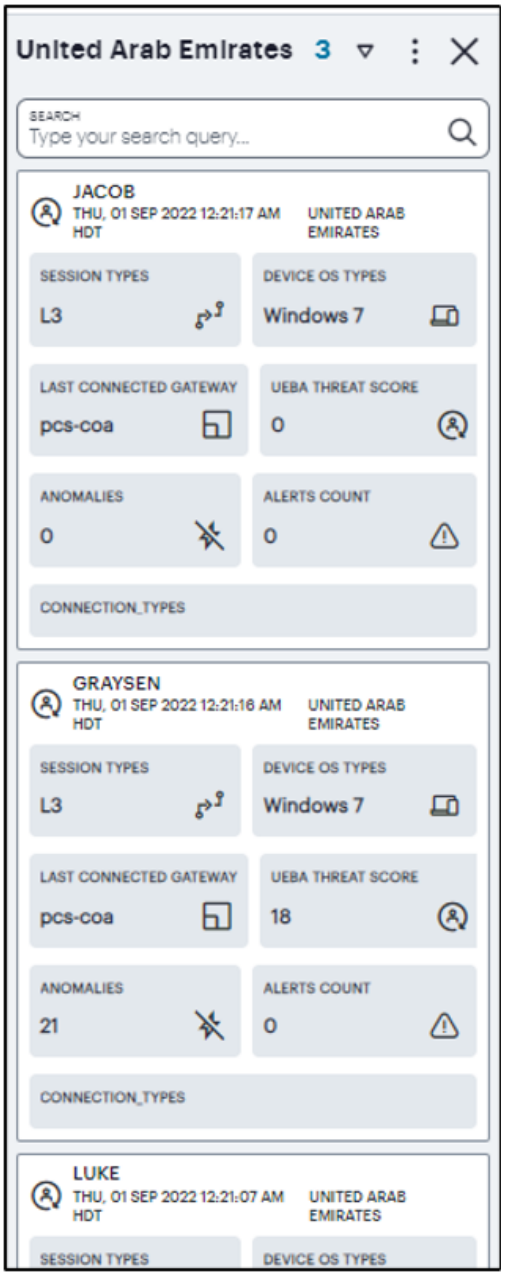


FIGURE 6.21 : Viewing the Users info-panel

The panel displays the following details:

- Session type
- Device OS type
- Last connected gateway
- Average UEBA Threat score
- Anomalies
- Alerts count

Using the Sankey Chart View

The Network Sankey chart provides an alternate visualization of your services, showing directed flow between related objects. The width of each stream in the flow is proportional to the utilization of the object the flow passes through, allowing an administrator to view significant usage and relationships across your user base and application infrastructure.

To activate the Sankey chart view, use the toggle icons at the top-right:

FIGURE 6.22 : Toggle between Map view and Sankey chart view

By clicking the toggle display icon, the Sankey chart replaces the world map in the display. All other components remain unchanged.

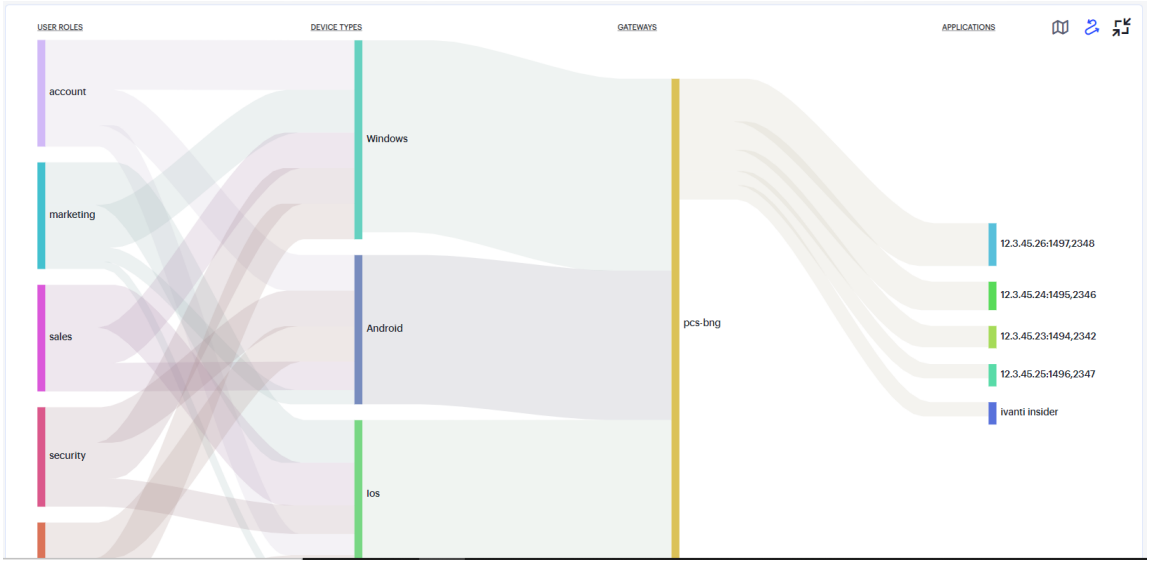


FIGURE 6.23 : Displaying the Network Overview Sankey Chart View

The Ivanti Connect Secure Sankey chart maps **User Roles** > **Device Types** > **Gateways** > **Applications**. By hovering your pointer over a flow of interest, Ivanti Connect Secure displays a tooltip confirming the scale of the activity between the two objects connected by the flow.

To focus the display on a specific flow, or to identify related objects that interact with this flow, click the chart at a point of interest. Ivanti Connect Secure provides highlighting to all flows that pass through the point selected.

Using the Sessions, Non-Compliances, Connected Clients Version and Pre-Auth Non-Compliances Charts

The **Network Overview** page includes bar charts to provide a breakdown of **Sessions**, **Non-Compliances**, **Connected Clients Version** and **Pre-Auth Non-Compliances** events.

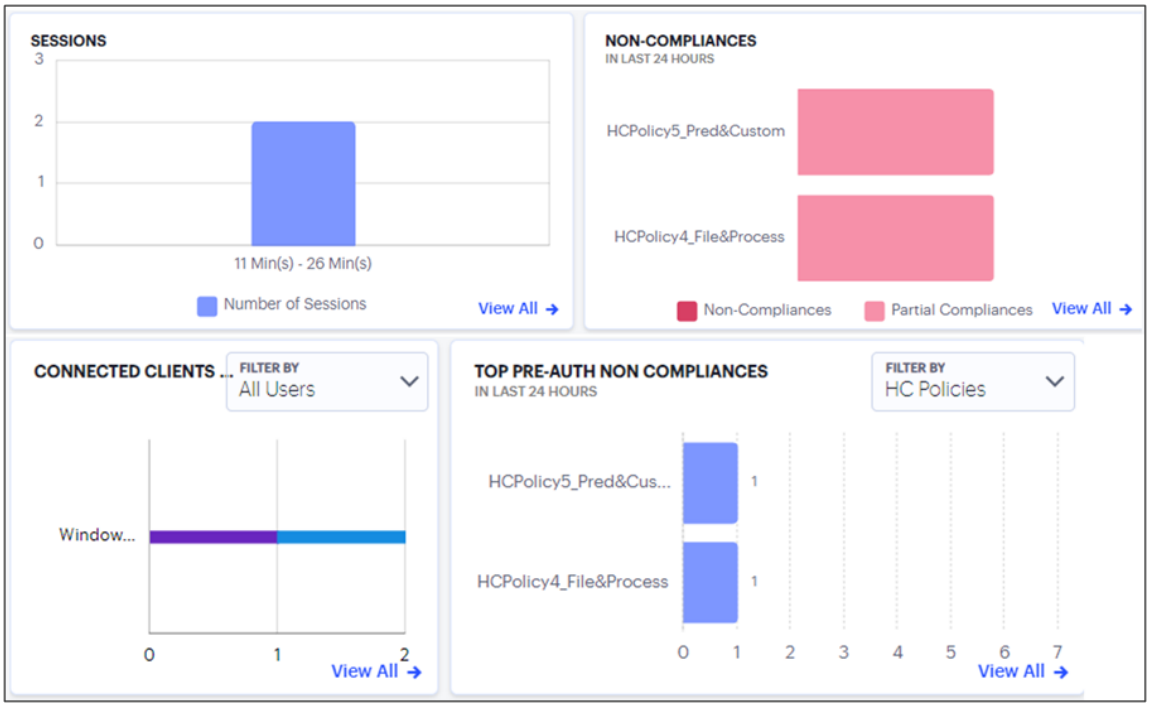


FIGURE 6.24 : Viewing a breakdown of Active Anomalies and Non-compliance

The **Sessions** chart provides the total number of sessions over a period. That is, user sessions that took place during the period.

To view a detailed list of events that contributed to the totals, click **View all**:

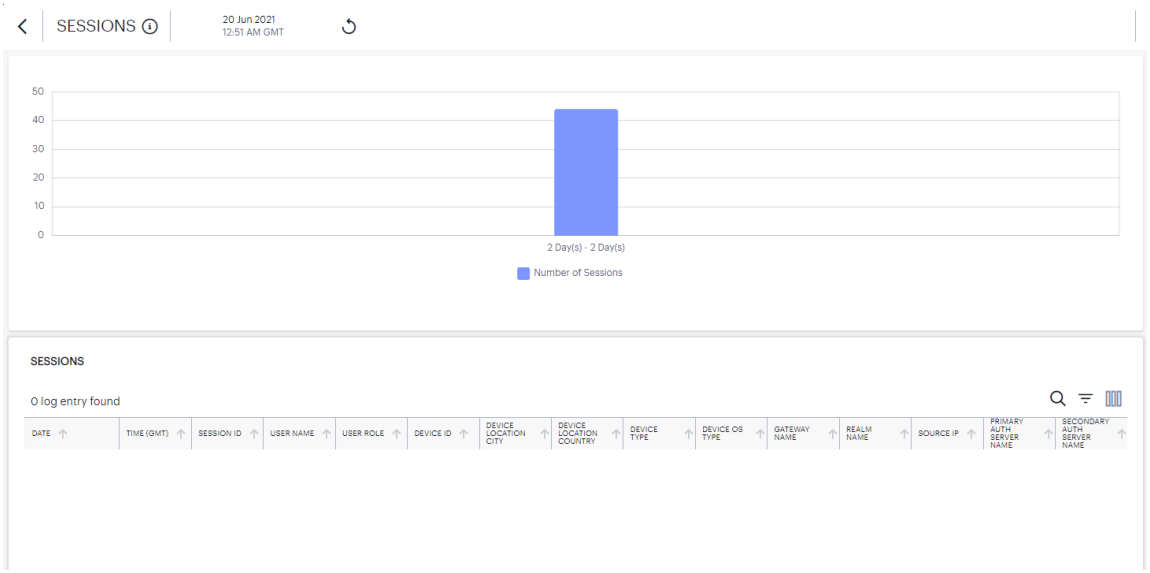


FIGURE 6.25 : Viewing Sessions events

The **Non-compliances** chart provides a breakdown of non-compliant device activity that contravened a configured device policy. Totals are given for the highest policy contraventions recorded during the period.

To view a detailed list of events that contributed to the totals, click **View all**:

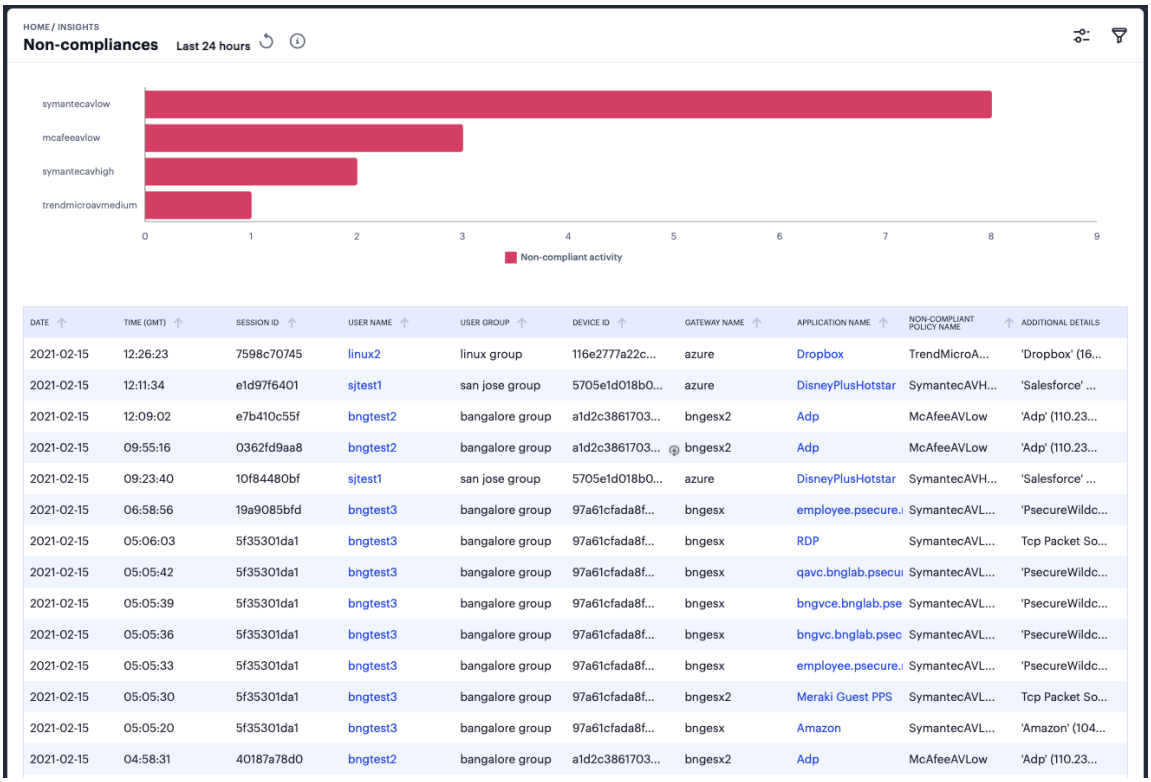


FIGURE 6.26 : Viewing Non-compliances events

Click on the legend labels to toggle that element on or off in the chart. Use your

pointer to scroll the event messages pane to view more details in the columns to the right.

The **Connected Clients Version** chart provides the distribution of various versions of Ivanti Secure Access client across different device OS in the tenant.

You can view the chart based on *Active Users* for Ivanti Secure Access client versions distribution from the currently active sessions or *All Users* for Ivanti Secure Access client versions distribution from the sessions in the last 30 days.

To view a detailed list of events that contributed to the totals, click **View all**:

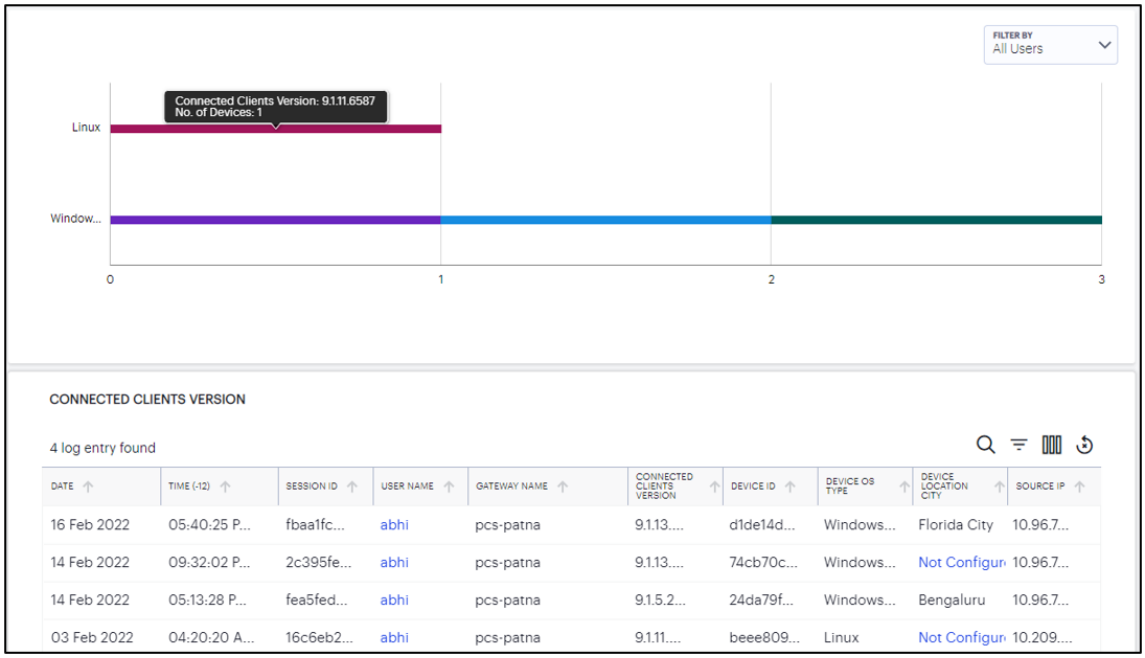


FIGURE 6.27 : Viewing Connected Clients Version Details

The **Pre-Auth Non-Compliances** provides the occurrences of non-compliance in the last 24 hours, in the tenant even before the authentication.

You can view the chart based on *Device Types*, *User Locations*, *Gateways* and *HC Policies*.

To view a detailed list of events that contributed to the totals, click **View all**:

FIGURE 6.28 : Viewing Pre-Auth Non-Compliances Details

Using the Top Active Breakdown Charts

The *radar* charts at the bottom of the page show a breakdown of **Gateways**, **Device Types**, and **User Locations** across your organization. Each chart shows the *top active items* in each category.

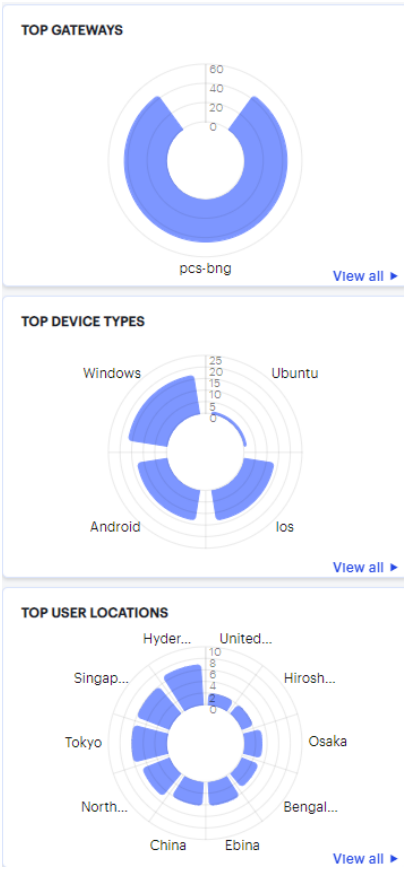


FIGURE 6.29 : Viewing the breakdown radar charts

Hover your pointer over a particular element to view a tooltip showing the label and total. To view more details for a chart, click the corresponding **View all** link. For example:

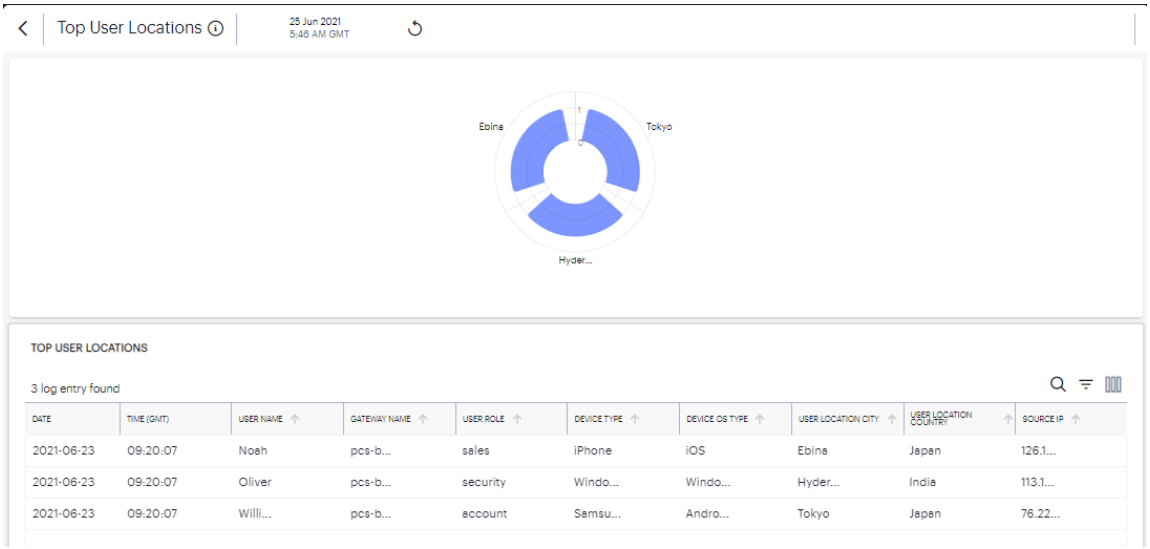


FIGURE 6.30 : Viewing details for the top active User Locations

Click the **View All** link that provides access to a detailed view showing logs for the

corresponding chart.

In the detailed log page:

- Double-click on any log to view additional details of that log in the Info Panel to the right.
- Use the Group by option and select the field type to view the table information in groups. Then click > to view the logs in that group.

FIGURE 6.31 : Group by icon

- Use the Advanced Filter icon to view logs based on the pre-defined filter, operator and value.

Advanced Filtering

In the logs section, click the **Advanced Filter** icon and view logs based on the pre-defined filter, operator and value.

To create a custom filter:

1. Click the **Advanced Filter** icon to open the Advanced Filter window.

FIGURE 6.32 : Advanced Filtering

2. Choose the required column from the **Filter by** list, select an operator, enter a value and click **Add**.
3. Repeat to add more filters if required.
4. Enter a name for the filter and click **Save**. The new filter will be listed in the **Filters** list.

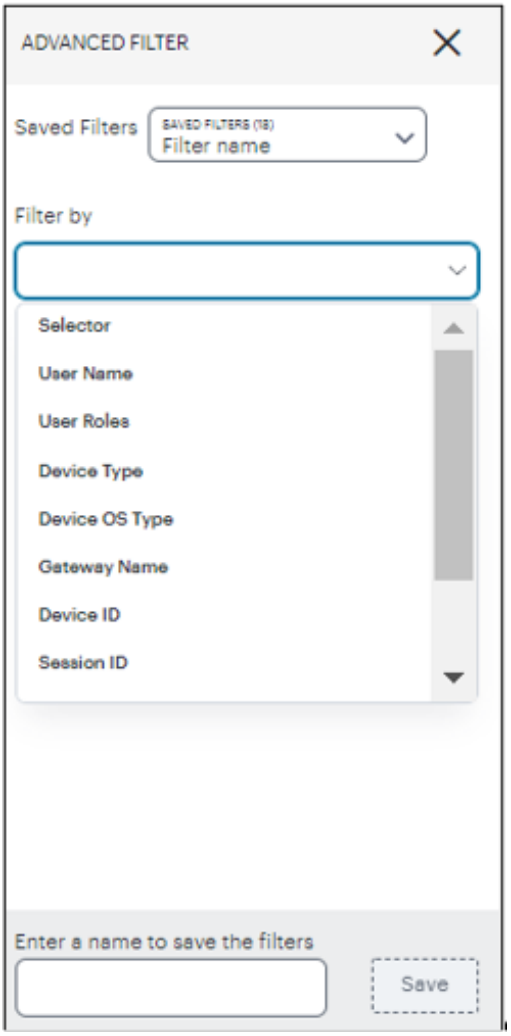


FIGURE 6.33 : Creating Advanced Log Filter

5. To load a previously-saved filter, select your filter from the **Saved Filters** drop-down list and click **Apply**.

   When you apply a filter, the filter information is retained in the new session/login.

6. You can individually remove filters that are applied on the table or you can use the **Reset Filter** icon to clear all the filters applied on the table.
7. To delete one or more previously-saved filters, select the filters from the **Saved Filters** drop-down list and click **Delete**.

Reviewing Users Activity

The *Users Overview* page shows activity relating to users in your Ivanti Connect Secure deployment.

To access the *Users Overview* page:

1. Log in to the Ivanti Neurons for Secure Access Admin portal as a Tenant Admin, and select Ivanti Connect Secure from the Gateway Switcher. See *Logging in to Ivanti Neurons for Secure Access* (page 5).

   The *Network Overview* page appears by default.

2. From the Ivanti Connect Secure menu, click the **Insights** icon, then select **Users**.

   The *Users Overview* page appears.

FIGURE 6.34 : An overview of activity for all users

Understanding the Display

The *Users Overview* page contains the following components:

- **Filter bar**, allowing the selection of active or data. For details, see *Using the Filter Bar* (page 58).
- **Summary ribbon**, showing metrics for user activity. For more details, see *Viewing the Users Summary Ribbon* (page 58).
- **User Top Stats**, **Top 10 Users By UEBA Threat**, **UEBA Threat Types**, showing graphs and metrics for UEBA Threat scores across your user groups. For more details, see *Viewing a Summary of UEBA Threat Scores for your Users* (page 59).
- **User Session Trends**, showing a timeline chart of user sessions. For more details, see *Viewing the Users Session Trend* (page 61).
- **Activity charts**, showing charts for *Adaptive authentication*, *Top user count*, *Top auth failures*, and *Session types*.

Each chart on this page includes a **View All** link. This link provides access to a detail view showing logs for the corresponding chart. For example:

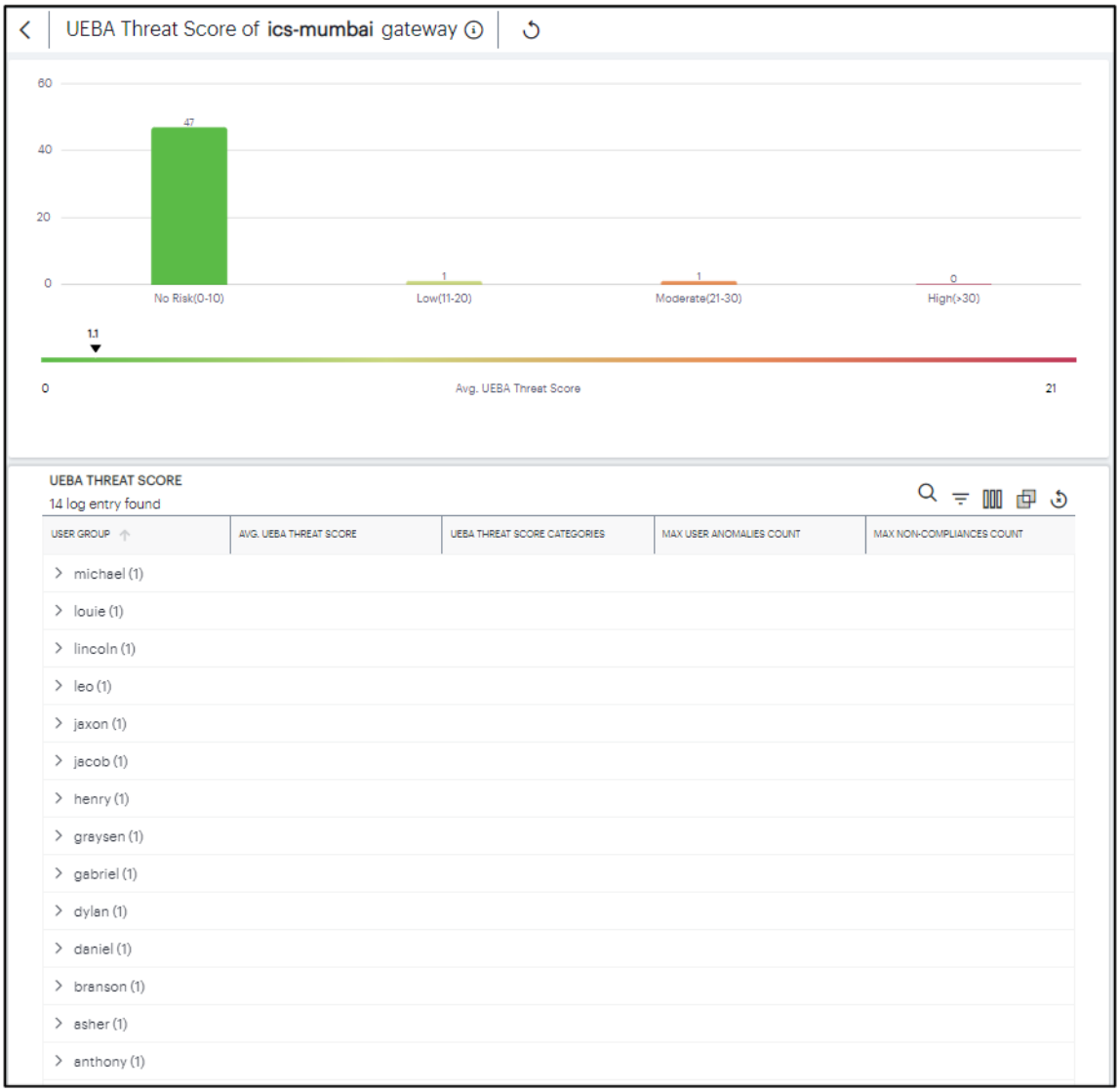


FIGURE 6.35 : Viewing UEBA Threat Score detailed logs

Each detail view shows logs for the corresponding chart or category. For each column, click the *arrow* icon adjacent to the column name to sort in ascending or descending order. Use your pointer to scroll the log messages pane to view more details in the columns to the right.

Where a log message is too long for the display, hover your pointer over the message to view a tooltip containing the full text. Furthermore, to view a single log entry in a dedicated panel, click the log message text to activate the info-panel view.

Using the Filter Bar

Ivanti Connect Secure uses the top part of the display on all **Insights** data analysis pages to show the current page title, the default time period, and options to:

- Manually refresh the data
- Set a filter for a specific Ivanti Connect Secure gateway
- Ask a predefined question (Intent):
  - Show me Top Risky Users
  - Show me users with Geo Anomaly
  - Show me user roles with most Non-Compliances
  - Show me top users with Auth Failures
  - Show me users with MFA

By default, analytics data on this page and others is shown for the last hour or current day. To manually refresh the data, click the circular arrow:

FIGURE 6.36 : Refreshing the data

Ivanti Connect Secure provides the ability to show focused metrics for a specific Ivanti Connect Secure Gateway. To select a specific gateway, use the filter icon:

FIGURE 6.37 : The Filter icon

In the Filter panel, from the drop-down list select the required gateway and click **Apply**. To clear the selection, click **Clear All**.

Viewing the Users Summary Ribbon

The Summary ribbon at the top of the *Users Overview* page shows activity totals for the selected time filter:

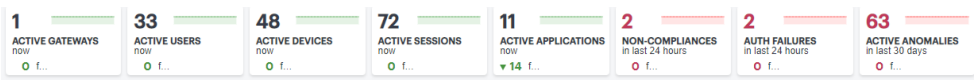


FIGURE 6.38 : Viewing the Summary Ribbon

The ribbon indicates the totals accrued for each category during the displayed time period, as indicated adjacent to the category name. Hover your pointer over the category elements to show a descriptive tooltip.

- **Active Gateways**: The total number of active Ivanti Connect Secure Gateways.
- **Active Users**: The number of active users during the selected time period.
- **Active Devices**: The number of active devices.
- **Active Sessions**: The number of active sessions.
- **Active Applications**: The number of in-use applications.
- **Non-Compliances**: The number of non-compliant sessions (full/partial non-compliant) across all gateways in the last 24 hours.
- **Auth failures**: The number of authentication failures in the last 24 hours.
- **Active Anomalies**: The number of anomalies detected by Ivanti Connect Secure in the last 30 days.

By default, the data presented in the ribbon corresponds to the current day, since midnight GMT. The number of hours over which the data applies is displayed in each category. To change the time period, use the filter bar (see *Using the Filter Bar* (page 32)).

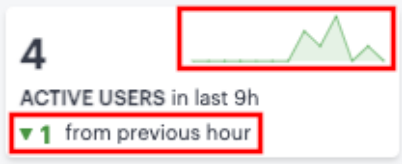


FIGURE 6.39 : Data trends for last full hour versus the previous hour

Viewing a Summary of UEBA Threat Scores for your Users

On the **Insights > Users** page, the *User Top Stats* panel displays information concerning UEBA threat across your user base:

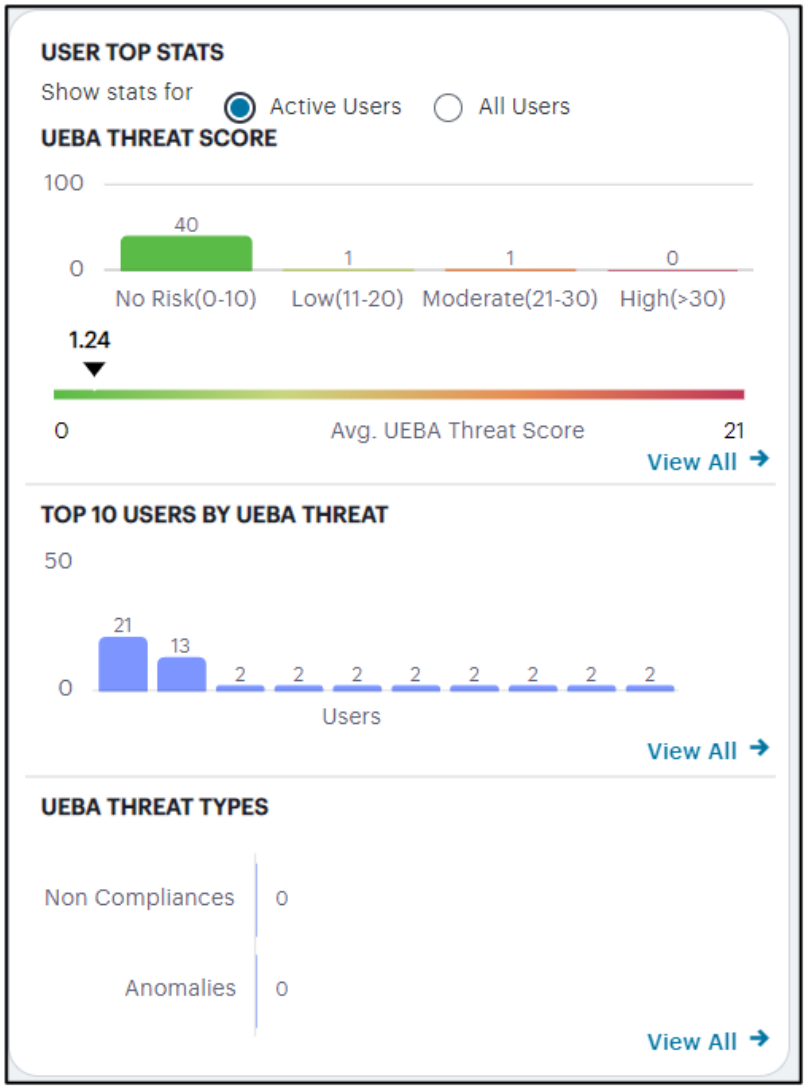


FIGURE 6.40 : Viewing user group UEBA threat data

The User Top Stats contains:

- **Active Users** tab to view user stats of the active users.
- **All Users** tab to view user stats that include users logged in for the last 30 days.

The panel provides:

- A breakdown of UEBA threat by user.
- The average UEBA threat score across all users.
- The top-10 users scoring highest for UEBA threat. It also shows the UEBA threat score threshold set, to terminate the user sessions with applicable rule on reaching the permissible limit.
- A break-down of UEBA threat types.
- The policies with highest non-compliance.

A user's UEBA Threat score is calculated from a combination of:

- Application access attempts originating from anomalous geographic locations.
- Non-compliant user devices that attempted to access your applications.

Each additional incident increments a user's overall UEBA Threat score.

The *No. of users* chart provides a visual indication of the number of users that fall into each of the UEBA Threat categories. These categories are shown as a range of UEBA Threat scores and number of users. The upper and lower bands for each category are shown in brackets. The categories are:

- No risk (0-10)
- Low (11-20)
- Moderate (21-30)
- High (>31)

Note: Where a particular threat category matches no users for the selected time period, that category label is not shown.

Below this chart, Ivanti Connect Secure displays the **Average UEBA Threat Score** for all users on a scale between zero UEBA Threat and the highest UEBA Threat score measured at the end of the current time period.

Note: The maximum value shown in the chart corresponds to the highest UEBA Threat score for all users as they stand at the end of the time period, not the highest they have been within that period.

The *Top 10 Users by UEBA Threat Score* chart shows the top-10 users with the highest cumulative UEBA Threat score across the selected time period. Hover your pointer over each bar in the chart to see the name of the corresponding user.

The *UEBA Threat Type* chart provides a breakdown of all geolocation anomalies and non-compliances that occurred during the selected time period.

The *Top Policies with Non-compliances* chart shows the device policies that recorded the highest number of non-compliances for the active users. Hover your pointer over each bar in the chart to see the name of the corresponding policy.

Viewing the Users Session Trend

Ivanti Connect Secure uses this section to show user sessions trends that occurred during the period:

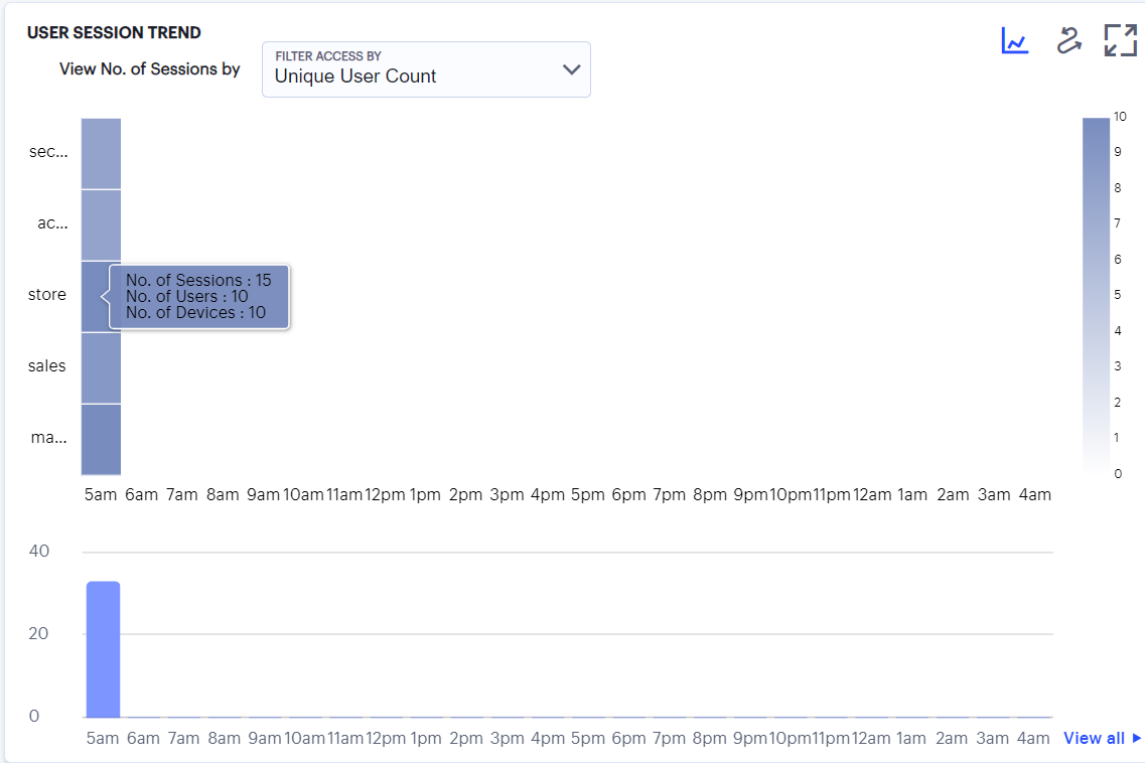


FIGURE 6.41 : Viewing top user sessions trends

You can choose to display this information through bar charts (as shown), or in a Sankey chart. Use the toggle icon at the top-right to select the required view:

FIGURE 6.42 : Toggle between bar chart view and Sankey chart view

To expand the current view, click the Full Screen icon:

FIGURE 6.43 : Expand the current view

In bar chart view, the bar chart shows one of following data types, selected using the drop-down control:

- Unique User Count
- Unique Session Count
- Unique Device Count

In the Sankey chart view, Ivanti Connect Secure provides an alternate visualization of user sessions, showing directed flow between related objects.

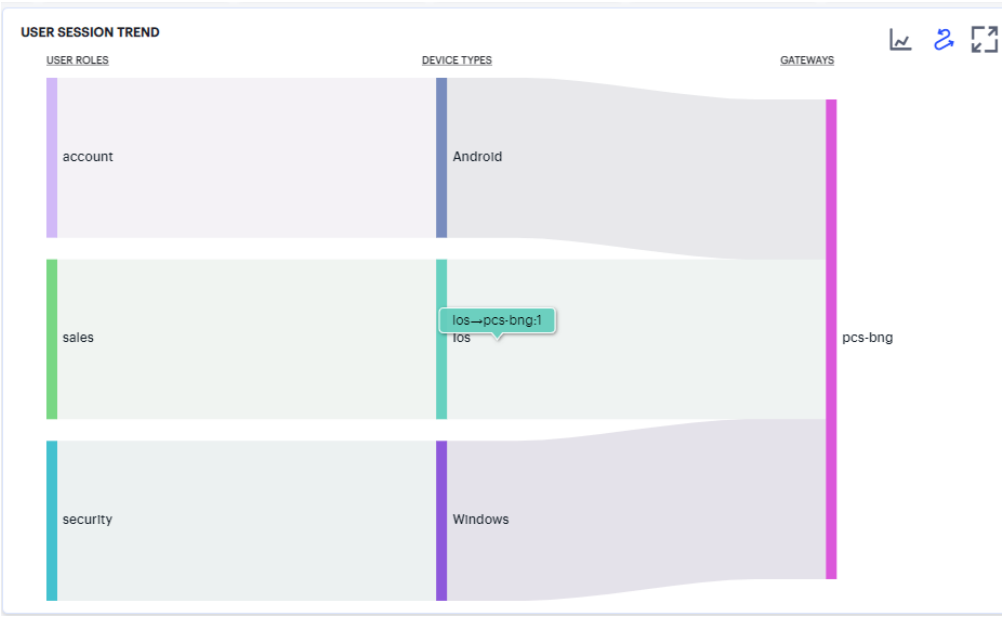


FIGURE 6.44 : User Session Trends Sankey chart

The chart maps **User Roles** > **Device Types** > **Gateways**. By hovering your pointer over a flow of interest, Ivanti Connect Secure displays a tooltip confirming the scale of the activity between the two objects connected by the flow.

To focus the display on a specific flow, or to identify related objects that interact with this flow, click the chart at a point of interest. Ivanti Connect Secure provides highlighting to all flows that pass through the point selected.

Viewing the Users Activity Charts

Ivanti Connect Secure provides charts to represent user activity:

FIGURE 6.45 : Viewing Activity Charts

- **Adaptive Authentications**: a chart of adaptive authentication in the last 24 hours based on Location, Realm, or Reason.

- **Top User Counts**: a chart showing users that accrued the highest number of successful accesses based on Location, Auth Server, Gateway, Device Type or Session.
- **Top Auth Failures**: a chart of authentication failures observed based on the Location, Auth Server, or Gateway.
- **Session Types**: a chart showing number of Imported IF-MAP sessions, Exported IF-MAP sessions and Local sessions.
- **Top 10 Non-Compliant Host Checker Policies**: a chart showing the top 10 host checker policies that recorded the highest number of non-compliances.
- **Top User Roles**: a chart showing the totals for the number of user roles such as marketing, sales, account, security, store.

Click the **View All** link that provides access to a detailed view showing logs for the corresponding chart.

In the detailed log page:

- Double-click on any log to view additional details of that log in the Info Panel to the right.
- Use the Group by option and select the field type to view the table information in groups. Then click > to view the logs in that group.

FIGURE 6.46 : Group by icon

- Use the Advanced Filter icon to view logs based on the pre-defined filter, operator and value.

Advanced Filtering

In the logs section, click the **Advanced Filter** icon and view logs based on the pre-defined filter, operator and value.

To create a custom filter:

1. Click the **Advanced Filter** icon to open the Advanced Filter window.

FIGURE 6.47 : Advanced Filtering

2. Choose the required column from the **Filter by** list, select an operator, enter a value and click **Add**.
3. Repeat to add more filters if required.

4. Enter a name for the filter and click **Save**. The new filter will be listed in the **Filters** list.

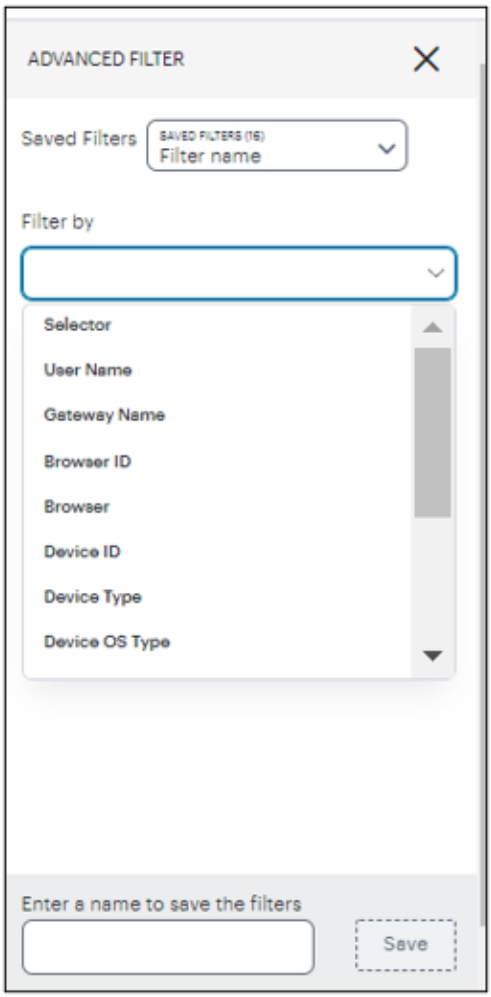


FIGURE 6.48 : Creating Advanced Log Filter

5. To load a previously-saved filter, select your filter from the **Saved Filters** drop-down list and click **Apply**.

   When you apply a filter, the filter information is retained in the new session/login.

6. You can individually remove filters that are applied on the table or you can use the **Reset Filter** icon to clear all the filters applied on the table.
7. To delete one or more previously-saved filters, select the filters from the **Saved Filters** drop-down list and click **Delete**.

Reviewing Application Usage

Applications are defined primarily by the URI you use to access them, and can be fully *defined* (for example, a complete URI denoting a specific application at a location).

Ivanti Connect Secure provides views for your application usage metrics for all defined applications in your Ivanti Connect Secure deployment..

To view application usage:

1. Log in to the Ivanti Neurons for Secure Access Admin portal as a Tenant Admin, and select Ivanti Connect Secure from the Gateway Switcher. See *Logging in to Ivanti Neurons for Secure Access* (page 5).

   The *Network Overview* page appears.

2. From the Ivanti Connect Secure menu, click the **Insights** icon, then select **Applications**.

   The *Applications Overview* page appears, showing the selected metrics.

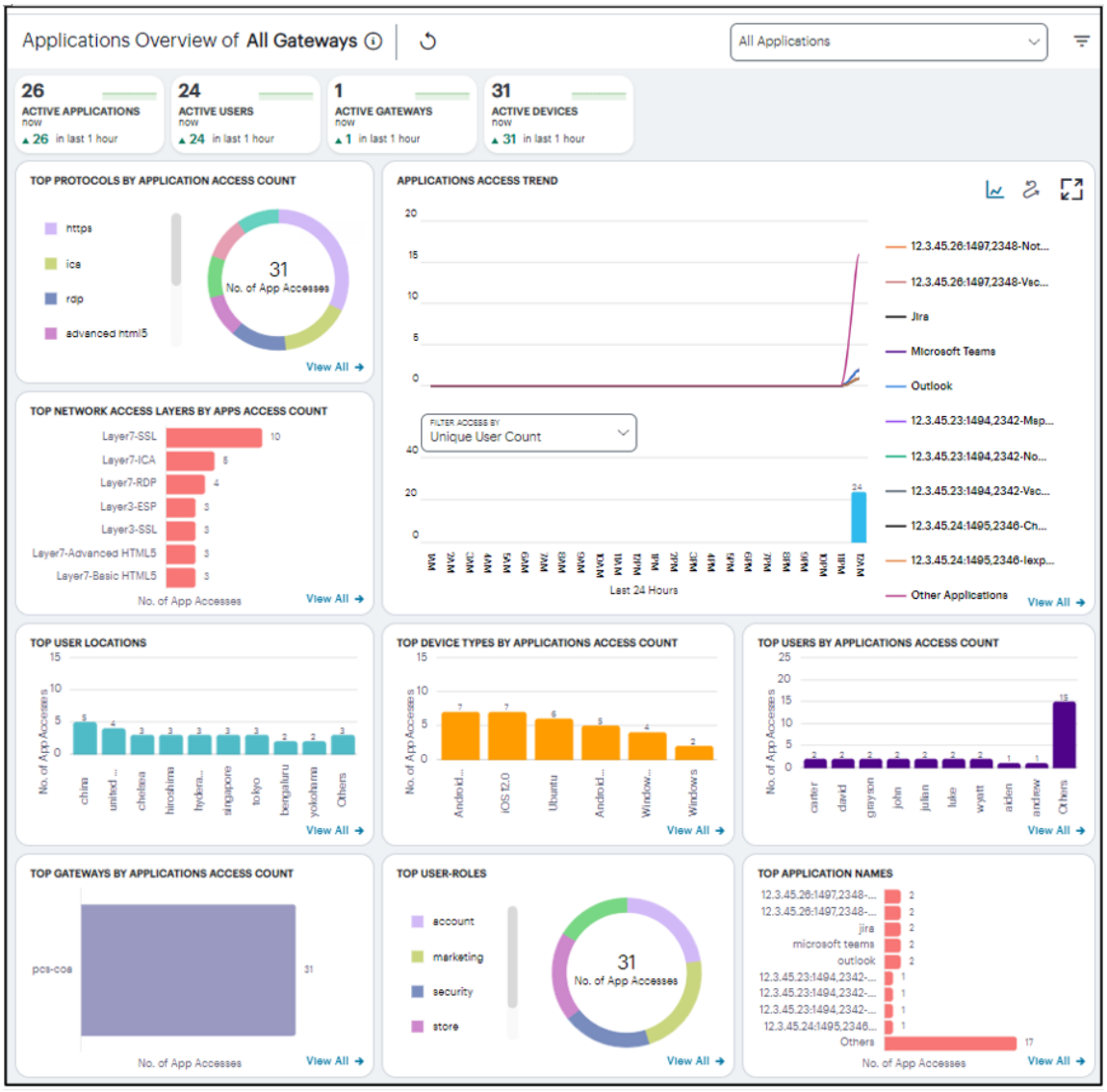


FIGURE 6.49 : Viewing usage charts and graphs for your applications

Understanding the Display

The Applications page contains the following components:

- **Filter bar**, allowing the selection of Ivanti Connect Secure Gateway. For details, see *Using the Filter Bar* (page 68).
- **Summary ribbon**, showing details of the selected gateway. For more details, see *Using the Applications Summary Ribbon* (page 69).
- **Top Protocols by Application Access Count**, showing number of top protocols that attracted the greatest number of application accesses. For more details, see *Viewing Top Protocols by Application Access* (page 69).
- **Applications Access Trend**, showing applications accesses trends that occurred over a period. For more details, see *Viewing Applications Access Trend* (page 70).

- **Activity charts**, showing application access details of *Top Network Access Layers*, *Top User Locations*, *Top Device Types*, *Top Users*, *Top Gateways*, *Top User Roles*, and *Top Application Names*. For more details, see *Viewing the Activity Charts* (page 73).

Each chart on this page includes a **View All** link. This link provides access to a detail view showing logs for the corresponding chart. For example:

Using the Filter Bar

Ivanti Connect Secure uses the top part of the display on all **Insights** data analysis pages to show the current page title, the default time period, and options to:

- Manually refresh the data
- Set a filter for a specific Ivanti Connect Secure Gateway
- Select Layer 3 and Layer 7 Applications

By default, analytics data on this page and others is shown for the last hour or current day. To manually refresh the data, click the circular arrow:

FIGURE 6.50 : Refreshing the data

Ivanti Connect Secure provides the ability to show focused metrics for a specific Ivanti Connect Secure Gateway. To select a specific gateway, use the filter icon:

FIGURE 6.51 : The Filter icon

In the Filter panel, from the drop-down list select the required gateway and click **Apply**.

To clear the selection, click **Clear All**.

Ivanti Connect Secure provides the ability to show focused metrics for Layer 3 and Layer 7 applications. By default, data on this page shows for **All Applications**. Select the required application access from the list to view the corresponding charts and trends in the Applications page. Within Layer 3 Applications, you can choose ESP or SSL applications.

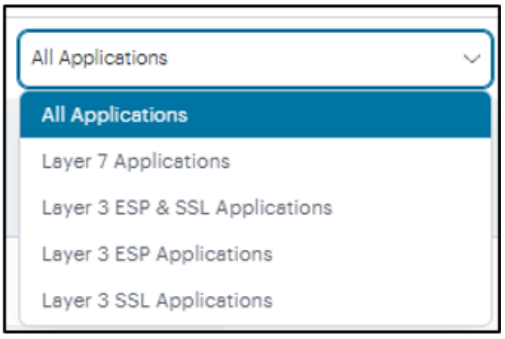


FIGURE 6.52 : The Layer 3 and Layer 7 Applications Selection

Using the Applications Summary Ribbon

The Summary ribbon provides the following metrics:

- **Active Applications**: The total number of active applications defined on the Ivanti Connect Secure.
- **Active Users**: The number of active users.
- **Active Gateways**: The number of active Gateways.
- **Active Devices**: The number of active devices.

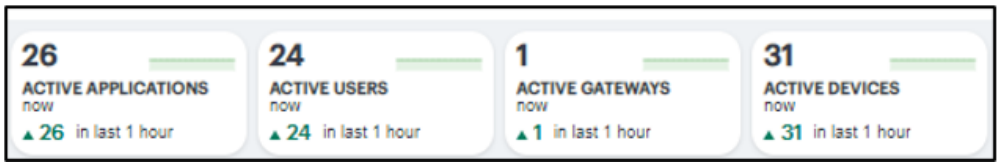


FIGURE 6.53 : Viewing Summary Ribbon

Viewing Top Protocols by Application Access

The **Top Protocols by Application Access Count** radar chart shows the top protocols that attracted the greatest number of application accesses during the period (for example, Web, RDP, SSH or Bookmark).

Hover your pointer over each bar to display a tooltip of the protocol type and number of accesses recorded.

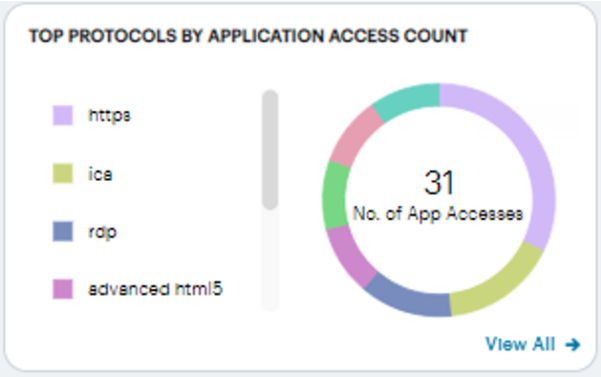


FIGURE 6.54 : Viewing Top Protocols by Application Access

To view a detailed list of events that contributed to the totals, click **View all**.

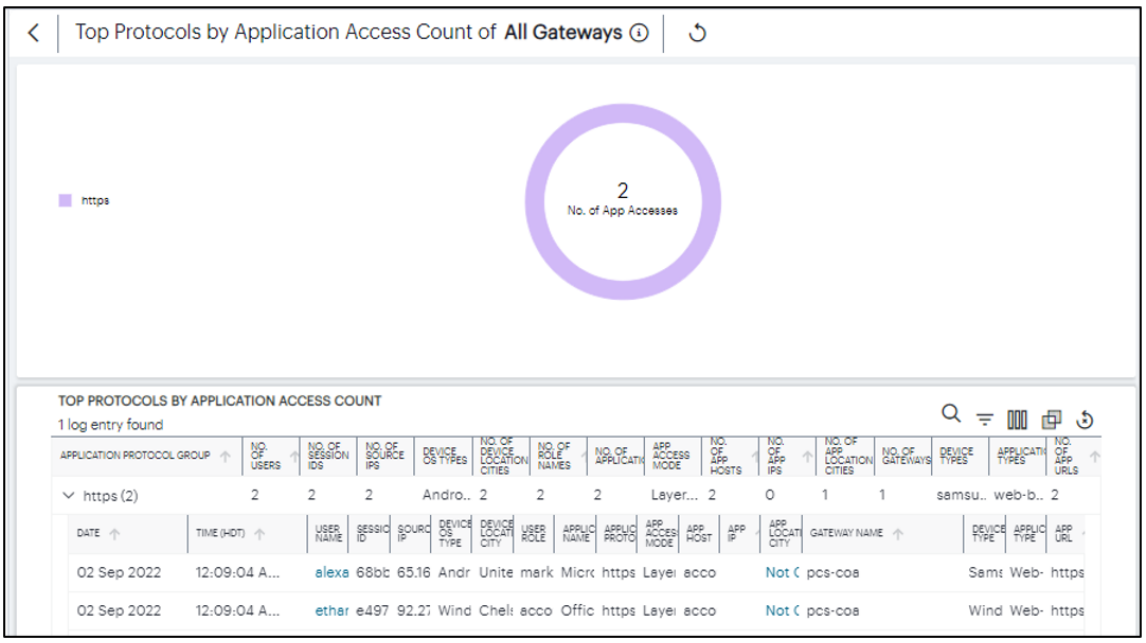


FIGURE 6.55 : Viewing Top Protocols by Application Access Detailed View

Viewing Applications Access Trend

The **Applications Access Trend** panel shows application access trends that occurred during the period. Choose to display this information through line and bar charts, or in a Sankey chart.

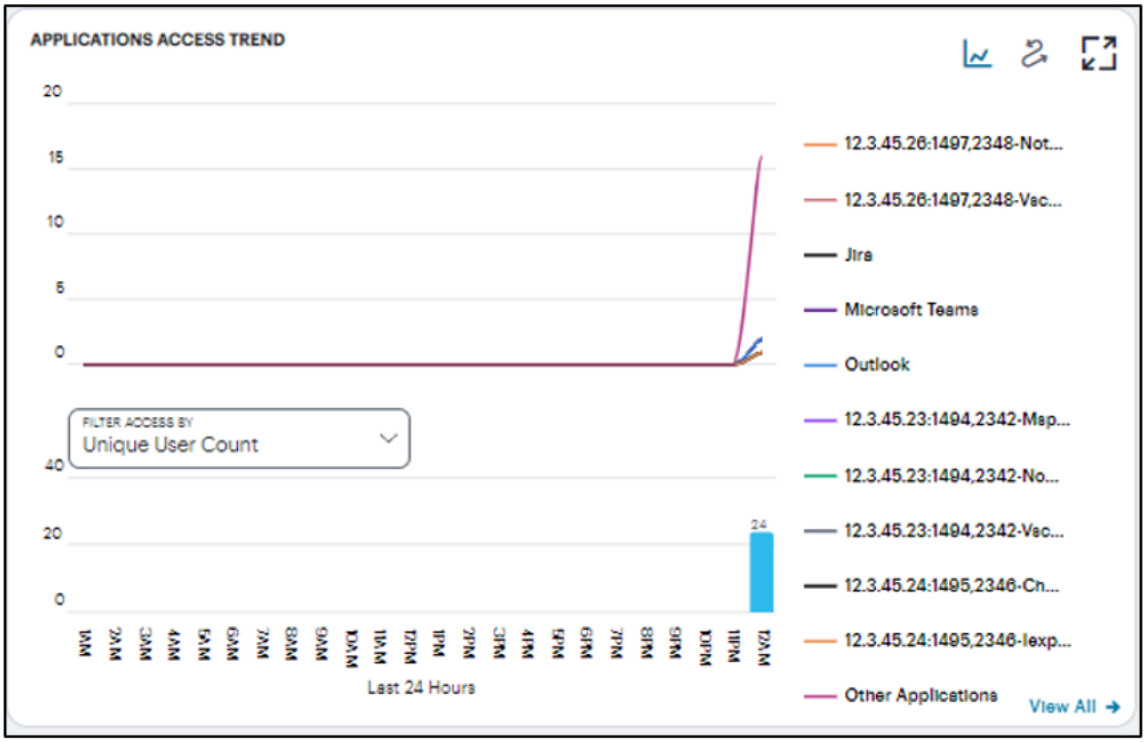


FIGURE 6.56 : Viewing Web Bookmark Access Trend

Use the toggle icon at the top-right to select the required view. Also at the top-right, use the full-screen icon to toggle the current view between normal and full screen.

- In line/bar chart view:

  The display is split into two charts:

  - A line chart showing the number of accesses for the top-10 applications during each hourly period of the day
  - A bar chart showing one of four data types, selected using the **Filter Access By** drop-down control:
    - **Unique User Count**: Shows a count of unique user activity identified during each hourly period.
    - **Unique Device Type Count**: Shows a count of unique device types identified during each hourly period.
    - **Unique Location Count**: Shows a count of activity from unique user locations identified during each hourly period.
    - **Unique User Group Count**: Shows a count of activity from unique user groups identified during each hourly period.

  In this chart, you can:

  - Hover your pointer over each hourly interval to view a tooltip showing the corresponding data totals.
  - Click and drag a select box across a shorter time period to zoom in on a narrower time window. To return to the full 24 hour period, click the *zoom*

out icon.

- Click the corresponding line in the graph to view only the data for that specific user group.

Using the Sankey Chart View

The Sankey chart provides an alternate visualization of application access activity, showing directed flow between related objects. The width of each stream in the flow is proportional to the utilization of the object the flow passes through, allowing an administrator to view significant usage and relationships across your user groups and application infrastructure.

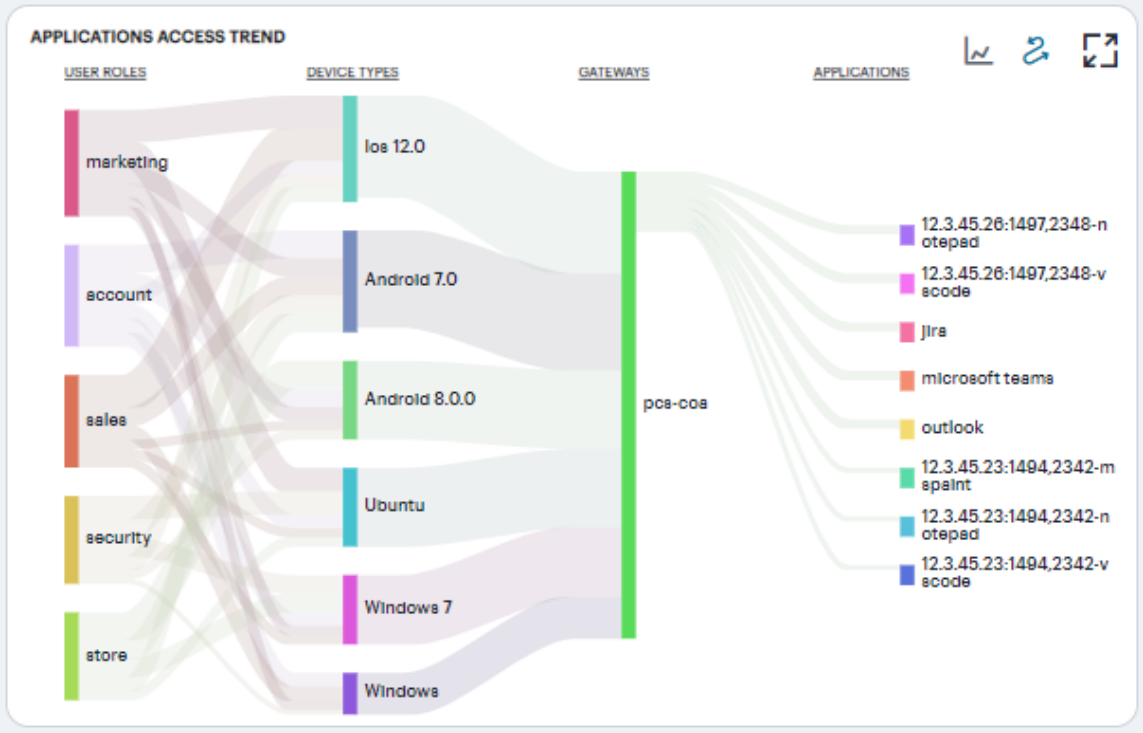


FIGURE 6.57 : Viewing Applications Access Trend

Hover your pointer over a flow of interest to display a tooltip confirming the scale of the activity between the two objects connected by the flow.

To focus the display on a specific flow, or to identify related objects that interact with this flow, click the chart at a point of interest. Ivanti Connect Secure provides highlighting to all flows that pass through the point selected.

Viewing the Activity Charts

The **Activity Charts** on this page represent top application access totals in the following categories:

- **Top Network Access Layers by Apps Access Count**: a bar chart showing the count of Layer 3 and Layer 7 applications accesses.
- **Top User Locations**: a bar chart showing the count of application accesses made from various user locations.
- **Top Device Types by Applications Access Count**: a bar chart showing a count of number of applications accesses made from various devices.
- **Top Users by Applications Access Count**: a bar chart showing a count of number of applications accesses made by the users.
- **Top Gateways by Applications Access Count**: a bar chart showing a count of number of applications accesses made from Gateways.
- **Top User Roles**: a bar chart showing the count of application accesses made by various user roles (example: Marketing, Sales, Accounts, Security).
- **Top Application Names**: a bar chart showing the count of application accesses made to various applications (example: Microsoft Teams, Outlook).

Hover your pointer over a particular element to view a tooltip showing the label and total.

Use the Filter to view active access count by Gateway, Device Type, User Name, User Role, or User Location City.

Click the **View All** link that provides access to a detailed view showing logs for the corresponding chart.

In the detailed log page:

- Double-click on any log to view additional details of that log in the Info Panel to the right.

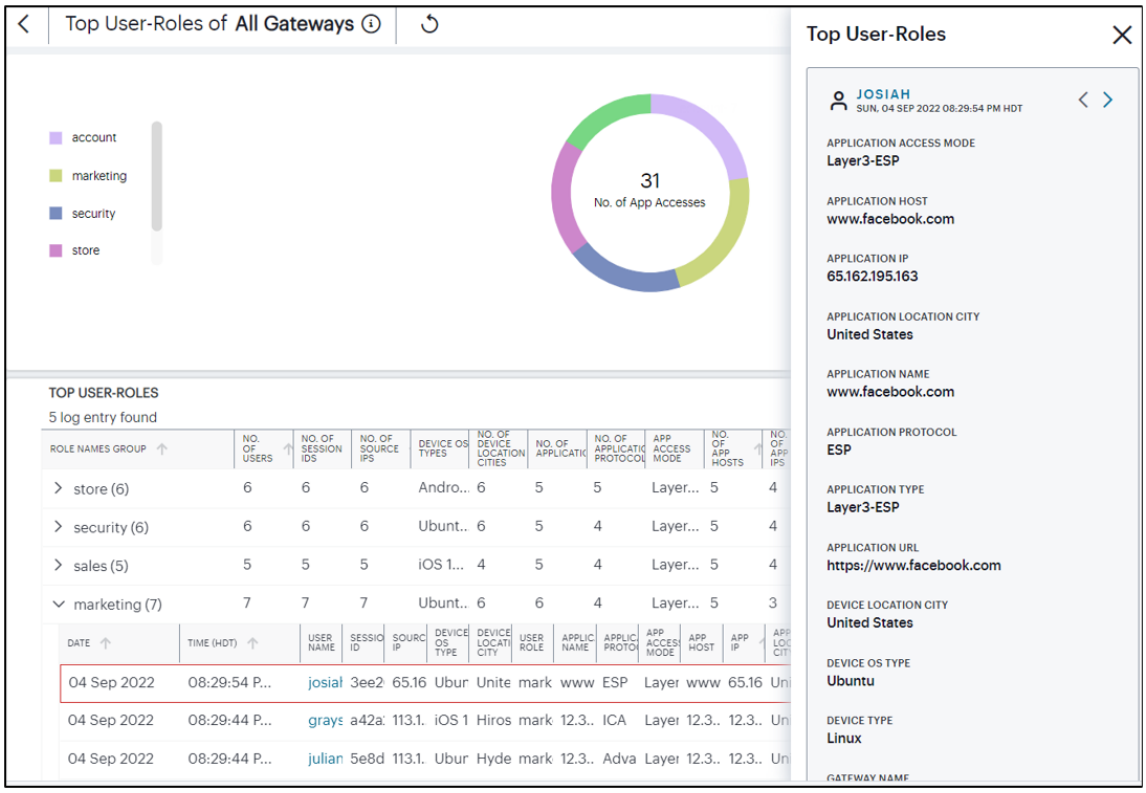


FIGURE 6.58 : Viewing details in Info Panel

- Double-click on any log to view additional details of that log in the Info Panel to the right.
- Use the Group by option and select the field type to view the table information in groups. Then click > to view the logs in that group.

FIGURE 6.59 : Group by icon

- Use the Advanced Filter icon to view logs based on the pre-defined filter, operator and value.

Advanced Filtering

In the logs section, click the **Advanced Filter** icon and view logs based on the pre-defined filter, operator and value.

To create a custom filter:

1. Click the **Advanced Filter** icon to open the Advanced Filter window.

FIGURE 6.60 : Advanced Filtering

2. Choose the required column from the **Filter by** list, select an operator, enter a value and click **Add**.
3. Repeat to add more filters if required.
4. Enter a name for the filter and click **Save**. The new filter will be listed in the **Filters** list.

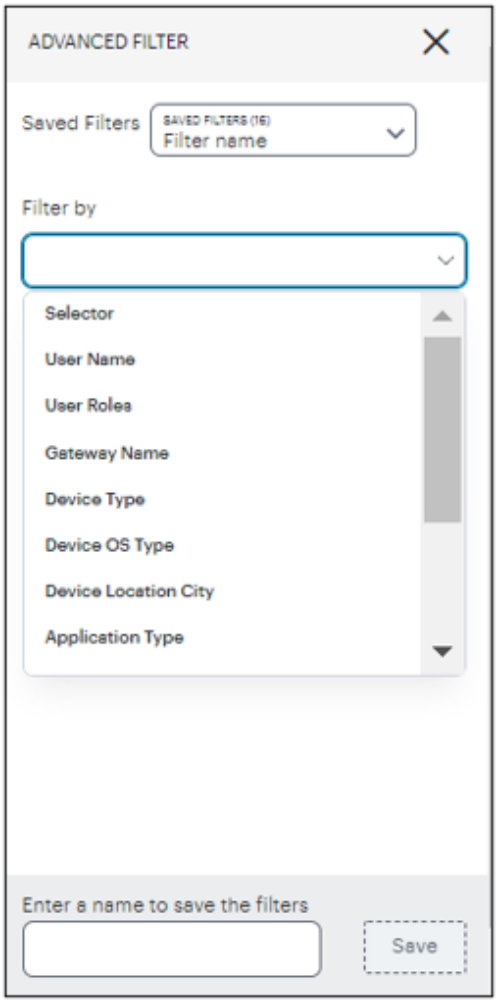


FIGURE 6.61 : Creating Advanced Log Filter

5. To load a previously-saved filter, select your filter from the **Saved Filters** drop-down list and click **Apply**.

   When you apply a filter, the filter information is retained in the new session/login.

6. You can individually remove filters that are applied on the table or you can use the **Reset Filter** icon to clear all the filters applied on the table.

7. To delete one or more previously-saved filters, select the filters from the **Saved Filters** drop-down list and click **Delete**.

Configuring nZTA Policy to an ICS Application

Administrators can now configure ICS application with nZTA Secure Access Policy from the nSA-ICS Applications page. This feature requires nZTA license. The Secure Access Policy defines how end users can connect to nSA to access applications.

A Configure button is provided in the ICS Applications page to configure nZTA Secure Access Policy to an ICS application.

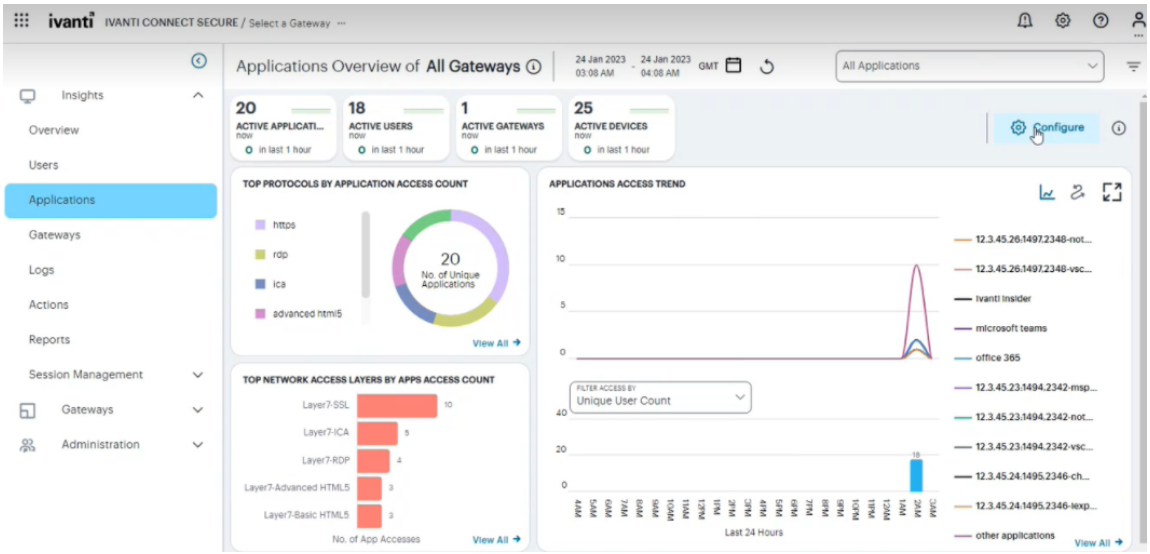


FIGURE 6.62 : Applications page with Configure option (nZTA license enabled)

To configure nZTA policy to the ICS application:

1. In the ICS applications page, click **Configure**.

   The *Configure Applications* page is displayed showing a list of accessed applications behind the ICS gateway.

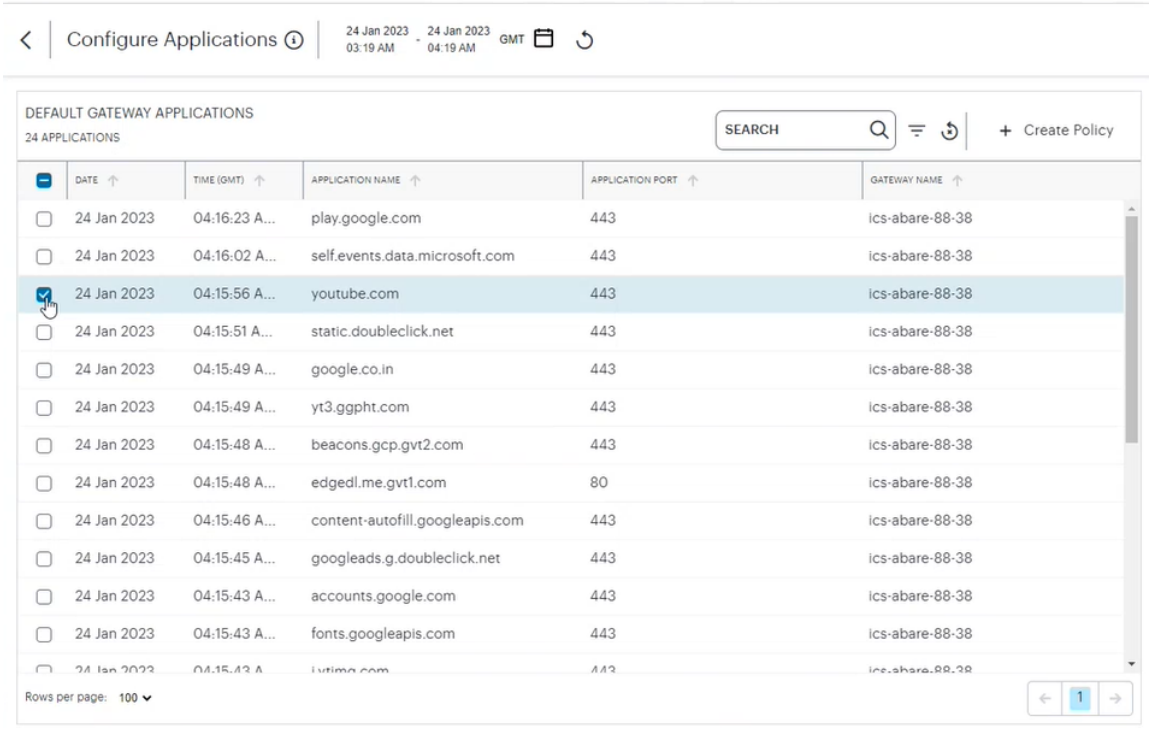


FIGURE 6.63 : Configure ICS applications

2. In the search box provided, start typing the application name. ICS auto-completes any matching application name.
3. Select an application from the list and click **Create Policy** to create a nZTA Policy.

   The nZTA Create Secure Access Policy page is displayed. The Application Name, Application Detail and Description fields are pre-filled in the page.

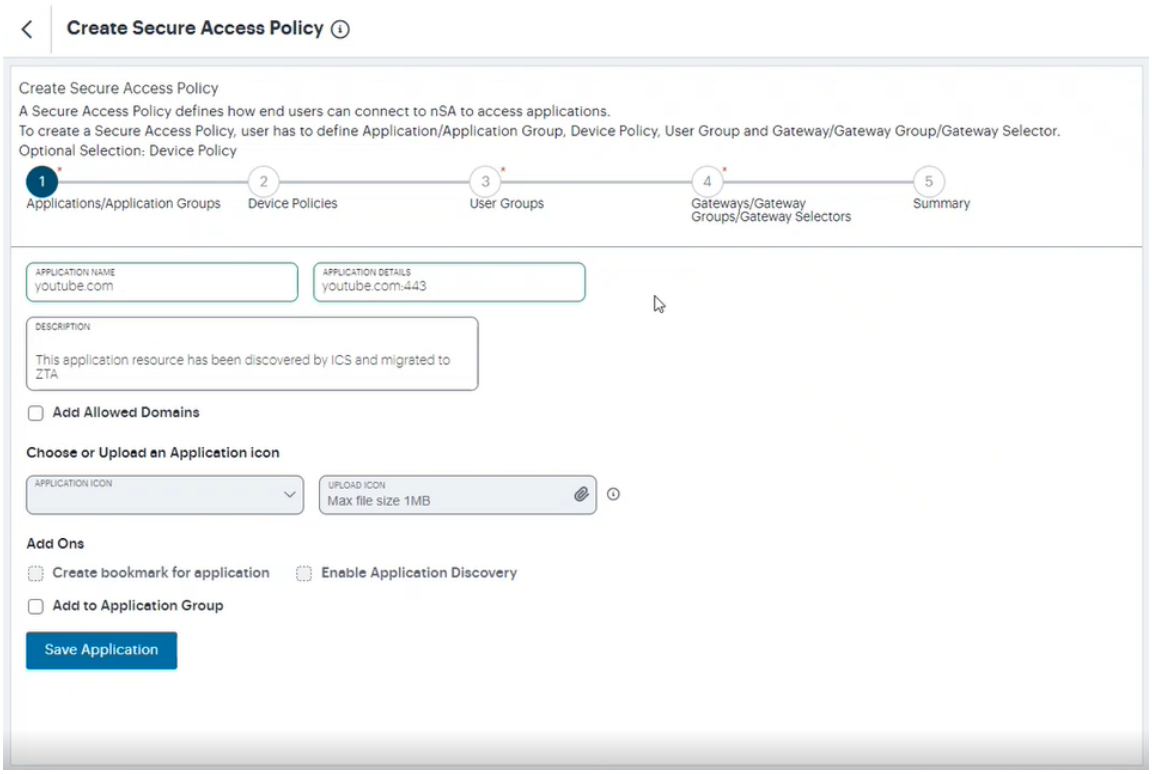


FIGURE 6.64 : Create nZTA policy

4. Click **Save Application** and then click **Next**.
5. Define Device Policy, User Group and Gateway/Gateway Group/Gateway Selector. For details, see the section Creating a Secure Access Policy (https://help.ivanti.com/ps/help/en_US/nSA/22.x/pzta-docs-latest/pzta-aguide/html/tadmin_se

Reviewing Individual User Activity

This page shows activity relating to a specific user in your Ivanti Connect Secure deployment.

To access the User Overview page:

1. Log in to the Ivanti Neurons for Secure Access Admin portal as a Tenant Admin, and select **Ivanti Connect Secure** from the Gateway Switcher. See *Logging in to Ivanti Neurons for Secure Access* (page 5).

   The Network Overview page appears by default.
2. Launch the User Overview page by doing one of the following:
   - In the **Search** field on Filter bar, type the username for which you want to see the activities.
   - In the Summary ribbon, click **Active Users**. In the Active Users panel displayed, click the username link for which you want to see the activities.

- Click the **View All** link in any of the charts. In the logs table displayed, click the username link for which you want to see the activities.

The User Overview page is displayed.

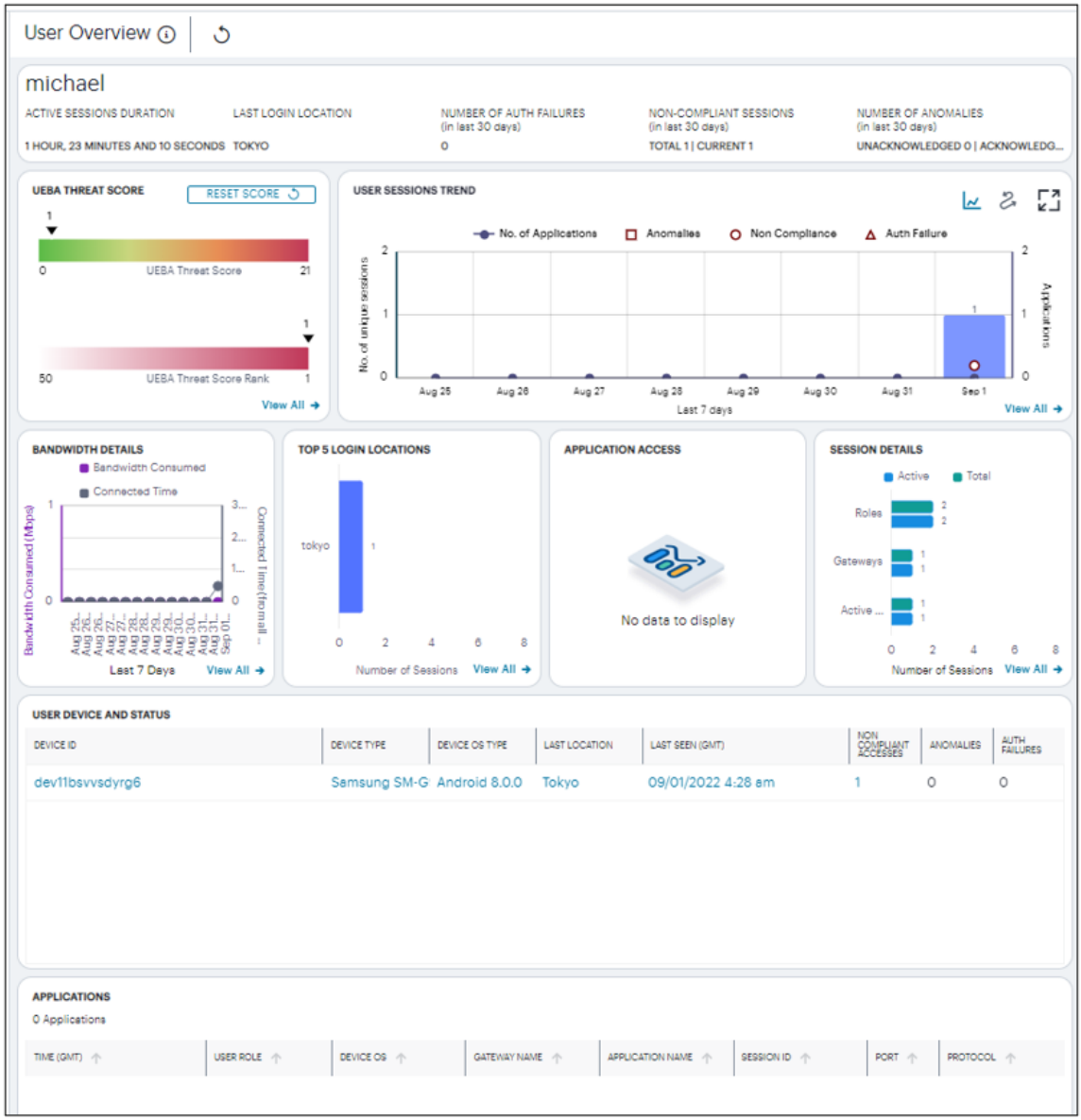


FIGURE 6.65 : Viewing User Activity

The page has the following areas:

- The Filter bar
- The Summary ribbon
- UEBA Threat Score and UEBA Threat Score Rank
- User Sessions trend
- Activity charts, showing charts for Bandwidth details, Last 5 Login Locations, Application Access and Session Details

- Table showing User Device and Status

Each chart on this page includes a View All link. This link provides access to a detail view showing logs for the corresponding chart.

Using the Filter Bar

The top part of the page has the option to manually refresh the data.

Viewing the User Summary Ribbon

The Summary ribbon provides the following metrics:

- **Active Sessions Duration** – All active sessions duration combined of the user, displayed in hours, minutes, and seconds.
- **Last Login Location** – The location from where the user has last logged in.
- **Number of Auth Failures** – The number of authentication failures for this user in the last 30 days.
- **Number of Non-Compliant Sessions** – The number of Non-compliant sessions (full/partial non-compliant) for this user across all gateways in the last 30 days.
- **Number of Anomalies** – The number of anomalies (acknowledged and unacknowledged) detected by Ivanti Connect Secure in the last 30 days.

FIGURE 6.66 : Viewing User Summary Ribbon

Viewing the UEBA Threat Score

The UEBA Threat Score panel contains:

- **UEBA Threat Score** – It is the cumulative value of number of anomalies and number of non-compliant sessions of this user. Click the **View All** link to see the log details in a table.
- **UEBA Threat Score Rank** – It is the UEBA Threat score position of this user based on the UEBA Threat scores of all the users in the tenant.
- **Reset Score** – As an administrator, you can reset the UEBA Threat score of this user.

Note: A user's UEBA Threat score is calculated from a combination of geographic anomalies, non-compliance with device policies, and activity deviations.

Viewing the User Session Trend

This section shows the following user activities per day that occurred during the last seven days. You can hover over the trend to view details.

- Number of unique Active Sessions
- Number of Applications accessed
- Number of Anomalies
- Number of Non-Compliance sessions
- Number of Auth Failures

Viewing the User Activity Charts

This Ivanti Connect Secure provides charts to represent user activity:

- **Bandwidth Details** – shows the Bandwidth Consumed per day and Total Time connected per day by the user for the last seven days.
- **Last 5 Login Locations** – shows the last top five Login Locations accessed by the user in the last 30 days.
- **Application Access** – shows the number of Applications accessed by the user in the active sessions and in the last 30 days based on Bookmark, VDI and HTML5 access.
- **Session Details** – shows the number of Active Sessions and Total number of sessions in the last 30 days based on Role, Gateways and Active sessions

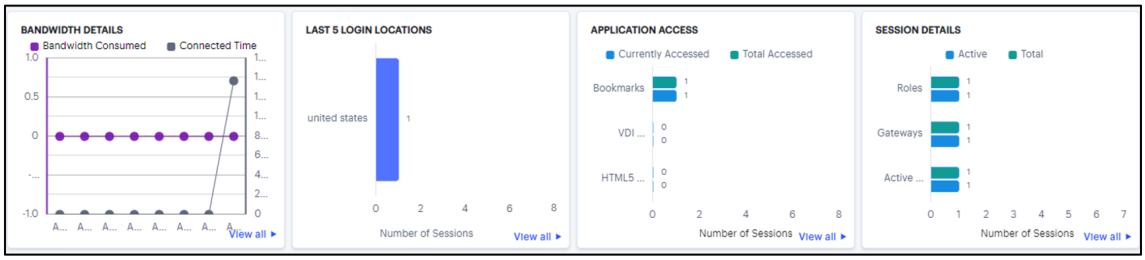


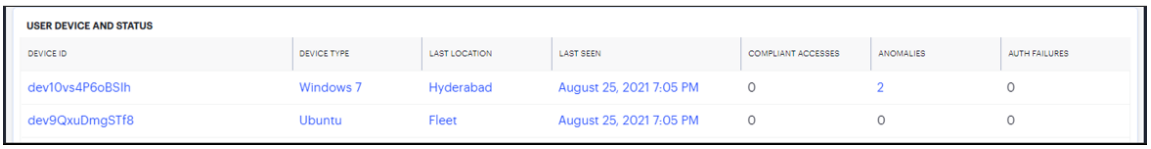
FIGURE 6.67 : Viewing User Activity Charts

Click the **View All** link that provides access to a detailed view showing logs for the corresponding chart.

Viewing the User Device and Status

This table provides the status of the devices used by the user for connecting to VPN in the last 30 days. Each row in the table includes Device ID and Device Type of a device among other user session details.

Click the link in each column to drill-down for additional details.



USER DEVICE AND STATUS

DEVICE ID	DEVICE TYPE	LAST LOCATION	LAST SEEN	COMPLIANT ACCESSES	ANOMALIES	AUTH FAILURES
dev10vs4P6oBSIh	Windows 7	Hyderabad	August 25, 2021 7:05 PM	0	2	0
dev9QxuDmgSTf8	Ubuntu	Fleet	August 25, 2021 7:05 PM	0	0	0

FIGURE 6.68 : Viewing User Device and Status

Reviewing Gateways Status and Versions

The Gateway Overview page gives an overall detail of all the gateways that are registered in the tenant.

To access the Gateway Overview page:

1. Log in to the Ivanti Neurons for Secure Access Admin portal as a Tenant Admin, and select Ivanti Connect Secure from the Gateway Switcher. See *Logging in to Ivanti Neurons for Secure Access* (page 5).
2. From the Ivanti Connect Secure menu, click the **Insights** icon, then select **Gateways**.

   The *Gateway Overview* page appears.

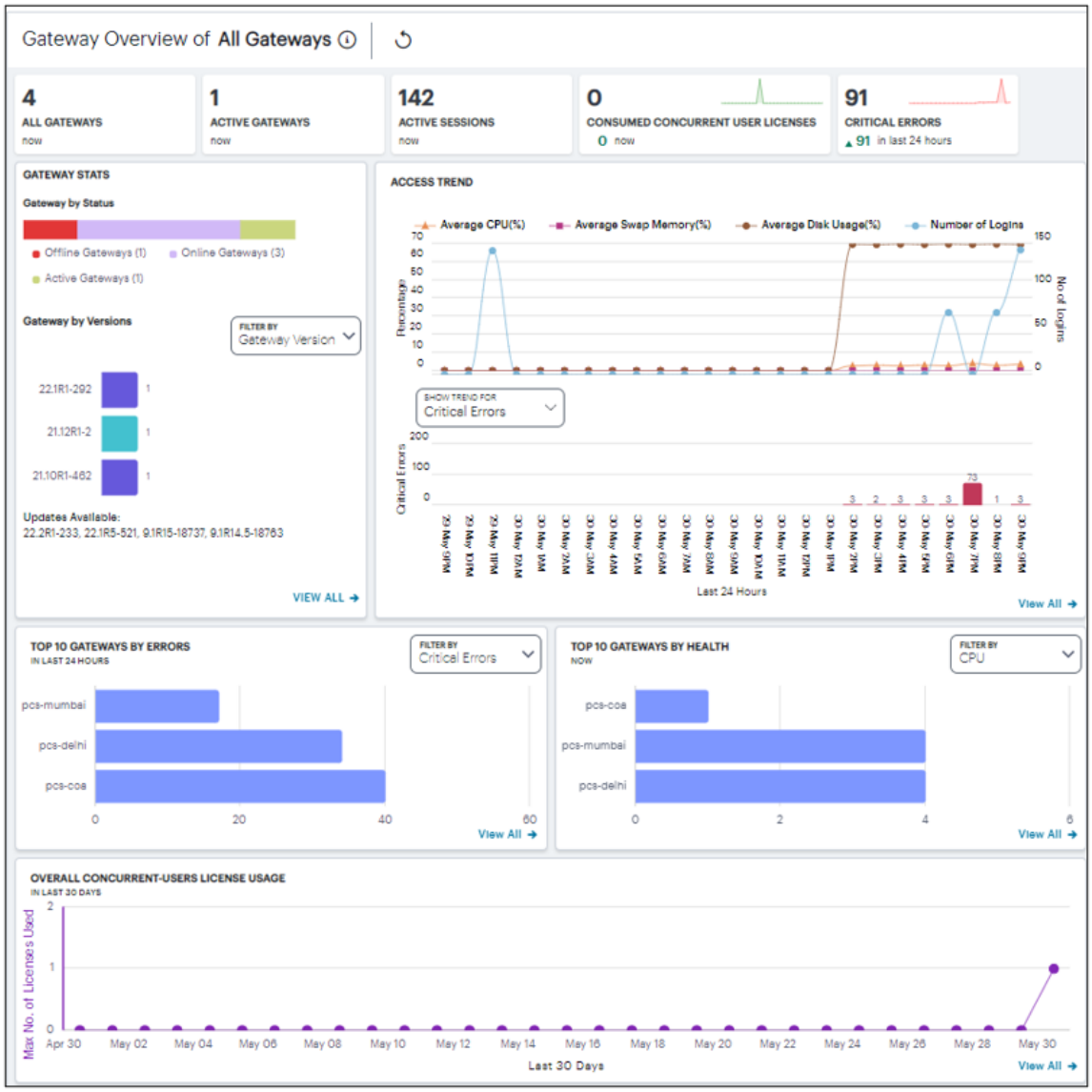


FIGURE 6.69 : Gateway Overview

Understanding the Display

The Gateway Overview page contains the following components:

- Summary ribbon
- Gateway Status and Versions
- Access Trend View
- Top 10 Gateways by Errors
- Top 10 Gateways by Health
- Overall Concurrent Users License Usage

Use the Filter bar, located on the top-right-corner of the page, that allows the selection of any individual Ivanti Connect Secure Gateway.

Each chart on this page includes a **View All** link. This link provides access to a detail view showing logs for the corresponding chart.

Viewing the Gateways Summary Ribbon

The Gateway Overview Summary panel gives the following details:

- **All Gateways**: Shows the total number of Ivanti Connect Secure Gateways that are registered with the tenant.
- **Active Gateways**: The total number of active gateways within the tenant.
- **Active Sessions**: The total number of active sessions across all the connected gateways within the tenant.
- **Consumed Concurrent User Licenses**: The total number of concurrent user licenses consumed across all the gateways.
- **Critical Errors**: The total number of critical errors in the last 24 hours across all the gateways. The trend shows the critical error occurrence in the last 24 hours. It also shows the number of errors increased or decreased in the last 24 hours.

Viewing the Gateways Status and Versions

The Gateways by status chart shows the distribution of gateways by their status:

- **Offline Gateways**: All gateways that are registered with the tenant, but not connected.
- **Online Gateways**: All gateways that are registered with the tenant and connected but are not running any sessions.
- **Active Gateways**: All gateways that have at least one active session.

The Gateway by versions chart shows the distribution of latest 10 gateway versions across all the gateways within the tenant. The Gateways by ESAP version chart shows the distribution of latest 10 ESAP versions across all the gateways within the tenant.

To view a detailed list of events that contributed to the totals, click **View All**.

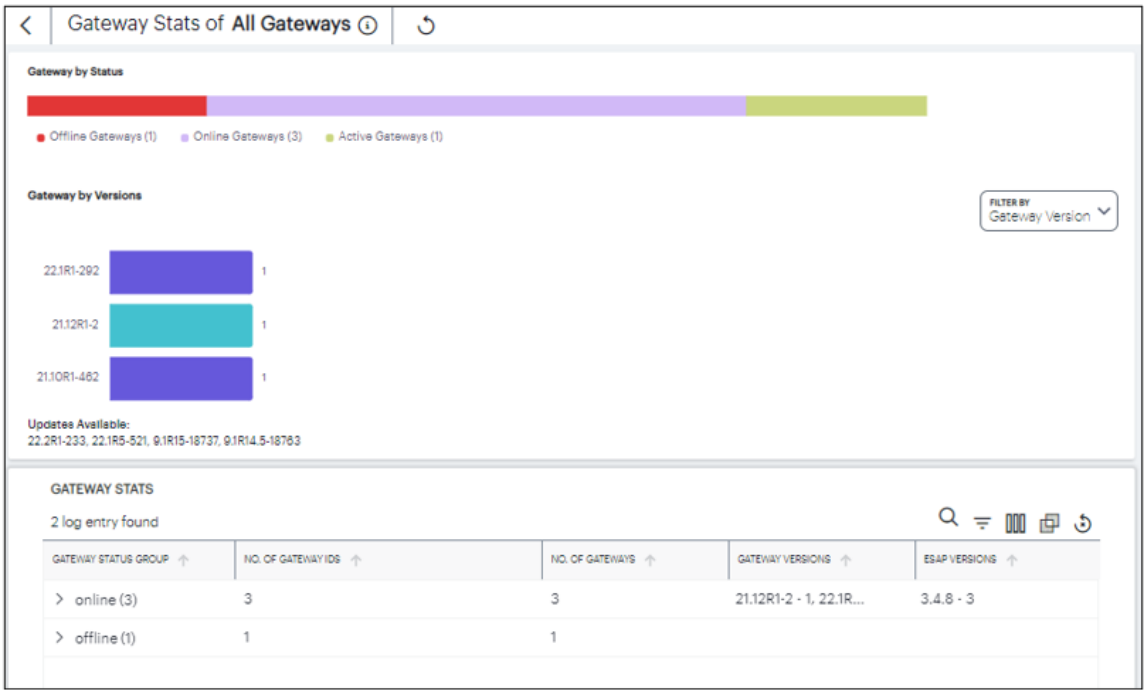


FIGURE 6.70 : Gateway Status and Versions

Viewing the Gateways Access Trend

Ivanti Connect Secure uses the Gateways Access Trend section to show:

- the hourly distribution of the number of logins, average CPU usage, average memory usage, average disk usage, average network throughput across all the gateways during the last 24 hours.
- the hourly distribution of critical errors across all the gateways during the last 24 hours.

You can check the trend for **Critical Errors** and **Throughput (MB)**.

To view a detailed list of events that contributed to the totals, click **View All**.

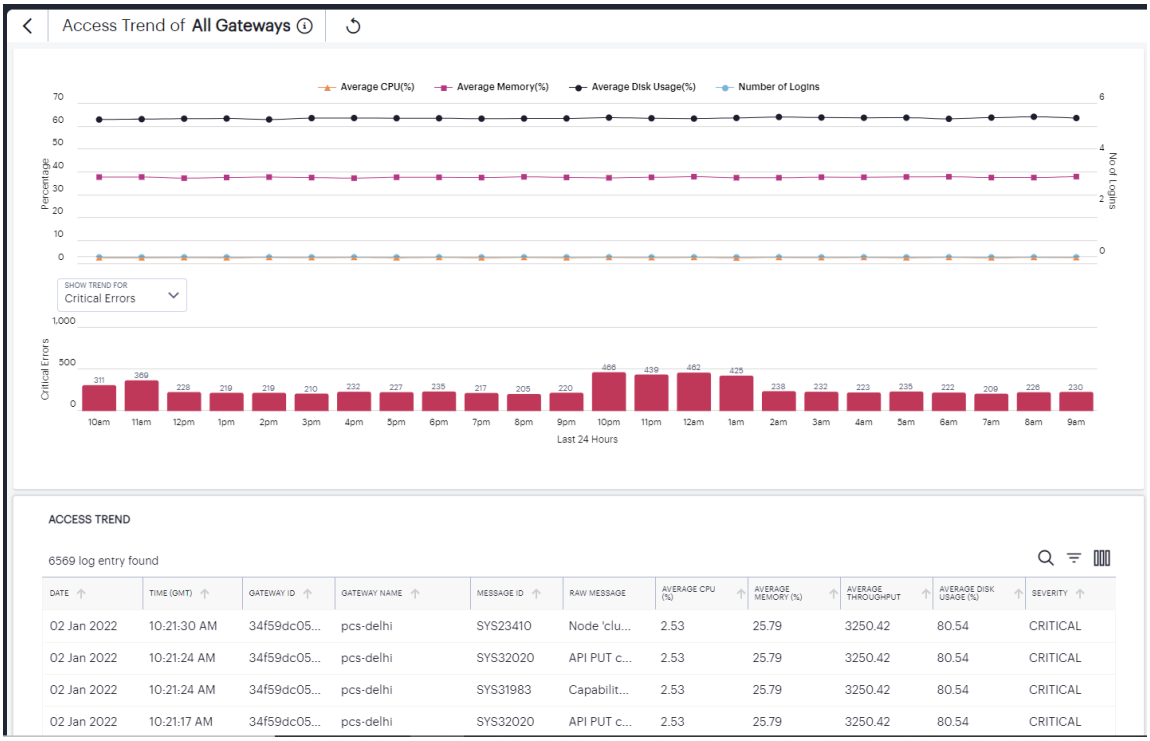


FIGURE 6.71 : Gateways Access Trend

Viewing the Top Gateway Activity Charts

Ivanti Connect Secure provides charts to show breakdown of Top 10 Gateways by Errors and Top 10 Gateways by Health.

The Gateways by Errors chart provides the total number of Critical Errors or Integrity Check Violations across top 10 gateways over the last 24 hours. Use the Filter drop-down to select the option from the list.

To view a detailed list of events that contributed to the totals, click **View All**.

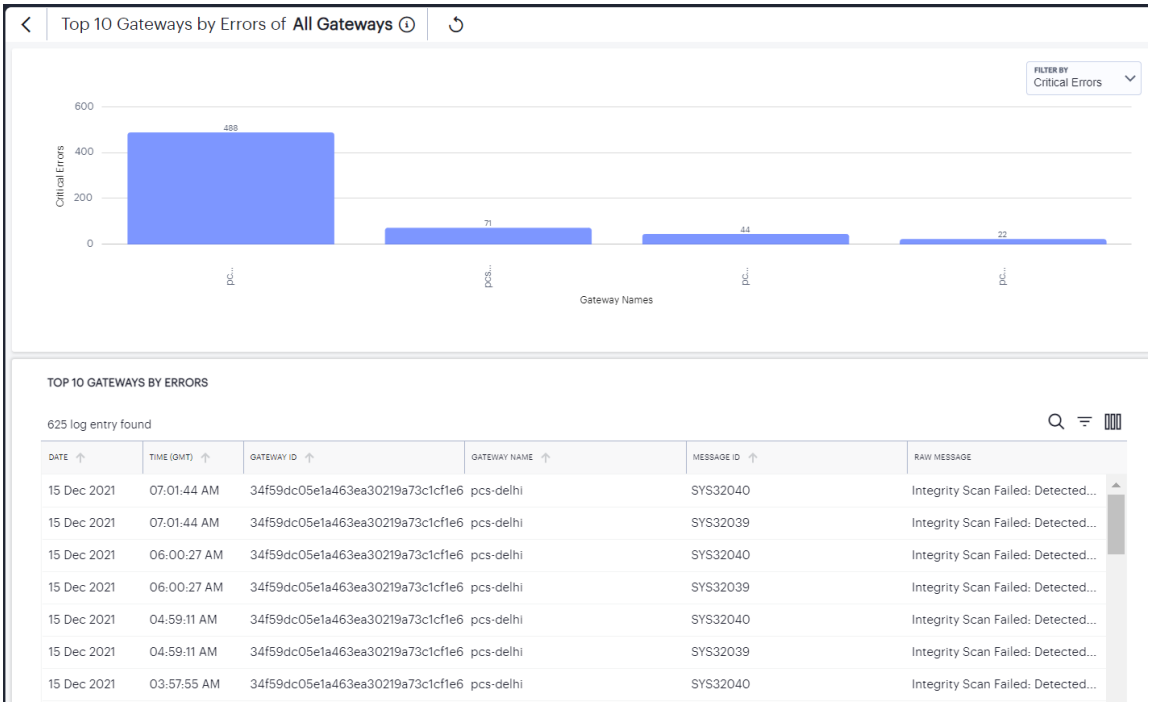


FIGURE 6.72 : Top Ten Gateways by Errors

The Gateways by Health chart shows the top 10 gateways that have high CPU usage, Memory usage, Disk usage, or Network throughput. Use the Filter drop-down to select the option from the list.

To view a detailed list of events that contributed to the totals, click **View All**.

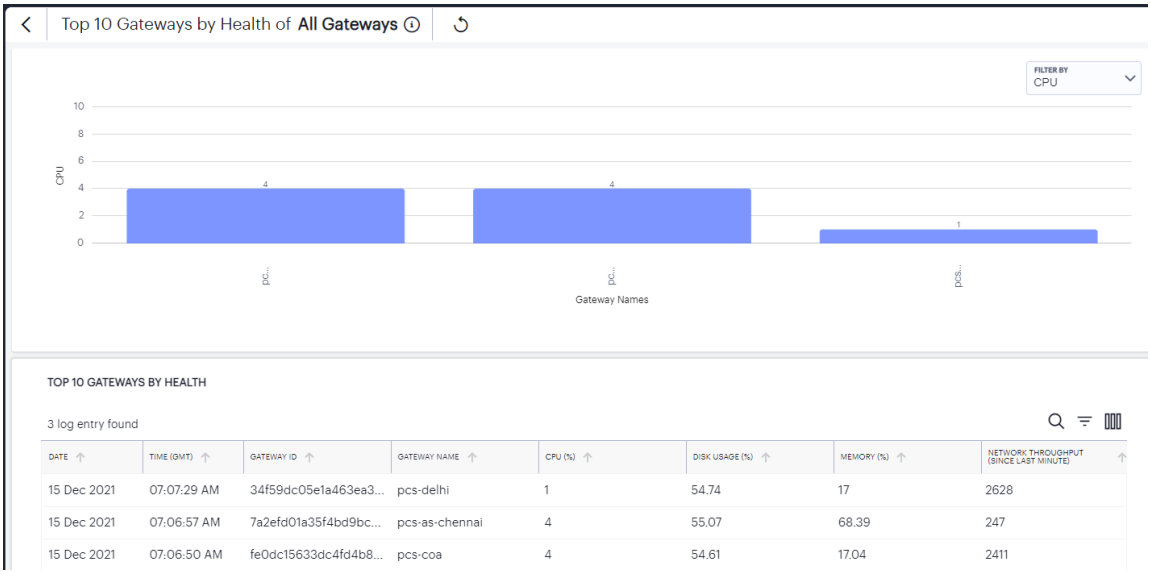


FIGURE 6.73 : Top Ten Gateways by Health

The Overall Concurrent Users License Usage chart provides the maximum licenses used on a daily basis across all the gateways over the last 30 days.

To view a detailed list of events that contributed to the totals, click **View All**.

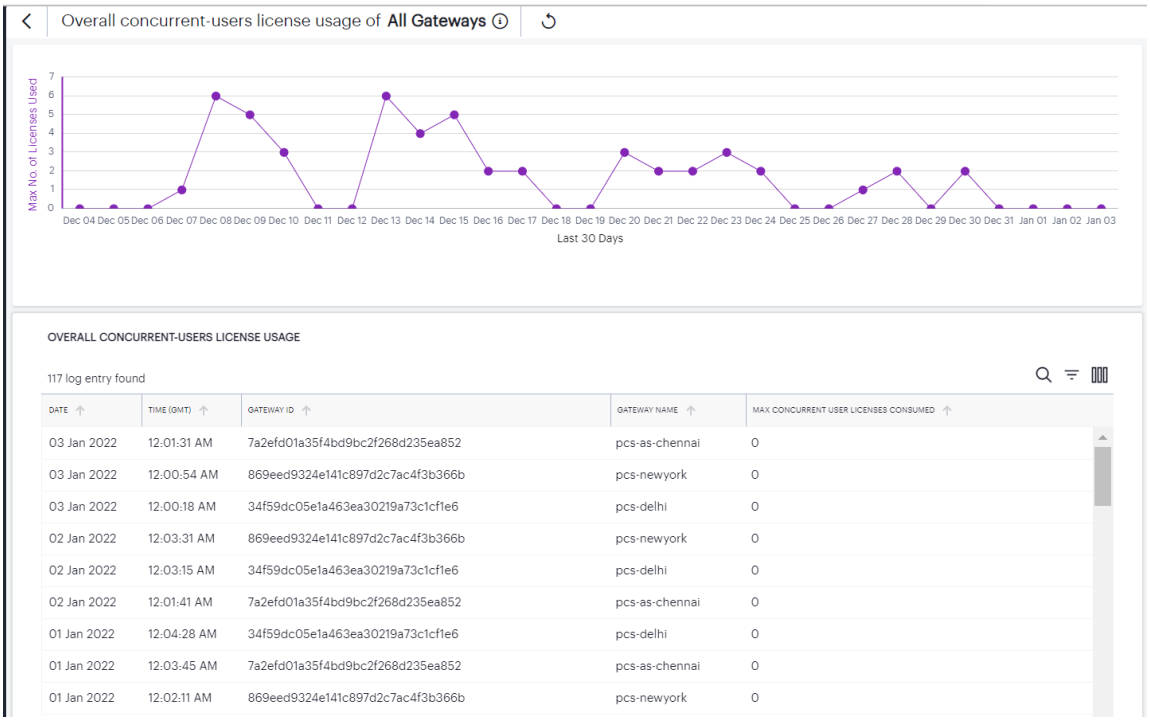


FIGURE 6.74 : Overall Concurrent Users License Usage

Checking the Logs

The Ivanti Connect Secure Logs page displays audit and activity events observed by your Ivanti Connect Secure access infrastructure. These events are reported to the Ivanti Neurons for Secure Access by your Gateways and Authentication, Authorization and Accounting (AAA) service.

To view the Logs page:

1. Log in to the Ivanti Neurons for Secure Access Admin portal as a Tenant Admin, and select Ivanti Connect Secure from the Gateway Switcher. See *Logging in to Ivanti Neurons for Secure Access* (page 5).
2. From the Ivanti Connect Secure menu, click the **Insights** icon, then select **Logs**.

   The *Logs* page appears.

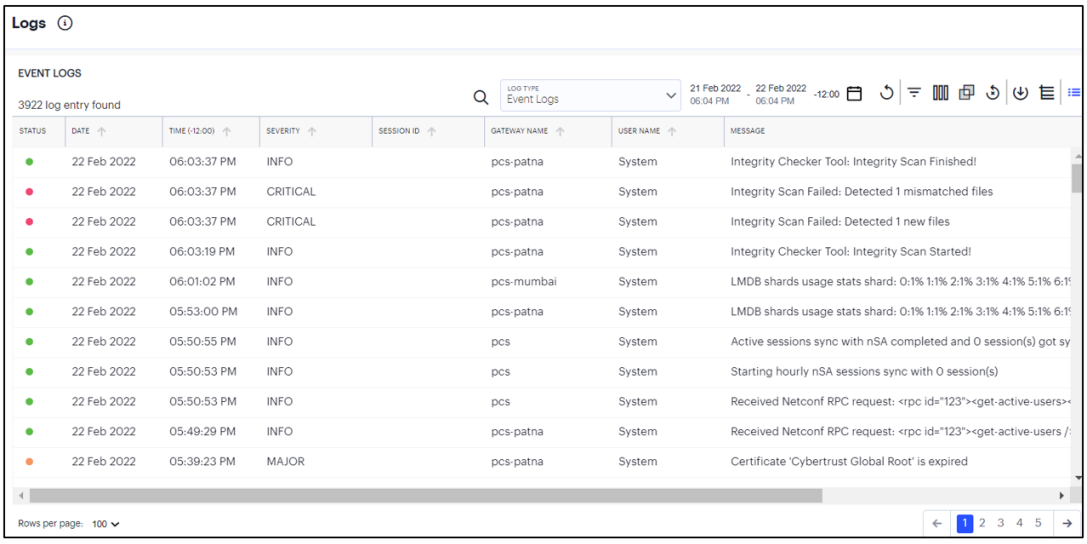


FIGURE 6.75 : Viewing the Logs

This page comprises the following sections:

- Log selection and filtering controls, see *Setting Log Criteria and Filtering the Output* (page 90).
- The log record display, see *Viewing Log Records* (page 92).

Note: Ivanti Connect Secure additionally provides a separate log records page pertaining to activity for specific Gateways.

Setting a Log Time Period

Use the time period selectors at the top of the page to set a time period or time range for your log results.

To switch between **Time Period** and **Time Range**. use the following icon:

FIGURE 6.76 : A choice of time period or time range

The adjacent time selection boxes update according to your choice. For **Time Period**, set the time period you want to view. Choose from:

- Last 60 minutes
- Last 24 hours (default)
- Last 7 days
- Last 1 month

For **Time Range**, set a specific *Date* and *Time* for both the start and end of your time range.

Setting Log Criteria and Filtering the Output

To set the criteria you want to use for viewing log data, use the controls above the main log display. This section also contains functions to highlight search terms, apply filters, and schedule log export jobs.

Select the primary log type you want to display by using the **Log Type** drop-down list:

FIGURE 6.77 : Selecting a log type

Choose from:

- Access Logs
- Admin Logs
- Event Logs

Then, use the icons adjacent to the log selector to further control your log selection. Choose from the following:

- To search for a term in the displayed logs, click the following icon:

FIGURE 6.78 : Search term highlighting

  Ivanti Connect Secure highlights all matches is the log display.

- Logs are refreshed automatically by changing the criteria. To manually refresh the log display, click the following icon:

FIGURE 6.79 : Page refresh

- To change the fields displayed for each log line, click the following icon:

FIGURE 6.80 : Show or hide log fields

In the field selector, click a field name to toggle between show or hide. A *tick* icon indicates a displayed field. After you are finished, click the context menu icon to close the selector. See *Viewing Log Records* (page 92).

- To trigger the advanced filter selection, use the following icon:

FIGURE 6.81 : Advanced Filtering

To learn more, see *Filtering the Logs* (page 94).

- To group the logs based on the fields, use the Group by option and select the field type to view the table information in groups.

FIGURE 6.82 : Group by icon

Click > to view the logs in that group.

FIGURE 6.83 : Group by logs

- To export the displayed log as a CSV or JSON text file, or to set up a new scheduled log export job, click the following icon:

FIGURE 6.84 : Export filtered logs

To learn more about log export jobs, see *Exporting Logs* (page 95).

- To view the status of currently-scheduled log export jobs, click the following icon:

FIGURE 6.85 : View scheduled log export jobs

To learn more about log export jobs, see *Exporting Logs* (page 95).

- To change the view density, click the following icon:

FIGURE 6.86 : Switching between default and dense log record views

Viewing Log Records

The main part of the page shows the log records that match your selected criteria. The number of matching log records is displayed at the top-left.

Each log line includes the following fields:

- A status indicator showing the level of severity associated with each log event. Use the following table for a guide to the meaning of each indicator color:

Severity	Status Color
INFO	Green
MINOR	Amber
MAJOR	Amber
CRITICAL	Red

- The date and time of the event.
- The message ID that identifies this type of event.
- The severity of the event in words.
- The session ID that was the source of the event, where applicable.
- The ID of the Ivanti Connect Secure Gateway that reported the event, where applicable.
- The name of the Ivanti Connect Secure Gateway that reported the event, where applicable.

- The IP address identified as the source of the event.
- The user name associated with the event, where applicable.
- The ID of the device associated with the event, where applicable.
- The message (description) of the event.

Use the page controls at the bottom to select the number of log records/rows per page:

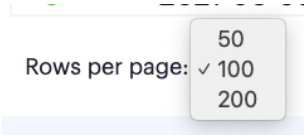


FIGURE 6.87 : Setting the number of log rows per page

Choose from:

- 50
- 100 (default)
- 200

To cycle through the log pages, use the page controls at the bottom-right.

Where a single log message is too long for the display, use your pointing device to scroll the optional fields display to the left or right.

Furthermore, to view a single log entry in a dedicated panel, click the log message text to activate the info-panel view:

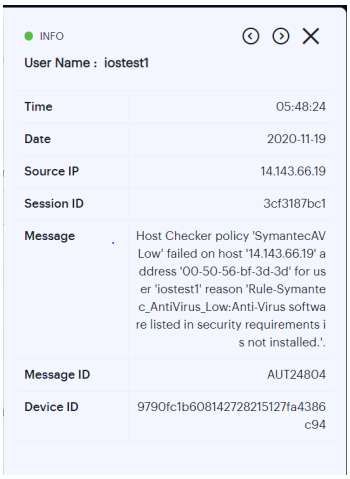


FIGURE 6.88 : Viewing a single log entry in the info-panel

Note: In the info-panel, use the **Previous** and **Next** icons to cycle through each log entry in turn.

Filtering the Logs

The **Logs** page provides an advanced field filter through which you can narrow down the displayed log entries to a sub-set that matches the filters you apply.

To add a filter, click the following icon:

FIGURE 6.89 : Activating the advanced filter

Next, use the pop-up dialog to add one or more new field filters.

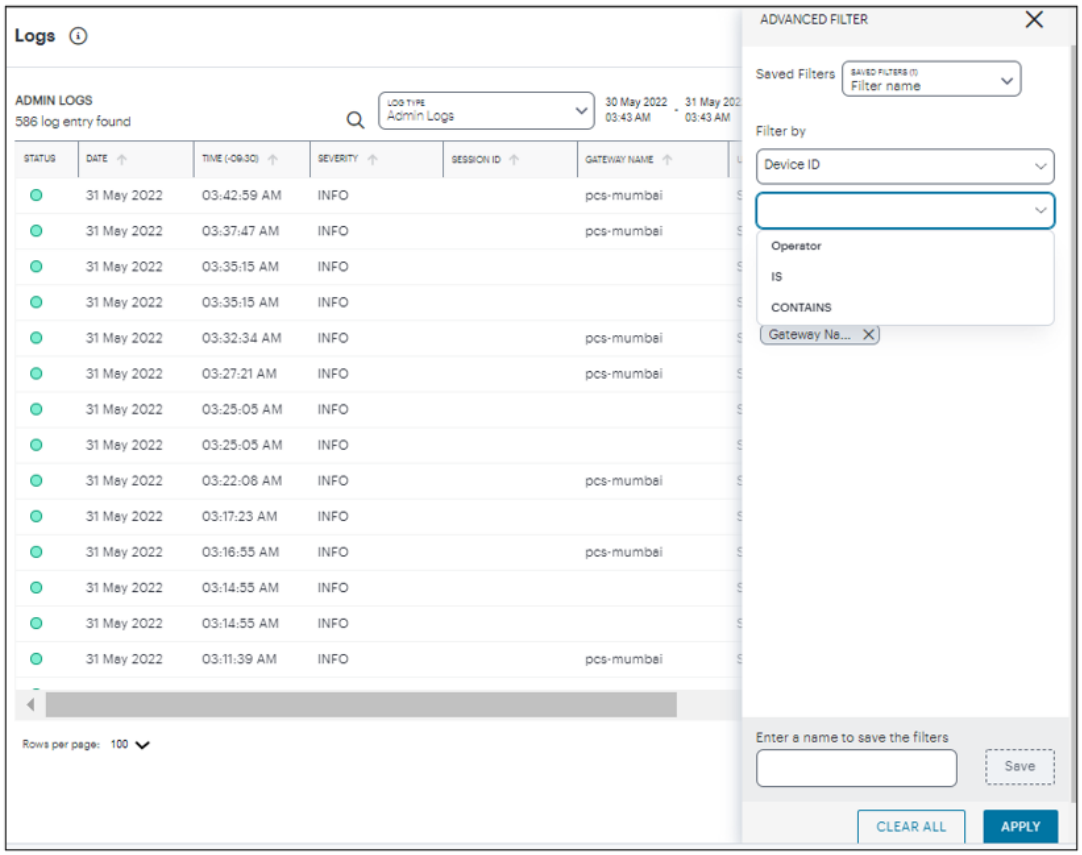


FIGURE 6.90 : Adding a new log filter

Use the **Selector** drop-down list to choose the field you want to filter on, add an **Operator** type, and then enter the **Value** you want to apply.

For the operator, choose from:

- **IS**: The selected field matches exactly the value you specify.
- **CONTAINS**: The selected field contains as a sub-string the value you specify.

Click the *plus* symbol to add your filter, then repeat the process to add any further filters you want to apply.

To apply your filters to the log data, click **APPLY**.

Your filters remain in place through data refreshes and are displayed at the bottom of the screen. To remove a filter, click the corresponding *X* icon.

In addition, Ivanti Connect Secure enables you to store advanced filters for future use. After you have applied filter criteria, enter a filter name into the box provided and click **Save**.

To load a previously-saved filter, select your filter from the **Saved Filters** drop-down list and click **Apply**.

To delete one or more previously-saved filters, select the filters from the **Saved Filters** drop-down list and click **Delete**.

Exporting Logs

Ivanti Connect Secure provides the ability to export the currently-displayed log as a Comma-Separated Value (CSV) or JavaScript Object Notation (JSON) text file. You can download the log immediately or set up a scheduled job to activate or repeat the export action at a defined time and interval of your choosing.

To access the Export Logs page:

1. Log in to the Ivanti Neurons for Secure Access Admin portal as a Tenant Admin, and select Ivanti Connect Secure from the Gateway Switcher. See *Logging in to Ivanti Neurons for Secure Access* (page 5).
2. From the Ivanti Connect Secure menu, click the **Insights** icon, then select **Logs**.

   The *Logs* page appears.
3. Select the log type you want to display in the **Log Type** drop-down list. Choose from:
   - Access Logs
   - Admin Logs
   - Event Logs
4. Click the *cloud* icon at the top of the page:

FIGURE 6.91 : Accessing the Export Logs Settings page

The Export Logs page appears:

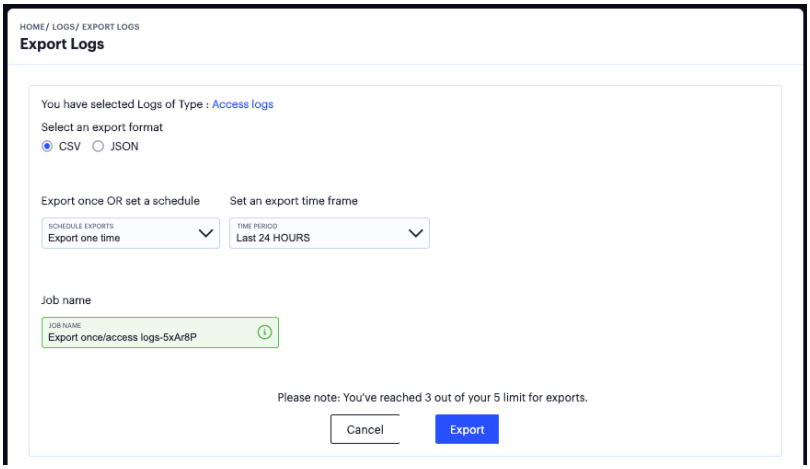


FIGURE 6.92 : The Export Logs settings page

Use the Export Logs settings page to configure an export operation, either to execute immediately as a one-off job, or as a scheduled job.

Configure the following settings:

- Select either **CSV** or **JSON** as the output format.
- Select the frequency of the export operation. Choose from:
  - **Export one time**: Perform the log export now as a single job.
  - **Daily data export**: Create a daily export job executed once per day from the selected start date, up to and including the stop date (if defined).
  - **Weekly data export**: Create a weekly export job executed once per week on the selected start day, up to and including the stop date (if defined).
  - **Monthly data export**: Create a monthly export job executed once per month on the selected start day, up to and including the stop date (if defined).

  If a stop date is specified, this is the date the schedule ceases. In the case of weekly or monthly jobs, if this date falls before the expected run date for that period, the job is terminated without running. For example, in a weekly run scheduled to execute every Thursday, if the stop date is set as a Tuesday, the final run of the job would be the previous Thursday.

  Note: A daily data export job continues to run for one extra day beyond the selected end date in order to process the logs for the final scheduled day.

  Note: For daily/weekly/monthly frequency export jobs, Ivanti Connect Secure allows for a maximum of 5 runs per scheduled export job. That is, each schedule runs a maximum of 5 times. On the sixth run, the first run is deleted (together with the log file), and so on.

- Set an export time frame. For one-time exports, choose from:

  - **Last 60 minutes**
  - **Last 24 hours**
  - **Last 7 days**
  - **Last 1 month**
  - **Set a date range (30d max)**: This option presents a configurable start and end date.

  For daily, weekly, and monthly exports, this option switches to show start and end date parameters. You do not need to specify an end date; in this case, the job remains active until deleted.

- Enter a **Job name** for the export operation. Ivanti Connect Secure suggests an appropriate name; use this, or type your own.
- To execute the defined job, click **Export**.

  To view all scheduled export logs jobs, and to download the log files created by each job, see *Viewing Scheduled Log Export Jobs and Downloading Log Files* (page 97).

Note: Ivanti Connect Secure allows for a maximum of 5 defined export jobs. Each job that you add reduces the total, as displayed at the bottom of the page. This is a separate limit to the maximum number of job runs described earlier.

Viewing Scheduled Log Export Jobs and Downloading Log Files

To view the status of your current log export jobs:

1. Log in to the Ivanti Neurons for Secure Access Admin portal as a Tenant Admin, and select Ivanti Connect Secure from the Gateway Switcher. See *Logging in to Ivanti Neurons for Secure Access* (page 5).
2. From the Ivanti Connect Secure menu, click the **Insights** icon, then select **Logs**.

   The *Logs* page appears.
3. Click the *list* icon at the top of the page:

FIGURE 6.93 : Accessing the Job Status page

The Job Status page appears:

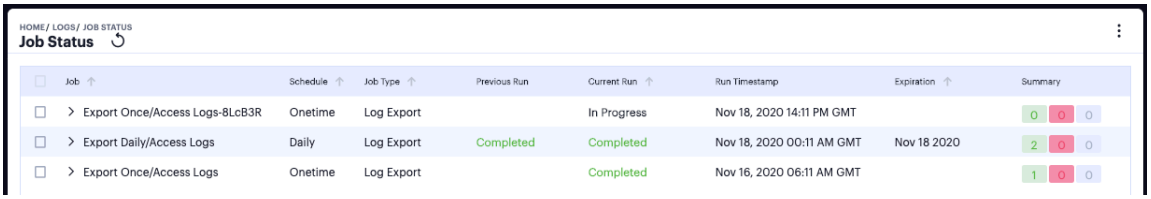


FIGURE 6.94 : The Job Status page

Use the Job Status page to:

- View the status and progress of currently scheduled log export jobs.
- Download log files for completed job runs.

For each job on the Job Status page, you can view the configured details of the export operation along with status indicators for progress of the previous and outstanding job runs.

Note: A job run refers to a single run of a scheduled job. For example, in a weekly data export job, a job run refers to the export operation scheduled or completed for one specific week within the start and end dates. Thus, a scheduled log export job is comprised of one or more job runs.

The **Summary** column provides totals of successful job runs, unsuccessful/failed job runs, and inactive job runs.

Click any of the fields in a single job row to display an info-panel at the side showing more details about the scheduled job:

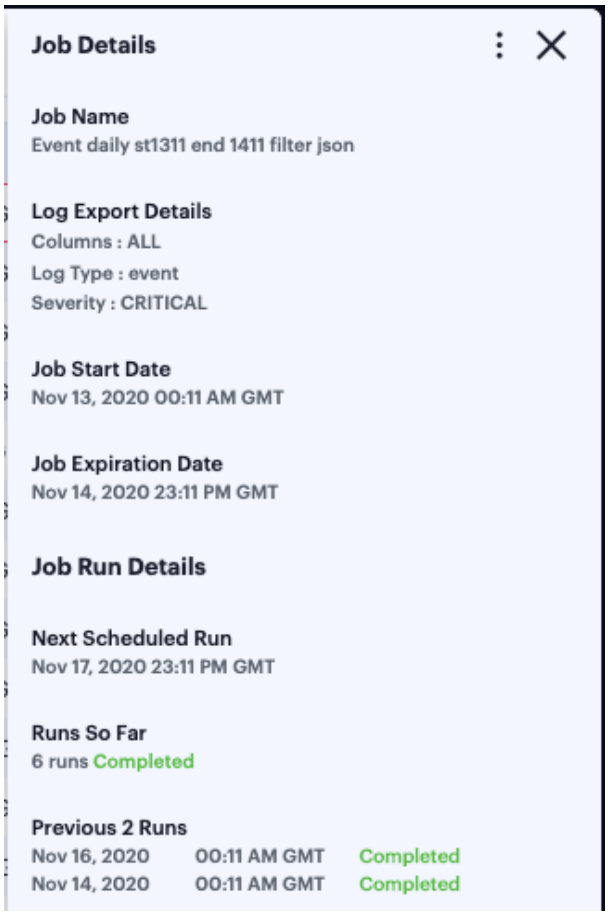


FIGURE 6.95 : The Job Details info-panel

To access the log files and view more information about each individual job run, click the down-arrow adjacent to the *Job* name:

FIGURE 6.96 : Showing all job runs for a scheduled export job.

Note: For daily/weekly/monthly frequency export jobs, Ivanti Connect Secure allows for a maximum of 5 runs per scheduled export job. That is, each schedule runs a maximum of 5 times. On the sixth run, the first run is deleted (together with the log file), and so on.

As with a scheduled job, click on any of the fields in the job run row to display an info-panel at the side showing more details about the job run:

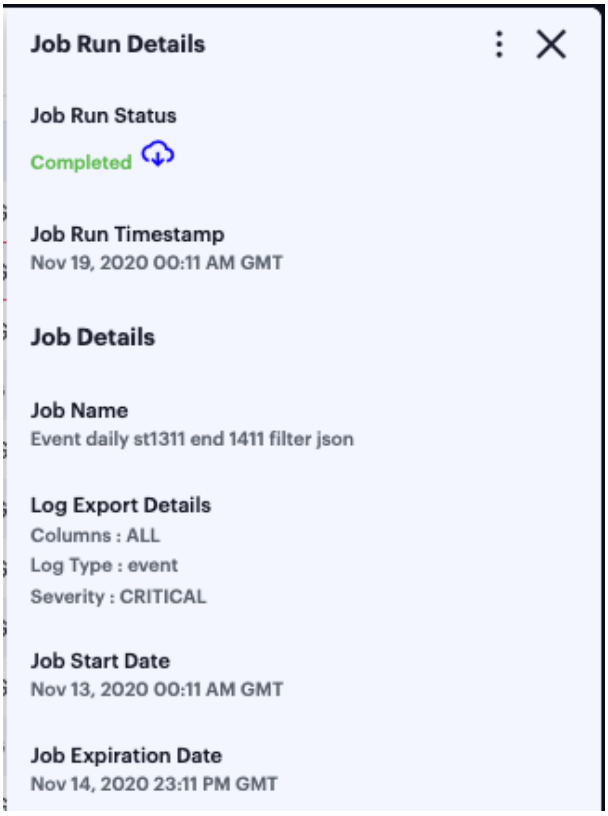


FIGURE 6.97 : The Job Run Details info-panel

To download the log file generated by the job run, click the *cloud* icon for a completed job run:

FIGURE 6.98 : Downloading a log file

To remove a scheduled log export job, or any of the completed job runs within the job, tick the checkbox adjacent to the job/job run and then access the context menu at the top of the page:

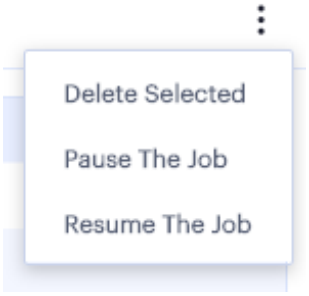


FIGURE 6.99 : The Job Status menu

Select from the following options:

- **Delete Selected**: Remove all jobs or job runs that have been selected.
- **Pause the Job**: Instruct the outstanding job runs in the schedule to become inactive. The schedule continues chronologically, but no further log export operations are completed while in this state.
- **Resume the Job**: Resume the schedule starting at the next scheduled job run.

Note: If you choose to delete a complete job, all job runs and log download files are removed permanently.

Associating Geographical locations to IP Addresses

Ivanti Connect Secure provides the mapping of Gateway geographic location to IP address.

Before you start, make sure that you have the following information:

- The public IP address/range for the Gateway. This is the IP address at which clients can externally reach the Gateway.
- The Gateway geographic location information such as country, state/province and city.

To add a new location:

1. Log in to the Ivanti Neurons for Secure Access Admin portal as a Tenant Admin, and select Ivanti Connect Secure from the Gateway Switcher. See *Logging in to Ivanti Neurons for Secure Access* (page 5).
2. From the Ivanti Connect Secure menu, click the **Administration** icon, then select **Custom Geo IP**.

   The *Custom Geo IP* page appears. This page lists all defined geographical associations to IP addresses.
3. Click the **+** icon at the top of the page:

FIGURE 6.100 : The Custom Geo IP

4. Enter the **IP Address/range**.
5. Select the **Country**.
6. Select the **State/Province**.
7. Select the **City**.
8. Enter a **Tag** for this IP Address/range.
9. Click **Save**.

Configuring Actionable Insights

The Actionable Insights function enables the tenant admin to create a policy/action to terminate all the existing sessions, with applicable rule, of a user when the UEBA threat score goes beyond the permissible limit.

To configure actionable insights:

1. Log in to the Ivanti Neurons for Secure Access Admin portal as a Tenant Admin, and select Ivanti Connect Secure from the Gateway Switcher. See *Logging in to Ivanti Neurons for Secure Access* (page 5).
2. From the Ivanti Connect Secure menu, click the **Insights** icon, then select **Actions**.

   The Actionable Insights page is displayed.

FIGURE 6.101 : The Actionable Insights page

3. From the **Set Actionable Insights for** drop-down list, select **UEBA Threat Score**.
4. Click **Add Actionable Insights**.

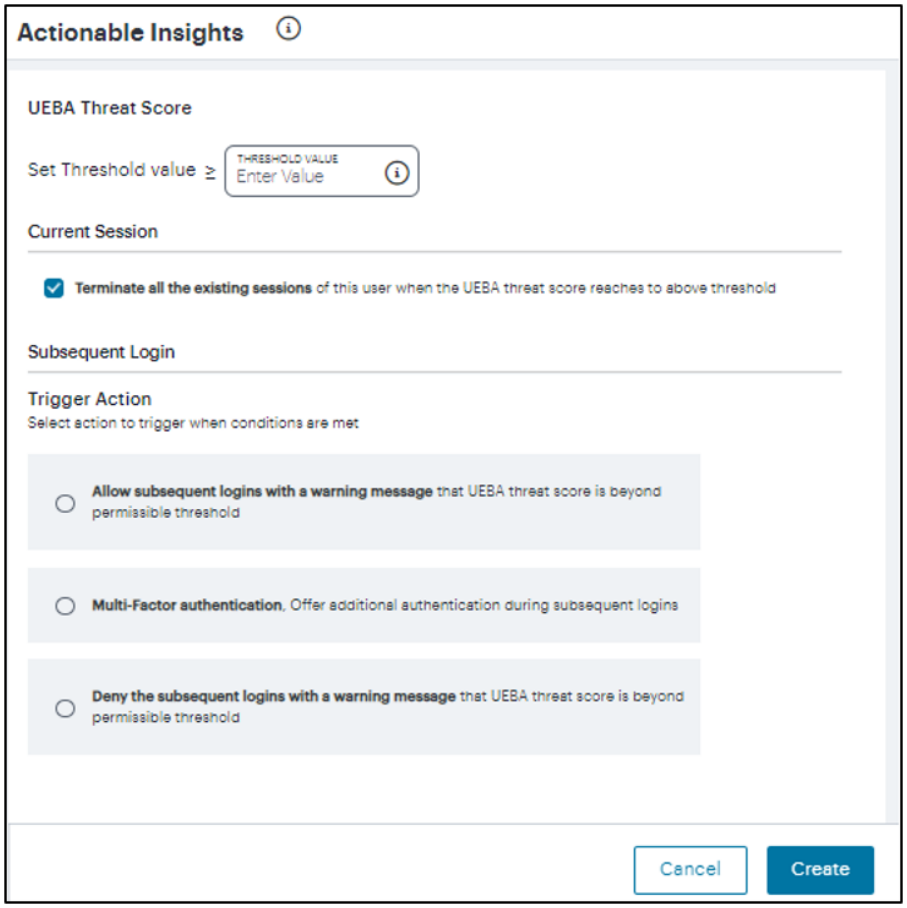


FIGURE 6.102 : Set UEBA Threat Score Threshold

5. Enter a **Threshold Value**.
6. In the Current Session section, select the **Terminate all the existing sessions of this user when the UEBA threat score reaches the threshold value** option. This is selected by default.
7. From the Subsequent Login section, select one of the following actions to

trigger when conditions are met:

Note: The newly added trigger actions will be supported with the ISAC Client version 22.3R1. For more details, refer KB: https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB45603.

- Allow subsequent logins with a warning message
- Offer Multi-factor Authentication during the subsequent logins
- Deny subsequent logins with a warning message

Note: A maximum of three thresholds can be created using the subsequent login conditions.

8. Click **Create**. A table showing the metric name, threshold value that is set, and the action to trigger when the condition is met, is shown in the Actionable Insights page.

   A confirmation message for the successful creation of the action is displayed. Click **Close** to close the message box.

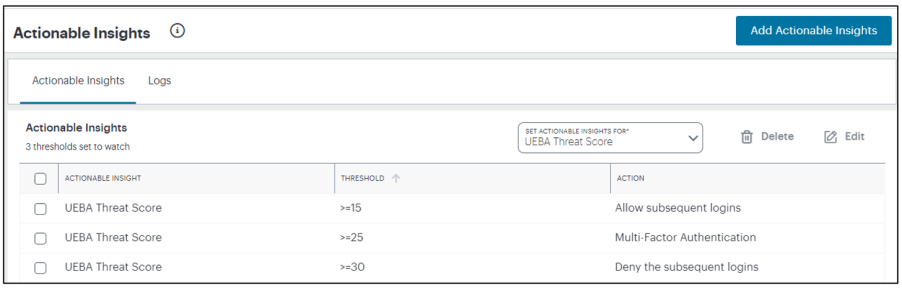


FIGURE 6.103 : The Actionable Insights page

9. To modify an action, select the check box corresponding to the action from the list, click the Edit icon, make the changes and then click **Update**.
10. To change the sequence of the rule, drag up or down the rule.
11. To remove one or more actions, select the check box(es) corresponding to the action from the list, and click **Delete**. Click **Yes, Delete** to confirm.

When a user session is terminated due to reaching the threshold UEBA Threat score, the following admin log message is generated in nSA: “User <username> session <session id> has been terminated due to UEBA Threat score based Actionable Insights configuration”. Select the **Logs** tab to view the list of log messages.

Generating Reports

The Reports function provides the ability to generate reports from the pre-defined templates or from the custom report. You may choose any of the pre-defined templates from User Activity Summary report, Application Access report, User Risk report or User Session Report. It also provides options to generate reports in PDF, JSON or CSV formats.

Accessing the Reports Page

To access the Reports page:

1. Log in to the Ivanti Neurons for Secure Access Admin portal as a Tenant Admin, and select Ivanti Connect Secure from the Gateway Switcher. See *Logging in to Ivanti Neurons for Secure Access* (page 5).
2. From the Ivanti Connect Secure menu, click the **Insights** icon, then select **Reports**.

   The Reports page is displayed.

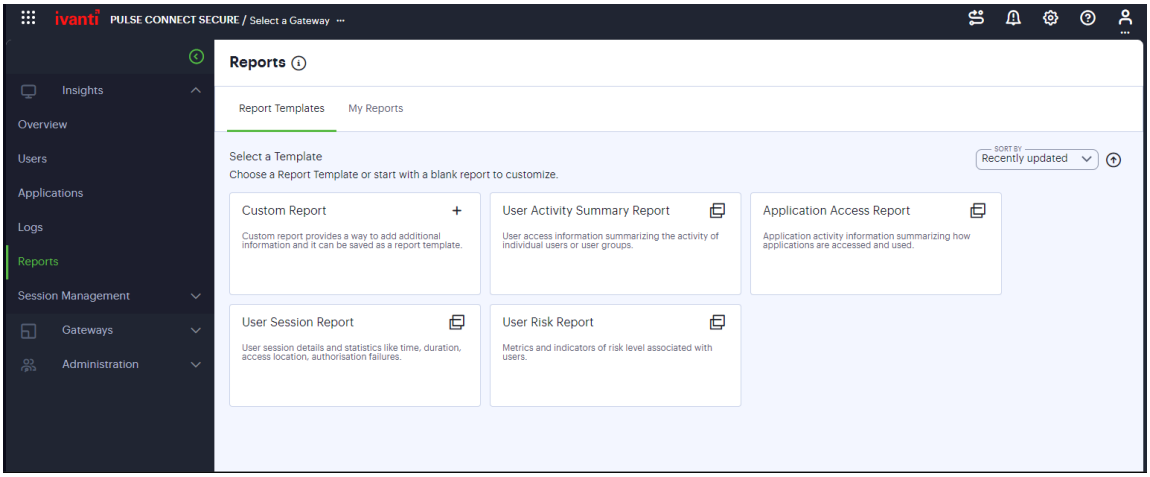


FIGURE 6.104 : The Reports page

The Reports page provides the following tabs:

- **Report Templates** – You can use the Custom Report option or the pre-defined report templates, and go through the wizard to configure and schedule the required report.
- **My Reports** – You can view a list of generated reports for all users of this tenant.
  - Click the report name link to view the summary of the configured details.
  - Click the download icon located next to the report to view report in the specified format (PDF, JSON, or CSV)

Configuring a Report

For scheduling a report, you can select one of the pre-defined report templates if that meets your requirement. Otherwise, select the Custom Report option.

Configuring Custom Report

To configure Custom report:

1. In the Reports page, select **Report Templates > Custom Report**.
2. In the Clone page, enter unique name for the report and click **Next**.
3. In the Format page:
   a. Select the required charts from User, Device and Application sections.
   b. Select the report format (PDF, JSON, or CSV).
   c. Select the check box if you want to save the report as a template.

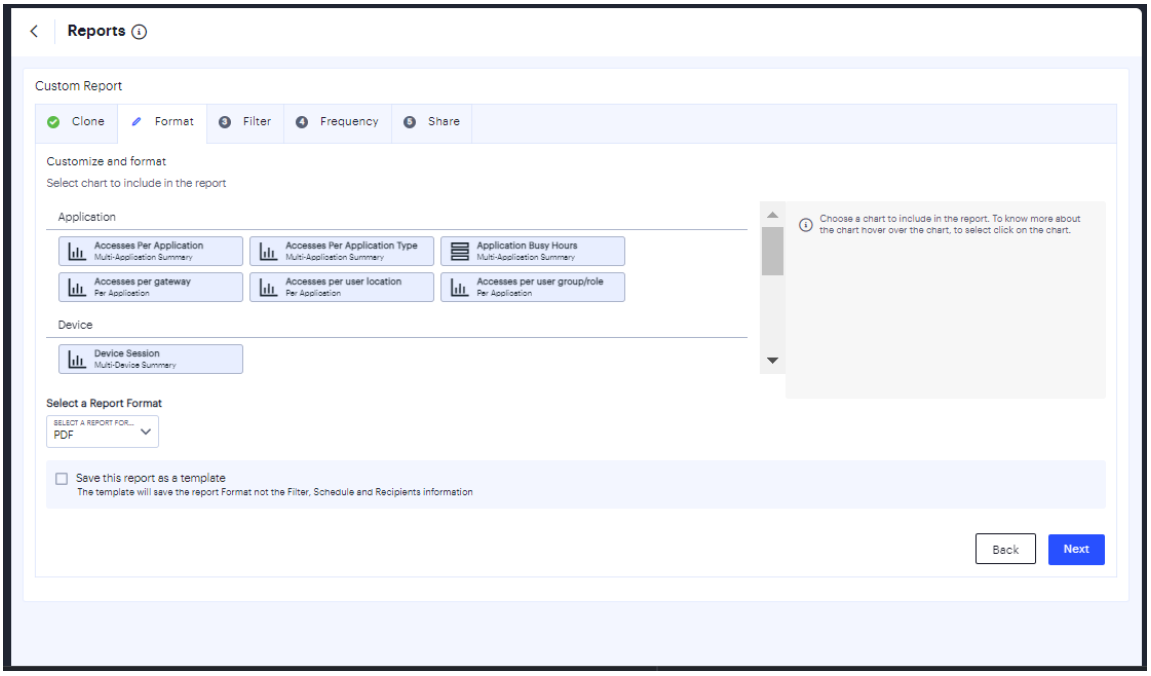


FIGURE 6.105 : The Format page

4. Click **Next**.
5. In the Filter page, select the data filter from User, Device, Gateway and Application attributes. Then click **Next**.

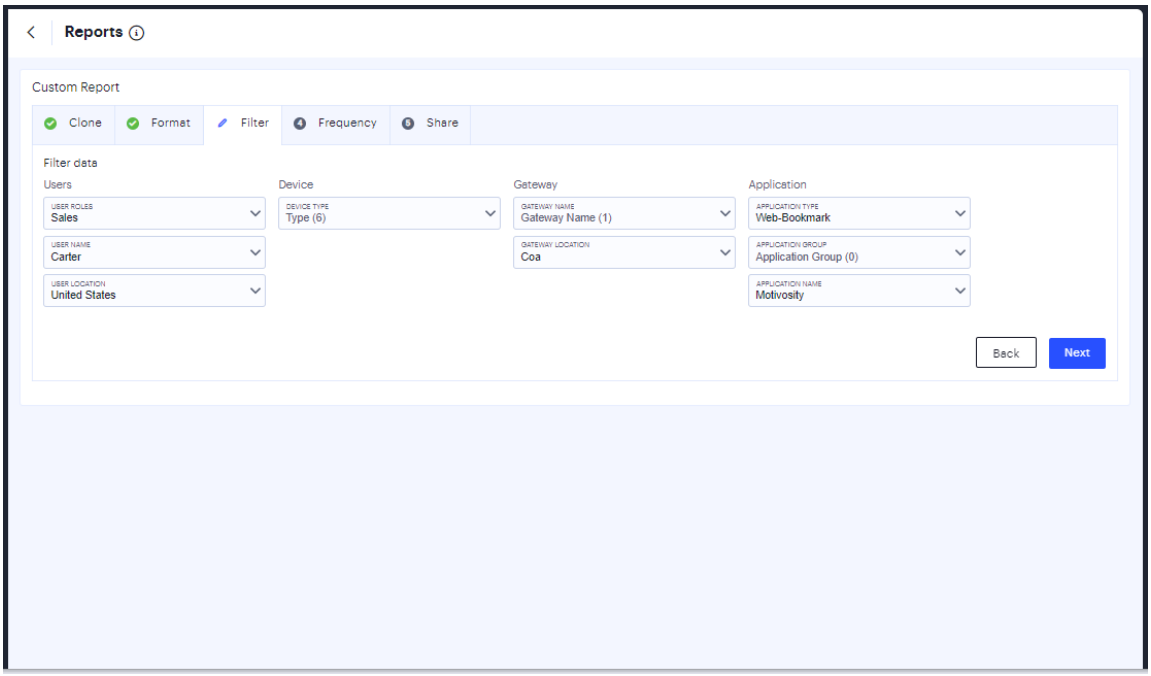
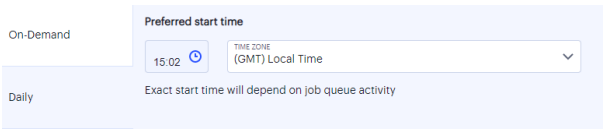


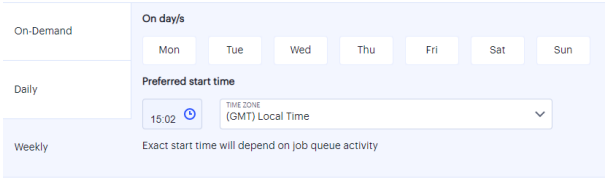
FIGURE 6.106 : The Filter page

6. In the Frequency page:
   - **Set recurring date range** - Click the calendar icon, specify the start date and the end date, and then click **Apply**.
   - **Frequency** - Select one of the options:
     - **On Demand**: Click the calendar icon, select the start date and the end date of the report, and then click **Apply**.

     - **Daily**: Click the time icon and select the start time. Then select the time zone from the drop-down list.



     - **Weekly**: Select the days of the week. Click the time icon and select the start time. Then select the time zone from the drop-down list.



7. Click **Next**.
8. In the Share page, select the admin users from the list to whom the notifications need to be sent, and click **Confirm and Schedule**.

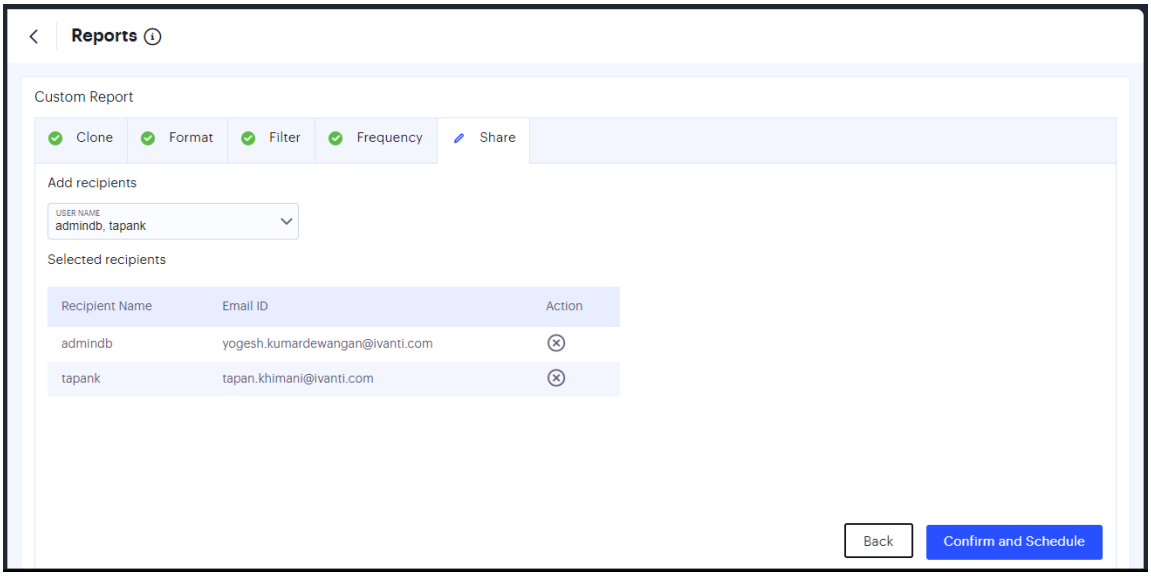


FIGURE 6.107 : The Share page

9. In the Confirm Submission page, verify the details and then click **Schedule Report**.

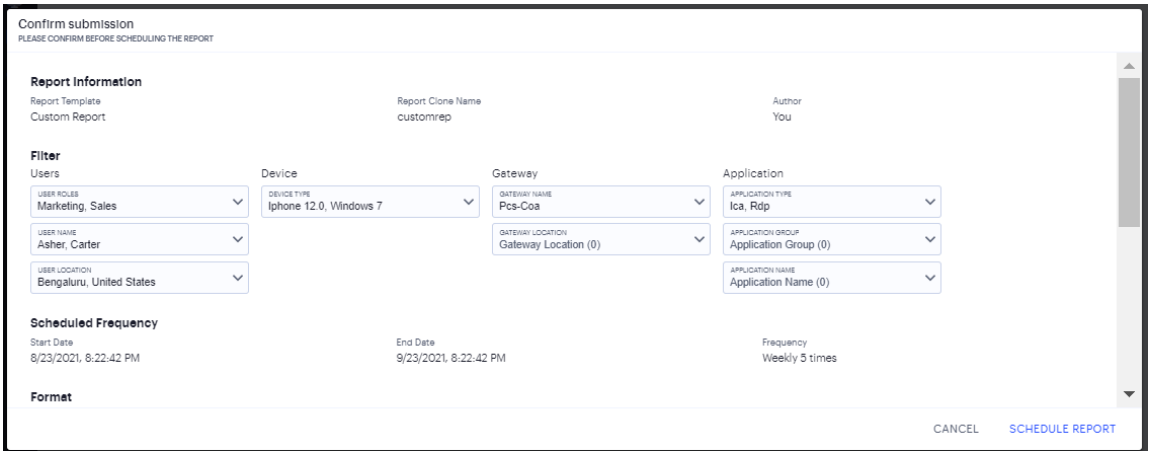


FIGURE 6.108 : The Share page

10. The report will be generated per schedule and listed in the My Reports page.

- Click the report name link to view the summary of the configured details.
- Click the download icon located next to the report to view report in the specified format (PDF, JSON, or CSV)

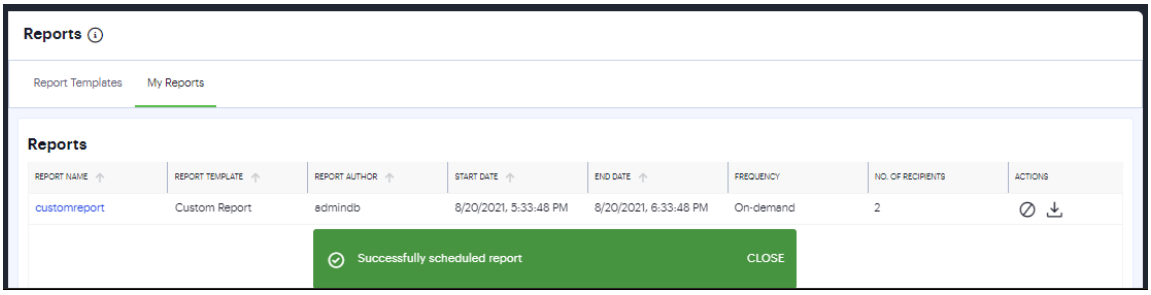


FIGURE 6.109 : The My Reports page

Configuring Pre-defined Report

To configure pre-defined report:

1. In the Reports page, select **Report Templates > <pre-defined report>**.
2. In the Clone page, enter unique name for the report and click **Next**.
3. In the Format page:
   a. Select the required charts from User, Device and Application sections, as applicable. By default, all the pre-defined template charts are selected.
   b. Select the report format (PDF, JSON, or CSV).
4. Click **Next**.
5. Configure the Filter, Frequency and Share pages as described in *Configuring Custom Report* (page 106)
6. In the Confirm Submission page, verify the details and click **Schedule Report**.
7. The report will be generated per schedule and listed in the My Reports page.
   - Click the report name link to view the summary of the configured details.
   - Click the download icon located next to the report to view report in the specified format (PDF, JSON, or CSV)

Managing the Sessions

Ivanti Connect Secure Sessions Management page allows you to manage the Active Sessions, Exported IF-MAP Sessions, Imported IF-MAP Sessions and ActiveSync Devices.

To navigate to Session Management page:

1. Log in to the Ivanti Neurons for Secure Access Admin portal as a Tenant Admin, and select Ivanti Connect Secure from the Gateway Switcher (9 dots). See *Logging in to Ivanti Neurons for Secure Access* (page 5).
2. From the Ivanti Connect Secure menu, click the **Insights** icon, then select **Session Management > Active Sessions**.

   The Session Management page is displayed. It presents the various sessions tabs to manage the sessions.

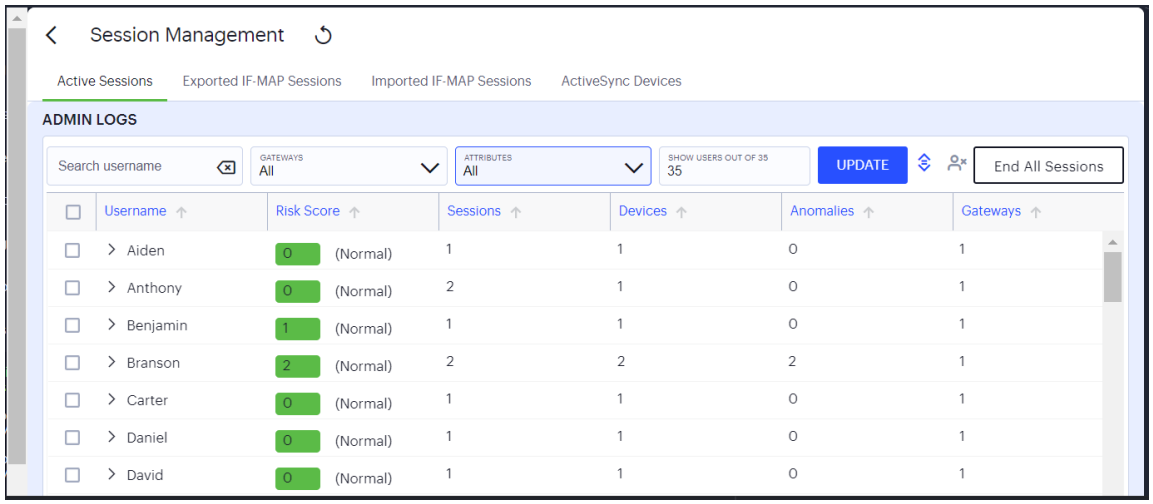


FIGURE 6.110 : Session Management page

3. The logs data presented can be sorted based on the column.
4. To manually refresh the data, click the circular arrow:

FIGURE 6.111 : Refreshing the data

Managing Active Sessions

To view Active Sessions:

1. In the Session Management page, select the **Active Sessions** tab.

   The Users list is displayed.
2. Click the > icon that is present next to a user name.

   An expanded list shows all the active sessions of that user.

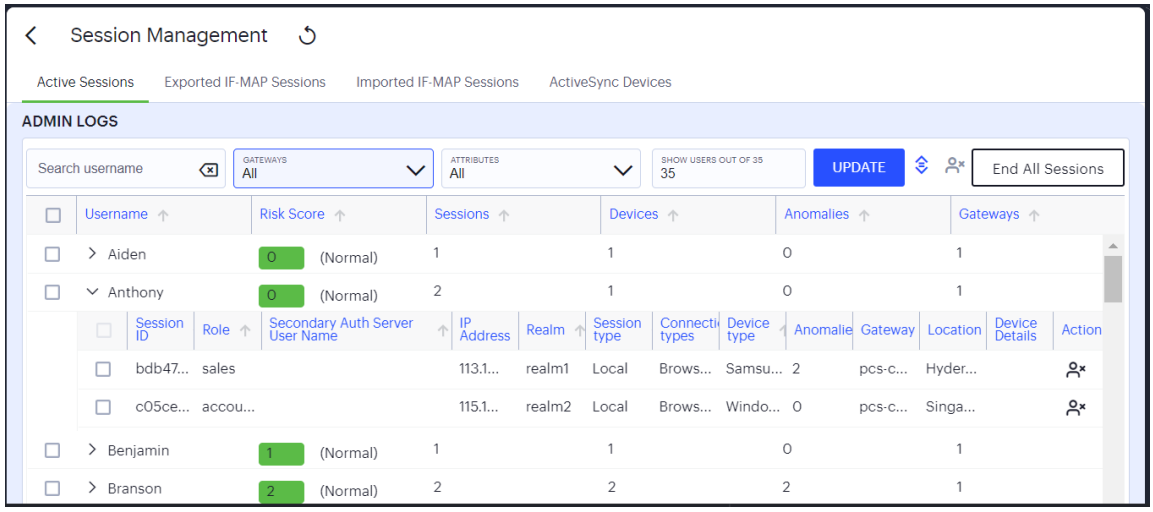


FIGURE 6.112 : Active Sessions

3. To view active sessions of all the users, click the **Expand/Collapse** icon.

FIGURE 6.113 : Expand/Collapse rows icon

4. To view the active sessions in a specific Gateway, select the Gateway from the Gateways list and click **Update**.
5. To view sessions based on the risk, select the appropriate option from the **Attributes** list.

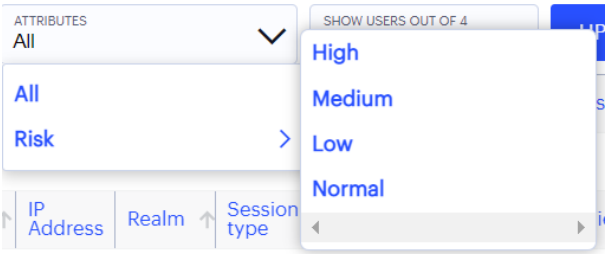


FIGURE 6.114 : Sessions based on risk type

To terminate user session:

1. In the Users list, click the > icon that is present next to the user name.

   An expanded list shows all the active sessions of that user. .

2. Click the **Terminate User Session** icon available in the **Action** column corresponding to the session you want to delete.

FIGURE 6.115 : Terminate User Session icon

3. To terminate all the sessions, click the **End All Sessions** button provided at the top-right corner of the page.

Viewing Exported IF-MAP Sessions

To view Exported IF-MAP Sessions:

1. In the Session Management page, select the **Exported IF-MAP Sessions** tab.

   The Exported IF-MAP Sessions page is displayed. The page shows a list of Exported IF-MAP Sessions.

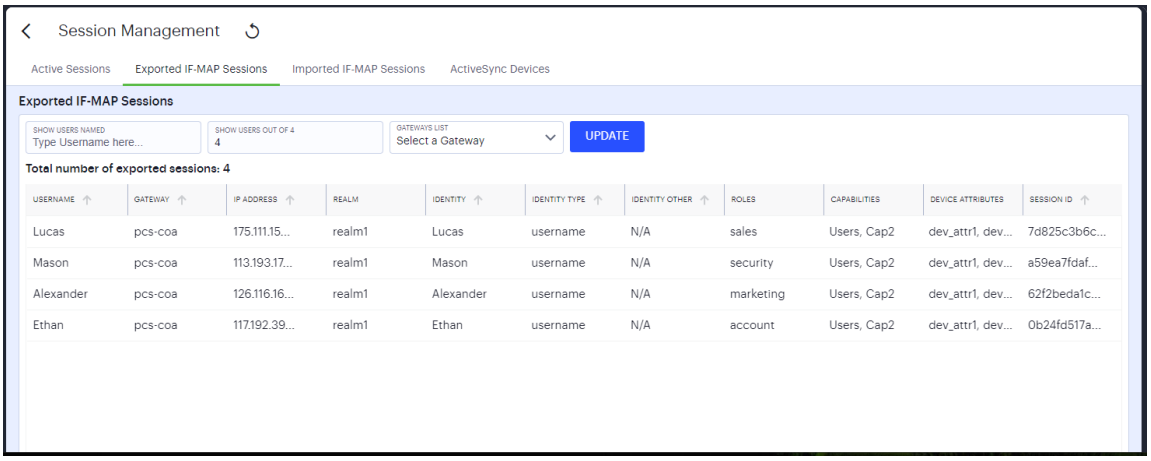


FIGURE 6.116 : Exported IF-MAP Sessions

2. You can sort the list based on the column.
3. To view the sessions by a specific user, enter the username in the Username field and click **Update**.
4. To view all the sessions associated to a specific Gateway, select the Gateway from the drop-down list and click **Update**.

Managing Imported IF-MAP Sessions

To manage Imported IF-MAP Sessions:

1. In the Session Management page, select the **Imported IF-MAP Sessions** tab.

   The Imported IF-MAP Sessions page is displayed. The page shows a list of Imported IF-MAP Sessions.

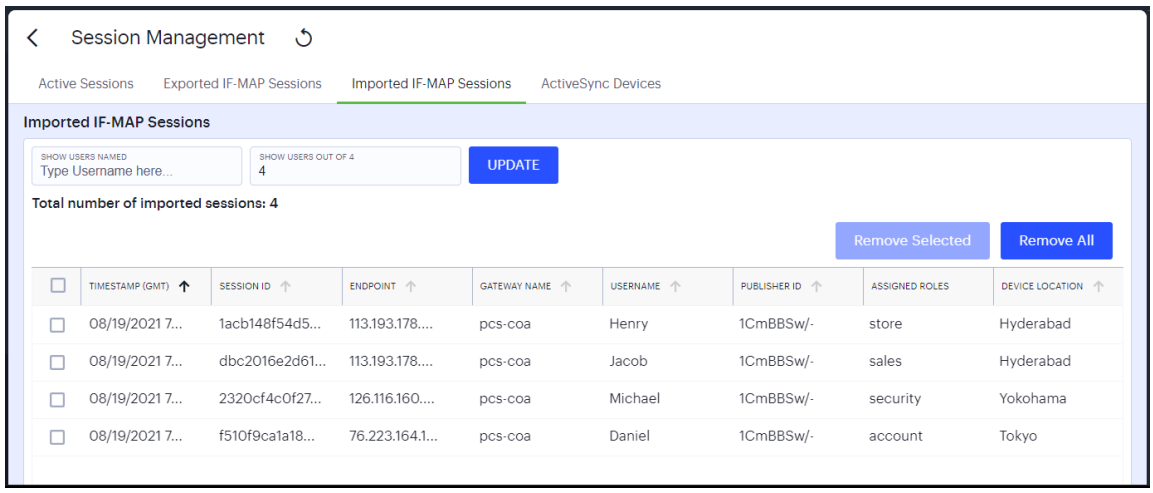


FIGURE 6.117 : Imported IF-MAP Sessions page

2. You can sort the list based on the column.
3. To view the sessions by a specific user, enter the username in the Username field and click **Update**.

To remove session:

1. In the IF-MAP Imported Sessions page, select the check box(es) present next to the sessions that you want to remove and click the **Remove Selected** button.
2. To remove all the sessions, click the **Remove All** button.

Managing ActiveSync Devices

The ActiveSync Devices page shows all ActiveSync Device sessions that are currently active across all Gateways that are registered with nSA.

To view ActiveSync Devices:

1. In the Session Management page, select the **ActiveSync Devices** tab.

   The ActiveSync Devices page is displayed. The page shows a list of devices.

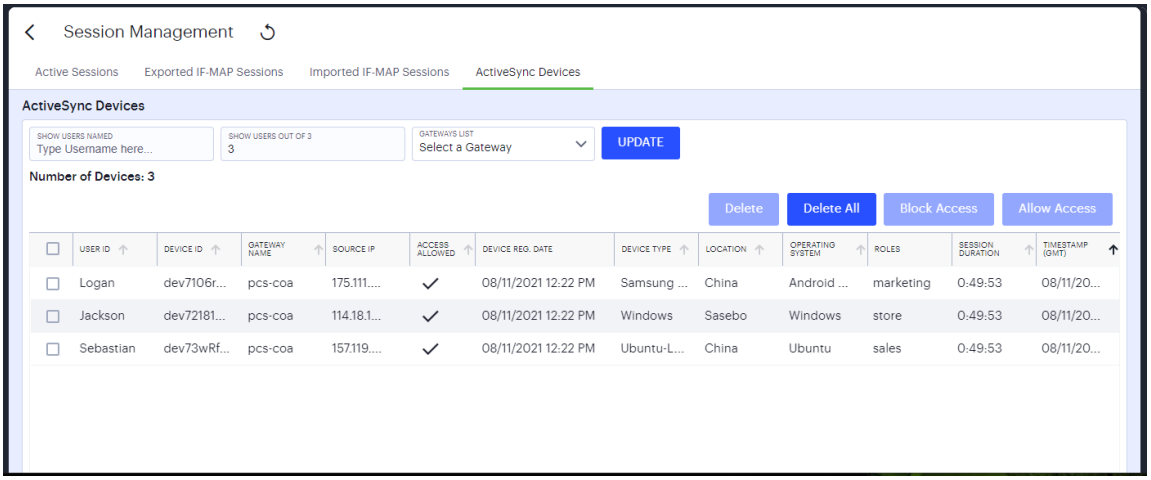


FIGURE 6.118 : ActiveSync Devices page

2. You can sort the devices list based on the column.
3. To view the devices accessed by a specific user, enter the username in the Username field and click **Update**.
4. To view all the devices associated to a specific Gateway, select the Gateway from the drop-down list and click **Update**.

To block/unblock one or more devices:

1. In the Session Management page, select the **ActiveSync Devices** tab.

   The ActiveSync Devices page is displayed that shows a list of devices.

   The Access Allowed column shows if the device is blocked/allowed for use. The tick mark means the access is allowed for that device.
2. To block a device, select the check box(es) next to the device that you want to block and click **Block Access**.

   The device is blocked, and a confirmation message is displayed.
3. To unblock a device, select the check box(es) next to the blocked device that you want to unblock and click **Allow Access**.

   The devices is unblocked, and a confirmation message is displayed.

To remove one or more devices:

1. In the Session Management page, select the **ActiveSync Devices** tab.

The ActiveSync Devices page is displayed. The page shows a list of devices.

2. To remove one or more devices, select the check box(es) next to the device that you went to remove and click **Delete**.
3. To remove all the devices, click **Delete All**.

Viewing Alerts and Notifications

The **Alerts** page lists all alerts and notifications that have been raised by nZTA.

To view the **Alerts** page, click the **Alerts** icon and then click **See all Alerts**:

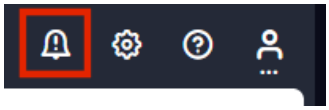


FIGURE 6.119 : Alerts icon

The **Alerts** page appears. For example:

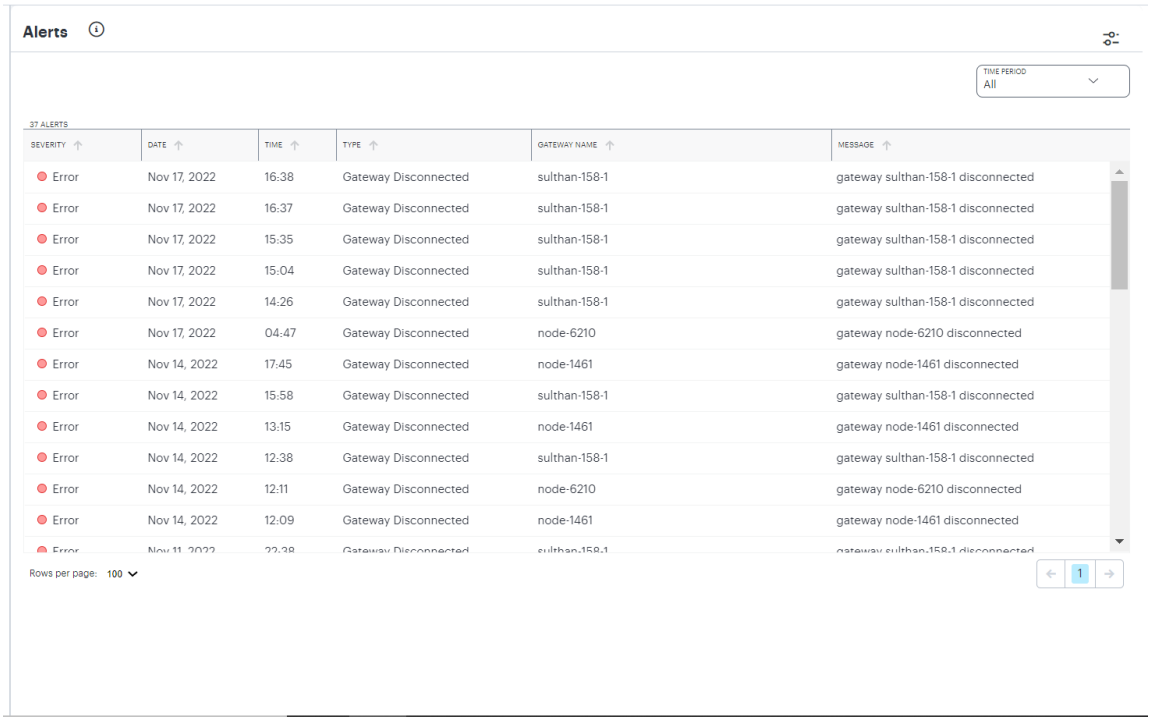


FIGURE 6.120 : Alerts page

The alerts table supports the following alert types:

- AAA Config Pull Failure

- AAA Config Pull Success
- AAA Config Pull Success - Failure Resolved
- AAA Journal Update Failed
- AAA Journal Update Success
- Config Sync Rule Deleted
- Config Sync Rule Updated
- Config Sync Target Cluster Deleted
- Custom Domain Certificate for mTLS Domain Due for Renewal
- Custom Domain Certificate for mTLS Domain Expired
- Custom Domain Certificate for TLS Domain Due for Renewal
- Custom Domain Certificate for TLS Domain Expired
- Device Vulnerability Risk Rating (VRR) Critical
- Device Vulnerability Risk Rating (VRR) High
- Device Vulnerability Risk Rating (VRR) Medium
- Device Vulnerability Risk Rating (VRR) Low
- Gateway Config Apply Failed
- Gateway Config Import Failed
- Gateway Disconnected
- Gateway Invalid Configurations Cleared
- Gateway Upgrade Failed

To filter the alerts table by type:

1. Click **Configure Alert Rules** icon.

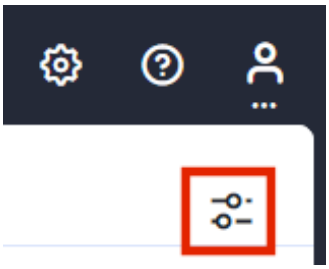


FIGURE 6.121 : Configure Alert Rules icon

   The **Configure Alerts & Notifications** page appears.
2. Click **Alert Types** and select the required type.
3. Click **Close**.

To filter the alerts table by time period, click **Time Period** and select the required time period.

To sort the alerts table into ascending or descending order of a specific property, click on one of the following column headings in the alerts table:

- **Severity**
- **Type**
- **Message Type**

Ivanti Connect Secure Gateway Management

Introduction

An admin can manage the ICS Gateway/Cluster with the following operations:

- **Restart Services**: Kills all processes and restarts the Gateway/Cluster. The Gateway/Cluster is available again after a few minutes. See *Restarting Services* (page 123).
- **Reboot Gateway**: Reboots the Gateway. The Gateway is available again after a few minutes. See *Rebooting ICS Gateway/Cluster* (page 123).
- **Reboot Cluster**: Reboots all nodes in the Cluster. See *Rebooting ICS Gateway/Cluster* (page 123).
- **Rollback to <version>**: Reverts the registered Gateway virtual machine instance to the specified version. See *Rolling Back a Gateway/Cluster* (page 124).
- **Rollback Cluster**: Reverts the cluster instance to the previous version. See *Rolling Back a Gateway/Cluster* (page 124).

- **Upgrade to <version>**: Upgrades the registered Gateway virtual machine instance to the specified version. See *Upgrading a Gateway and Cluster* (page 125)
- **Upgrade to <version> Cluster**: Upgrades all the nodes in the Cluster to the specified version. See *Upgrading a Gateway and Cluster* (page 125).
- **Delete Gateway**: Removes the Gateway record. See *Removing Ivanti Connect Secure Gateway* (page 130).
- **Configure Integrity Scanner**: Scans the system periodically to check for any integrity anomalies.
- **Upgrade multiple Gateways/Clusters to new version**: Upgrades multiple Gateways/Clusters to the specified version. See *Upgrading Multiple Gateways and Clusters* (page 126)

Note: The available menu options vary depending on whether the selected Gateway is registered and connected to the nSA.

Viewing ICS Gateway/Cluster Details

To view the list of ICS Gateways and Clusters:

1. Log in to the Ivanti Neurons for Secure Access portal as a Tenant Admin. See *Logging in to Ivanti Neurons for Secure Access* (page 5).
2. Use the Gateway Switcher and select **Ivanti Connect Secure**.
3. From the Ivanti Connect Secure menu, click the **Gateways** icon, then select **Gateways > Gateways List**.

   The All Gateways page is displayed showing a list of standalone ICS Gateways and Cluster nodes.

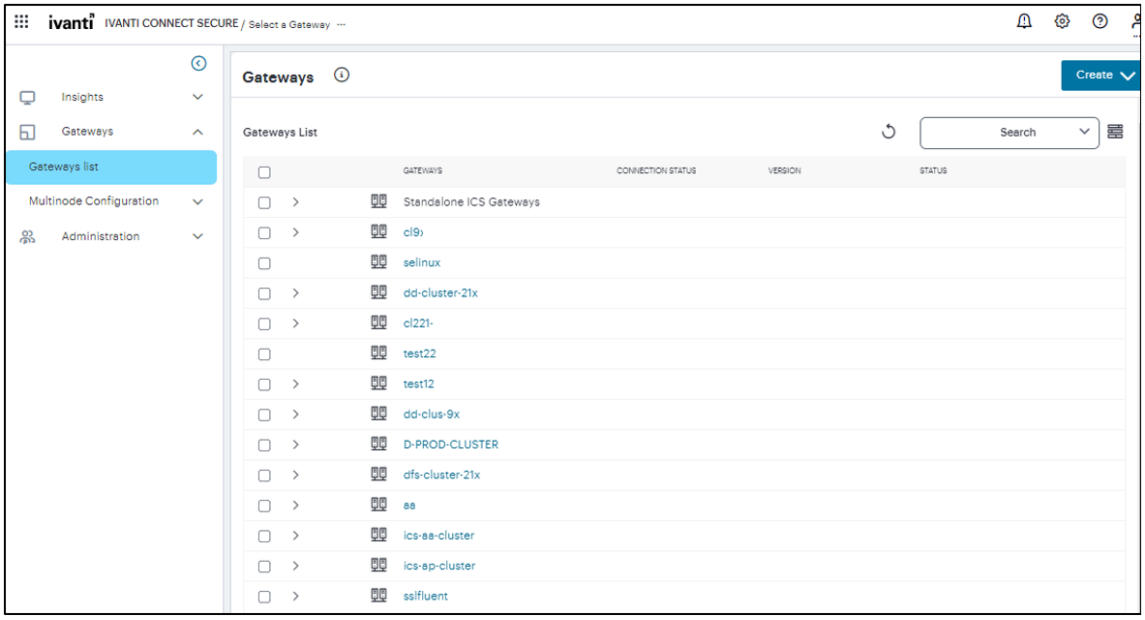


FIGURE 7.1 : Gateways list

Note: The Gateway management functions can be performed only if the status of the Gateway is green.

To view the details of a specific Gateway:

1. In the All Gateways page, double-click the required Gateway from the Standalone Gateways list.

   The Gateway Overview page is displayed showing the Gateway Status, Version, Registration State, and last Updated time.

FIGURE 7.2 : ICS Gateway Details

2. Click the context menu icon present at the top-right of the page to access the options applicable to the selected Gateway.

To view the details of an Active-Active Cluster:

1. In the All Gateways page, double-click the Active-Active Cluster from the list.

   The Gateway Overview page is displayed showing the Model, Cluster Name and Configuration of the Cluster.

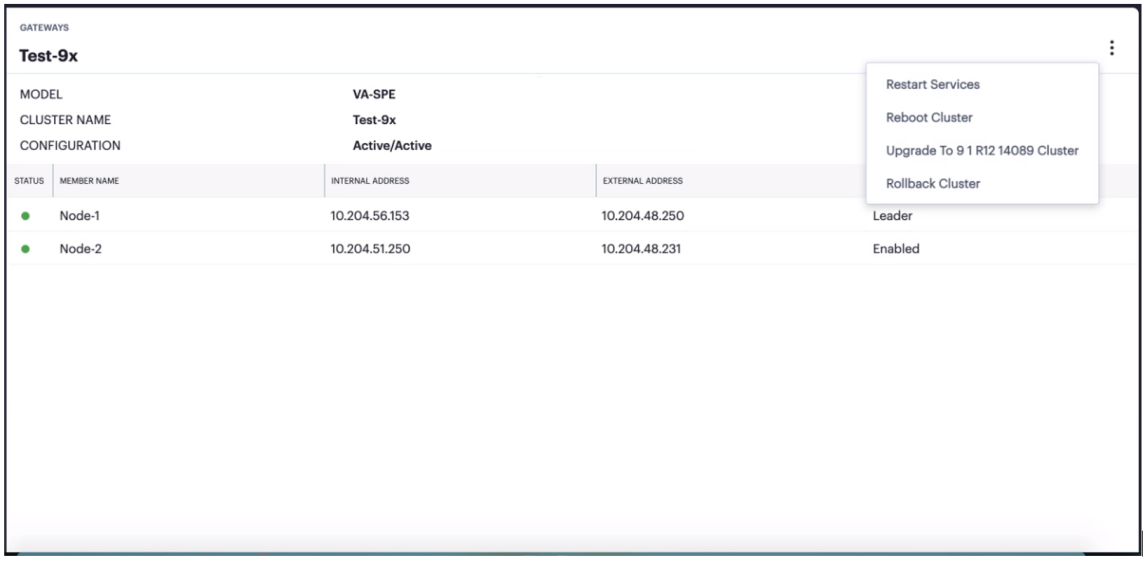


FIGURE 7.3 : Active-Active Cluster Details

2. Click the context menu icon present at the top-right of the page to access the options applicable to the selected Cluster.

To view the details of an Active-Passive Cluster:

1. In the All Gateways page, double-click the Active-Passive Cluster from the list.

   The Gateway Overview page is displayed showing the Model, Cluster Name, Configuration, External and Internal VIP Owner, External and Internal VIP IPV4/IPV6 of the Cluster.

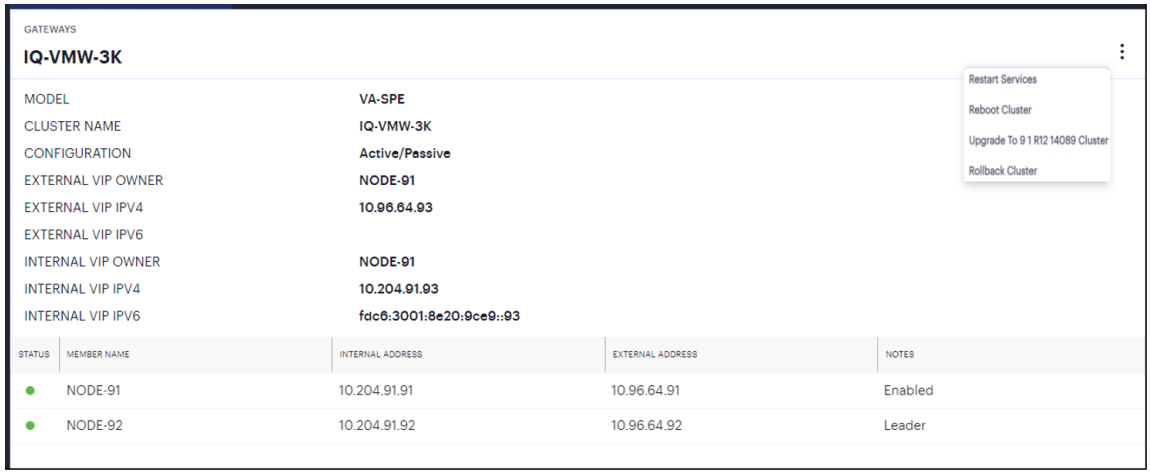


FIGURE 7.4 : Active-Passive Cluster Details

2. Click the context menu icon present at the top-right of the page to access the options applicable to the selected Cluster.

Restarting Services

To restart services:

1. In the Gateway Overview page, click the context menu icon at the top-right to access the options applicable to the selected Gateway or Cluster.
2. Select the **Restart Services** option.

   The Gateway/Cluster is available again after a few minutes.

Rebooting ICS Gateway/Cluster

To reboot ICS Gateway:

1. In the Gateway Overview page, click the context menu icon present at the top-right of the page to access the options applicable to the selected Gateway.
2. Select the **Reboot Gateway** option.

   The Gateway is available again after a few minutes.

To reboot ICS Cluster:

1. In the Gateway Overview page, click the context menu icon present at the top-right of the page to access the options applicable to the selected A/A or A/P Cluster.
2. Select the **Reboot Cluster** option.

   The Cluster is available again after a few minutes.

Rolling Back a Gateway/Cluster

Your ICS Gateway/Cluster can be rolled back to a previously-installed version through the Tenant Admin Portal. You might want to return to an earlier version if, for example, you encounter an unforeseen issue with a newly-upgrading Gateway instance, or for testing purposes.

You can roll back to a version only where that Gateway instance has been previously upgraded through the Tenant Admin Portal, and only to the previously-installed version.

To roll back a Gateway to an earlier version:

1. In the Gateway Overview page, click the context menu icon present at the top-right of the page to access the options applicable for the selected Gateway.

   If a rollback function is available for this Gateway, a corresponding link is displayed in the drop-down menu:

2. Select the **Rollback to <version>** link.

   As the rollback process starts, your Gateway remains operating on the current version and continues to serve traffic. After the earlier version is reinstated, the Gateway reboots and becomes unavailable for a short time.

   If the procedure is successful, the new software version is displayed in the Gateway Overview page.

To roll back a Cluster to the previous version:

1. In the Gateway Overview page, click the context menu icon present at the top-right of the page to access the options applicable for the selected Cluster.

   If a rollback function is available for this Cluster, a corresponding link is displayed in the drop-down menu:

2. Select the **Rollback Cluster** link.

   As the rollback process starts, your Cluster remains operating on the current version and continues to serve traffic. After the earlier version is reinstated, the Cluster reboots and becomes unavailable for a short time.

   If the procedure is successful, the new software version is displayed in the Gateway Overview page.

Upgrading a Gateway and Cluster

Ivanti periodically creates and releases new software versions to address updates and issues, and to improve performance. As new version packages become available, you can trigger an upgrade for your Gateway/Cluster through the nSA to take advantage of the updates available in the new version.

To upgrade a Gateway to a higher version:

1. In the Gateway Overview page, click the context menu icon present at the top-right of the page to access the options applicable for the selected Gateway.

   If the upgrade function is available for this Gateway, a corresponding link is displayed in the drop-down menu:

2. Select the **Upgrade to <version>** link.

   Note: In some cases, there might be more than one version available. Select the version you want, or contact your support representative for details.

   As the upgrade process starts, your Gateway remains operating on the current version and continues to serve traffic. After the upgrade to new version, the Gateway reboots and becomes unavailable for a short time.

   If the procedure is successful, the upgrade task is marked with a status of “Success” and the new software version is displayed in the Gateway Overview page.

To upgrade a Cluster to a higher version:

1. In the Gateway Overview page, click the context menu icon present at the top-right of the page to access the options applicable for the selected Cluster.

   If the upgrade function is available for this Cluster, a corresponding link is displayed in the drop-down menu:

2. Select the **Upgrade to <version> Cluster** link.

   Note: In some cases, there might be more than one version available. Select the version you want, or contact your support representative for details.

   As the upgrade process starts, your Cluster remains operating on the current version and continues to serve traffic. After the upgrade to new version, the Cluster reboots and becomes unavailable for a short time.

   If the procedure is successful, the upgrade task is marked with a status of “Success” and the new software version is displayed in the Gateway Overview

page.

Upgrading Multiple Gateways and Clusters

This feature allows you to upgrade one or more gateways and clusters in a tenant with a selected version.

Viewing the Installed Packages

To view the installed packages:

1. Log in to the Ivanti Neurons for Secure Access portal as a Tenant Admin. See *Logging in to Ivanti Neurons for Secure Access* (page 5).
2. Use the Gateway Switcher and select **Ivanti Connect Secure**.
3. Select **Administration > Upgrade > Installation Packages**.

   The Installation Packages page shows the list of installed packages of Secure Access client, ESAP, and Connect Secure Gateways.

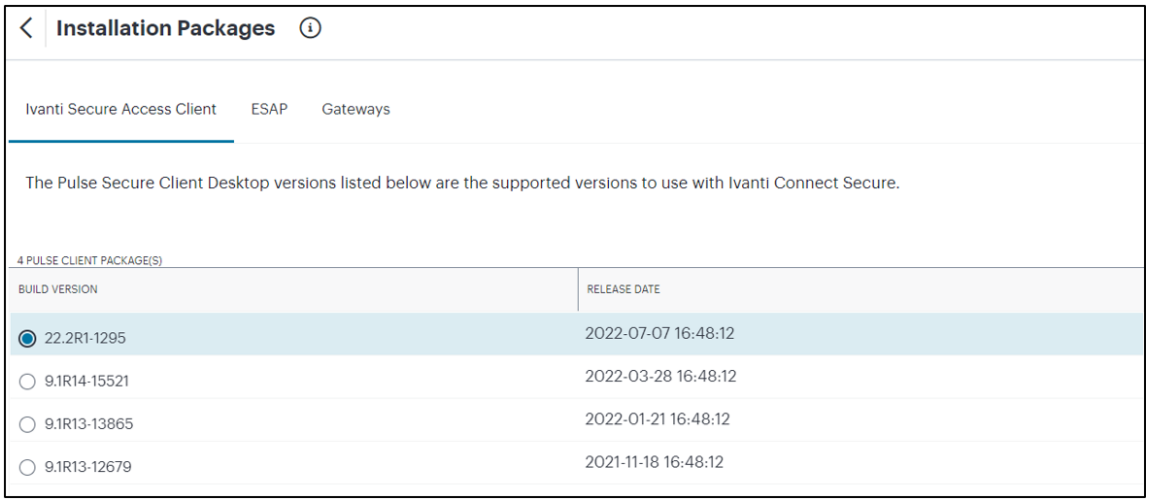


FIGURE 7.5 : Installation Packages page

Upgrading Gateways and Clusters with Ivanti Secure Access Client

To upgrade one or more Gateways and Clusters with an Ivanti Secure Access Client package newer version:

1. Select **Administration > Upgrade > Installation Packages**.
2. In the Installation Packages page, select the **Ivanti Secure Access Client** tab.

   A list of available Ivanti Secure Access Client packages appears.

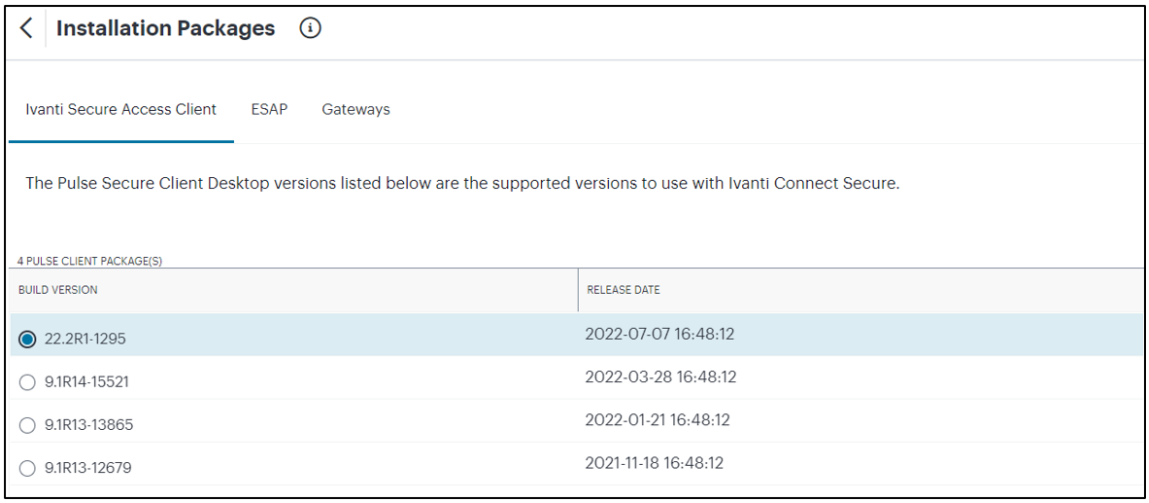


FIGURE 7.6 : Ivanti Secure Access Client Packages page

3. Select any of the listed Ivanti Secure Access Client packages. This is the version of the Ivanti Secure Access Client software that you want users to have on their device.

As each user next logs into Ivanti Secure Access Client on their device, if their software is at a different version, Ivanti Secure Access Client provides a prompt to the user to change to the version you selected in nSA.

Note: After the Client package download starts from nSA to ICS Gateway, any other operations in nSA, for example a Role or Realm creation and any configuration change, do not work unless the download is complete. After the successful download, config creations or modifications appear.

Upgrading Gateways and Clusters with a New Gateway Version

To upgrade one or more Gateways and Clusters:

1. Select **Administration > Upgrade > Installation Packages**.
2. In the Installation Packages page, select the **Gateways** tab.

   The Gateways page shows the list of installed packages of Connect Secure Gateway.
3. Select the required build version from the list and click **Select Gateways/Clusters to Upgrade**.
4. In the Select Gateways / Clusters for Upgrade dialog, from the **Select Gateways** drop-down list, select one or more Gateways.

   Note: The UI shows the applicable Gateways and Clusters running on version 21.12 and above.

   ---

5. From the **Select Clusters** drop-down list, select one or more Clusters.

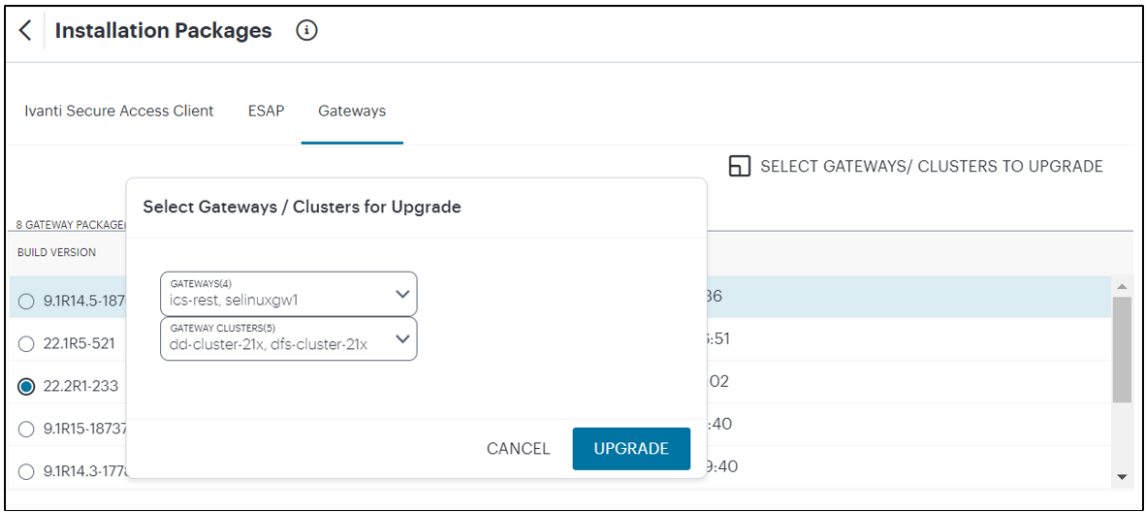


FIGURE 7.7 : Select Multiple Gateways and Clusters - Gateway Package

Note: The Select Gateways and Select Clusters list shows only those Gateways and Clusters that have lower versions than the selected version.

6. Click **Upgrade**. The upgrade task is scheduled, and a notification is displayed.
7. On the Ivanti Connect Secure menu, select Gateways > Gateways List to see the progress of the Upgrade process.

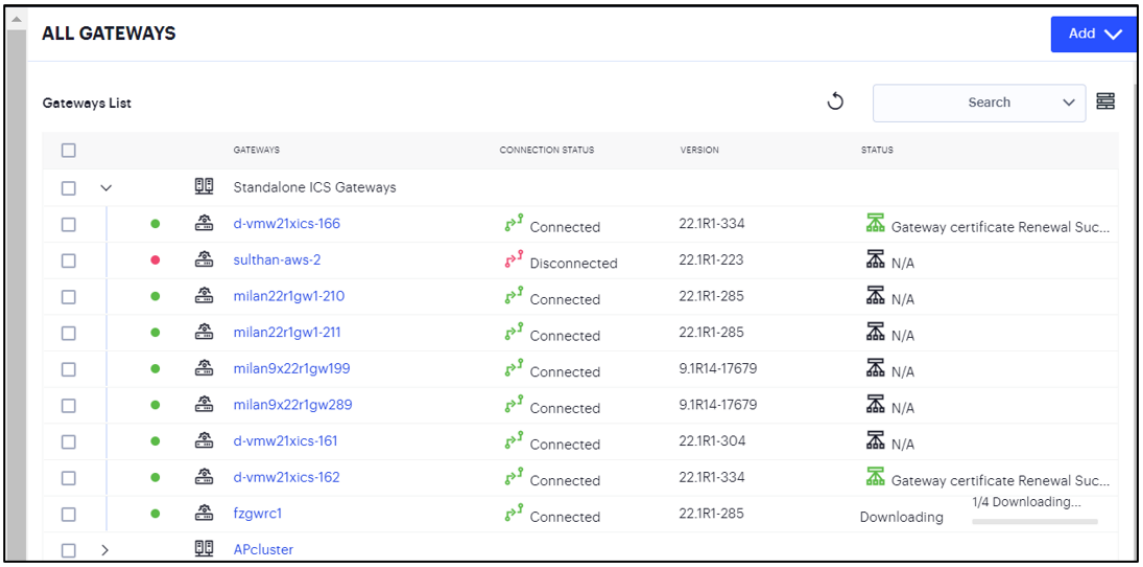


FIGURE 7.8 : Upgrade Progress

Upgrading Gateways and Clusters with ESAP

Uploading an ESAP Package

To upload an ESAP package version:

1. Select **Administration > Upgrade > Installation Packages**.
2. In the Installation Packages page, select the **ESAP** tab.
3. Click the **Upload ESAP file** box.

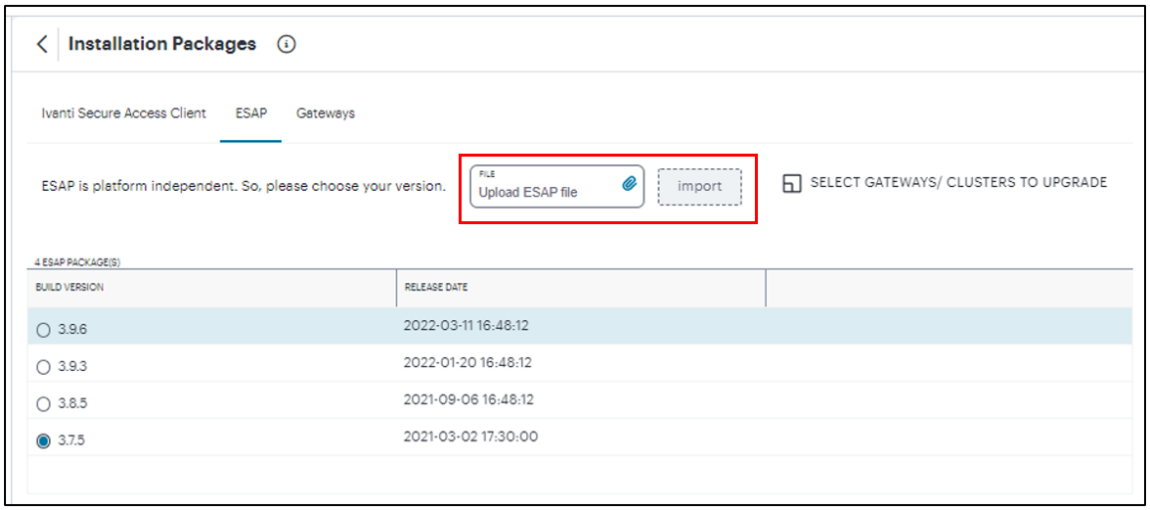


FIGURE 7.9 : Upload ESAP file

4. Browse and select the latest ESAP package that you want to upload and then click **Import**.

   After successful upload to nSA, the ESAP package gets listed in the ESAP packages page.

   Note: You can upload only one ESAP package.

Upgrading with ESAP

To upgrade one or more Gateways and Clusters to a newer ESAP package version:

1. Select **Administration > Upgrade > Installation Packages**.
2. In the Installation Packages page, select the **ESAP** tab.
3. Select the required build version from the list and click **Select Gateways/Clusters to Upgrade**.
4. In the Select Gateways / Clusters for Upgrade dialog, from the **Select Gateways** drop-down list, select one or more Gateways.

Note: The UI shows the applicable Gateways/Clusters running on version 21.12 and above.

5. From the **Select Clusters** drop-down list, select one or more Clusters.

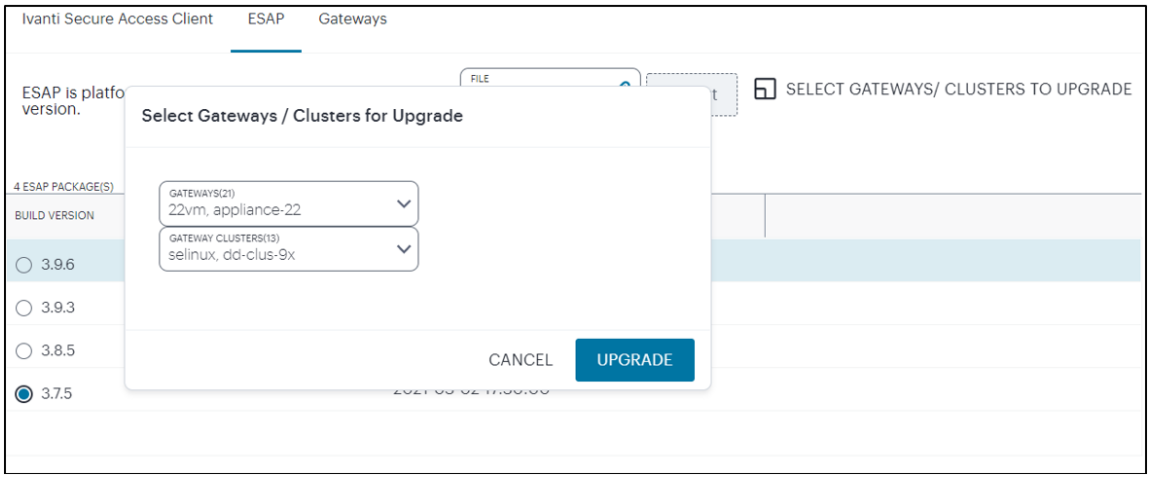


FIGURE 7.10 : Select Multiple Gateways and Clusters - ESAP Package

Note: The Select Gateways and Select Clusters list shows only those Gateways and Clusters that have lower versions than the selected version.

6. Click **Upgrade**. The upgrade task is scheduled, and a notification is displayed in the logs.

Note: nSA deletes all the existing ESAP packages from the ICS Gateway after the upgrade and retains only the upgraded ESAP version.

Removing Ivanti Connect Secure Gateway

To remove Ivanti Connect Secure Gateway:

1. In the Gateway Overview page, click the context menu icon present at the top-right of the page to access the options applicable to the selected Gateway.
2. Select **Delete Gateway**.

   The selected Gateway is removed from the list of Gateways.

Configuring Integrity Scanner

You can configure scan the system to periodically check for any integrity anomalies. If any anomaly found, information is displayed in the dashboard.

To configure Integrity Scanner Interval:

1. Log in to the Ivanti Neurons for Secure Access portal as a Tenant Admin. See *Logging in to Ivanti Neurons for Secure Access* (page 5).
2. Use the Gateway Switcher and select **Ivanti Connect Secure**.
3. From the Ivanti Connect Secure menu, click the **Gateways** icon, then select **Gateways > Gateways List**.

   The All Gateways page is displayed showing a list of standalone ICS Gateways and Cluster nodes.
4. Select one or more gateways, click **Select Configuration**, and select **ICT**.

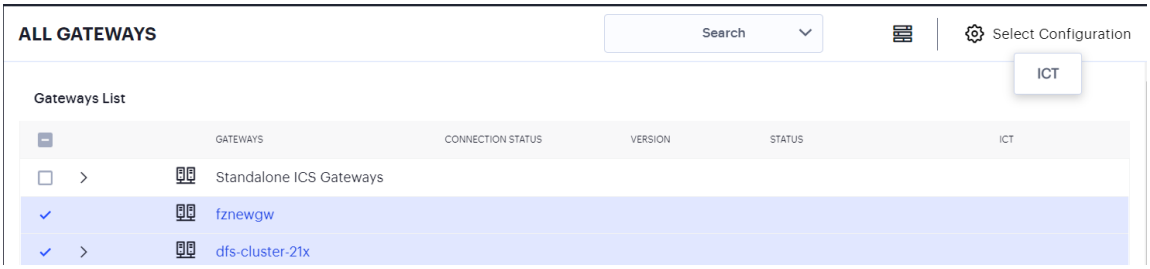


FIGURE 7.11 : Switch Configuration - ICT

5. Select the scanner interval.
   - **Periodic Scan**: Select the time interval to run the integrity scanner during run time.

     For example: Select 2 hrs to run the integrity scanner every 2 hrs.
   - **Scheduled Scan**: Select to run integrity scanner at a specified time every day.

     For example: When 13 hr 25 min is specified, the scanner runs at the same time every day.

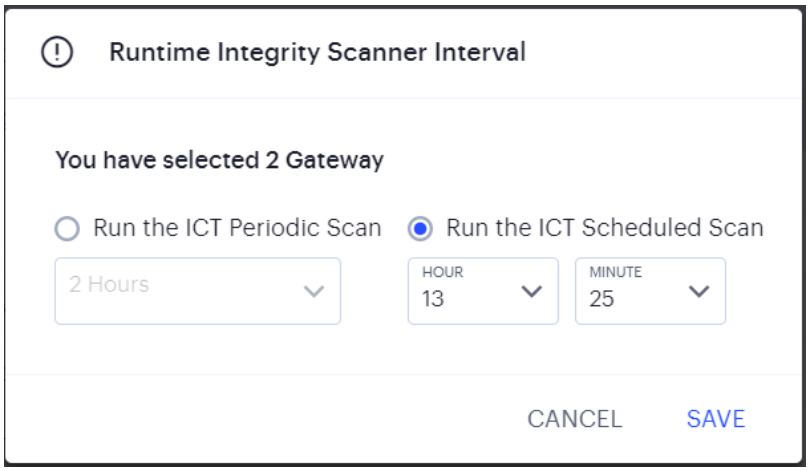


FIGURE 7.12 : Integrity Scanner Interval

Ivanti Connect Secure Cluster Management

Clusters define a collection of servers that operate as if they were a single machine. A cluster pair is used to refer to a cluster of two units and a multiunit cluster refers to a cluster of more than two units. Once two or more units are joined in a cluster, they act as one unit.

Creating ICS Cluster

1. Log into the nSA as a Tenant Admin.
2. From the ICS menu, click **Gateways > Gateways List**.
3. In the Gateways List page, click **Create** and then select **ICS Cluster**.

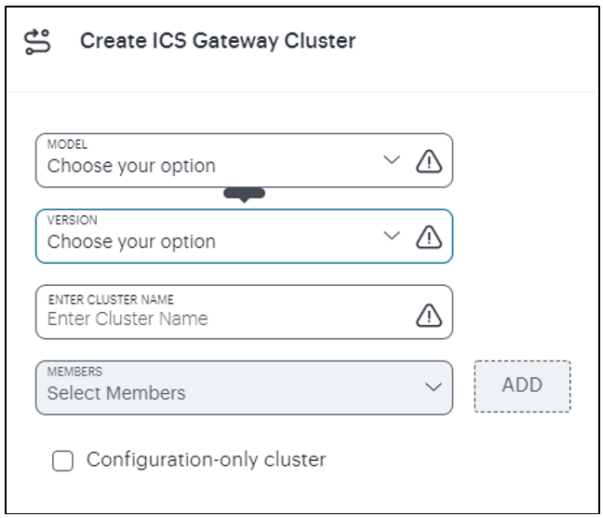


FIGURE 8.1 : Create cluster

4. Select the **ISA Model**.
5. Select the **Gateway Version**.

6. Enter a unique **Cluster Name**.

   Note: The name should be maximum 15 characters, only alphanumeric and hyphens are allowed between characters, and **must start with a letter**.

7. Select a member node and click **Add** to add the nodes.
8. Enable **Configuration Only Cluster** to limit data transfer between cluster nodes. User and session specific limits are only enforced on the node and not across the cluster.
9. Click **Create Cluster**.

   An Active/Active cluster is created by default.

Editing a Cluster

To edit a cluster:

1. In the Gateways List page, click the cluster name that you want to edit.
2. In the Cluster details page, click the context menu icon present at the top-right of the page to access the options applicable to the selected Cluster.
3. Click **Edit Cluster**.
4. Add additional Gateways to the cluster and then click **Update Cluster**.

Removing a Cluster

To remove a cluster:

1. In the Gateways List page, click the cluster name that you want to delete.
2. In the Cluster details page, click the context menu icon present at the top-right of the page to access the options applicable to the selected Cluster.
3. Click **Delete Cluster only** to remove only the cluster and retain the Gateways, or click **Delete Cluster and Gateways** to remove the Cluster along with the Gateways.
4. Click **Confirm** in the confirmation box.

Deploying an Active/Active Cluster

An active/active clustering provides high availability and load balancing when deployed with an external load balancer. An active/active cluster deployment requires an external device to distribute the load among the members because the cluster does not have a VIP address. The load balancing devices are equipped with algorithms that balance the load, as well as detect whether a device is down.

Active/active configuration allows increased aggregate system Clustering Property Settings throughput as well as seamless failover, which is achieved by state synchronization between the two devices for all the configurations so that the devices are virtually identical.

Configuring an Active/Active Cluster

When you add members, you are prompted for settings unique to the member, such as the name and IP address configuration for the internal and external interfaces. A few additional settings are also unique, namely the management port and VLAN port settings, so you add these manually after the add node procedure that follows, but before the join cluster operation.

To configure Active/Active cluster:

1. Log into the nSA as a Tenant Admin.
2. From the ICS menu, click **Gateways > Gateways List**.
3. In the Gateways List page, select the cluster that you want to configure.

   The cluster status page appears.
4. From the ICS menu, select **Gateways List > Properties**.

   The cluster configuration page appears.

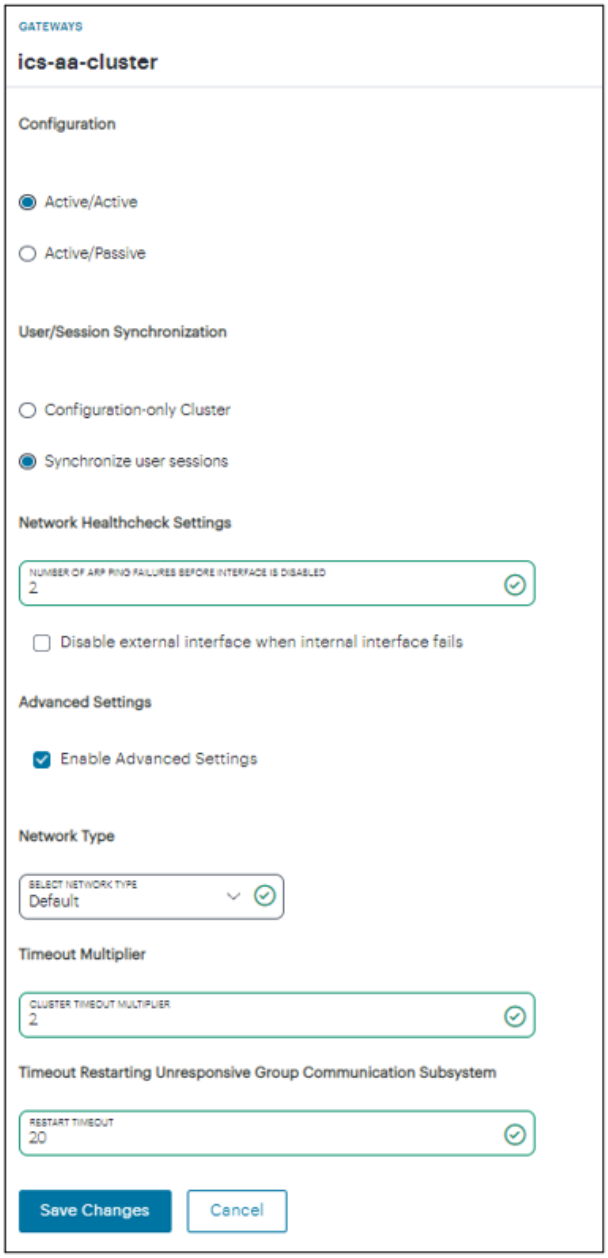


FIGURE 8.2 : Configure Active/Active cluster

5. Select **Active/Active** option to run a cluster pair in active/active mode.
6. Select **Configuration only cluster** option to disable synchronization of session data and to replicate only configuration data and user records (for example, web bookmarks, NFS and windows shared files, terminal servers, telnet sessions, SAM, preferences, and passwords).

   Enabling this option limits data transfers between the cluster nodes. User and Session specific limits are only enforced on the node and not across the cluster.
7. Select **Synchronize user sessions** option to synchronize all user session information (for example, instances of access to intranet services) among all the devices in the cluster.

8. Specify the number of ARP ping failures allowed before the internal interface is disabled.
9. Select **Disable external interface when internal interface fails** to disable the external interface of the device if the internal interface fails.
10. Select the **Advanced Settings** check box to specify the timeouts for the underlying cluster system. Do not change any values under this setting unless instructed to do so by Ivanti Technical Support.
11. Select the appropriate **Network Type**. Network type selection controls the timeouts used by the underlying cluster system. Change this value only when you observe repeated cluster partitions that may be related to long network delays or significant load in any of the cluster nodes.
12. Default cluster timeouts have been picked to be optimal for typical cluster installations. Administrators have the ability to adjust the cluster timeouts over a linear scale of 1-20. Smaller timeouts result in faster failure detection. Larger timeouts minimize the risk of cluster splits during transient network glitches. The system can be instructed to pick a reasonable default for the current cluster configuration by specifying a value of 0.
13. Click **Save Changes**.

Deploying an Active/Passive Cluster

Active/passive clustering is supported only if the members of the cluster pair are in the same subnet because the VIP address must be shared by both the members. An active/passive cluster configuration provides high availability. Active/passive configurations allows seamless failover without the need to set up any external equipment, which is achieved by state synchronization between the two devices for all the configurations so that the devices are virtually identical.

The Ivanti access control service uses a virtual IP (VIP) address to address the cluster pair in addition to addressing each device. The IP address takeover (IPAT) approach is used for the VIP address. If the active node fails, the passive node takes over the VIP address and sends a gratuitous Address Resolution Protocol (ARP) message notifying other networking devices that it now owns the VIP address. You should check that other devices in your network, especially the next-hop gateways, will honor the gratuitous ARP messages.

Configuring an Active/Passive Cluster

Active/passive clustering is supported only if the members of the cluster pair are in the same subnet because the VIP address must be shared by both the members. An active/passive cluster configuration provides high availability. Active/passive configurations allows seamless failover without the need to set up any external equipment, which is achieved by state synchronization between the two devices for all the configurations so that the devices are virtually identical.

The Ivanti access control service uses a virtual IP (VIP) address to address the cluster pair in addition to addressing each device. The IP address takeover (IPAT) approach is used for the VIP address. If the active node fails, the passive node takes over the VIP address and sends a gratuitous Address Resolution Protocol (ARP) message notifying other networking devices that it now owns the VIP address. You should check that other devices in your network, especially the next-hop gateways, will honor the gratuitous ARP messages.

To configure Active/Passive cluster:

1. Log into the nSA as a Tenant Admin.
2. From the ICS menu, click **Gateways > Gateways List**.
3. In the Gateways List page, select the cluster that you want to configure.

   The cluster status page appears.
4. From the ICS menu, select **Gateways List > Properties**.

   The cluster configuration page appears.

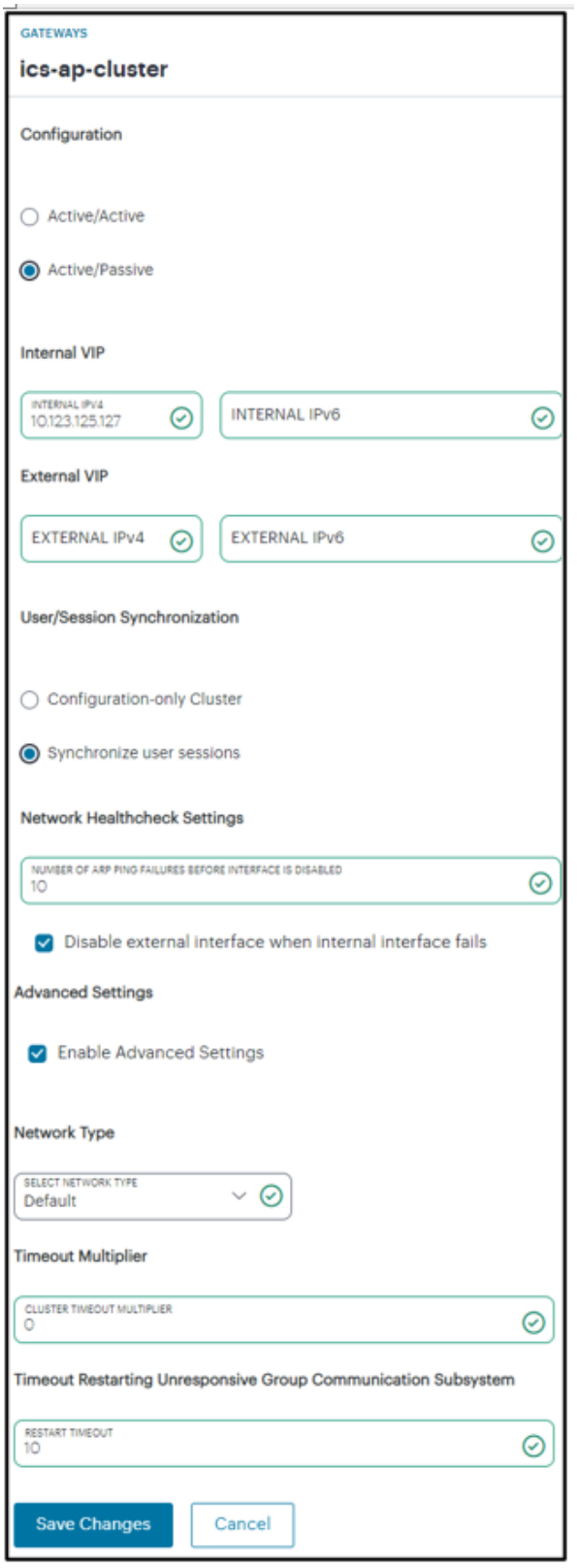


FIGURE 8.3 : Configure Active/Passive cluster

5. Select **Active/Passive** option to run a cluster pair in active/passive mode.
6. Then, specify an internal VIP (virtual IP address) and an external VIP if the

external port is enabled.

7. Select **Configuration only cluster** option to disable synchronization of session data and to replicate only configuration data and user records (for example, web bookmarks, NFS and windows shared files, terminal servers, telnet sessions, SAM, preferences, and passwords).

   Enabling this option limits data transfers between the cluster nodes. User and Session specific limits are only enforced on the node and not across the cluster.

8. Select **Synchronize user sessions** option to synchronize all user session information (for example, instances of access to intranet services) among all the devices in the cluster.
9. Specify the number of ARP ping failures allowed before the internal interface is disabled.
10. Select **Disable external interface when internal interface fails** to disable the external interface of the device if the internal interface fails.
11. Select the **Advanced Settings** check box to specify the timeouts for the underlying cluster system. Do not change any values under this setting unless instructed to do so by Ivanti Technical Support.
12. Select the appropriate **Network Type**. Network type selection controls the timeouts used by the underlying cluster system. Change this value only when you observe repeated cluster partitions that may be related to long network delays or significant load in any of the cluster nodes.
13. Default cluster timeouts have been picked to be optimal for typical cluster installations. Administrators have the ability to adjust the cluster timeouts over a linear scale of 1-20. Smaller timeouts result in faster failure detection. Larger timeouts minimize the risk of cluster splits during transient network glitches. The system can be instructed to pick a reasonable default for the current cluster configuration by specifying a value of 0.
14. Click **Save Changes**.

Multinode Configuration Management

Introduction

The configuration templates allow multiple ICS devices to be deployed following a single base configuration. With config templates, it makes admin users to easily roll out changes to all the gateways and maintain consistency across all the gateways.

It is most useful in cases where a large number of gateways exist that share a common configuration. With configuration templates, Admin's can easily manage multiple nodes using the templates based on their requirement.

For example, for enterprise customers who maintain multiple gateways such as a retail deployment with many stores, or a global enterprise having branches in many locations across globe. In these scenarios, the features can be synchronized to all the gateways in various locations using the configuration template.

Note: Ensure that the sample policy name does not exist in the individual gateway while creating configurations using the configuration templates to avoid any configuration conflicts.

Adding Configuration Template

The *Configuration* page enables you to Create Config Template.

To add a Template:

1. Log into the nSA as a Tenant Admin. See *Logging in to Ivanti Neurons for Secure Access* (page 5).
2. From the ICS menu, click **Gateways**, then click **Multinode Configuration**, and then select **Configuration Template**.

   The *Configuration Template* page appears, showing the full list of Templates currently configured on the nSA.
3. Click *Create Config Template* on top right corner of the screen.

   The *Create Configuration Template* page appears, showing the settings to be filled for the Template:

FIGURE 9.1 : Creating a Template

4. On this page, enter the following settings:

TABLE 9.1 : Template Settings

Setting	Description
Template Name	Enter a unique name for this Configuration Template.
Version	Select the Configuration Template version number.
Gateway	Select the Gateways that you want to be part of this template. A particular gateway can be part of any one Configuration Template, and not part of multiple Configuration Templates.
Gateway clusters	Select the Clusters that you want to be part of this template.

5. Enter any required Template details, then click **Create Template**.

   The created Configuration Template gets listed under Config Templates List. To add more Gateways/Clusters to this Configuration Template, see *Editing Configuration Template* (page 146).

Viewing Configuration Templates

To view, configure and check the status of your configured Templates, use the **Gateways > Configuration Templates** section of the nSA Tenant Admin portal. The pages in this section remain inactive until you select a Config Template.

To view information for a Config Template:

1. Log into the nSA as a Tenant Admin.
2. From the ICS menu, click **Gateways**, then click **Multinode Configuration**, and then select **Configuration Template**.

   The *Config Templates List* page appears with the following details: Configuration Template name, Configuration Template version and features managed by the Configuration Template

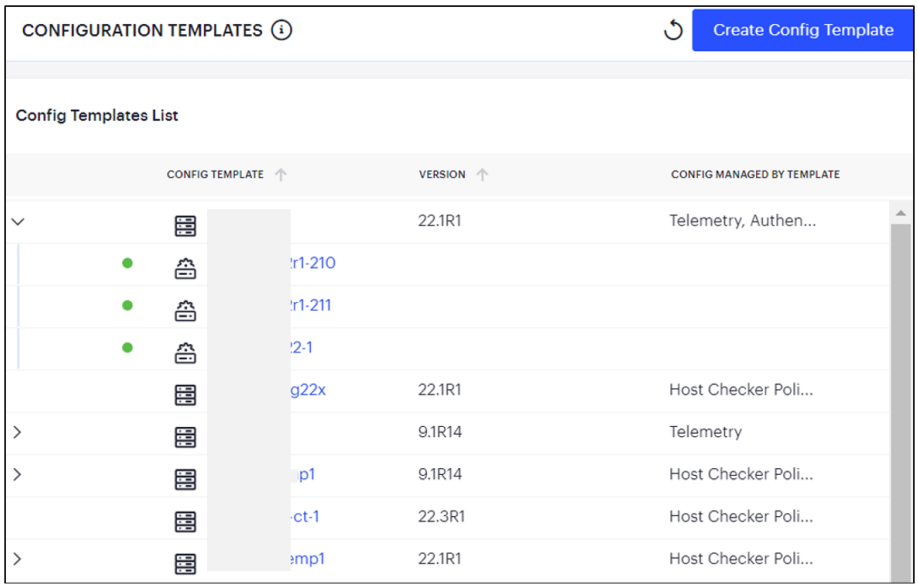
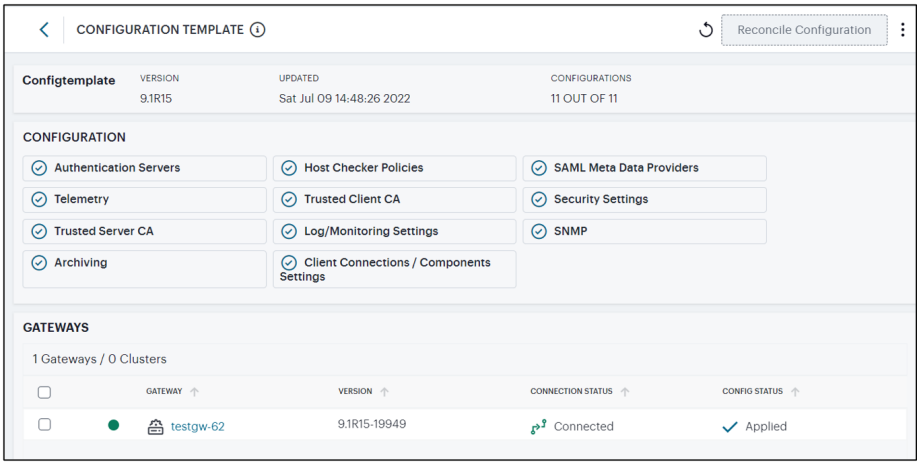


FIGURE 9.2 : Viewing All Templates

3. Select a Template from the list to view the *Template Overview* page.



This page provides the following details:

- Configuration Template name
- Configuration Template version
- Last updated date and time
- Number of features managed by the Configuration Template
- Configured features shown with blue check mark
- Details of Gateways and Clusters managed by the Configuration Template:

- Gateway/Cluster name
- Configuration Template version
- Connection status - Connected / Disconnected
- Configuration status - “Pending” if a Gateway/Cluster is newly added and the configuration is not synchronized yet; “Applied” if configuration is successfully synchronized to a Gateway/Cluster; “Failure” if the configuration synchronization failed.

4. To view the details of different Templates, select **Configuration Template** and choose an alternative instance.
5. Use the context menu icon at the top-right to access the options applicable to the selected Template.

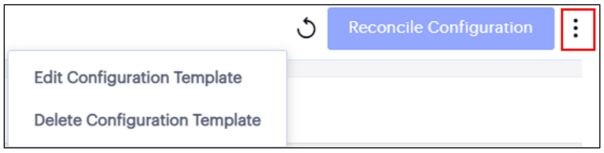


FIGURE 9.3 : Edit a Template

- **Edit Configuration Template**: Use this to add additional Gateways and Clusters, or remove existing Gateways and Clusters.
- **Delete Configuration Template**: Use this to delete the Configuration Template. When you delete a Configuration Template, only the template is removed. The features synchronized by the Configuration Template to the Gateways/Clusters will not be removed from the Gateways/Clusters.

Viewing the Configuration Template Supported Features

The Configuration Template supports the following features:

- Authentication Server, see *Configuring Authentication Servers* (page 181)
- Host Checker Policies, see *Configuring Host Checker Policy* (page 159)
- SAML Metadata Provider, see *Configuring SAML* (page 155)
- Telemetry, see *Telemetry Settings* (page 158)
- Trusted Client CA, see *Configuring Certificates* (page 153)
- Security Settings, see *System Configuration* (page 203).
- Trusted Server CA, see *System Configuration* (page 203).
- Log/Monitoring Settings, see *System Configuration* (page 203).
- SNMP, see *System Configuration* (page 203).
- Archiving, see *Archiving Servers* (page 200)
- Client Connections/Components Settings, see *Users Configuration* (page 365).

Select the Configuration Template from the list. The following are enabled on the ICS menu:

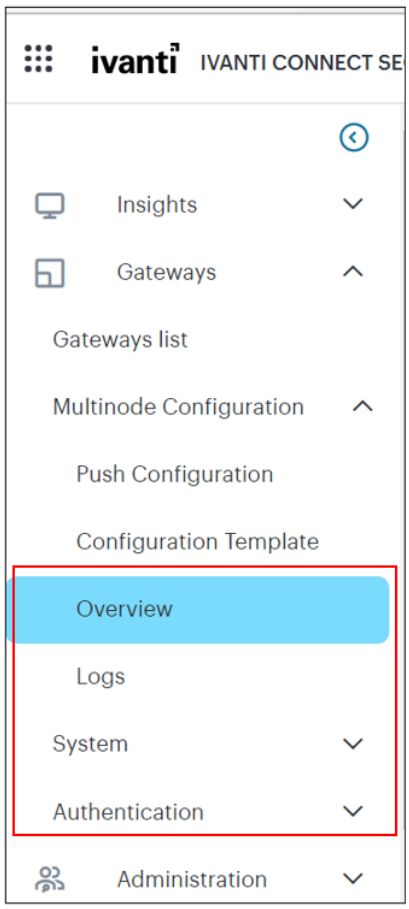


FIGURE 9.4 : Configuration Template Features

Editing Configuration Template

The *Configuration* page enables you to edit the selected Template configuration. Using this page, you can add more Gateways/Clusters to the template or remove existing Gateways/Clusters from the template.

When you register a new Gateway and add it to the existing Configuration Template, the group configuration is synchronized to the newly registered Gateway. This is called as “Auto reconciliation”.

To edit a Template:

1. Log into the nSA as a Tenant Admin.
2. From the ICS menu, click **Gateways**, then click **Multinode Configuration**, and then select **Configuration Template**.

   The *Configuration Template* page appears, showing the full list of Templates currently configured on the nSA.
3. Select the required Template.

The *Template Overview* page appears for the selected Template.

4. Click **Edit Configuration Template** from the context menu at the top-right.

   The *Edit Configuration Template* page appears, showing the current settings for the selected Template:

FIGURE 9.5 : Editing a Template

   On this page, you cannot modify the Configuration Template name and version. You can only add more Gateways/Clusters to the template.

5. Click **Update Template**.

Reconcile Configuration

If an admin makes changes to the features in a Gateway managed by the configuration template, then there will be a conflict. To resolve the conflict, use the Reconcile Configuration option. It will overwrite the Gateway configuration with the template configuration.

To Reconcile the configuration

1. On the Template Configuration page select one or more Gateways and click **Reconcile Configuration**.

   A prompt “Are you sure you want to reconcile all the selected gateways with group configuration?” appears.

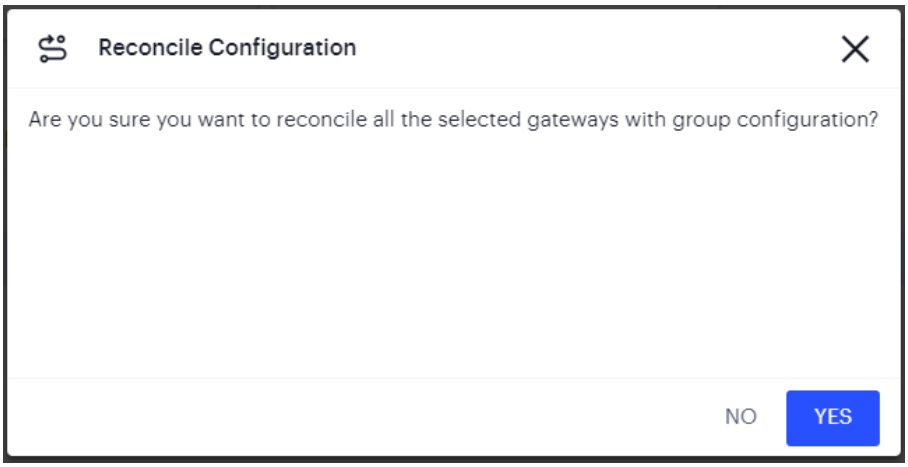


FIGURE 9.6 : Reconcile Configuration

2. Click **Yes**. It overwrites the configuration of all the selected Gateways with the group configuration.

Config Synchronization

The config synchronization feature supports simple configuration management across an enterprise without requiring you to deploy the systems as a cluster. You synchronize a partial configuration from the running configuration on the source system to the running configuration on one or more target systems.

To configure config synchronization rule:

1. Log into the nSA as a Tenant Admin.
2. From the ICS menu, click **Gateways**, then click **Multinode Configuration** and then select **Config Synchronization**.
3. In the Config Synchronization page, click **Create Config Sync Rule**.

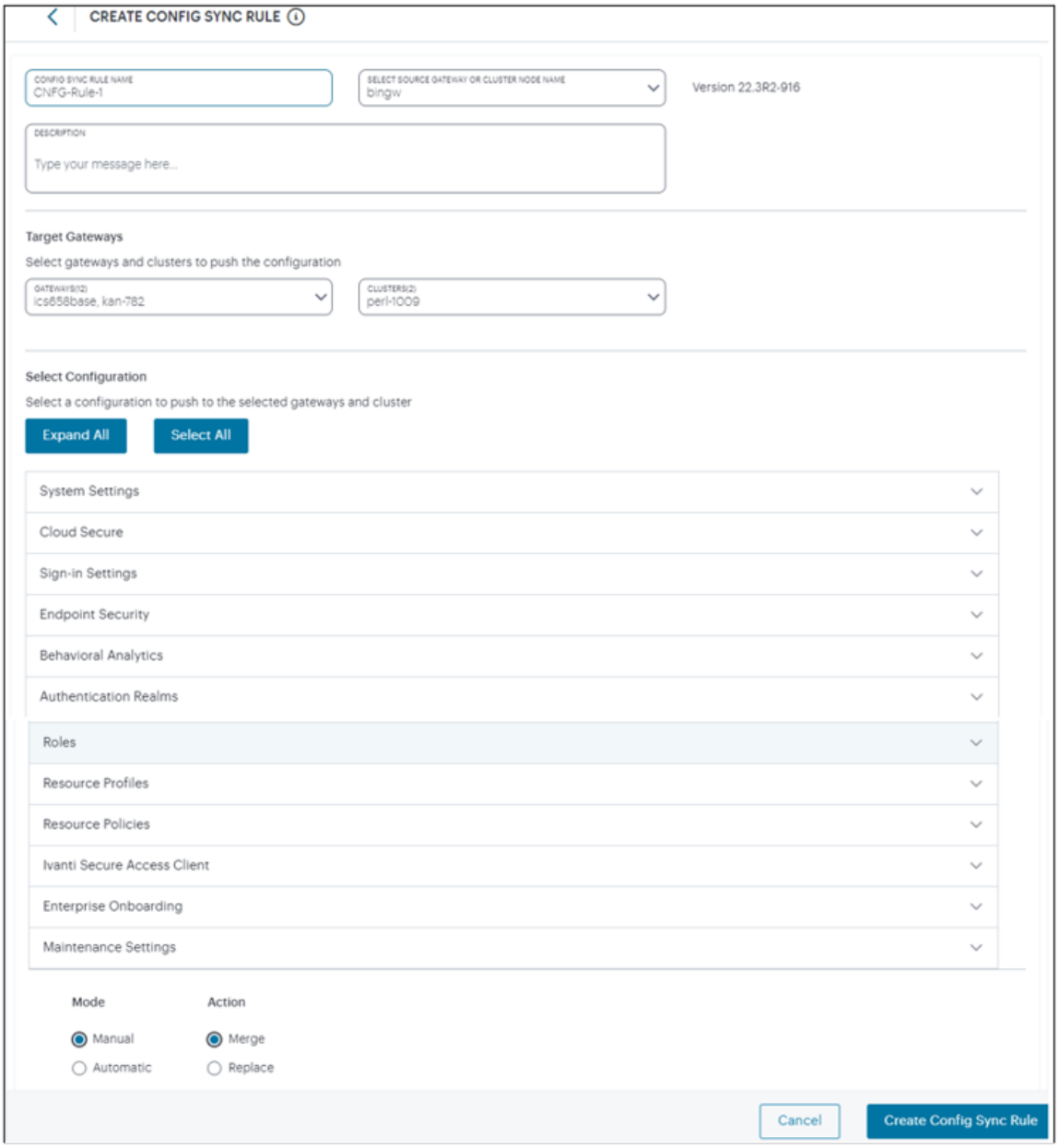


FIGURE 9.7 : Create Config Sync Rule

4. Enter **Config Sync Rule Name**, select a Gateway or Cluster, and enter **Description**.
5. Under Target Gateways, select Gateways and Clusters to synchronize.
6. Under Select Configuration, select a configuration to synchronize to the target Gateways and Clusters.
7. You can expand all the configurations using **Expand All** and select all the configurations using **Select All**. You can expand each group and select the required settings.
8. Select the Mode: **Manual** or **Automatic**. Automatic option will sync the targets whenever there is change in source configuration.

9. Select the Action: **Merge** or **Replace**. The Merge option applies only changes in source to the targets, whereas the Replace option replaces the targets configuration with the source configuration.
10. Click **Create Config Sync Rule**.

    The config sync rule gets listed in the Config Synchronization page.

To edit an existing config sync rule:

1. In the Config Synchronization page, click on the config sync rule name that you want to edit.
2. In the Update Config Sync Rule page, make the necessary changes. You cannot modify the rule name and source Gateway or Cluster.
3. Click **Update Config Sync Rule**.

To delete one or more config sync rule(s):

1. In the Config Synchronization page, select the check boxes next to the config sync rule names that you want to delete.
2. Click the Delete icon.
3. Click **OK** to confirm the deletion.

The following alerts are generated:

- Config Sync Rule Deleted - This alert is generated when the Config Sync rule is deleted.
- Config Sync Rule Updated - This alert is generated when the Config Sync rule is updated.
- Config Sync Target Cluster Deleted - This alert is generated when the Target Cluster, which is in the Config Sync rule, gets deleted.

Viewing Template Logs

The *Logs* page enables you to view the Admin logs of the Gateways for the selected Template.

To view Templates logs:

1. Log into the nSA as a Tenant Admin.
2. From the ICS menu, click **Gateways**, then click **Multinode Configuration**, and then select **Configuration Template**.

   The *Configuration Template* page appears, showing the full list of Templates currently configured on the nSA.
3. Select the required Template.

   The *Overview* page appears for the selected Template.

4. From the ICS menu, click **Gateways**, then click **Multinode Configuration**, and then select **Configuration Template > (one template) > Logs**.

   The *Template Logs* page appears showing the Admin logs.

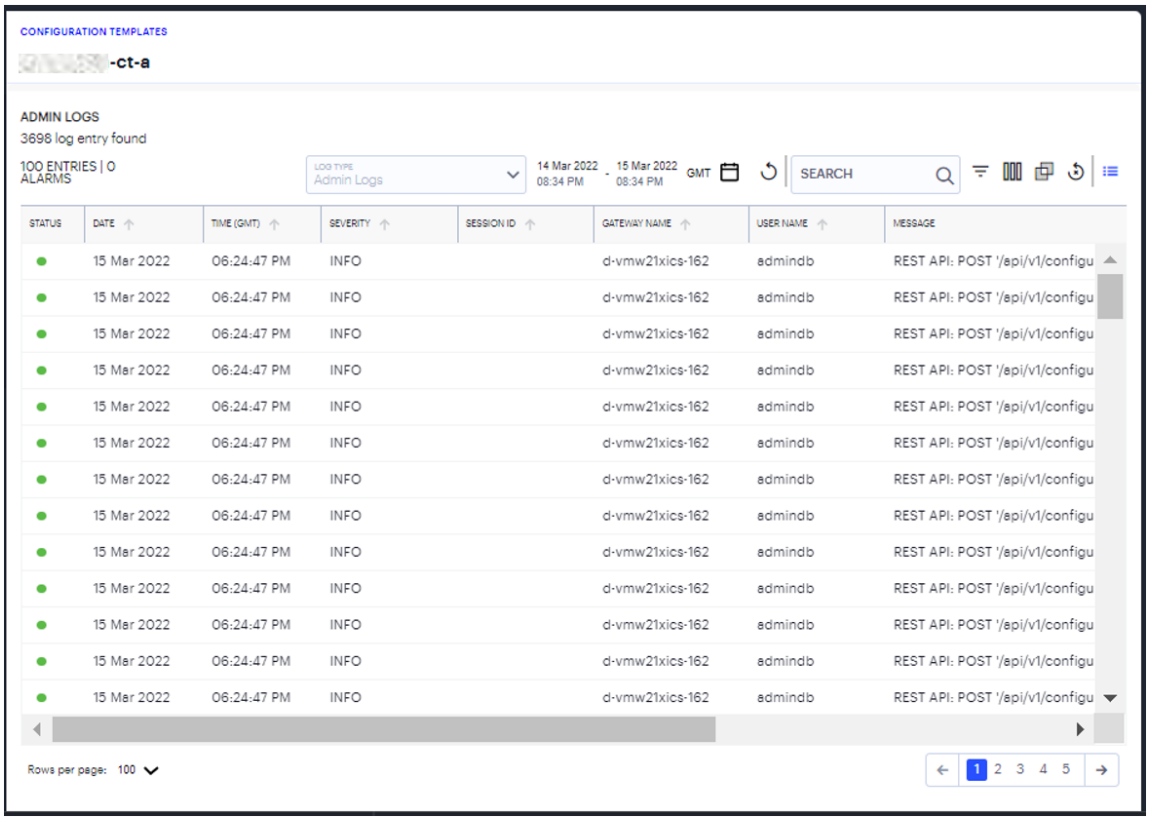


FIGURE 9.8 : Gateways Admin Logs

- To set a time period or range for the log results:
  1. Click the calendar to show the selector:

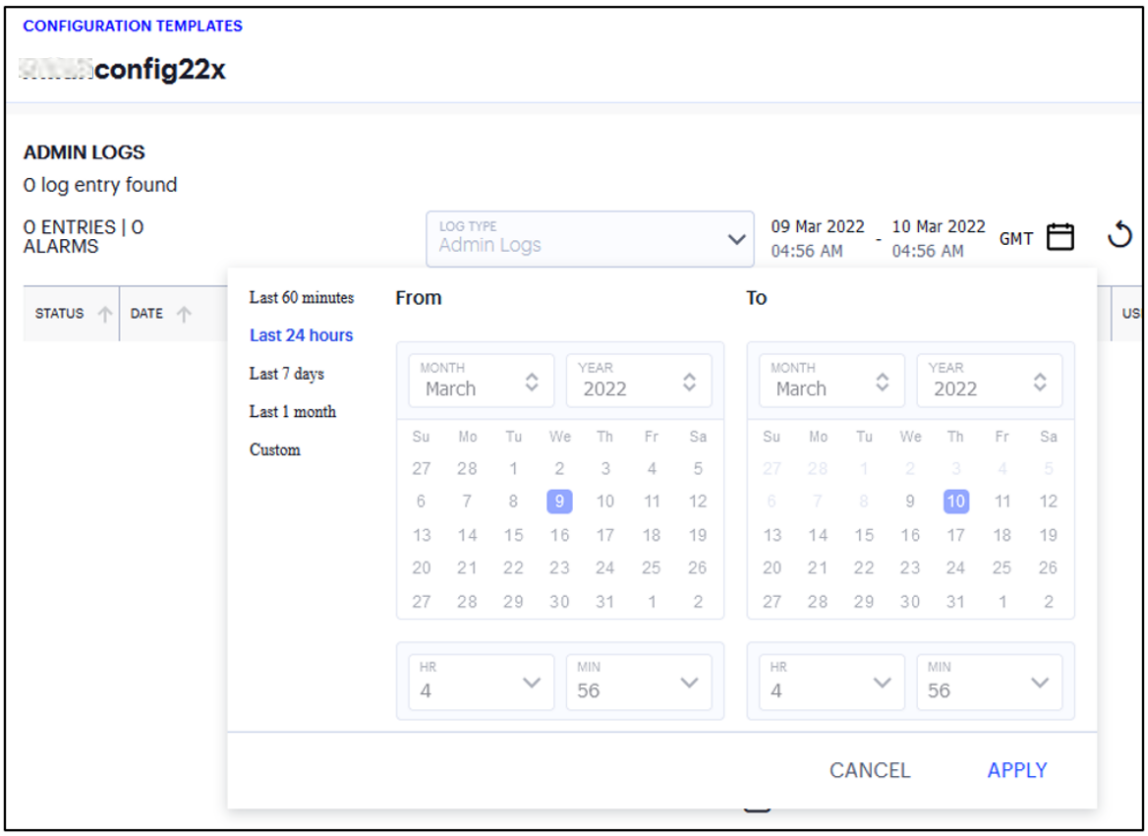


FIGURE 9.9 : Setting a log time period

2. Set the time period you want to view using the available ranges at the top-left. Choose from:
   - Last 60 minutes
   - Last 24 hours (default)
   - Last 7 days
   - Last 1 month
   - Custom

   For **Custom**, set a specific *From* and *To* to denote the start and end of your custom date/time range.

   Note: The custom date/time calendar controls are enabled for only the **Custom** option. However, the calendar continues to identify the applicable start and end date-time for all predefined time periods.

3. To apply your changes, click **Apply**. The selected time period is displayed in the filter bar and data on the page updates accordingly.

- Choose the Advanced filter icon to filter the logs based on Gateway name, User name, Severity, Log Message, and so on.

FIGURE 9.10 : Applying a filter to the log display

Configuring Certificates

A trusted client CA is a CA that you deem trusted by adding it to the trusted client CA store. The system trusts any certificate issued by that CA. To use client CA certificates, you must install and enable the proper certificates. Additionally, you must install the corresponding client-side certificates in your users' Web browsers.

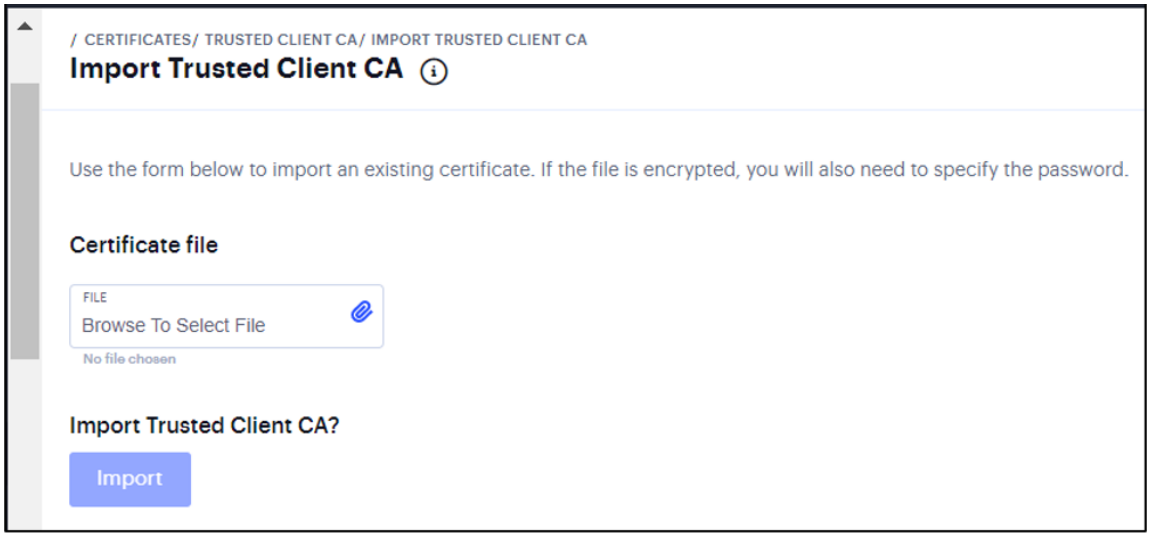
Importing a Trusted Client CA Certificate

To import a trusted client CA certificate:

1. Log into the nSA as a Tenant Admin.
2. From the ICS menu, click **Gateways**, then click **Multinode Configuration**, and then select **Configuration Template**.

   The *Configuration Template* page appears, showing the full list of Templates currently configured on the nSA.
3. Select the required Template.

   The *Overview* page appears for the selected Template.
4. Select **System > Configuration > Certificates > Trusted Client CAs** to display the configuration page.
5. Click **Import CA Certificate** to display the configuration page.



Import Trusted Client CA

6. Browse to the certificate file, select it, and click **Import Certificate** to complete the import operation.

Configuring Auto-Importing of Client Certificates

To enable auto-importing:

1. Select **System > Configuration > Certificates > Trusted Client CAs**.
2. Click the **Auto-Import Options** button to display the options.

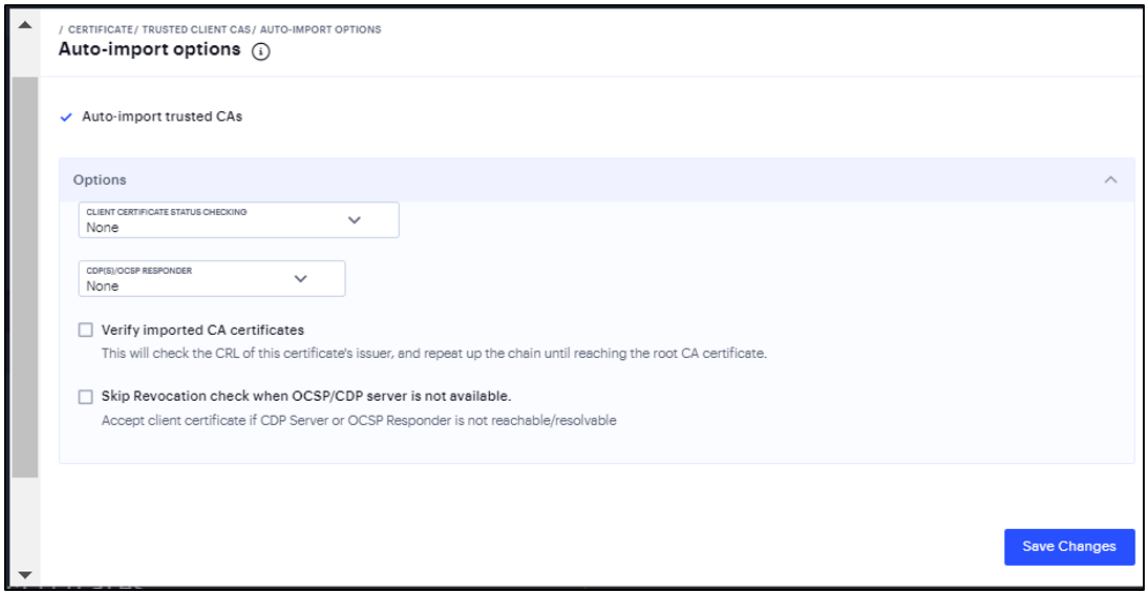


FIGURE 9.11 : Auto-Import Trusted CAs

3. Complete the configuration.
    - Select **Auto-import trusted CAs** option to enable auto-import and display its configuration settings.
    - Select a method to validate the trusted client certificate.
    - Select the location of the responder value.
    - Select **Skip Revocation check when OCSP/CDP server is not available** option to instruct ICS to skip revocation check and accept end user certificates when either OCSP server or CDP server is not accessible over the network.

Configuring a Proxy Server for CRL Downloads and OCSP Status Checks

You can configure the system to send CRL download requests and OCSP status checks to the proxy server and collect the response. You might want to do this if you deploy proxy server to control access to the Internet.

To configure a proxy server:

1. Select **System > Configuration > Certificates > Trusted Client CAs**.
2. Click **Proxy Settings** to display the page.

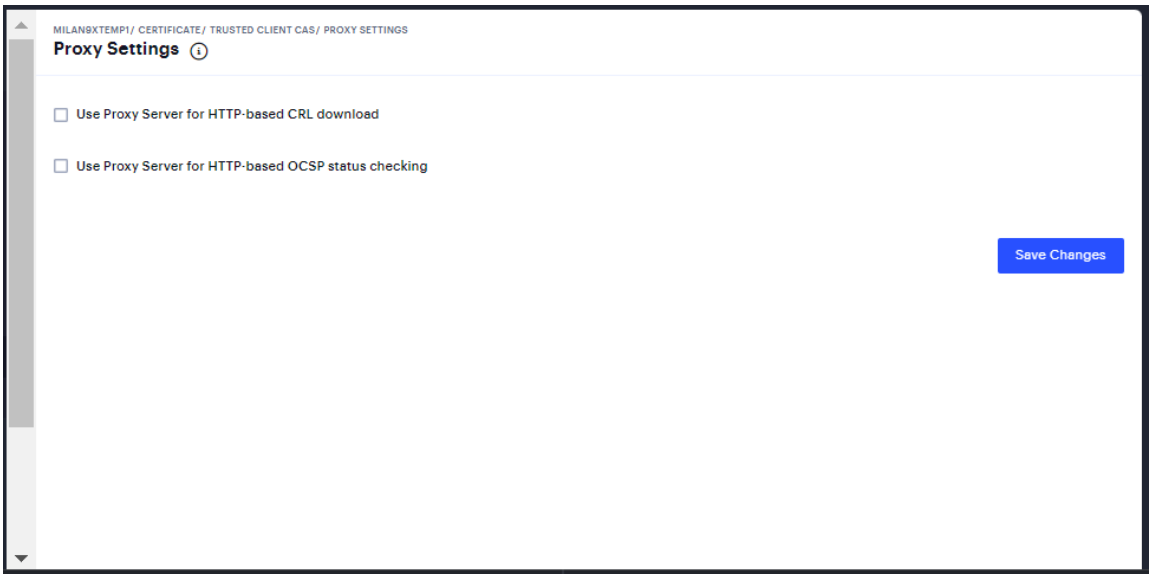


FIGURE 9.12 : Proxy Settings

3. Complete the configuration and save the configuration.
    - Select **Use Proxy Server for HTTP-based CRL download** to enable the CRL operations to use a proxy server.
    - Select **Use Proxy Server for HTTP-based OCSP status checking** to enable the OCSP operations to use a proxy server.

Configuring SAML

In a SAML deployment, the system can act as a SAML service provider, a SAML identity provider, or both.

Managing SAML Metadata Files

You use the System > Configuration > SAML pages to maintain a table of SAML metadata files for the SAML service providers and identity providers in your network.

To add metadata files:

1. Log into the nSA as a Tenant Admin.
2. From the ICS menu, click **Gateways**, then click **Multinode Configuration**, and then select **Configuration Template**.

   The *Configuration Template* page appears, showing the full list of Templates currently configured on the nSA.
3. Select the required Template.

   The *Overview* page appears for the selected Template.
4. Select **System > Configuration > SAML**.
5. Click the Add icon to display the configuration page.

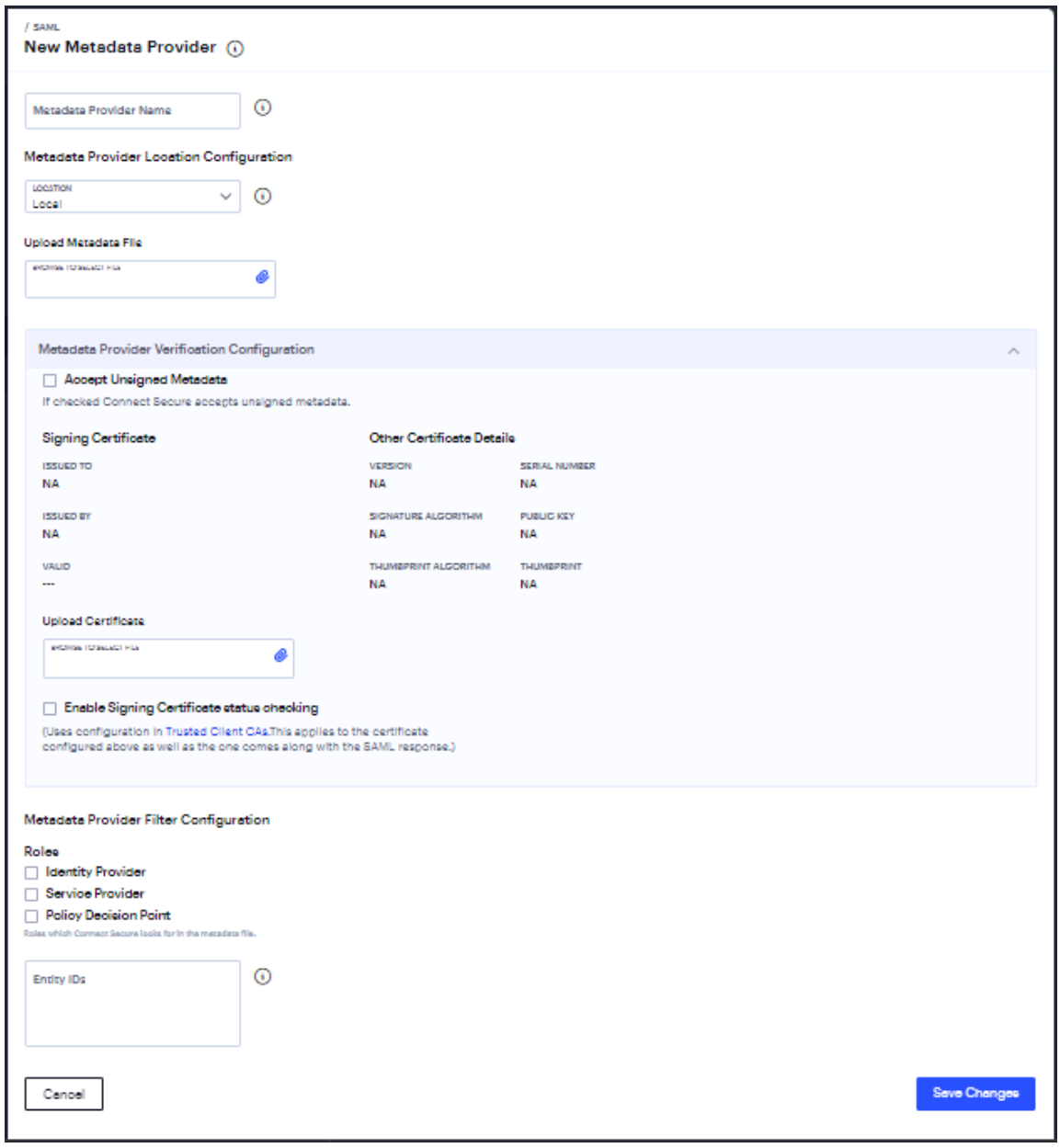


FIGURE 9.13 : SAML Metadata Configuration

6. Complete the configuration.
    - Metadata Provider Location Configuration - Select one of the following methods: Local, Remote
    - Accept Untrusted Server Certificate - Select this option to allow the system to download the metadata file even if the server certificate is not trusted.
    - Accept Unsigned Metadata - If this option is not selected, unsigned metadata is not imported.
    - Signing Certificate - Browse and locate the certificate that verifies the signature in the metadata file.

- Roles - Select whether the metadata file includes configuration details for a SAML service provider, identity provider, or Policy Decision Point.
- Entity IDs To Import - Enter the SAML Entity IDs to import from the metadata files.

7. Save changes. The Metadata provider will be listed in the SAML page.

Telemetry Settings

This page allows you to enable Google Analytics and Crash Analytics.

To configure Telemetry settings:

1. Log into the nSA as a Tenant Admin.
2. From the ICS menu, click **Gateways**, then click **Multinode Configuration**, and then select **Configuration Template**.

   The *Configuration Template* page appears, showing the full list of Templates currently configured on the nSA.
3. Select the required Template.

   The *Overview* page appears for the selected Template.
4. Select **System > Configuration > Telemetry**.
5. In the Telemetry Settings page, select the required check boxes and save changes.
   - Google Analytics helps in tracking how frequently customer is using a particular feature.
   - Crash Analytics collects logs when user faces any crash.

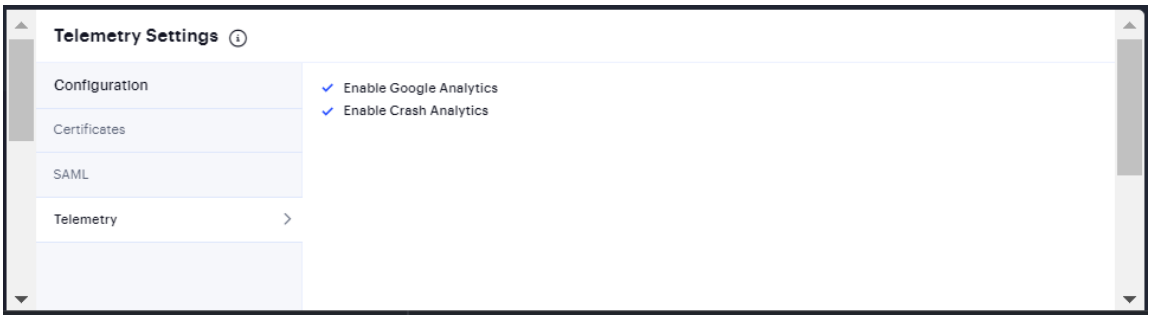


FIGURE 9.14 : Telemetry Settings

Configuring Host Checker Policy

Host Checker is a software component that performs endpoint compliance checks on hosts that connect to the IPS. It supports two types of rules within a policy; predefined and custom. The pre-defined inspection capabilities consist of health and security checks including antivirus versions, antispyware, OS versions, hard disk encryption status and patch checks. The pre-defined rules are provided by OPSWAT and it uses the ESAP plug-in for pre-defined checks.

To configure a Host Checker policy, perform these tasks:

1. Log into the nSA as a Tenant Admin.
2. From the ICS menu, click **Gateways**, then click **Multinode Configuration**, and then select **Configuration Template**.
3. From the Configuration Templates list, select the Configuration Template for which you want to configure Host Checker.
4. From the ICS menu, select **Authentication > Endpoint Security > Host Checker**.

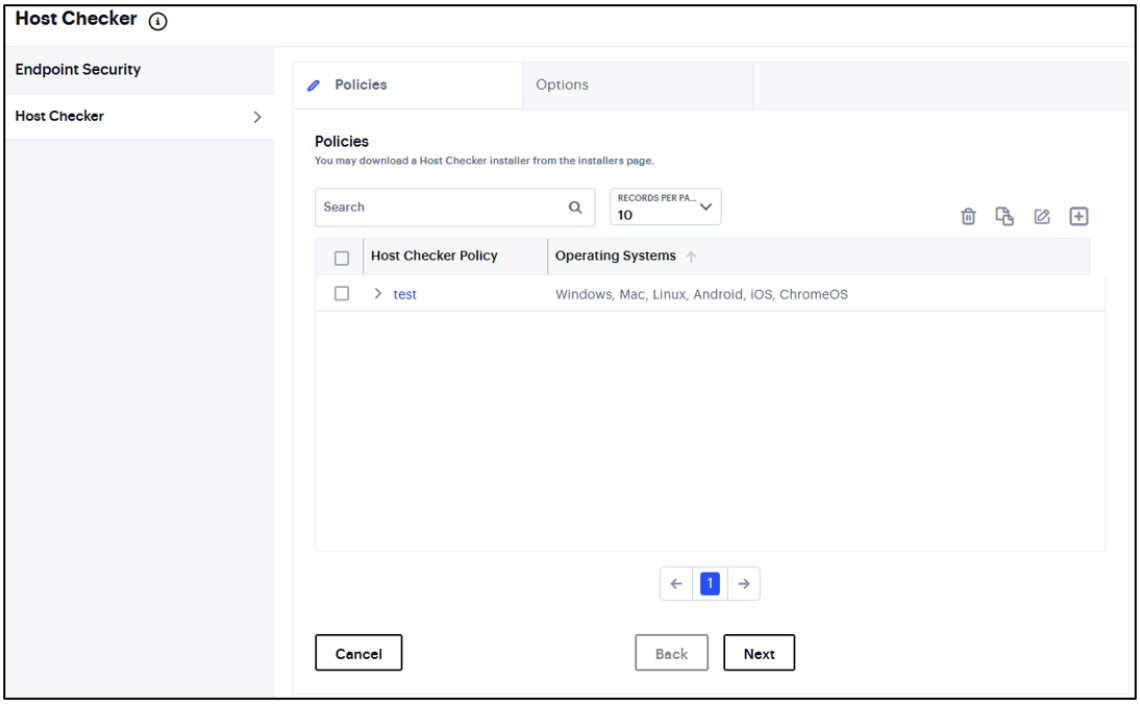


FIGURE 9.15 : Host Checker

5. Under Policies, click the '**+**' icon.
6. Enter a name for the policy and then click **Save Changes**.

   A list of all the added policies is displayed.
7. Create one or more rules to associate with the policy.

   In the **Options** tab, enter time limit for performance check and logout time if the device is inactive.

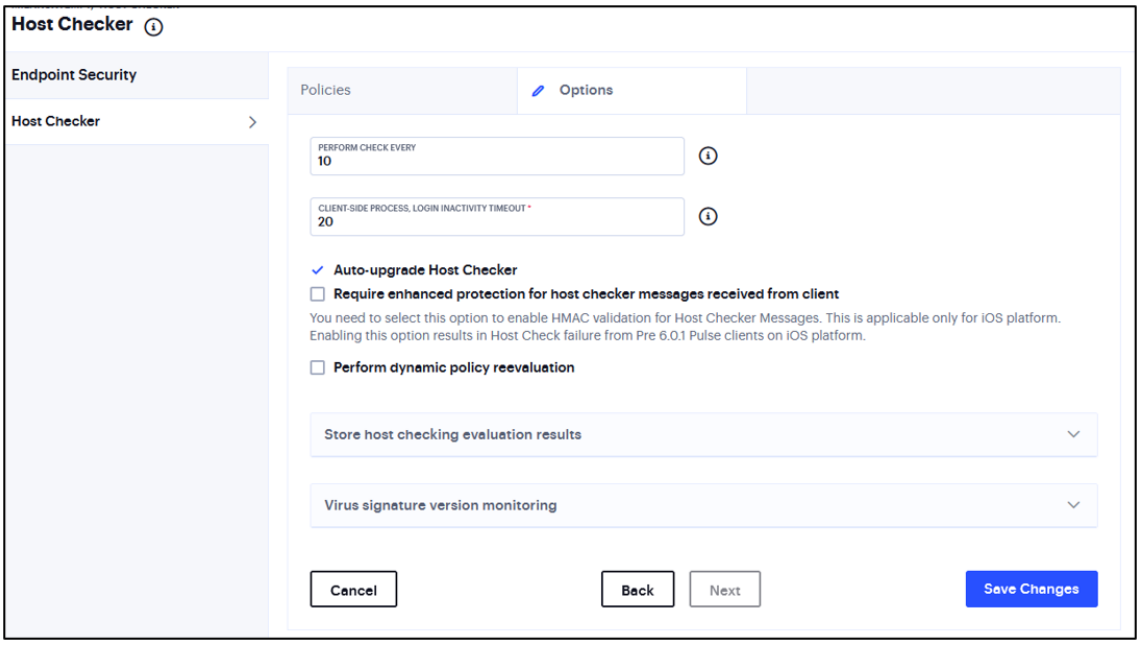


FIGURE 9.16 : Host Checker Options

8. You can select Auto-upgrade Host Checker, Require enhanced protection for host checker messages received from client, and Perform dynamic policy reevaluation.

Note: You need to select this option to enable HMAC validation for Host Checker messages. This is applicable only for iOS platform. Enabling this option results in Host Check failure from Pre 6.0.1 Ivanti Secure Access clients on iOS platform.

---

9. Select **Store Host Checking evaluation results** to cache the result for the certain number of days.
10. Select **Cache results if any of the roles is assigned** or **Cache results only if any of the selected roles are assigned** and select the roles from **Available Roles**.

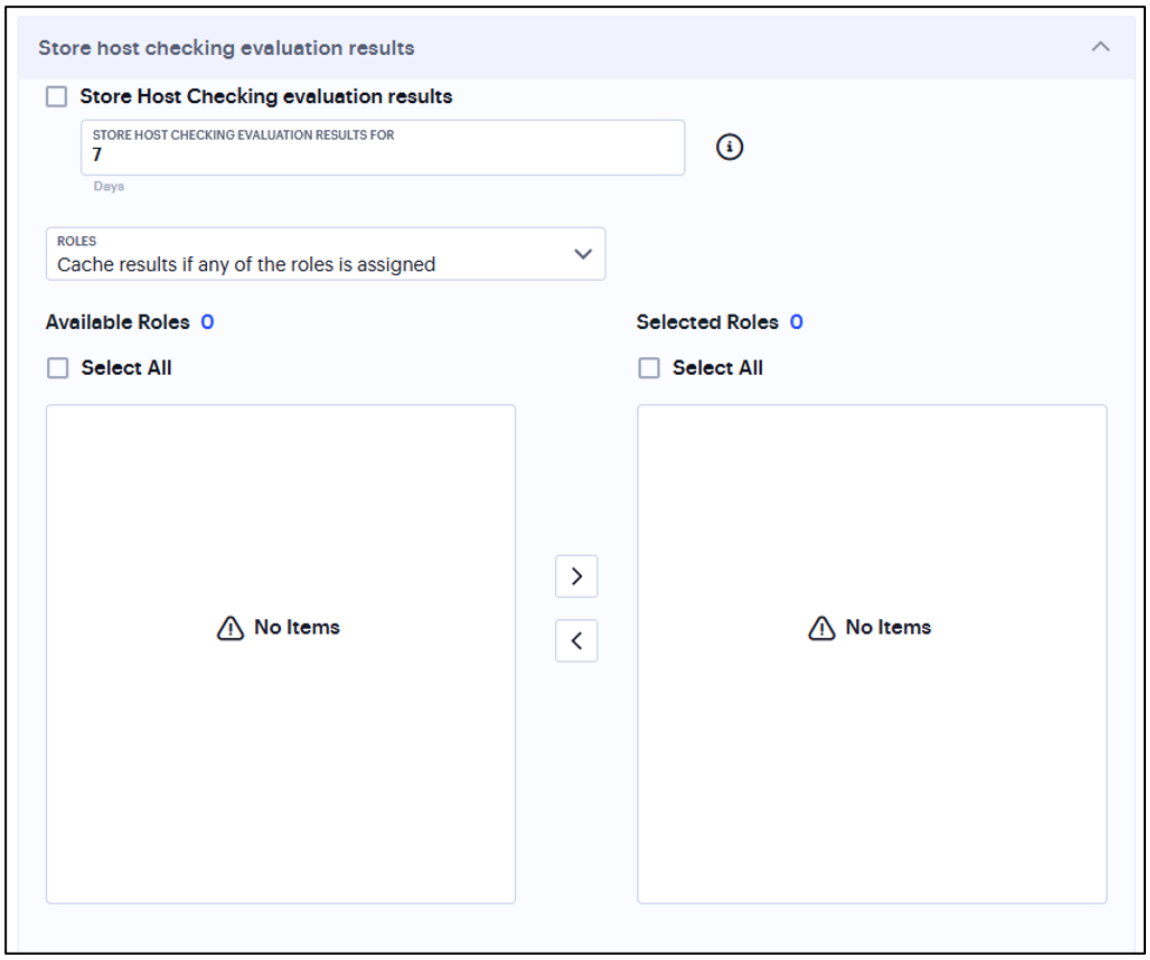


FIGURE 9.17 : Store Host Checking Evaluation Results

11. In Virus signature version monitoring, select **Auto-update virus signatures list**.
    - For Download path, leave the existing URL(s) of the staging site(s) where the current list(s) are stored.
    - For Download interval, specify how often you want the system to automatically import the current list(s).
    - For Username and Password, enter your Connect Secure credentials.
    - To use a proxy server as the auto-update server, select **Use Proxy Server** and provide the proxy server details.

Note: You can also import the virus signatures manually by importing signature list.

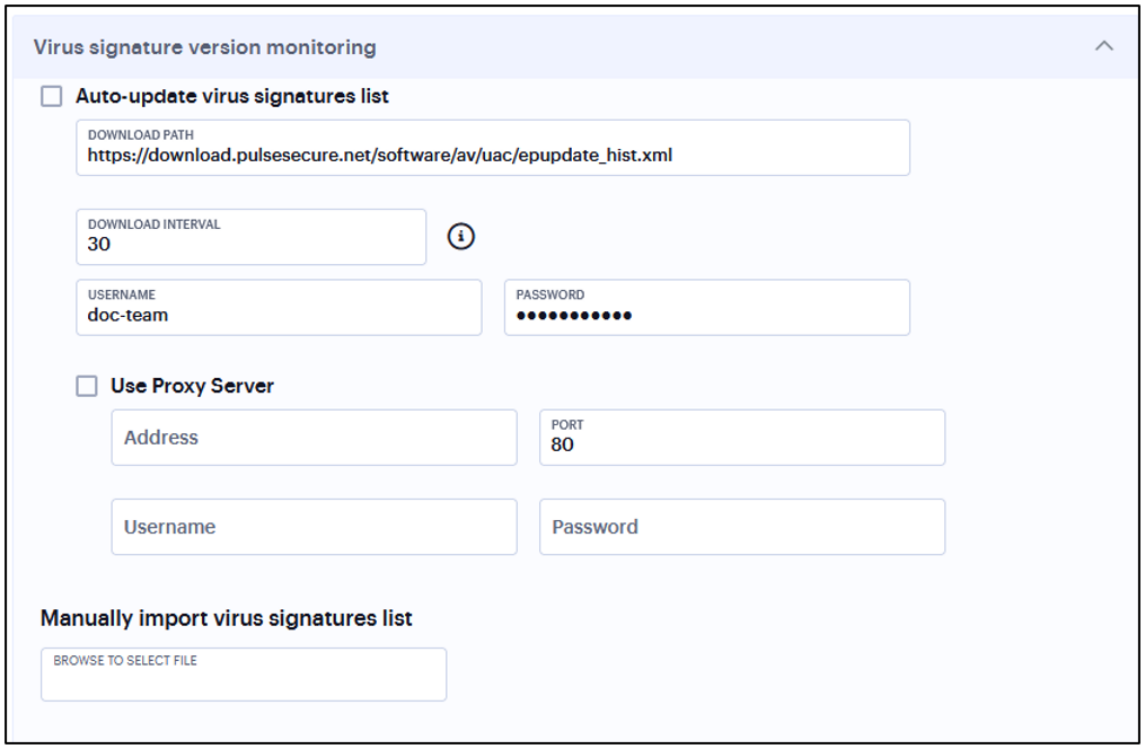


FIGURE 9.18 : Virus Signature Version Monitoring

12. To edit an existing policy, select the corresponding check box and click the Edit icon.
13. To delete one or more policies, select the corresponding check boxes and click the Delete icon.

Checking for Third-Party Applications Using Predefined Rules

Host Checker comes pre-equipped with a vast 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 users' computers in accordance with your specifications. For firewall and antivirus rules, you can specify remediation actions to automatically bring the endpoint into compliance.

Add Rule: Antivirus Rule with Remediation Options

To configure a Predefined Antivirus rule:

1. Select one of the following supported platforms:
   - Windows
   - Mac
2. Enter a Rule Name.
3. Under Criteria, click **Require specific products/vendors**. A new window will open with a list of all of the products that support the feature.
4. Select your vendor(s) and product(s) by using either the **Require any supported product from a specific vendor** or **Require specific products** check box.
5. If your product is supported, select the check box for any or all of the remediation actions that you want to apply.
6. (Optional) Select or clear the check box next to **Successful System Scan must have been performed in the last**, and enter the number of days in the field.
   - If you select this check box, a new option appears. If the remediation action to start an antivirus scan has been successfully begun, you can override the previous check.
7. (Optional) Select or clear the check box next to **Check for the Virus Definition files**. Enter a number between 1 and 20. If you enter 1, the client must have the latest update.
8. (Optional) Select **Monitor this rule for change in result** to continuously monitor the policy compliance of endpoints.

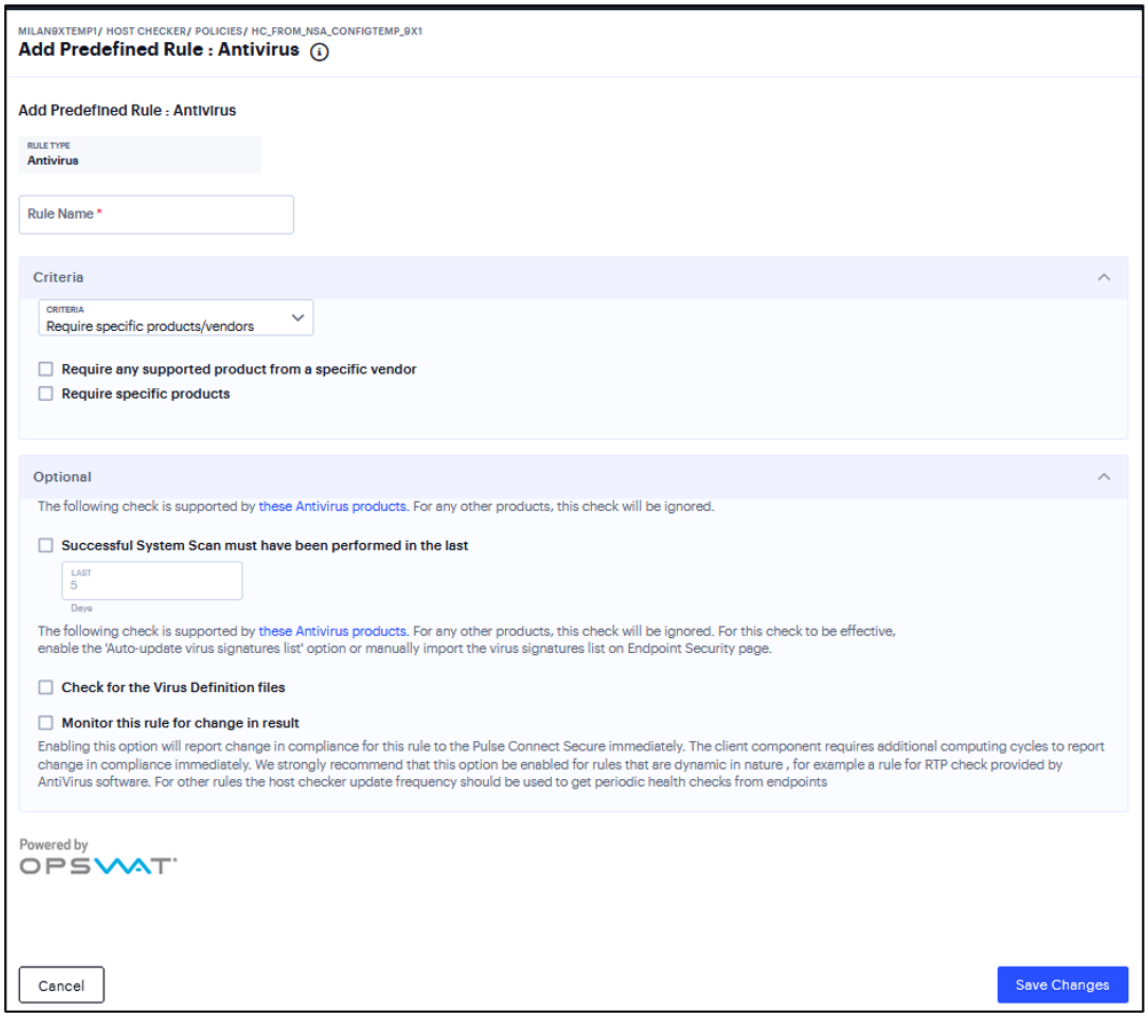


FIGURE 9.19 : Antivirus Rule

Note:

- Use this option only for dynamic rules, such as checking whether Real Time Protection is enabled on the antivirus software. Use the host checker update frequency to monitor other rules periodically.
- Monitor this rule for change in result for port check is applicable only for Windows and not for Linux or MAC machines.

Add Rule: Firewall Rule with Remediation Options

When you enforce the Host Checker rule with firewall remediation actions, if an endpoint attempts to log in without the required firewall running, Host Checker can attempt to enable the firewall on the client machine.

1. Select one of the following supported platforms:
   - Windows
   - Mac
2. Enter a Rule Name.
3. Under Criteria, click **Require specific products/vendors**. A new window will open with a list of all of the products that support the feature.
4. Select your vendor(s) and product(s) by using either the **Require any supported product from a specific vendor** or **Require specific products** check box.
5. (Optional) Select **Monitor this rule for change in result** to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, the system initiates a new handshake to re-evaluate realm or role assignments.

FIGURE 9.20 : Firewall Rule

Note: Monitor this rule for change in result for port check is applicable only for Windows and not for Linux or MAC machines.

Add Rule: AntiSpyware

You can configure Host Checker to check for installed antispyware on endpoints.

To configure a Host Checker Predefined Spyware rule:

1. Select one of the following supported platforms:
   - Windows
   - Mac
2. Enter a Rule Name.
3. Under Criteria, click **Require specific products/vendors**. A new window will open with a list of all of the products that support the feature.
4. Select your vendor(s) and product(s) by using either the **Require any supported product from a specific vendor** or **Require specific products** check box.
5. (Optional) Select **Monitor this rule for change in result** to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, the system initiates a new handshake to re-evaluate realm or role assignments.

FIGURE 9.21 : AntiSpyware

Note: Monitor this rule for change in result for port check is applicable only for Windows and not for Linux or Mac machines.

Add Rule: Hard Disk Encryption

You can configure Host Checker to check for installed Hard Disk Encryption on endpoints and specify the drives which needs to be encrypted using these software.

To configure a predefined hard disk encryption rule:

1. Select one of the following supported platforms:
   - Windows
   - Mac
2. Enter a Rule Name.
3. Under Criteria, click **Require specific products/vendors**. A new window will open with a list of all of the products that support the feature.
4. Select your vendor(s) and product(s) by using either the **Require any supported product from a specific vendor** or **Require specific products** check box.

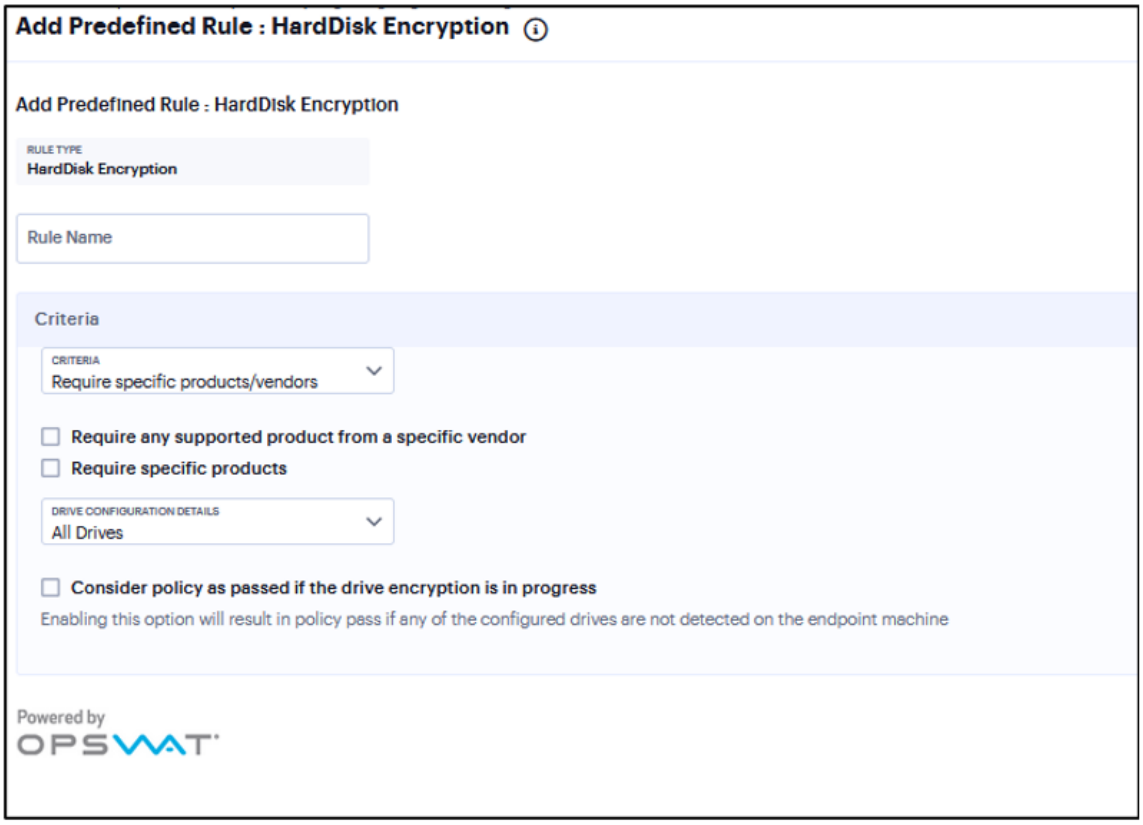


FIGURE 9.22 : HardDisk Encryption

5. Under Drive Configuration Details, select the required option:
   - All Drives - (Default) Select this option to check if all the drives on the client machine are encrypted.

- Specific Drives - Select this option to check if only specific drives on the client machine are encrypted.
  - Drive Letters - Enter the drive name. For example, C, D, E.
- Select the **Consider policy as passed if the drive Encryption is in progress** option to allow the Host Checker policy to pass if the encryption process is in progress and the drive is not fully encrypted.

Note:

- The drive encryption process takes time to complete depending up on the drive size and contents.
- For multiple drives, the Host Checker policy passes only if the encryption process is in progress in all the drives.

Add Rule: Patch Management

You can configure Host Checker to check for installed Patch management Software on endpoints.

To configure a predefined patch management rule:

1. Select one of the following supported platform options:
   - Windows
   - Mac
2. Enter a Rule Name.
3. Under Criteria, select the product name.
4. Default “Severity” options selected in policy are Critical, Important.
5. Default “Category” options selected in policy are Security Update, Critical Update, Regular Update, Driver Update.
6. To automatically enable patch deployment, select **Enable Automatic Patch Deployment**.

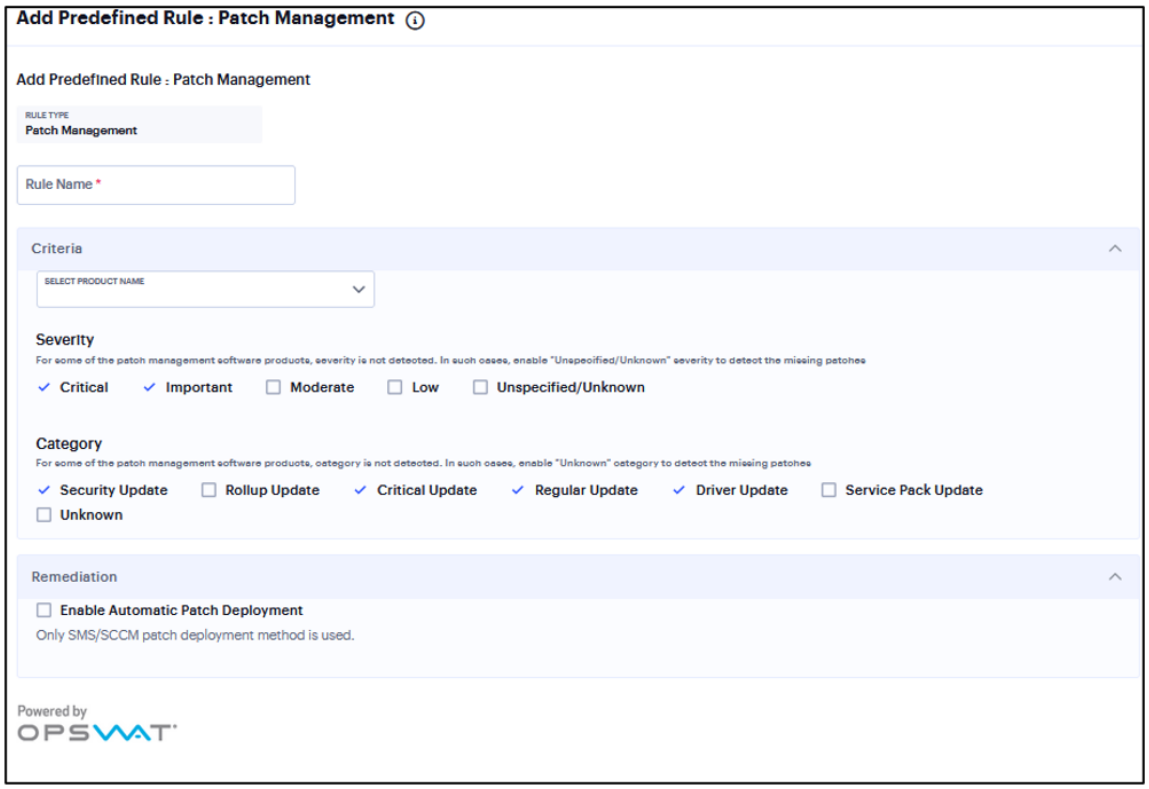


FIGURE 9.23 : Patch Management

Add Rule: Common Vulnerability and Exposure (CVE)

The CVE check rule helps in identifying the endpoints which are vulnerable using the OPSWAT library.

This rule is applicable only to Windows platform.

To configure a predefined CVE check rule:

1. Enter a Rule Name.
2. From the Criteria, select if you require all the CVE checks from OPSWAT or choose the specific CVE checks from the available CVE checks list.

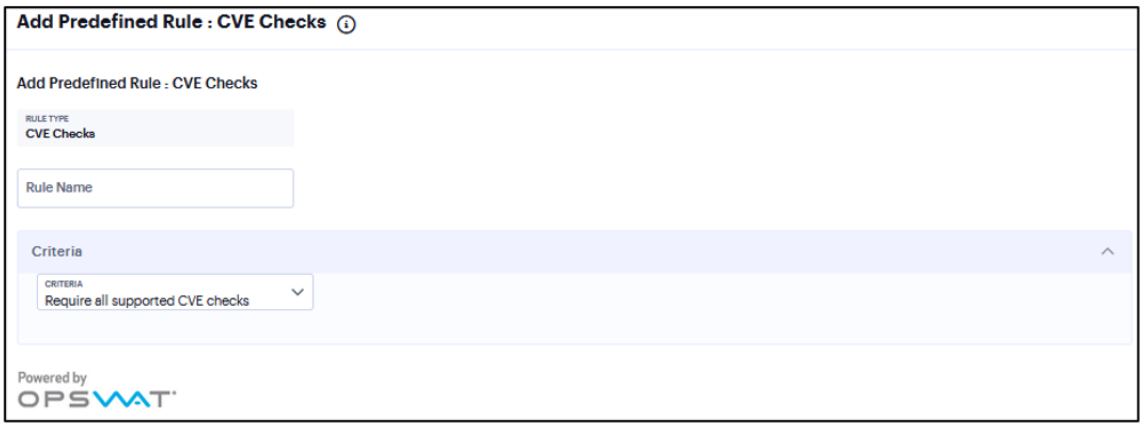


FIGURE 9.24 : CVE Checks

Add Rule: OS Checks

You can configure Host Checker to check the version of the windows operating systems and minimum service packs.

This rule is applicable only to Windows platform.

To configure a Host Checker Predefined OS Checks rule:

1. Enter a rule name.
2. Under Criteria, select the service pack/version to ignore.

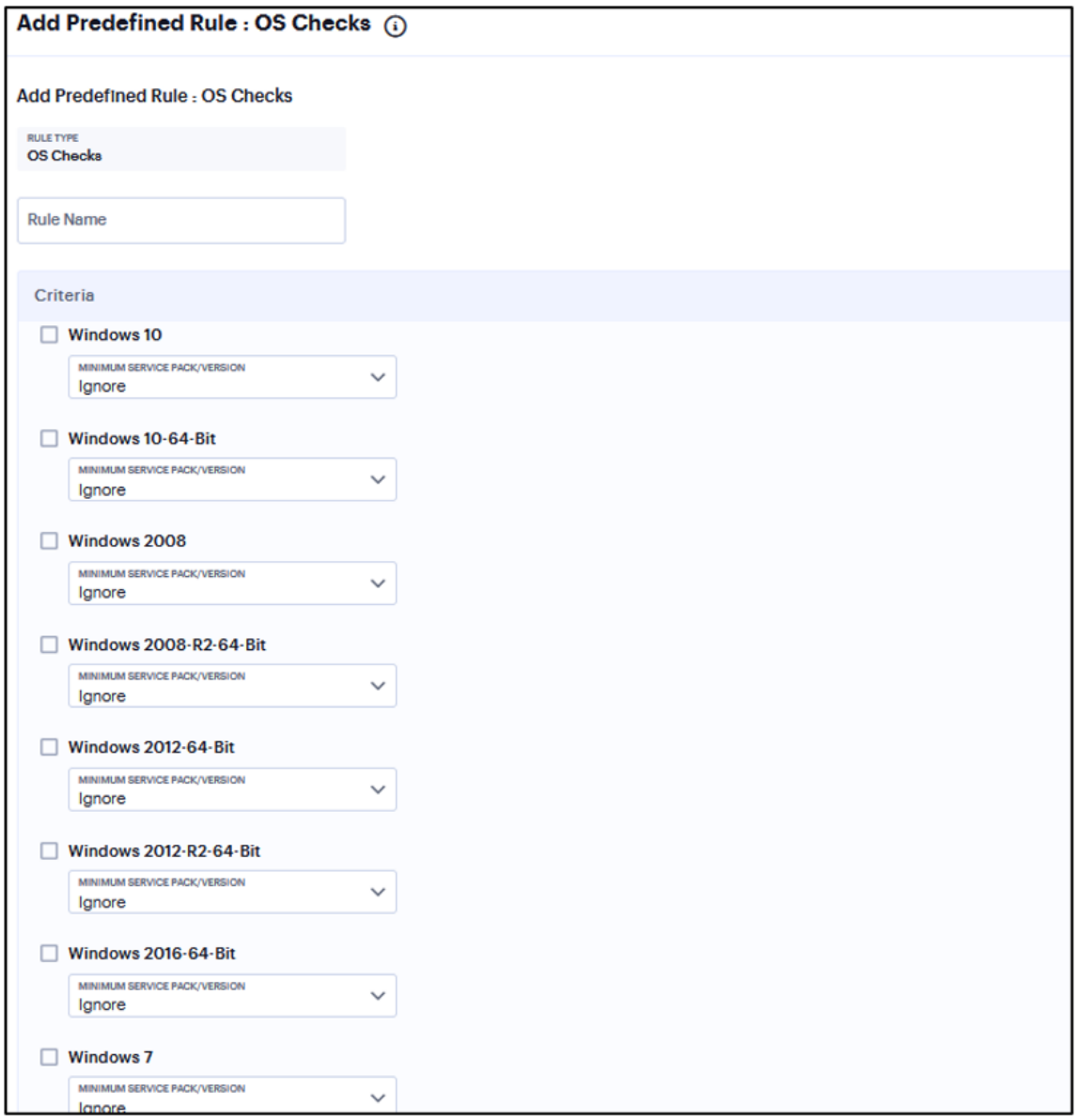


FIGURE 9.25 : CVE Checks

Specifying Customized Requirements Using Custom Rules

In addition to the predefined policies and rules that come with the system, you can create custom rules within a Host Checker policy to define requirements that your users' computers must meet.

Add Rule: Ports

Use this rule type to control 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 device.

To configure the Ports rule:

1. Select one of the following supported platform options:
   - Windows
   - Mac
   - Linux
2. Enter the rule name.
3. Under Criteria, enter the Port list.
4. Click Status and select Required/Deny.
   - Required: Select this to enable access from a listed port.
   - Deny: Select this to disallow access from a listed port.

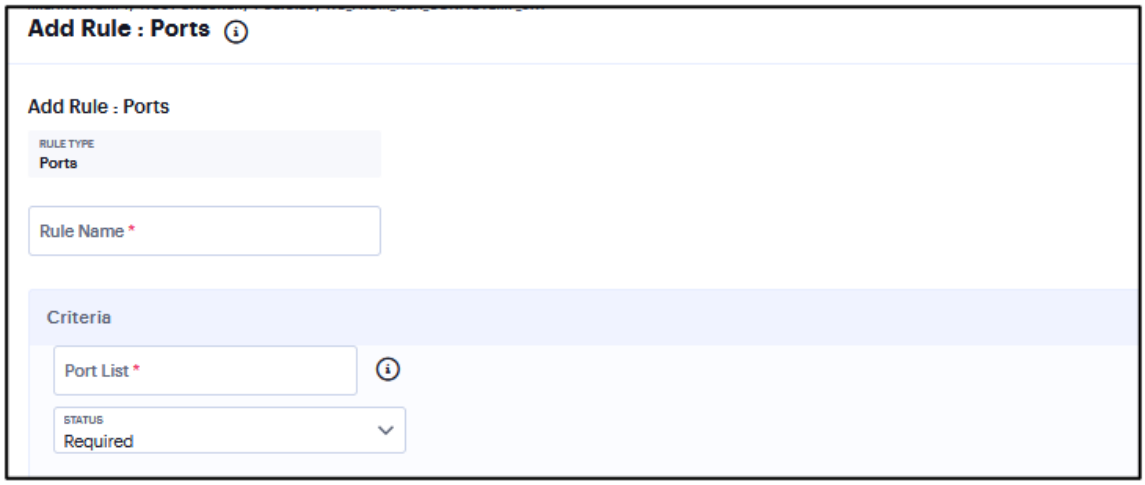


FIGURE 9.26 : Ports

Add Rule: Process

To configure the Process rule:

1. Select one of the following supported platform options:
   - Windows
   - Mac
   - Linux
2. Enter the rule name.
3. Under Criteria, enter the Process name. For example, explorer.exe.

4. Click **Status** and select **Required/Deny**.
    - Required: Select this to allow access if the process exists.
    - Deny: Select this to deny access if the process does not exist.
5. (Optional) Enter the MD5 Checksums/SHA256 Checksums.
6. Select Monitor this rule for change in result to check if there is any change in compliance result.

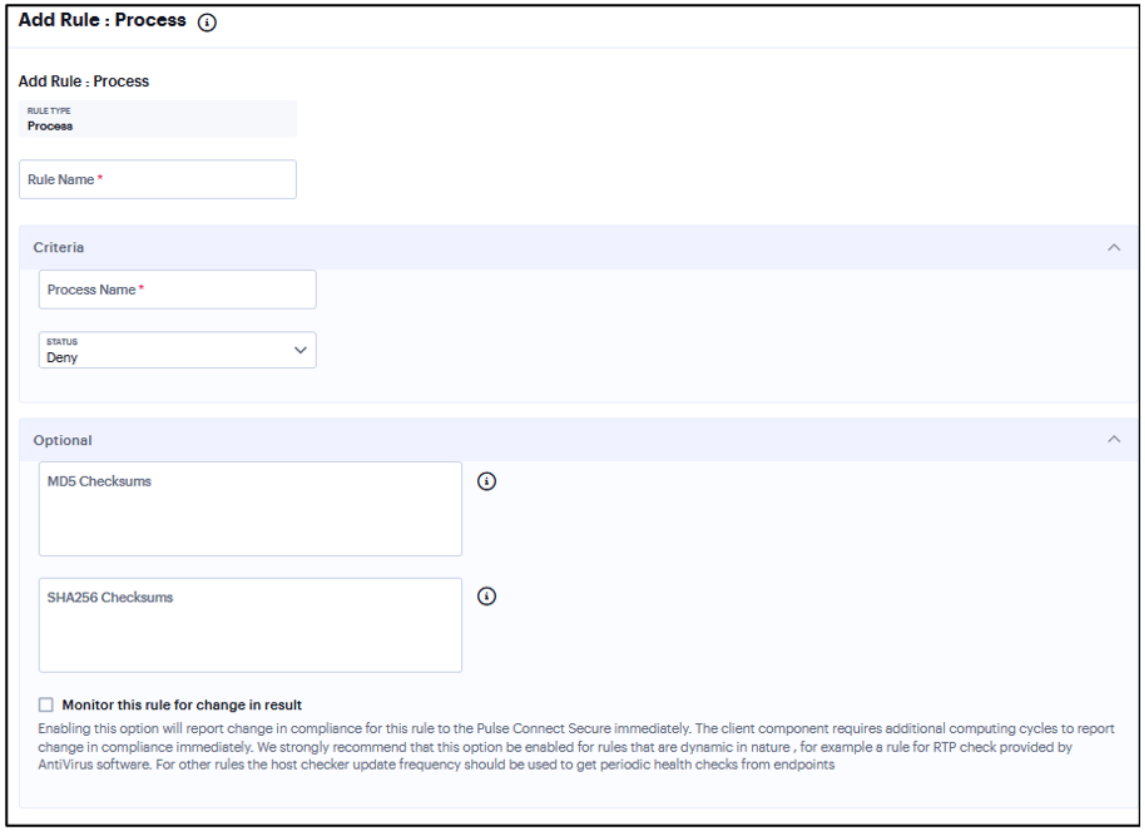


FIGURE 9.27 : Process Rule

Add Rule: File

To configure the File rule:

1. Select one of the following supported platform options:
    - Windows
    - Mac
    - Linux
2. Enter the rule name.
3. Enter a full file name and path in File Name. For example, “c:test.txt” or “/Users/exampleuser/Downloads/test.txt”.
4. Under Criteria, click **Status** and select **Required/Deny**.

- Required: Select this to allow access where the file exists and is valid.
- Deny: Select this to deny access if the file does not exist or is invalid.

5. (Optional) Enter the MD5 Checksums/SHA256 Checksums value for the file.
6. Select Monitor this rule for change in result to check if there is any change in compliance result.

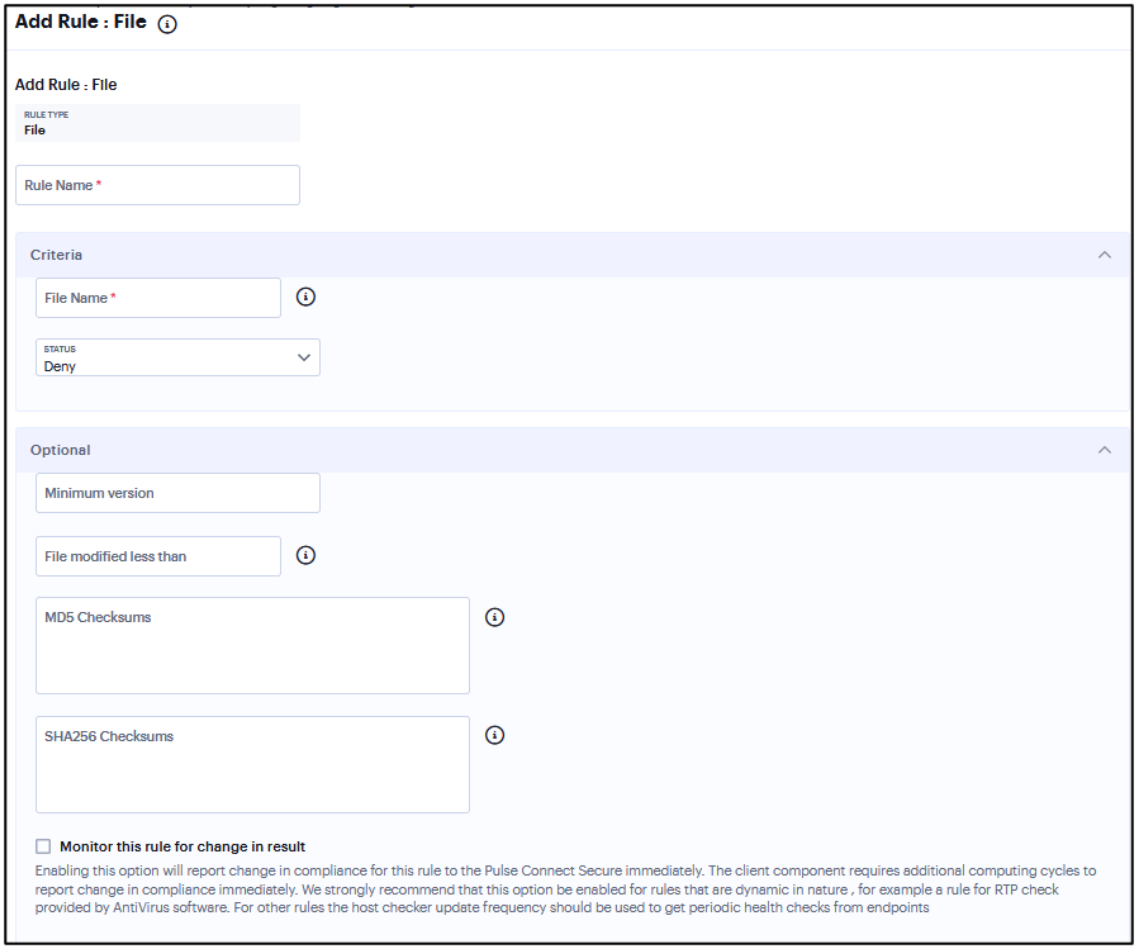


FIGURE 9.28 : File Rule

Add Rule: NetBIOS

To configure the NetBios rule:

1. Select one of the following supported platform options:
   - Windows
   - Mac
2. Enter the rule name.
3. Enter the Netbios domain Names as a comma-separated list (without spaces) of domain names. Each name can be 15 characters. Duplicate names are not supported. For example, WINDOWS-PC,WIN*-PC,*-PC,WINDOWS*

4. Under Criteria, click **Status** and select **Required/Deny**.
    - Required: Select this to allow access from a listed Netbios domain name.
    - Deny: Select this to deny access from a listed Netbios domain name.

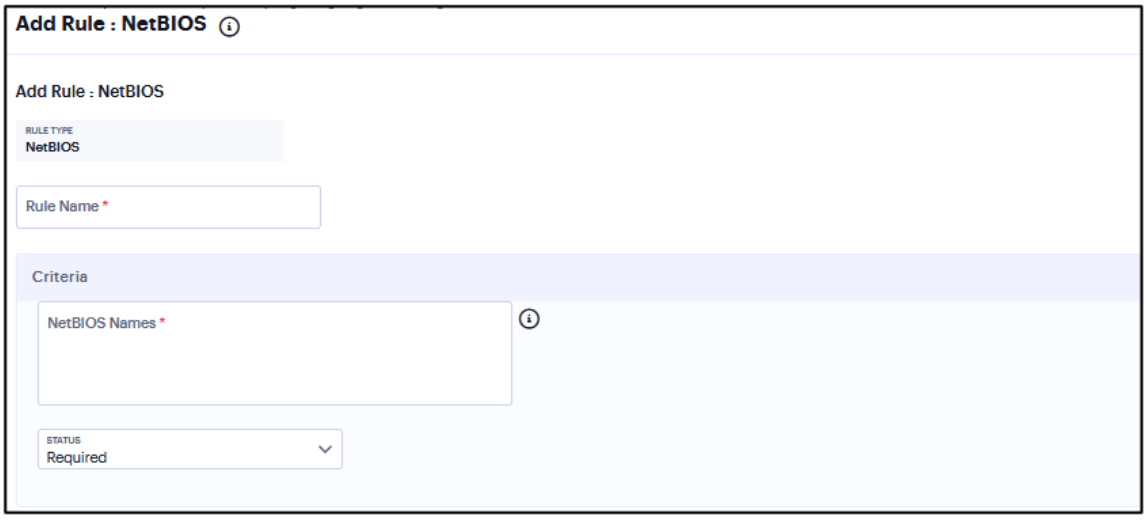


FIGURE 9.29 : NetBIOS Rule

Add Rule: MAC Address

To configure the MAC Address rule:

1. Select one of the following supported platform options:
    - Windows
    - Mac
2. Enter the rule name.
3. Under Criteria, Enter the MAC address as a comma-separated list (without spaces) of MAC addresses in the form HH:HH:HH:HH:HH:HH where the HH is a two-digit hexadecimal number. Duplicate MAC addresses are not supported.
4. Click **Status** and select **Required/Deny**.
    - Required: Select this to enable access from a listed MAC address.
    - Deny: Select this to disallow access from a listed MAC address.

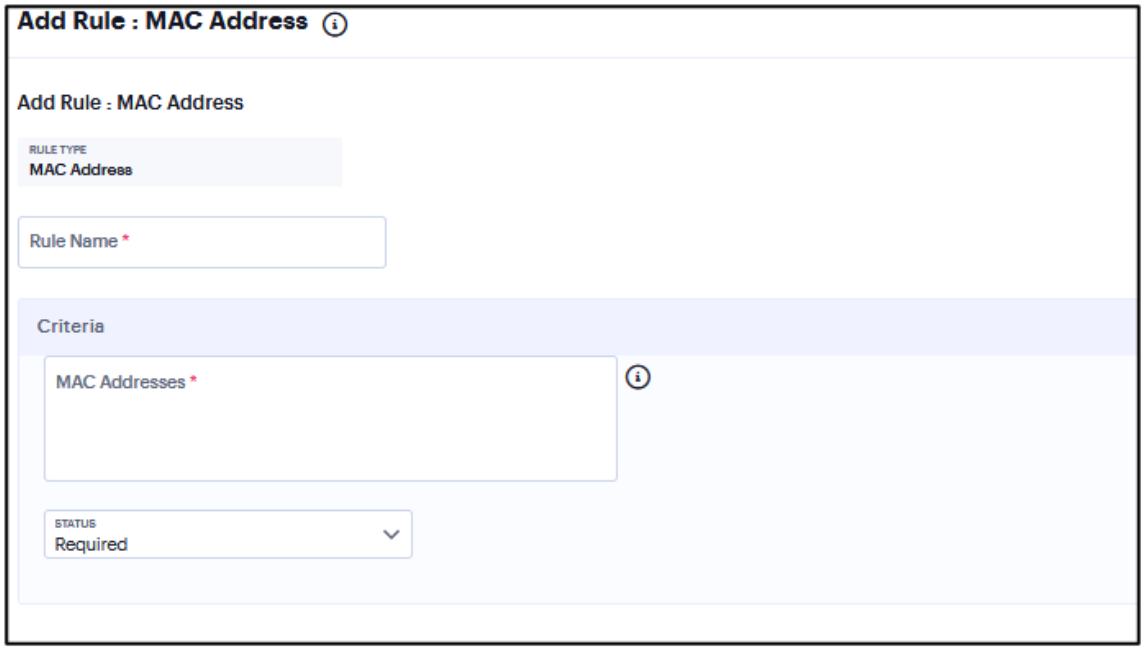


FIGURE 9.30 : MAC Address Rule

Add Rule: Machine Certificate

To configure the Machine Certificate rule:

1. Select one of the following supported platform options:
   - Windows
   - Mac
2. Enter the rule name.
3. Under Criteria, select Any certificate to allow access with any certificate.
4. (Optional) Enter specific values in the machine certificate.

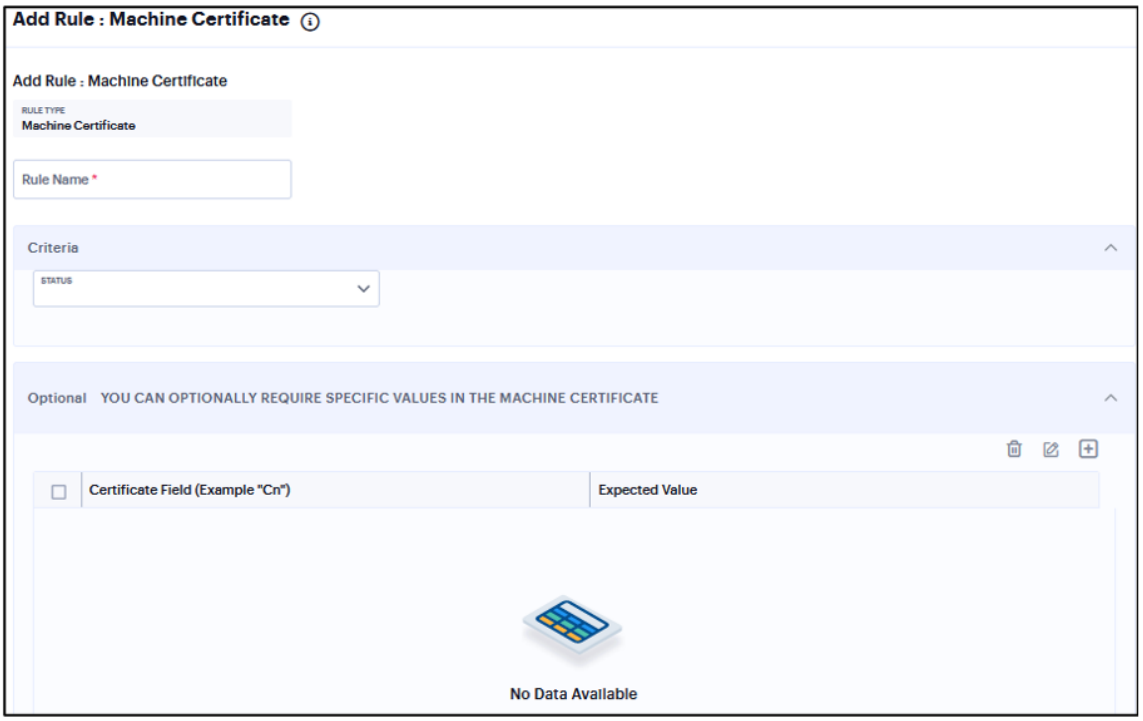


FIGURE 9.31 : Machine Certificate

Add Rule: Registry Setting

Note that Registry Setting rule is applicable only to Windows platform.

To configure the Registry Setting rule:

1. Enter the rule name.
2. Under Criteria, select one of the following options:
   - HKEY_LOCAL_MACHINE
   - HKEY_USERS
   - HKEY_CURRENT_USER
   - HKEY_CURRENT_CONFIG
   - HKEY_CLASSES_ROOT
3. Enter a Subkey for the registry path.
4. Under Key Type, select one of the following key types:
   - string
   - dword
   - binary
5. Enter a Key name.
6. Enter a Value for the registry key.

7. Select the 64-bit check box to use the 64-bit registry store. Clear this check box to use the 32-bit registry store.
8. (Optional) Select Monitor this rule for change in result to check if there is any change in compliance result.
9. Under Optional, select Monitor this rule for change in result to continuously monitor the policy compliance of endpoints.

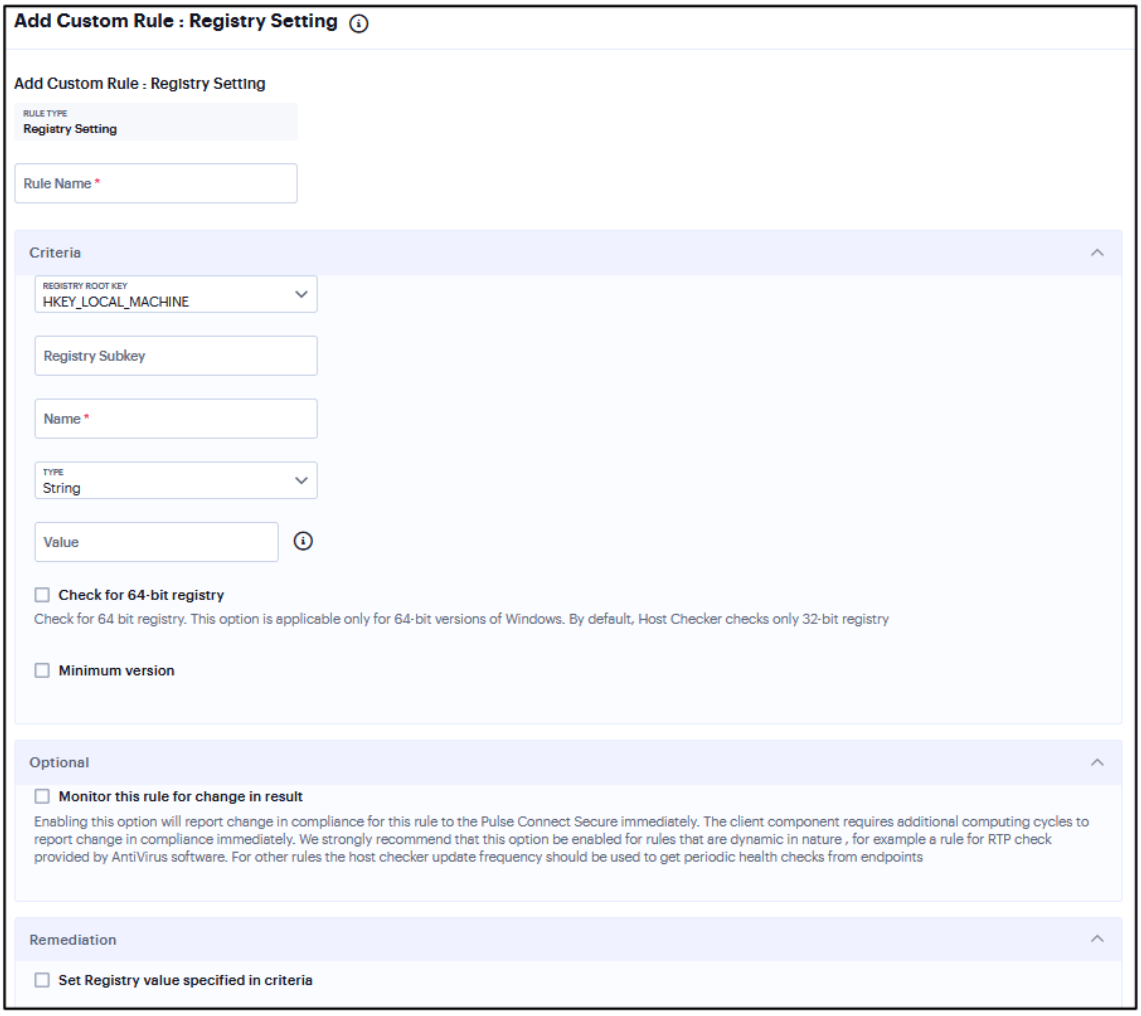


FIGURE 9.32 : Registry Setting

Add Rule: Advanced Host Checking

Note that Advanced Host Checking rule is applicable only to Windows platform.

To configure the Advanced Host Checking rule:

1. Enter the rule name.
2. Under Criteria, select one of the following options:
    - ports
    - process

- File
- NETBIOS
- MAC Address

3. Enable Required/Deny.
4. Select the registry root key- HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_USER, HKEY_CURRENT_CONFIG, or HKEY_CLASSES_ROOT.
5. Enter the registry subkey.
6. Enter the name of the registry.
7. Select the type of the registry- String, Binary, or DWORD.
8. Select “Check for 64-bit registry” to check the 64 bit registry on Windows. The default is 32 bit registry.

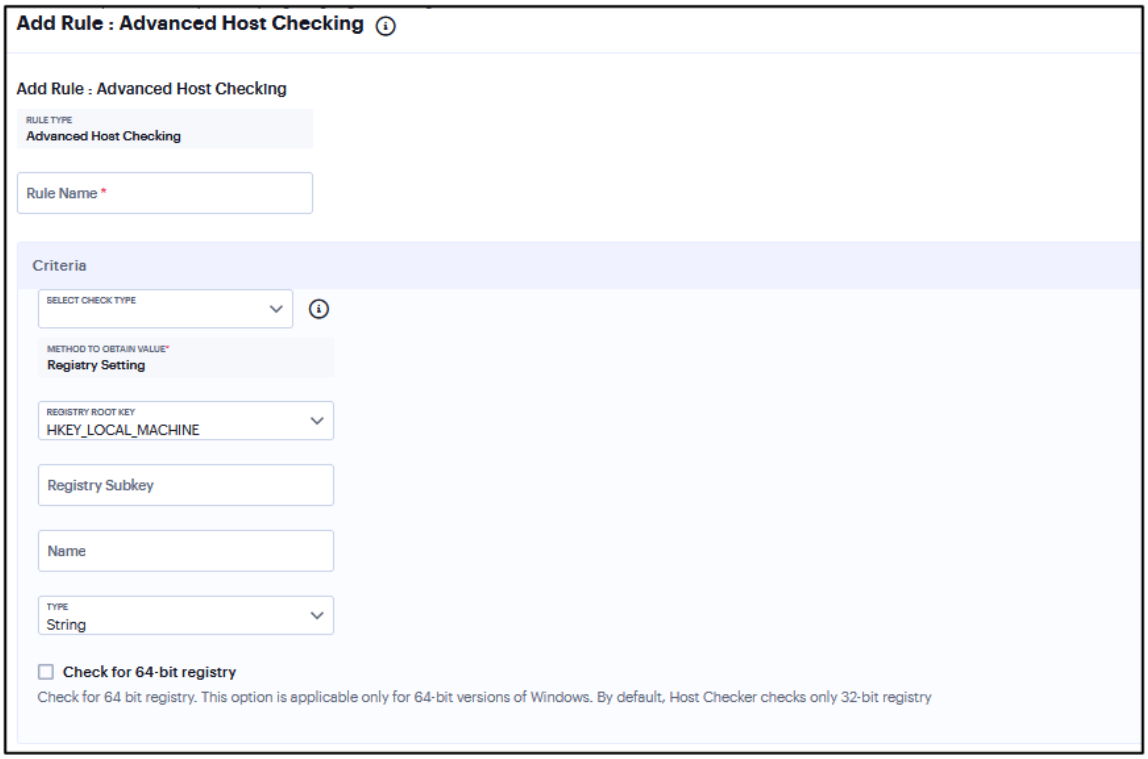


FIGURE 9.33 : Advanced Host Checking

Add Rule: Jail Breaking Detection

Note that Jail Breaking Detection rule is applicable only to iOS platform.

To configure the Jail Breaking Detection rule:

1. Select one of the supported iOS platform options.
2. Enter the rule name.
3. Under Criteria, select **Don’t allow Jail Broken devices**

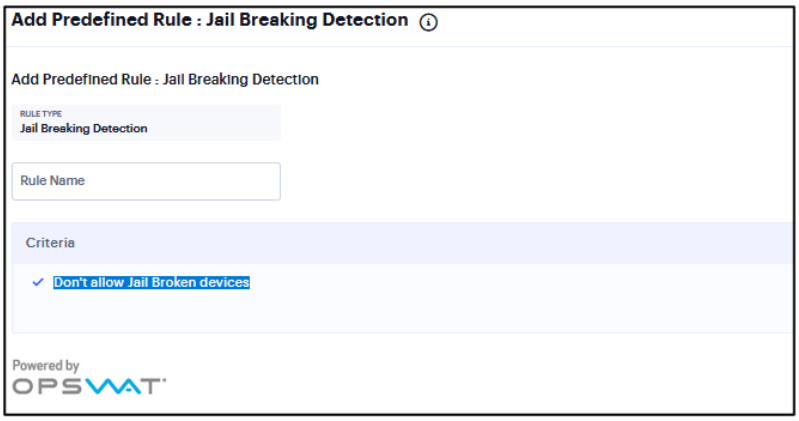


FIGURE 9.34 : Jail Breaking Detection

Add Rule: Rooting Detection

To configure the Rooting Detection rule:

1. Select one of the supported android platform options.
2. Enter the rule name.
3. Under Criteria, select **Don't allow Rooted devices**.

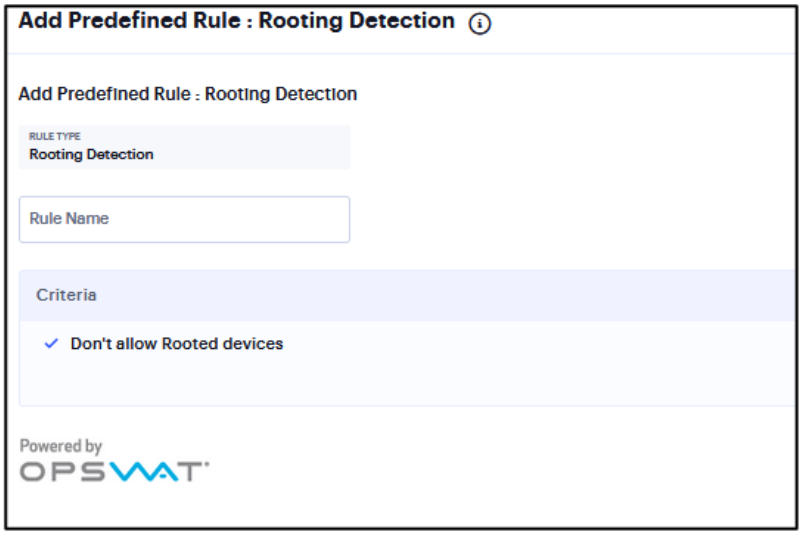


FIGURE 9.35 : Rooting Detection

Configuring Authentication Servers

The access management framework supports the following types of AAA servers: Local, External (standards-based), and External (other).

- Local includes “Local Authentication Server”, “Certificate Server”.
- External (standards-based) includes “LDAP Server”, “RADIUS Server”.
- External (other) includes “MDM Server”, “RSA ACE Server”, “TOTP Server”.

To add an authentication server, click the Add icon and select the Authentication server type from the list.

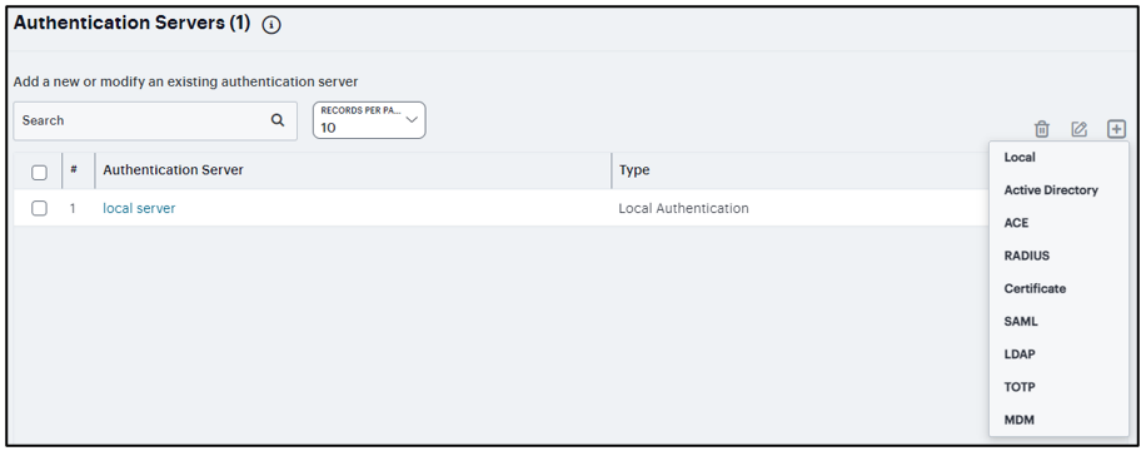


FIGURE 9.36 : Configuring Authentication Servers

Configuring Local Authentication Server

You can create multiple local authentication server instances. When you define a new local authentication server, you must give the server a unique name and configure options for passwords.

To create a local authentication server:

1. Select **Authentication > Authentication Servers**.
2. Click the Add icon and select **Local** from the list to display the configuration page.
3. Complete the configuration and save changes.
    - Enter a Server Name.
    - Select **Password Options**.
    - Select the **Allow users to change passwords** option if you want users to be able to change their passwords.

- Select the **Force password change after** option to specify the number of days after which a password expires. The default is 64 days.
- Select the **Prompt users to change password** option to specify when to prompt the user to change passwords.
- Select the **Enable account lockout for users** option to manage user authentication failures for admin users of local authentication server.
- Enter the number of consecutive wrong password attempts after which the admin user account will be locked. The default value is 3 retries.
- Enter the time in minutes for which admin user account will remain locked. The default value is 10 minutes.

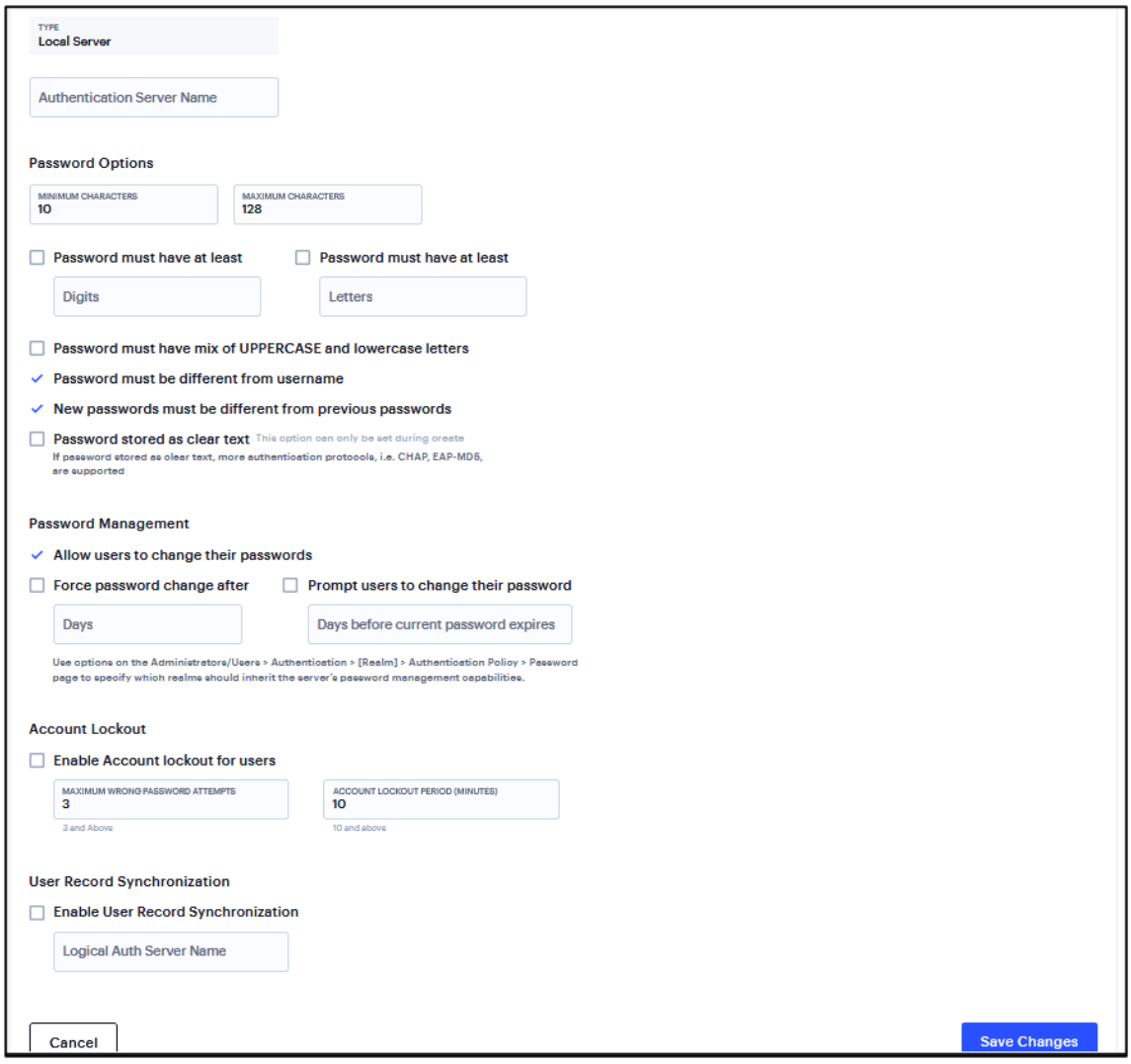


FIGURE 9.37 : Local Authentication Server

Configuring ACE Authentication Server

RSA Authentication Manager (formerly known as ACE/Server) is an authentication and authorization server that allows user authentication based on credentials from the RSA SecurID® product from RSA Security Inc.

To configure authentication with the ACE server:

1. Select **Authentication > Authentication Servers**.
2. Click the Add icon and select **ACE** from the list to display the configuration page.
3. Complete the configuration and save changes.
    - Enter a Server Name.
    - Enter the default port of the authentication server.
    - Click and browse **Import New Config File** to upload the sdconf.rec configuration file.
    - Select the **Enable User Record Synchronization** option to retain the bookmarks and individual preferences regardless of which system you log in to.
    - Enter a logical authentication server name.

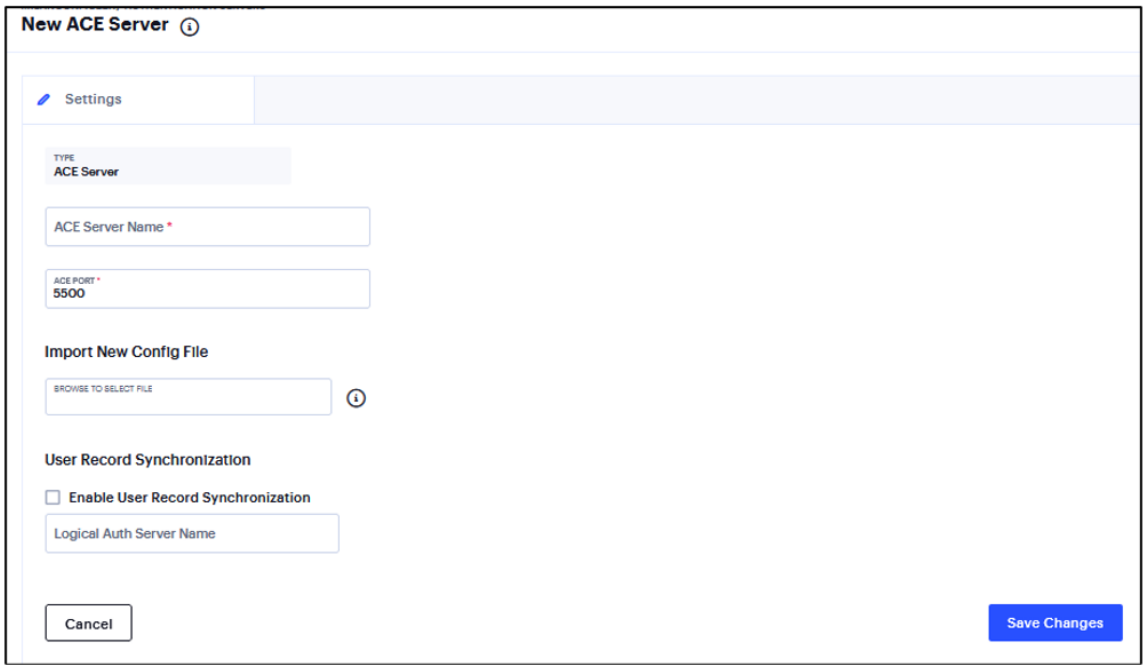


FIGURE 9.38 : ACE Authentication Server

Configuring RADIUS Authentication Server

To configure authentication with the RADIUS server:

1. Select **Authentication > Authentication Servers**.
2. Click the Add icon and select **RADIUS** from the list to display the configuration page.
3. Complete the configuration and save changes.

   Settings page

   - Enter a Server Name.
   - Enter the name that identifies the Network Access Server (NAS) client to the RADIUS server.
   - Enter the name or IP address of the RADIUS server.
   - Enter the authentication port value for the RADIUS server. Default port number: 1812, 1645 (legacy servers).
   - Enter the NAS IP address. If you leave this field empty, the internal IP address is passed to RADIUS requests. You can also fill this field with IPv6 address.
   - Enter the interval of time in seconds to wait for a response from the RADIUS server before timing out the connection.
   - Enter the number of times to try to make a connection after the first attempt fails.
   - Select the **Users authenticate using tokens or one-time passwords** option to prompt the user for a token instead of a password.
   - Click **Next**.

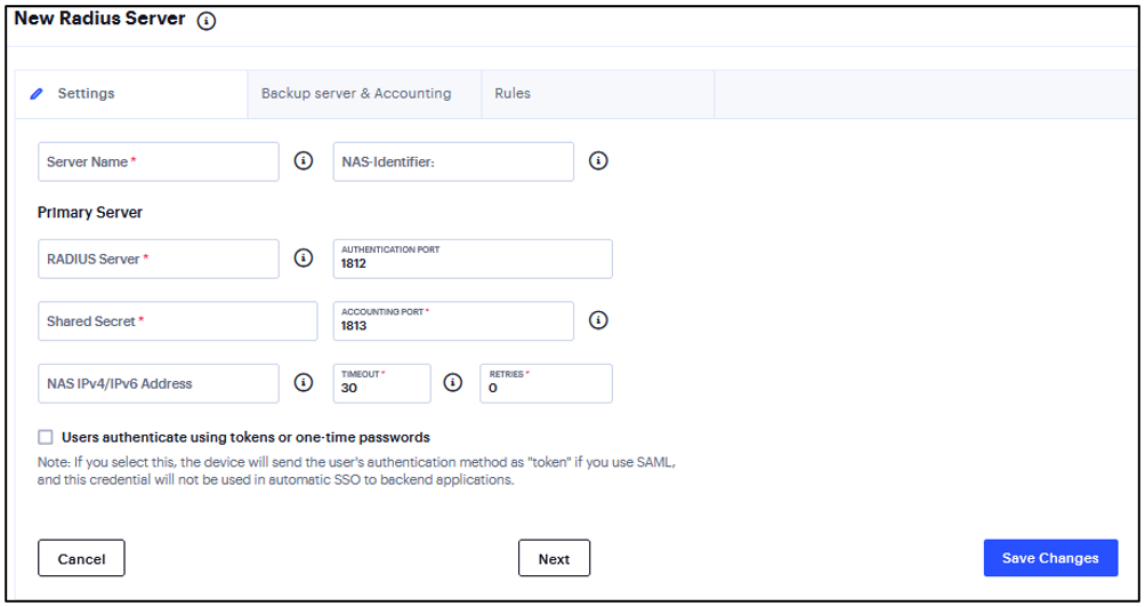


FIGURE 9.39 : RADIUS Authentication Server

Backup server & Accounting page (required only if Backup server exists)

- Enter the secondary RADIUS server.
- Enter the Authentication Port.
- Enter the Shared Secret.
- Enter the Accounting Port.
- Enter the user information to the RADIUS accounting server.
- Enter **Interim Update Interval** in minutes to achieve more precise billing for long-lived session clients and during network failure.
- Select the **Use VPN Tunnel assigned IP Address for FRAMED-IP-ADDRESS/FRAMED-IPV6-ADDRESS attribute value in RADIUS Accounting** option to use the VPN Tunneling IP address for the FRAMED-IP-ADDRESS/FRAMED-IPV6-ADDRESS attribute instead of the pre-authenticated (original) IP address. Framed IPv6 addresses based attribute fetching and parsing:
  - NAS-IPv6-Address
  - Login-IPv6-Host
- Enable the **Send Interim Updates for sub sessions created inside parent sessions** check box to send interim updates for sub sessions (child sessions) created inside parent sessions.
- Click **Next**.

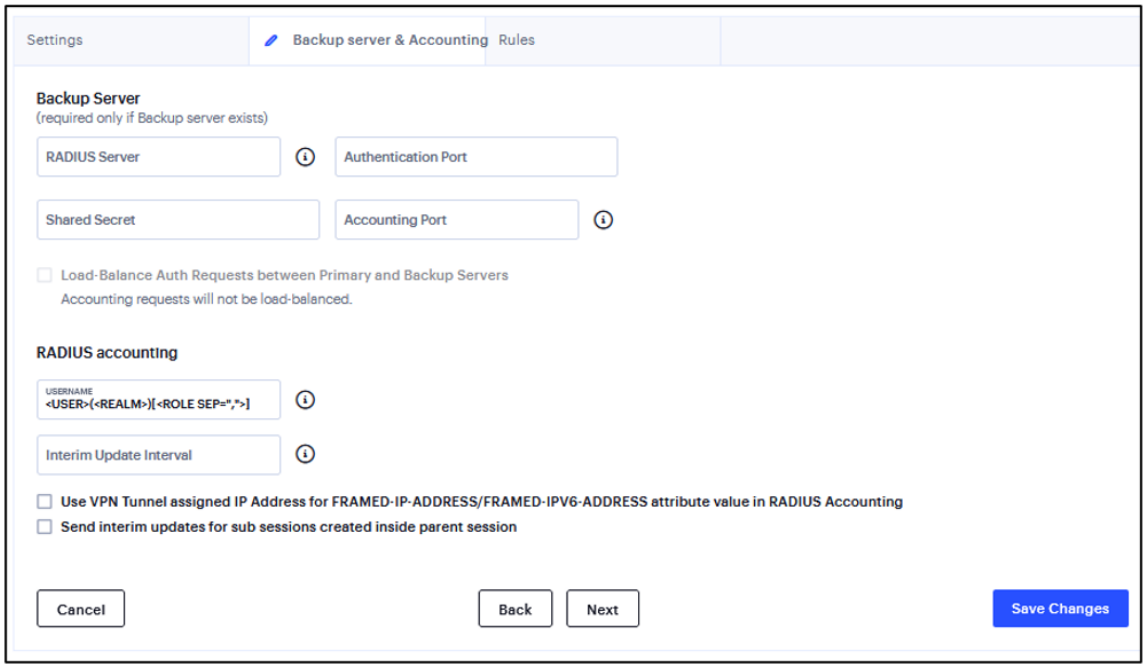


FIGURE 9.40 : RADIUS Authentication Server

Rules page

- Select the **Enable processing of Radius Disconnect Requests** check box. The Radius Disconnect requests received from the backend Radius server will terminate sessions that match the attributes in the request.
- Select the **Enable User Record Synchronization** option to retain the bookmarks and individual preferences regardless of which system you log in to.
- Enter a logical authentication server name.

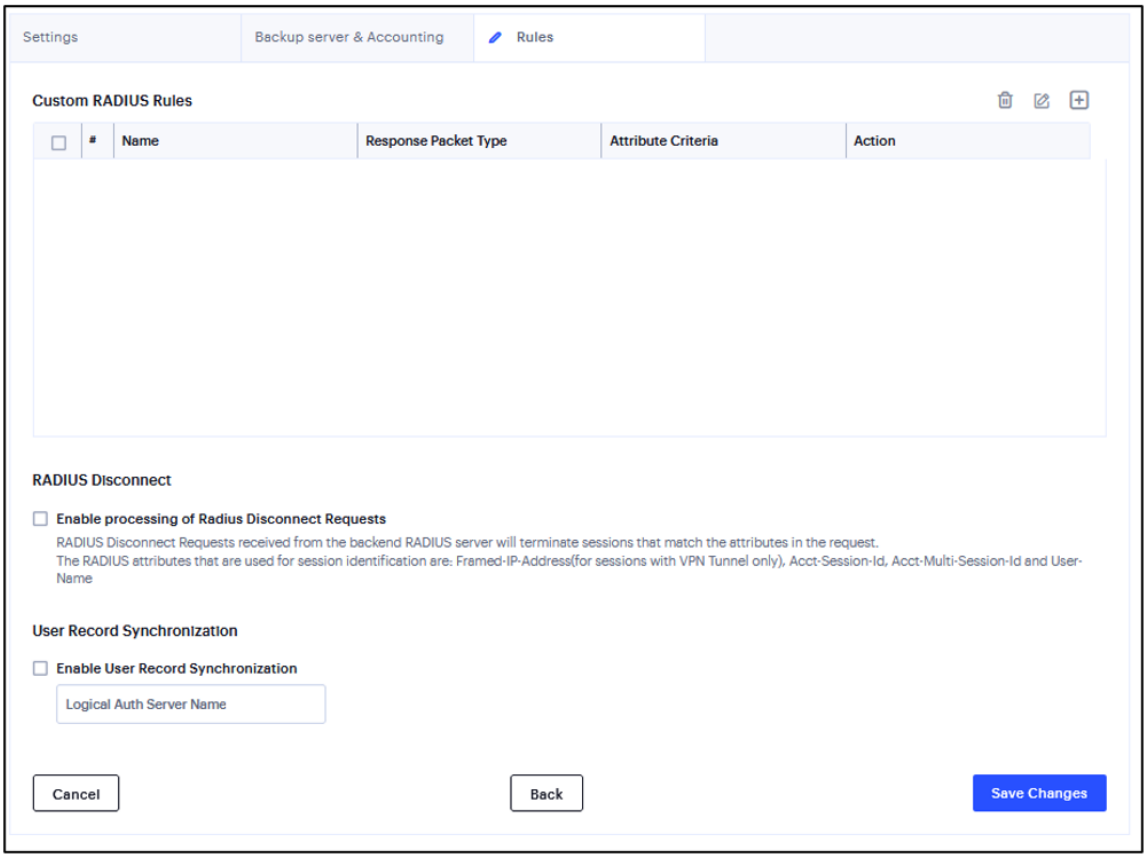


FIGURE 9.41 : RADIUS Authentication Server

Configuring Certificate Authentication Server

The certificate server is a local server that allows user authentication based on the digital certificate presented by the user without any other user credentials.

To configure authentication with the Certificate server:

1. Select **Authentication > Authentication Servers**.
2. Click the Add icon and select **Certificate** from the list to display the configuration page.
3. Complete the configuration and save changes.
   - Enter a Server Name.

- Enter a username template. Specify how the system should construct a username. You may use any combination of certificate variables contained in angle brackets and plain text.
- Select the **Enable User Record Synchronization** option to retain the bookmarks and individual preferences regardless of which system you log in to.
- Enter a logical authentication server name.

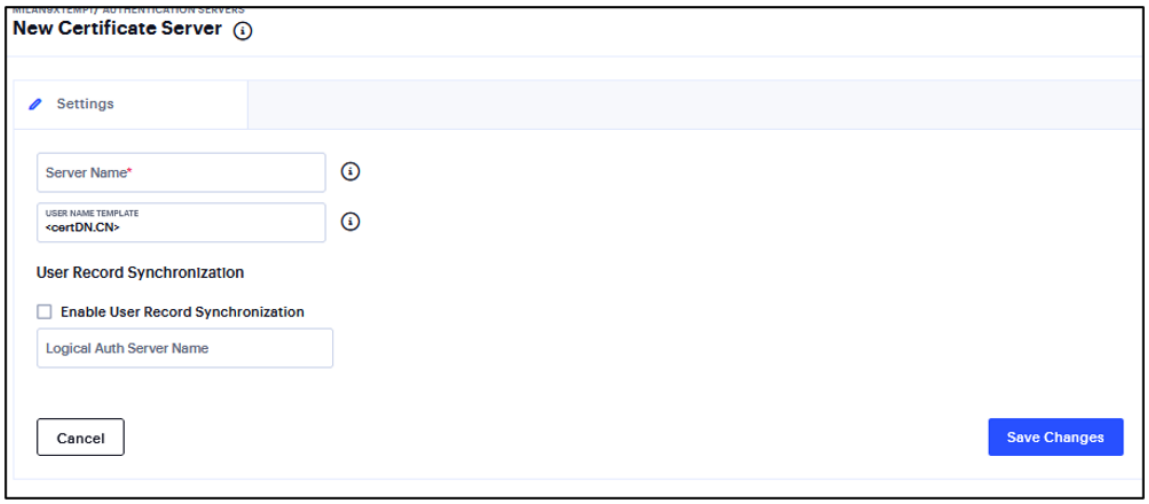


FIGURE 9.42 : Certificate Authentication Server

Configuring LDAP Authentication Server

Lightweight Directory Access Protocol (LDAP) facilitates the access of online directory services. LDAP directory consists of a collection of attributes with a name, known as a distinguished name (DN). Each of the entry's attributes, known as a relative distinguished name (RDN), has a type and one or more values. The types are typically mnemonic strings, such as CN for common name. The valid values for each field depend on the types.

To configure authentication with the LDAP server:

1. Select **Authentication > Authentication Servers**.
2. Click the Add icon and select **LDAP** from the list to display the configuration page.
3. Complete the configuration and save changes.

   Settings page

   - Enter a Server Name.
   - Select the **Enable Domain Name** option if you want to fetch a list of servers from the DNS server. Clear this option if you want to manually enter all the domain controllers host names.
   - Enter the LDAP server name or the IP address.

- (Optional) Enter the parameters for backup LDAP server1. Default port number: 389
- Enter the parameters for backup LDAP port1.
- (Optional) Specify the parameters for backup LDAP server2.
- Enter the parameters for backup LDAP port2.
- Select the backend LDAP server type from the following choices: Generic, Active Directory, iPlanet, Novell eDirectory.
- Select one of the following options for the connection to the LDAP server:
  - Unencrypted - The device sends the username and password to the LDAP Directory Service in cleartext.
  - LDAPS - The device encrypts the data in the LDAP authentication session using the Secure Socket Layer (SSL) protocol before sending it to the LDAP Directory Service.
  - Start TLS - The device allows both secure and plain requests against an LDAP server on a single connection.
- Enter the time (in seconds) to wait for connection to the primary LDAP server, and then to each backup LDAP server. Default: 15 seconds
- Enter the time (in seconds) to wait for search results from a connected LDAP server.

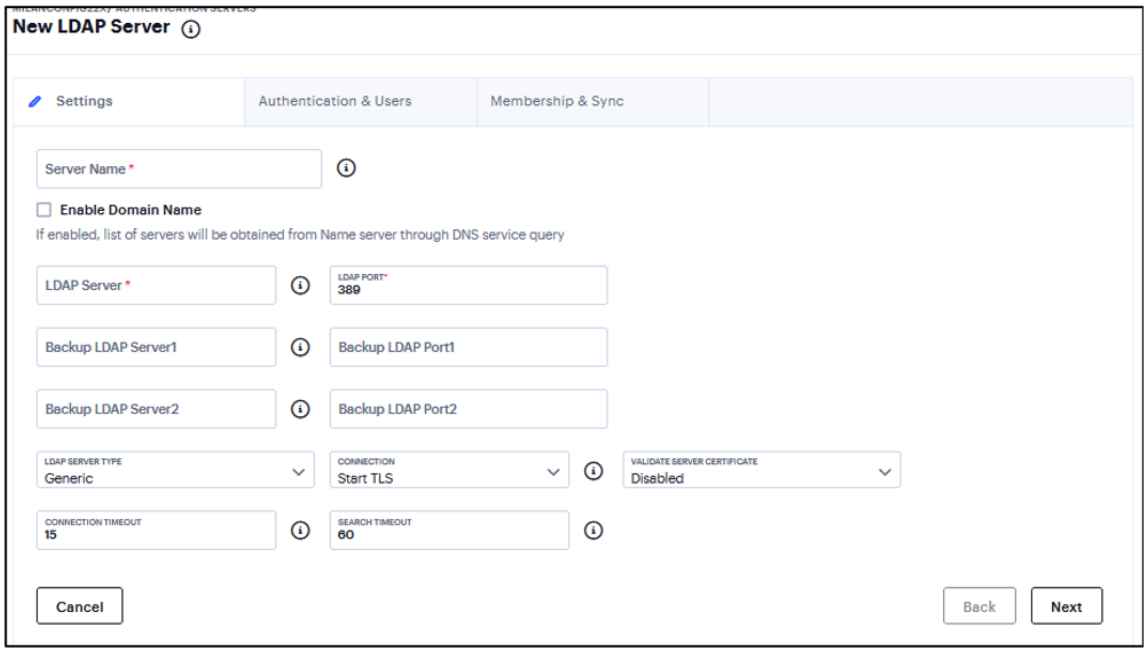


FIGURE 9.43 : LDAP Authentication Server

- Click **Next**.

Authentication & Users page

- Select the **Authentication required to search LDAP** option to require authentication when performing search or password management operations.
- Enter the administrator DN for queries to the LDAP directory.
- Enter the password for the LDAP server.
- Enter the backup administrator DN for queries to the LDAP directory, as a fallback when primary Admin DN fails (due to account expiration).
- Enter the backup administrator password for the LDAP server.

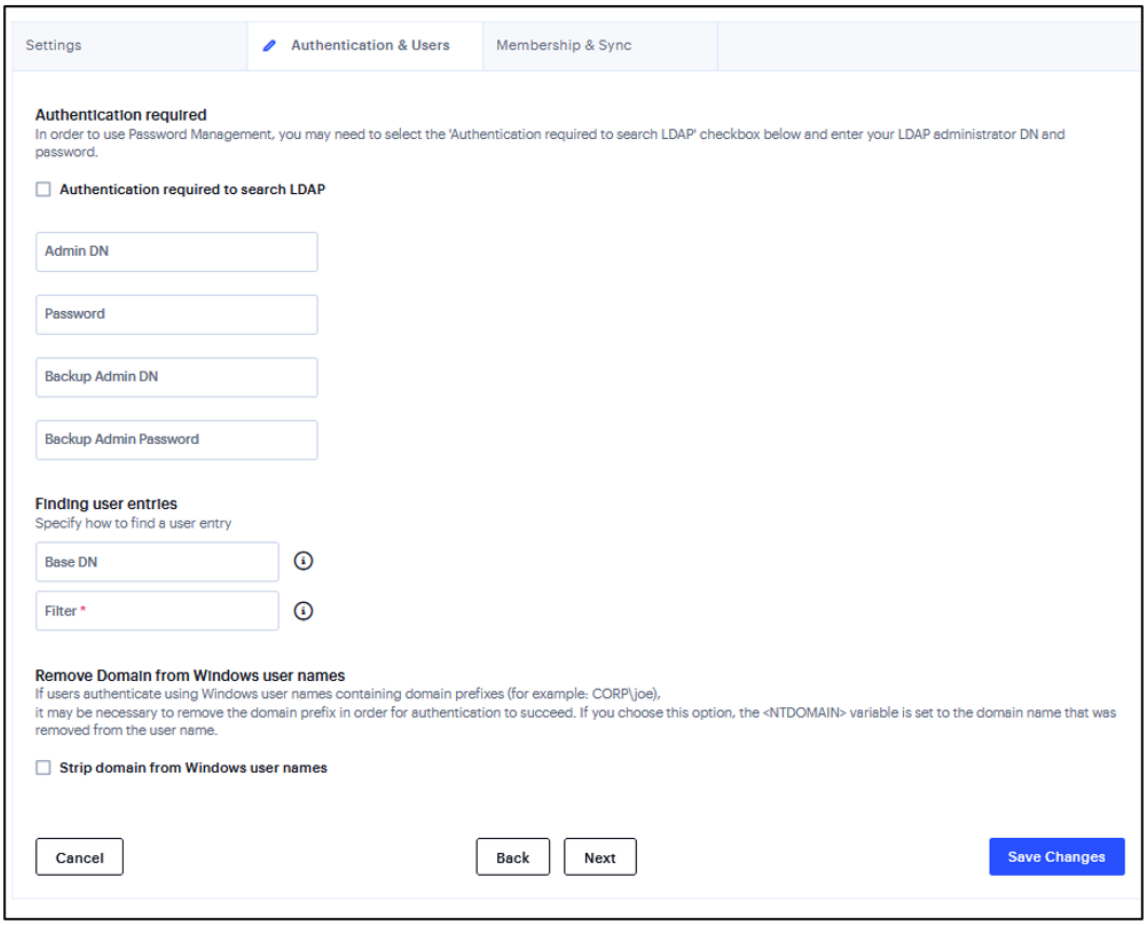


FIGURE 9.44 : Finding user entries

- Under **Finding user entries**:
  - Enter the base DN under which the users are located. For example, dc=sales,dc=acme, dc=com.
  - Enter a unique variable that can be used to do a fine search in the tree. For example, samAccountname=<username> or cn=<username>.
  - Select the **Strip domain from Windows username** option to pass the username without the domain name to the LDAP server.
- Click **Next**.

Membership & Sync page

- Enter the base DN to search for user groups.
- Enter a unique variable which can be used to do a fine search in the tree. For example, samAccountname=<username> or cn=<GROUPNAME>.
- Enter all the members of a static group. For example, member or uniquemember (iPlanet specific Deprecated for 21.x).
- Select the **Reverse group search** option to start the search from the member instead of the group. This option is available only for Active Directory server types.
- Enter an LDAP query that returns the members of a dynamic group. For example, memberURL.
- Enter how many levels within a group to search for the user. The higher the number, the longer the query time, so we recommend that you specify to perform the search no more than two levels deep.
- Select one of the following options: Nested groups in Server Catalog, Search all nested groups.

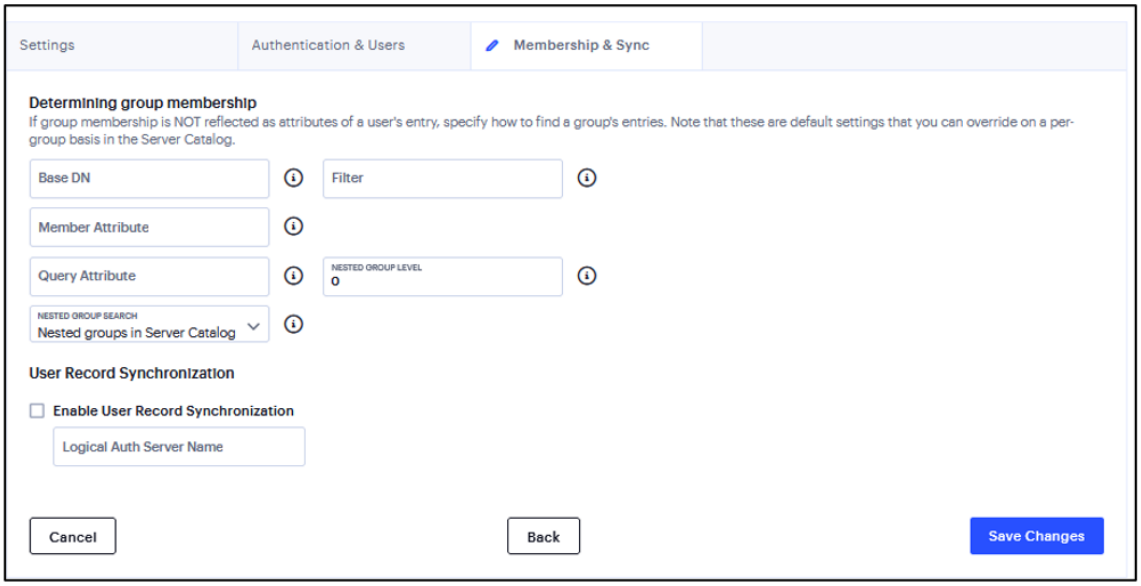


FIGURE 9.45 : Determining group membership

Configuring SAML Authentication Server

SAML is an XML-based framework for communicating user authentication, entitlement, and attribute information. The standard defines the XML-based assertions, protocols, bindings, and profiles used in communication between SAML entities. SAML is used primarily to implement Web browser single sign-on (SSO). SAML enables businesses to leverage an identity-based security system like Ivanti Connect Secure to enforce secure access to web sites and other resources without prompting the user with more than one authentication challenge.

For complete details on the SAML standard, see the OASIS web site:

To configure authentication with the SAML server:

1. Select **Authentication > Authentication Servers**.
2. Click the Add icon and select **SAML** from the list to display the configuration page.
3. Complete the configuration and save changes.

   Settings

   - Enter a name to identify the server instance.
   - Select SAML version used by the SAML IdP.
   - Select to override the Host FQDN for the SAML server. Host FQDN is used to update the Unique SAML Identifier and ACS URL of the SAML Authentication Server.
   - Select Manual or Metadata for Configuration Mode. If a metadata file or location is available from the SAML identity provider, use the metadata option to make configuration simpler and less prone to error.
   - Enter **Identity Provider Entity ID**. The identity provider entity ID is sent as the Issuer value in the assertion generated by the SAML identity provider.
   - Enter **Identity Provider Single Sign On Service URL**. The identity provider SSO service URL is a URL provisioned by the SAML identity provider. The setting is required to support service-provider-initiated SSO.
   - Specify **User Name Template** to derive the username from the assertion.
   - Specify the maximum allowed difference in time between the system clock and the SAML identity provider server clock.
   - Select **Support Single Logout**. Single logout is a mechanism provided by SAML for logging out a particular user from all the sessions created by the identity provider. Select this option if the system must receive and send a single logout request for the peer SAML identity provider.
   - Click **Save Changes**. The SAML Authentication Server gets listed in the Authentication Servers page.

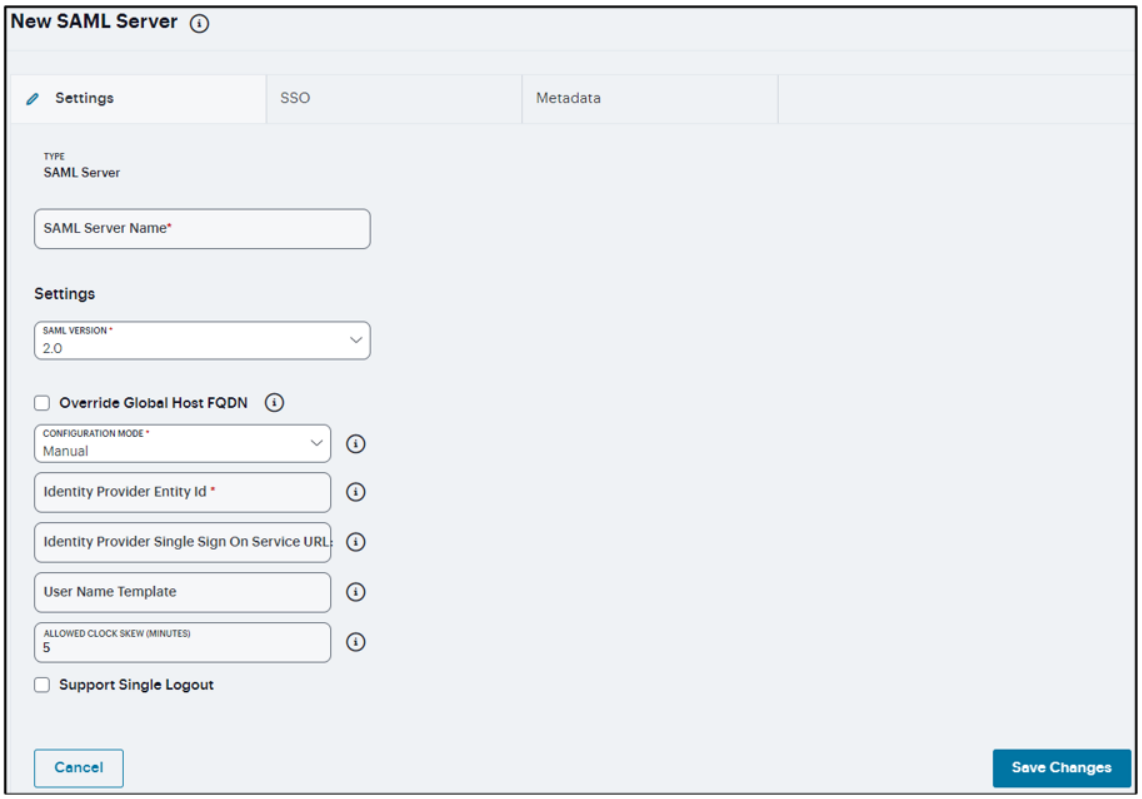


FIGURE 9.46 : SAML Authentication Server Settings

SSO

- Select the **SSO** tab.
- Select **Artifact** to use the Artifact binding. The system then contacts the Artifact Resolution Service (ARS) to fetch the assertion using SOAP protocol. If the ARS is hosted on a HTTPS URL, then the certificate presented by the ARS is verified by the system.
- Select **POST** to use the POST binding, the system uses a response signing certificate to verify the signature in the incoming response or assertion. The certificate file must be in PEM or DER format. The certificate you select should be the same certificate used by the identity provider to sign SAML responses.
- Use the **Add** and **Remove** buttons to select authentication context classes to be sent in the authentication requests to the SAML identity provider. These are included in the RequestedAuthnContext element.
- Click **Save Changes**.

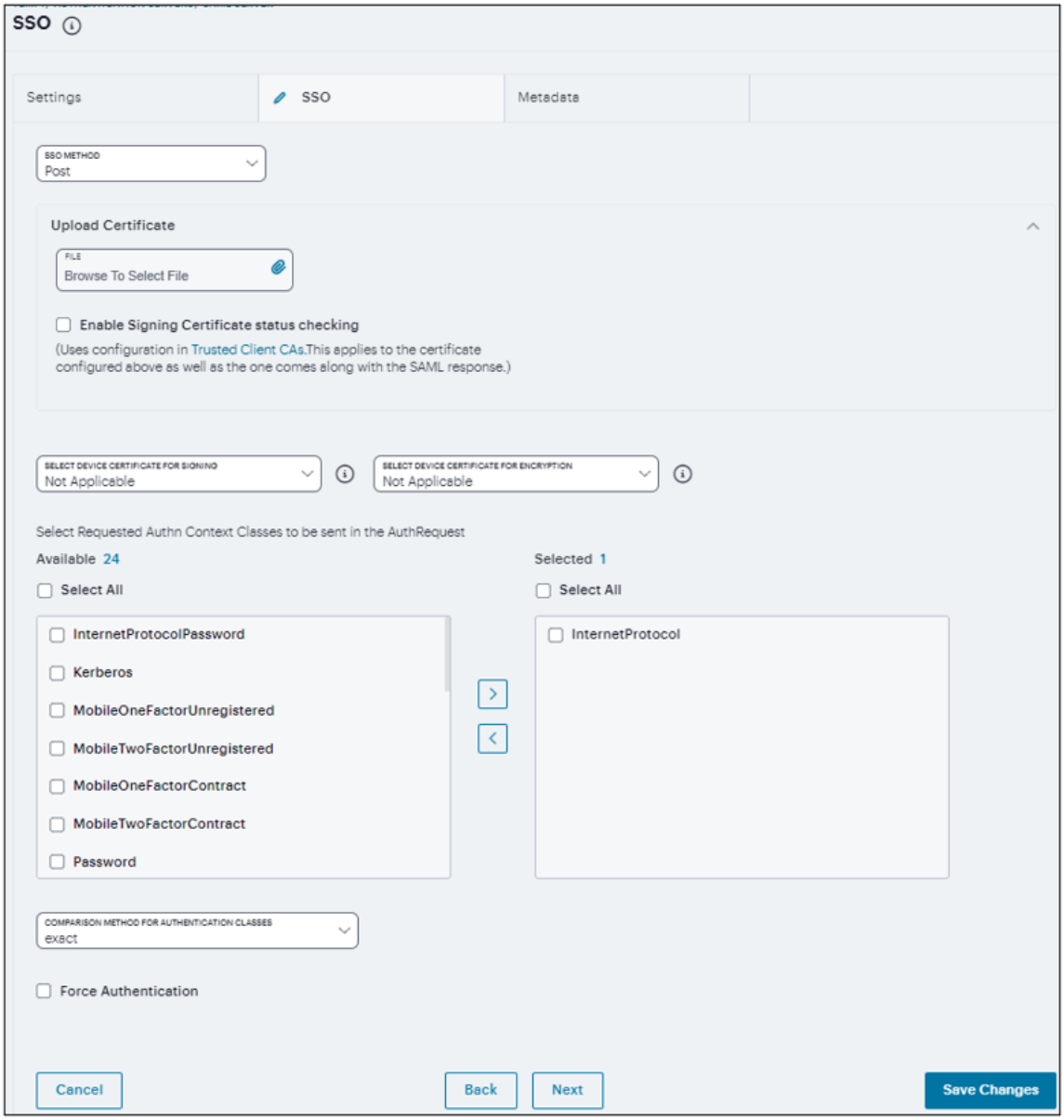


FIGURE 9.47 : SSO Settings

Metadata Settings

- Select the **Metadata** tab.
- Enter the number of days the metadata is valid. Valid values are 0 to 9999. 0 specifies the metadata does not expire.
- Select **Do Not Publish SA Metadata** if you do not want to publish the metadata at the location specified by the **Entity ID** field.
- Select **Download Metadata**. This button appears only after you have saved the authentication server configuration. Use this button to download the metadata of the current SAML service provider.
- Click **Save Changes**.

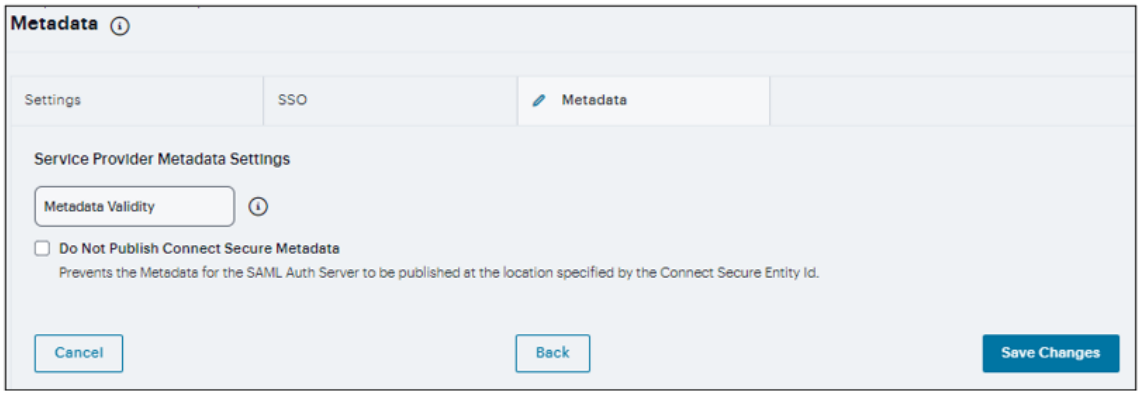


FIGURE 9.48 : Metadata Settings

Configuring TOTP Authentication Server

Time-based One-Time Password (TOTP) algorithm as defined in RFC6238 is an authentication mechanism where a one-time password (a.k.a token) is generated by the authentication server and client from a shared secret key and the current time. ICS can act as TOTP authentication server. Any third-party TOTP applications (for example, Windows Authenticator or Google Authenticator) available on the mobile and desktop client platforms generate TOTP tokens.

To configure the TOTP server as Local:

1. Select **Authentication > Authentication Servers**.
2. Click the Add icon and select **TOTP** from the list to display the configuration page.
3. Complete the configuration and save changes.

   TOTP Auth Server Settings - Local

   - Select **Local** as Server Type. TOTP context is created locally and user database is maintained locally on the same device.
   - Time Skew - Specify maximum time difference between Ivanti Connect Secure and end user device while authenticating a user's token. (minimum: 1 minute, maximum: 5 minutes).
   - Number of attempts allowed - Specify maximum number of consecutive wrong attempts allowed after which account will be locked (minimum: 1 attempt, maximum: 5 attempts).
   - Custom message for registration page - Specify a custom message which can be shown on new TOTP user registration web-page.
   - Allow Auto Unlock - When checked, locked account will be automatically unlocked after specified period. (minimum: 10 minutes, maximum: 90 days).
   - Allow new TOTP user registration to happen via external port - When unchecked (default), new TOTP user registrations will happen only via internal port.

- Accept TOTP authentication from remote ICS devices - When checked, REST access to this TOTP server is allowed from other Ivanti Connect Secure devices.
- Display QR code during user registration - When checked, displays QR code during user registration.
- Disable generation of backup codes - When unchecked, generates backup codes.

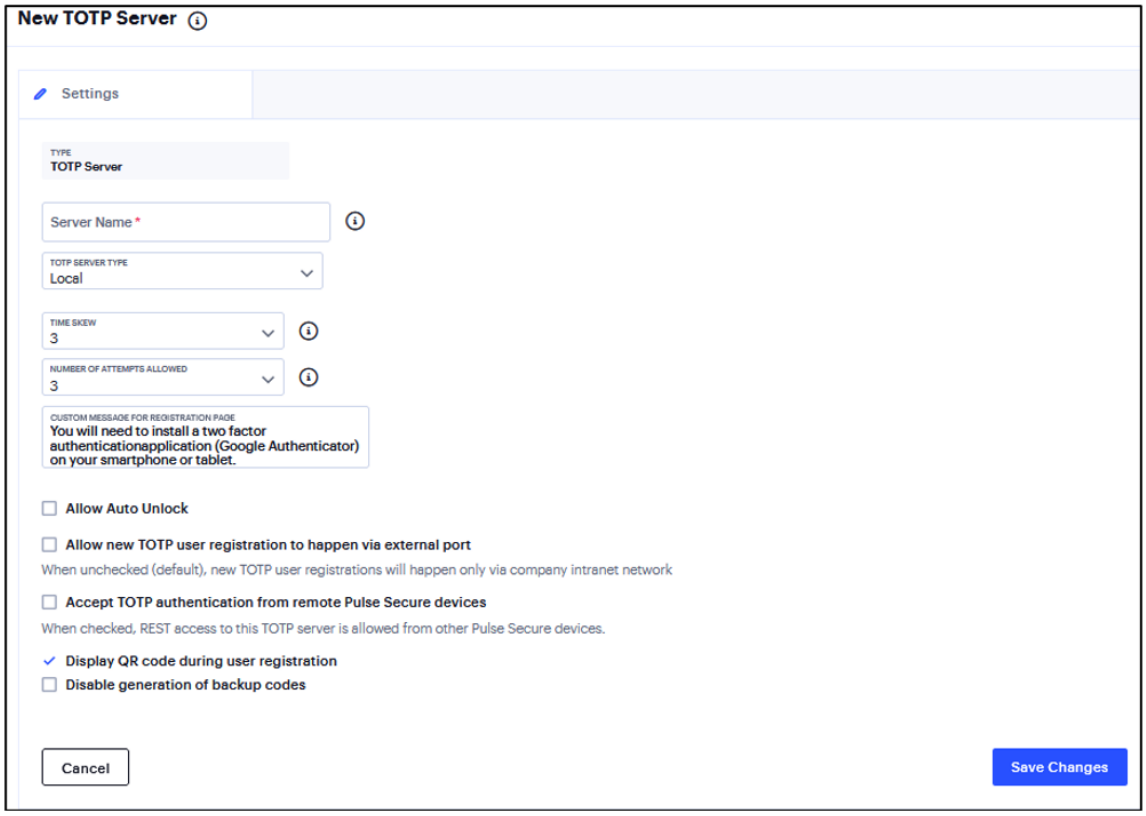


FIGURE 9.49 : TOTP Authentication Server

TOTP Auth Server Settings - Remote

- Select **Remote** as Server Type. In this configuration, authentication checks take place on the remote TOTP server.
- If the **Allow new TOTP user registration to happen via external port** option is not selected, new TOTP user registrations happen only via company intranet network.
- Enter remote host name or IP address where the TOTP server is configured. The IP address or host name must match the common name mentioned in the remote TOTP server certificate.
- Enter TOTP Server Name configured on the Remote TOTP server.
- Enter the REST API login name.
- Enter the REST API password.

- Enter the realm name, which refers to the realm that should be used for authenticating the REST user (using the auth. server mapped to the Realm).
- Use the Test Connection button to validate the connection to the remote TOTP server.

Configuring MDM Authentication Server

The access management framework MDM authentication server configuration includes details on how the system communicates with the MDM Web RESTful API service and how it derives the device identifier from the certificates presented by endpoints.

To configure authentication with the MDM server:

1. Select **Authentication > Authentication Servers**.
2. Click the Add icon and select **MDM** from the list to display the configuration page.
3. Complete the configuration and save changes.
   - Type - Select one of the following options: AirWatch, MobileIron, Microsoft Intune

   Applicable to AirWatch and MobileIron

   - Enter the URL for the MDM server. This is the URL the MDM has instructed you to use to access its RESTful Web API (also called a RESTful Web service).
   - Enter the URL for the MDM report viewer. This URL is used for links from the Active Users page to the MDM report viewer.
   - Enter a timeout period (5-60 seconds) for queries to the MDM server. The default is 15 seconds.
   - Enter the username and password for an account that has privileges to access the MDM RESTful Web API.
   - (AirWatch only) Copy and paste the AirWatch API tenant code.

   Applicable to Microsoft Intune

   - Enter Azure AD Tenant ID.
   - Enter Web application ID that has been registered in Azure AD.
   - Enter Secret key of the web application registered in azure AD.
   - Enter a timeout period (5-60 seconds) for queries to the MDM server. The default is 15 seconds.

   Device Identifier

   - Construct a template to derive the device identifier from the certificate attributes. The template can contain textual characters as well as variables for substitution.

- Select the device identifier type that matches the selection in the MDM SCEP certificate configuration:
  - UUID - The device Universal Unique Identifier. This is the key device identifier supported by MobileIron MDM.
  - Serial Number - The device serial number.
  - UDID - The device Unique Device Identifier. This is the key device identifier supported by AirWatch MDM.
  - IMEI - The device unique identifier. IMEI (15 decimal digits: 14 digits plus a check digit) or IMEISV (16 digits) includes information on the origin, model, and serial number of the device. This is the key device identifier supported by Microsoft Intune.

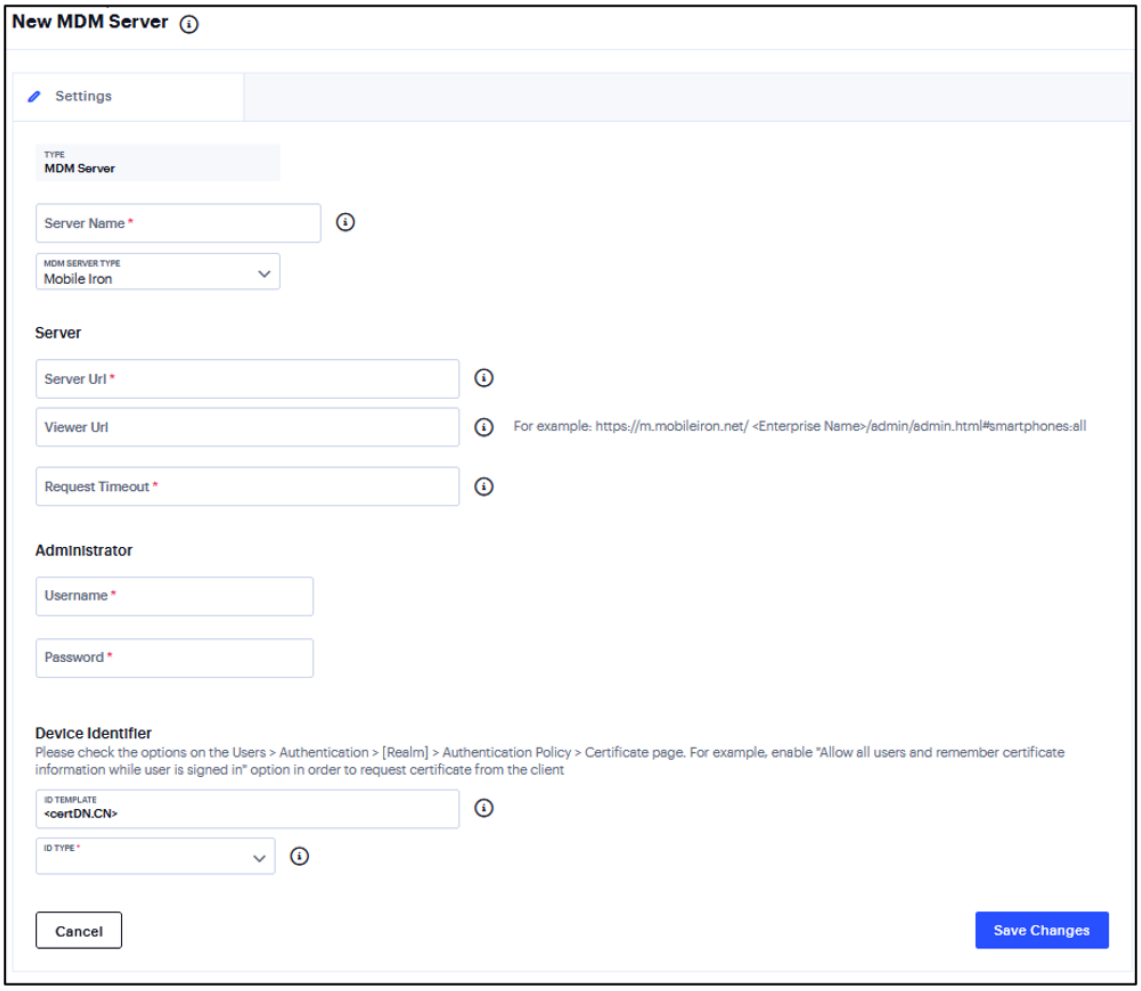


FIGURE 9.50 : MDM Authentication Server

Configuring Active Directory Authentication Server

Active Directory is a directory service used in Windows domain networks. It is included in most Windows server operating systems. Enterprise servers that run Active Directory are called domain controllers. An Active Directory domain controller authenticates and authorizes users and computers in a Windows domain network.

When you use Active Directory as the authentication and authorization service for your Ivanti access management framework, users can sign in to Ivanti Connect Secure using the same username and password they use to access their Windows desktops. You can also use Active Directory group information in role mapping rules.

To configure authentication with the MDM server:

1. Select **Authentication > Authentication Servers**.
2. Click the Add icon and select **Active Directory** from the list to display the configuration page.
3. Complete the configuration and save changes.
    - Specify a name to identify the server within the system.
    - Specify the NetBIOS domain name for the Active Directory domain.
    - Specify the FQDN of the Active Directory domain.
    - Specify a username that has permission to join computers to the Active Directory domain.
    - Specify the password for the special user.
    - Select **Save Credentials**. If this setting is not enabled, the credentials entered will be destroyed after successfully joining the domain.
    - Specify the machine account name. The default computer name is derived from the license hardware in the following format: 0161MT2L00K2C0. We recommend the Computer Name string contain no more than 14 characters to avoid potential issues with the AD/NT server. Do not include the '$' character.
    - Specify the protocol to use during authentication. The system attempts authentication using the protocols you have enabled in the order shown on the configuration page. For example, if you have selected the check boxes for Kerberos and NTLMv2, the system sends the credentials to Kerberos. If Kerberos succeeds, the system does not send the credentials to NTLMv2. If Kerberos is not supported or fails, the system uses NTLMv2 as the next protocol in order.
    - Contact trusted domains. Select this option to contact domain controllers of trusted domains directly without proxying authentication requests and group membership checks through the domain controller.
    - Enter the maximum number of simultaneous domain connections (1 to 10).

- Enable periodic password change of machine account. Select this option to change the domain machine account password for this configuration.
- Click **Save Changes**.

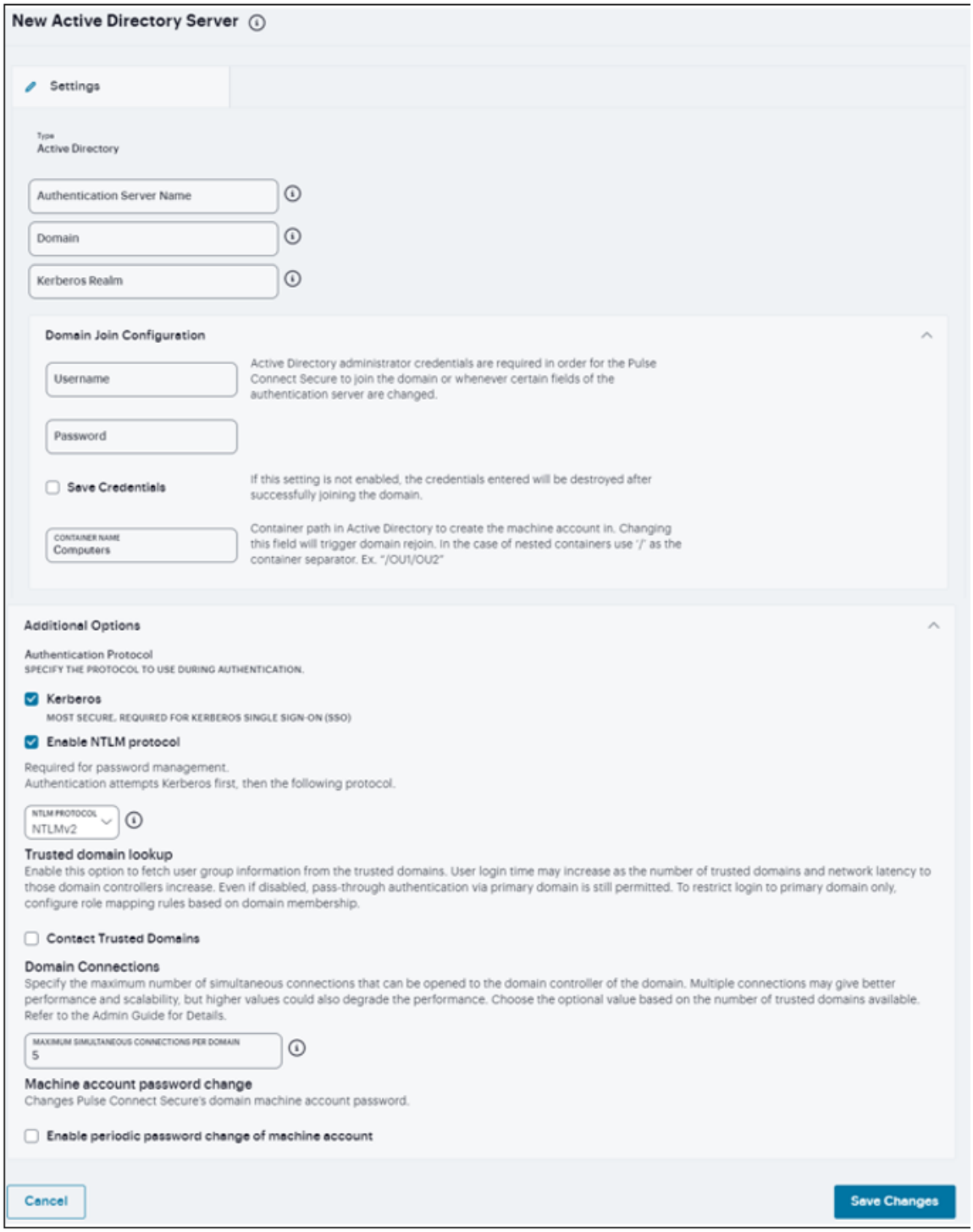


FIGURE 9.51 : Active Directory Authentication Server

Archiving Servers

You can schedule periodic archiving for system logs, system configuration files, and system snapshots. Periodic archiving occurs only at the scheduled time. “Unscheduled” archiving does not occur automatically.

To configure log archiving:

1. In the **Maintenance > Archiving > Archiving Servers** page, select **Method** from the drop-down list.

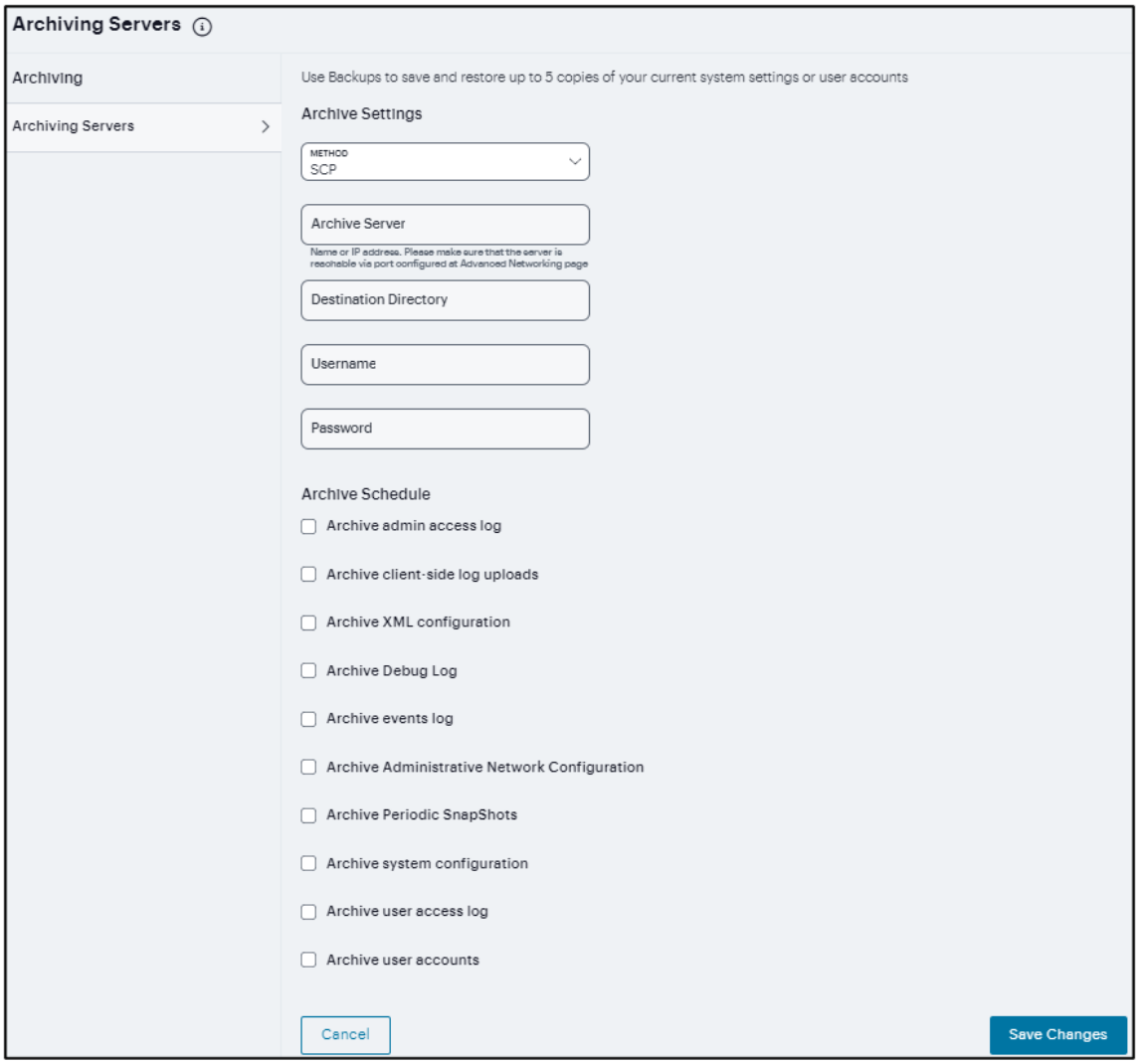


FIGURE 9.52 : Archiving Server

2. Enter the fully qualified Domain name or IP address of the server to which to send the archive files.
3. Enter the **Destination directory**.
4. Enter a **Username** and **Password** that has privileges to log into the server and write to the destination directory.

5. Select the required **Archive Schedule** options.
6. Click **Save Changes**.

System Configuration

Introduction

When you install and initially set up the device, you use the serial port console to set basic network and host settings. To get started, you must use the serial console to configure these settings for the internal interface. You have the option to use the serial console to configure network and host settings for the external interface and the management interface.

Once the internal interface has been configured, you can use the admin console Network Settings pages to modify settings for the internal interface, to enable and configure the external interface and the management interface, and to configure or manage advanced networking features, including:

- Hostname
- IPv6 addresses
- VLAN ports
- Virtual ports
- Route table entries
- Host mapping table entries
- ARP cache entries
- Neighbor discovery cache entries
- System date and time (manual configuration) or NTP

NTP Configuration

You can use the admin console to set the system date and time manually or by configuring a network time protocol (NTP) server. The system supports NTPv4, which is backwards compatible with NTPv3 and NTPv2.

Note: We recommend you use NTP to synchronize the date and time clocks on all network systems. Using NTP obviates issues that might occur with cluster synchronization, network communication that uses time-sensitive protocols, such as SAML, and implementation of time - based policies, such as local authentication server account expiration. In addition, using NTP as a standard in your network rationalizes timestamps in logs, which facilitates reporting and troubleshooting.

To configure NTP:

1. Log into the nSA as a Tenant Admin.
2. From the ICS menu, click the **Gateways > Gateways List** and then select any standalone ICS Gateway or Cluster node.
3. Navigate to **System > NTP** displays the System Status page with *System Date and Time*.

4. Select your **Time Zone**. Selecting the appropriate time zone enables the system to automatically adjust the time for Daylight Saving Time changes
5. Select **Time Source**.
    - If **Use Pool of NTP Servers** is selected, configuring one NTP server is mandatory, but keys are optional. Click **Save Changes**.

      Note: It is not recommended to use only two NTP servers. If more than one NTP server is required, four NTP servers is recommended minimum. Four servers protect against one incorrect timesource.

      Note: If you are using NTPv4, specify the symmetric key. The key must be pre-synchronized with the NTP server. For example, if you want to configure NIST's clock as the NTP server, you must request a key beforehand and have NIST send that key to you.

    - If **Set Time Manually** is selected, Specify the **Date** and **Time** with **Time Slot**.
    - You can click **Get from Browser** to automatically populate the *Date* and *Time* fields. Click **Save Changes**.

Licensing Mode

You can use either Gateway licenses or nSA Named User licenses. You can switch between these two licensing modes any time. Gateway Licensing mode is same as the existing 9.x Gateway licensing.

To choose the licensing mode:

1. Log into the nSA as a Tenant Admin.
2. From the ICS menu, click the *Gateways > Gateways List* and then select any standalone ICS Gateway and Cluster node.
3. Navigate to **System > Configuration > Licensing > Licensing Summary**. The License Summary page shows the two options, **Gateway Licensing Mode** and **nSA Named User Licensing Mode**. By default, *Gateway Licensing Mode* is selected.
4. Choose the required mode and click **Switch**. You can view the **Licensed capacity**.
5. Under **Installed license details** enter **License key(s)** in the field and click **Add**. You can view the nodes and corresponding license.

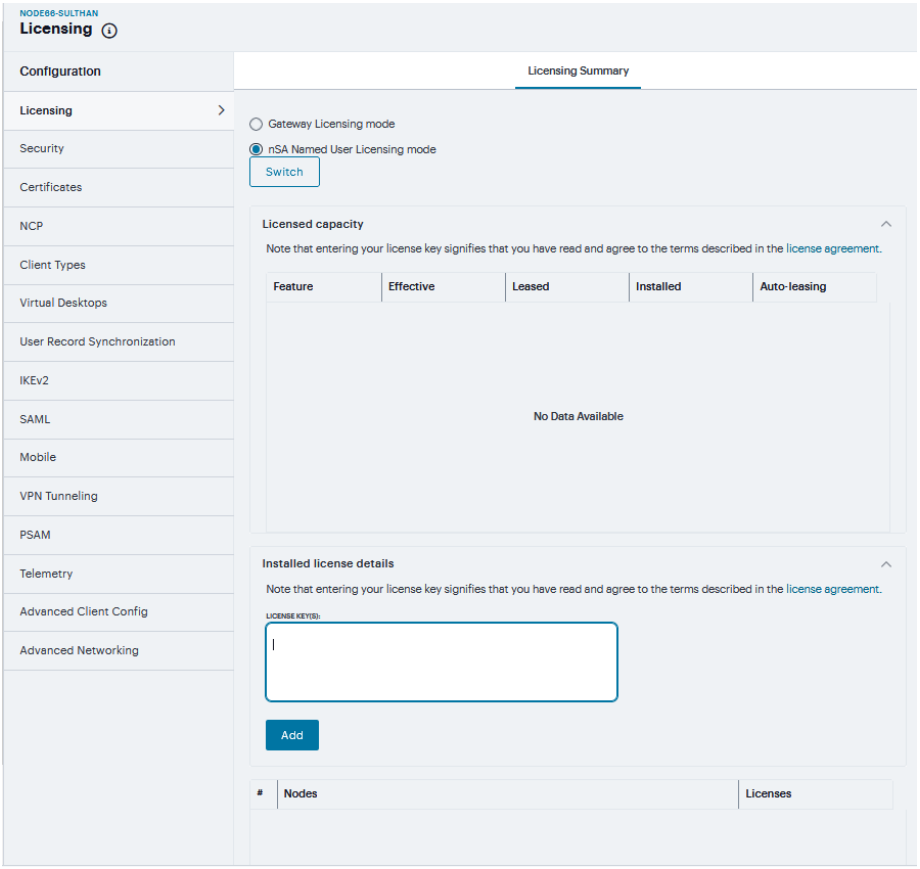


FIGURE 10.1 : Licensing

Security Configuration

Granular cipher selection provides an administrator the ability to select specific ciphers and the preferred ordering of the selected ciphers. This feature also provides presets like Suite and PFS. There are two tabs, Inbound OpenSSL options and Outbound OpenSSL options. With this feature admins can select the ciphers that TLS/SSL connections will use. The Inbound OpenSSL options apply to all incoming connections. Outbound OpenSSL options apply to the following services:

- Rewriter
- ActiveSync
- SCEP
- Syslog
- LDAPS

Inbound SSL Options

To enable the Inbound SSL options Mode:

1. Navigate to **System > Configuration > Security > Inbound SSL Options**.
2. Click on **Turn on JITC mode** check box.
3. Once Turn on JITC mode is enabled, Turn on NDcPP mode and Turn on FIPS mode are also automatically enabled.
4. In **Inbound settings**, select **Allowed SSL and TLS Version** and **Allowed Encryption Strength**.

Note: NDcPP mode can be enabled in the Inbound tab with a check box. This status is also applied over to the Outbound tab. Turning on NDcPP automatically turns on FIPS mode and disables SSL/TLS Version TLS1.0 and below. Also, NDcPP Mode allows to choose only 16 Ciphers under Custom Encryption Strength.

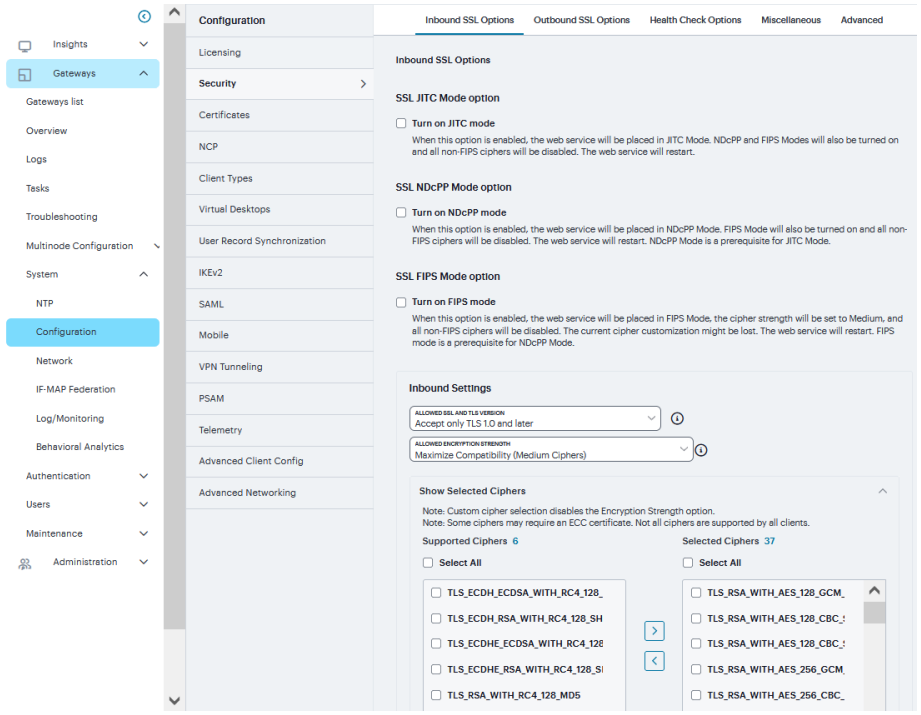


FIGURE 10.2 : Inbound SSL Options

5. The two panels of **Supported Ciphers** and **Selected Ciphers** are displayed. Supported ciphers has the entire list of ciphers supported for the selected SSL or TLS version. Selected ciphers list the currently selected ciphers list.
6. Select **Encryption Strength option** to strengthen the SSL session that is established.
7. Select **Key Exchange Options** to increase the key exchange strength to 2048bit DHE.

8. Select **Enable support for SSL legacy renegotiation** to allow new TLS Renegotiation Info extension.
9. Set **SSL Handshake Timeout option**
10. Select **Enable client certificate** to enable Client certificate on the external port and/or the virtual ports.
11. The two panels of **External Virtual Ports** and **Selected Virtual Ports** are displayed. External Virtual Ports has the entire list of ports available for the selected certificate. Selected Virtual Ports list the currently selected ports list.
12. The two panels of Internal Virtual Ports and Selected Virtual Ports are displayed. Internal Virtual Ports has the entire list of ports available for the selected certificate. Selected Virtual Ports list the currently selected ports list. You can move the virtual ports from the external/internal to selected list and vice versa.
13. Click **Save Changes**.

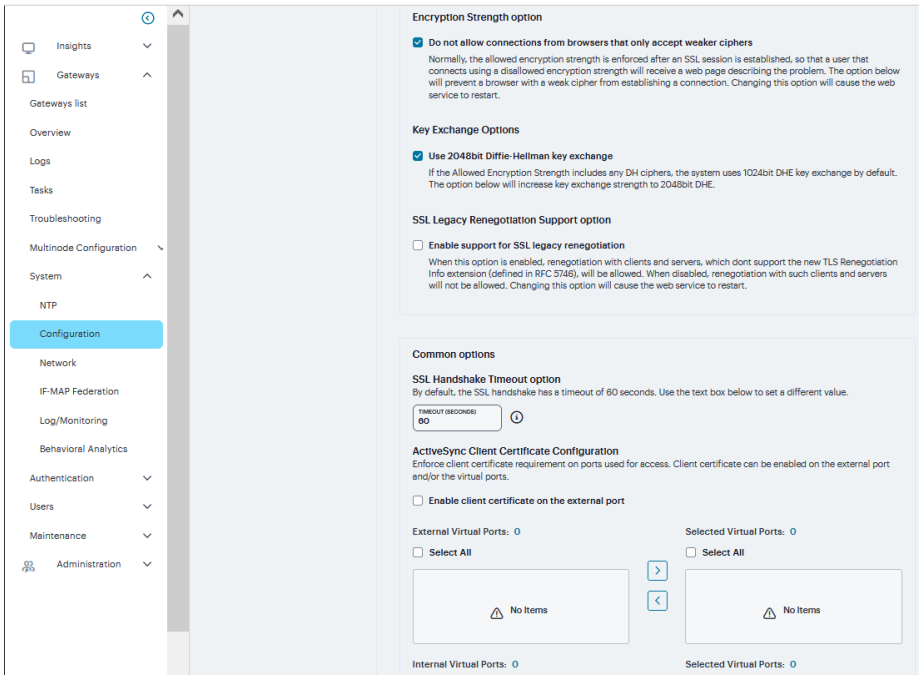


FIGURE 10.3 : Inbound SSL Options

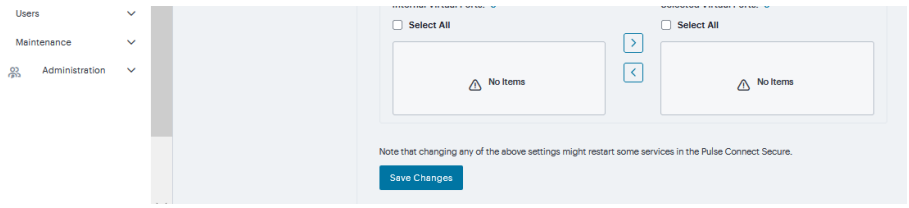


FIGURE 10.4 : Inbound SSL Options

Outbound SSL Options

To enable the Outbound SSL options Mode:

1. Navigate to **System > Configuration > Security > Outbound SSL Options**.

Note: Only for Outbound SSL Settings, we can configure Non FIPS Ciphers when FIPS is Enabled using Custom Cipher Selection Option. Now, there are options to change different SSL/TLS versions and different encryptions in the Outbound SSL Settings.

---

2. **DoD Certification Mode**, **SSL NDcPP Mode**, and **SSL FIPS Mode** are OFF all these can be enabled from **Inbound SSL options** tab.
3. In **Outbound settings**, select **Allowed SSL and TLS Version** and **Allowed Encryption Strength**
4. The two panels of **Supported Ciphers** and **Selected Ciphers** are displayed. Supported ciphers has the entire list of ciphers supported for the selected SSL or TLS version. Selected ciphers list the currently selected ciphers list. The following figure shows the two panels (Supported Ciphers and Selected Ciphers). Note that the Selected Ciphers and Supported Ciphers List will also be displayed for all Preset like PFS or Suite B or Medium or High.
5. Click **Save Changes**.

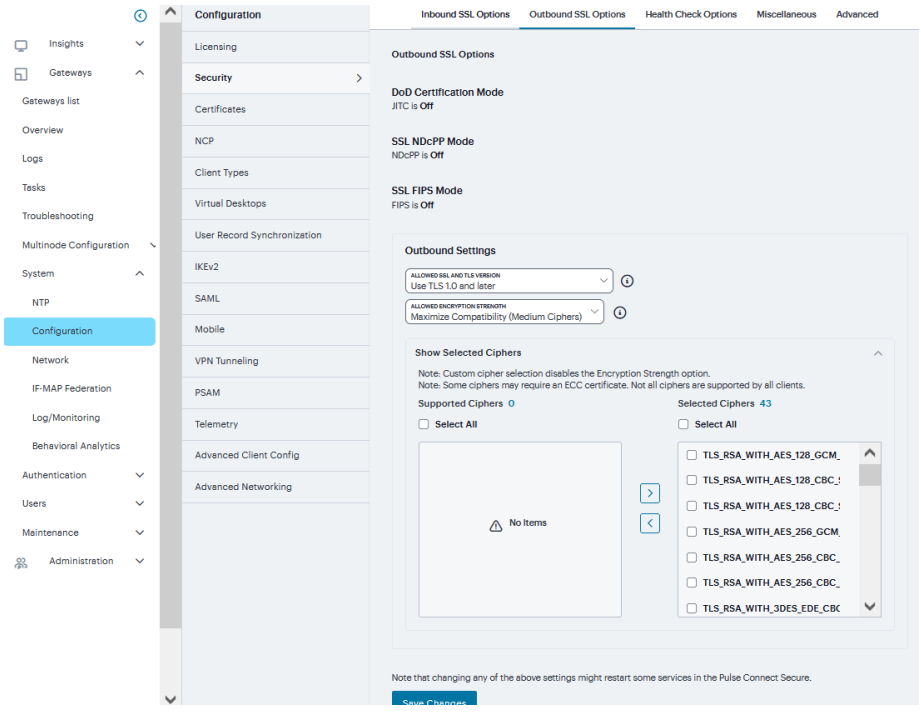


FIGURE 10.5 : Outbound SSL Options

Health Check Options

To configure health check options:

1. Navigate to **System > Configuration > Security > Health Check Options** to display the configuration page.

   Note: Enable additional information via healthcheck.cgi-This option is used by entities like load balancers to monitor the health status of the node.

2. Select the **Enable additional information via healthcheck.cgi** check box.
3. Click '**+**' to add the relevant IPv4/v6 addresses for which additional information is required to be made available.
4. Click **Save Changes**.

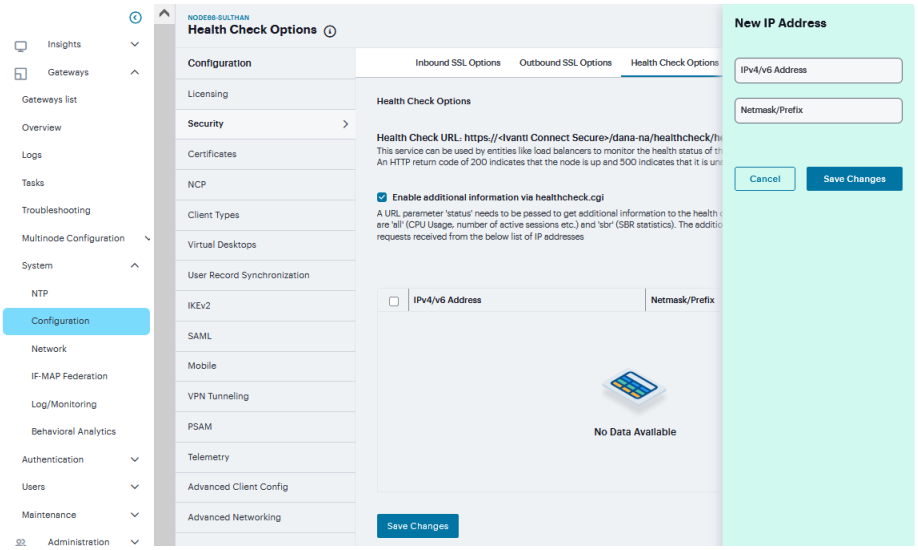


FIGURE 10.6 : Health Check

Miscellaneous Setup

You can use the **System > Configuration > Security > Miscellaneous** page to configure the following security options:

- Persistent cookie options - You can choose whether to preserve or delete persistent cookies when a session is terminated.
- Lockout options - You can configure lockout options to protect the system from denial of service (DoS), distributed denial of service (DDoS), and password-guessing attacks.
- Last login - You can choose whether to show users the time and IP address their user ID was used to sign in.

- X-Frame-Options protection - You can choose to defend against click-jacking attacks by adding X-Frame-Option header to all the IVE generated pages. If this is not enabled, then only welcome.cgi will have this header.
- Slow Post Attack Defense - You can configure to protect against slow-post DOS attacks from non-authenticated users.
- HSTS - HTTP Strict Transport Security (HSTS) is a HTTP special response header which will prevent any communications over HTTP
- Host Manifest Integrity Validation - You can configure to protect against integrity attacks.
- Host Header Validation – You can block open redirect attacks
- Username Validation – You can block unauthorized access
- Integrity checking options - You can configure scan the system to periodically check for any integrity anomalies. If any anomaly found, information is displayed in the dashboard.

To configure cookie and lockout options:

1. Select **System > Configuration > Security > Miscellaneous** to display the configuration page.
2. Complete the configuration as described in the following table.
3. Click **Save Changes**.

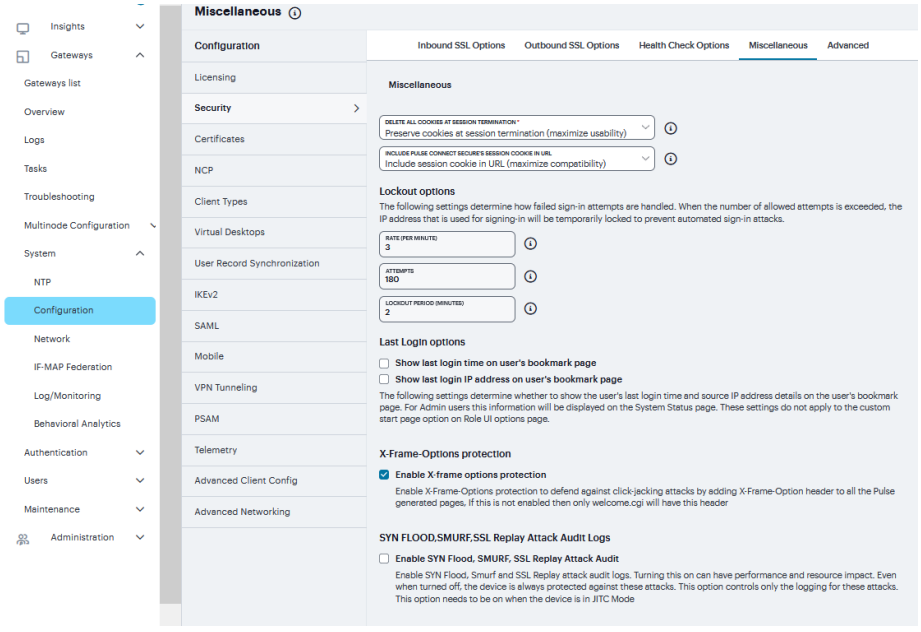


FIGURE 10.7 : Miscellaneous

TABLE 10.1 : Security Options Configuration Guidelines

Setting	Guidelines
Delete all cookies at session termination	
Delete / Preserve	For convenience, the system sets persistent cookies on the user's machine to support functions such as multiple sign-in, last associated realm, and the last sign-in URL. For additional security or privacy, you can choose not to set them.
Include Connect Secure's session cookie in URL	
Include / Not Include	Mozilla 1.6 and Safari may not pass cookies to the Java Virtual Machine, preventing users from running JSAM and Java applets. To support these browsers, the system can include the user session cookie in the URL that launches JSAM or a Java applet. By default, this option is enabled, but if you have concerns about exposing the cookie in the URL, you can disable this feature.
Lockout options	
Rate	Specify the number of failed sign-in attempts to allow per minute.
Attempts	Specify the maximum number of failed sign-in attempts to allow before triggering the initial lockout. The system determines the maximum initial period of time (in minutes) to allow the failed sign-in attempts to occur by dividing the specified number of attempts by the rate. For ex-ample, 180 attempts divided by a rate of 3 results in an initial period of 60 minutes. If 180 or more failed sign-in attempts occur within 60 minutes or less, the system locks out the IP address being used for the failed sign-in attempt.
Lockout period	Specify the length of time (in minutes) the system must lock out the IP address.
Last Login options	
Time / IP Address	Display the day and time and IP address the user last logged in to the system. For users, this information appears on their bookmark page. For administrators, this information appears on the System Status Overview page. These settings do not apply to the custom start page option on Role UI Options page.

continues on next page

TABLE 10.1 – continued from previous page

Setting	Guidelines
X-Frame-Options protection	
Enable X-Frame Options protection	By default, the Enable X-Frame-Options is checked. If the admin does not want to have this protection, they can uncheck this option. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a <frame>, <iframe> or <object>.
Slow Post Attack Defense	
Timeout	By default, the POST body is received within 10 seconds. If the browser is unable to send the POST body within 10 seconds the connection is eventually dropped. (Configurable from 3 - 60Sec)
Maximum Request Size	By default, now a connection is directly rejected if it tries to POST more than 4KB in POST body (Configurable from 256 Bytes to 24 KB)
HSTS	
Max Age	Specify the maximum age for HSTS. It can be disabled by configuring max age as 0.
Enable include Sub-domain directive	Select the check box to enable/disable the include Sub-domain directive. By default, it is turned off.
Enable preload directive	Select the check box to enable/disable the preload directive. By default, it is turned off.
Host Manifest Integrity Validation	
Enable Host Manifest Integrity Validation to stop booting if manifest integrity validation fails	Select the check box to enforce host manifest integrity validation. By default, it is turned off. The following integrity checks are performed: Checks the SHA512 digital signature of the manifest file. Checks the SHA256 digest of each individual file entries in the manifest. If enabled and integrity check fails, admin needs to roll back to previous working package or perform factory reset.
Host Header Validation	

continues on next page

TABLE 10.1 – continued from previous page

Setting	Guidelines
Enable Host header validation to block open redirect attacks	Select the check box to enforce host header validation. By default, it is turned off. When Host header validation is enabled, every http request will be validated against hostnames and IP v4/v6 addresses known to the ICS server. If match is not found, the request will be dropped and logs are recorded in admin access logs and user access logs, and a response will be sent back to client.
Username Validation	
Enable Username validation to block unauthorized access	Select the check box to enforce username validation for usage of unsupported characters. Max allowed length for username is 128 characters.
Runtime Integrity Scanner Interval	
Periodic Scan	Select the time interval to run the integrity scanner during run time. For example: Select 2 hrs to run the integrity scanner every 2 hrs.
Scheduled Scan	Select to run integrity scanner at a specified time everyday. For example: When 13 hours 25 min is specified, the scanner runs at the same time everyday.
Referrer Header Validation	
Enable Referrer Header validation to block CSRF attacks	Select the check box to enable referrer header validation.

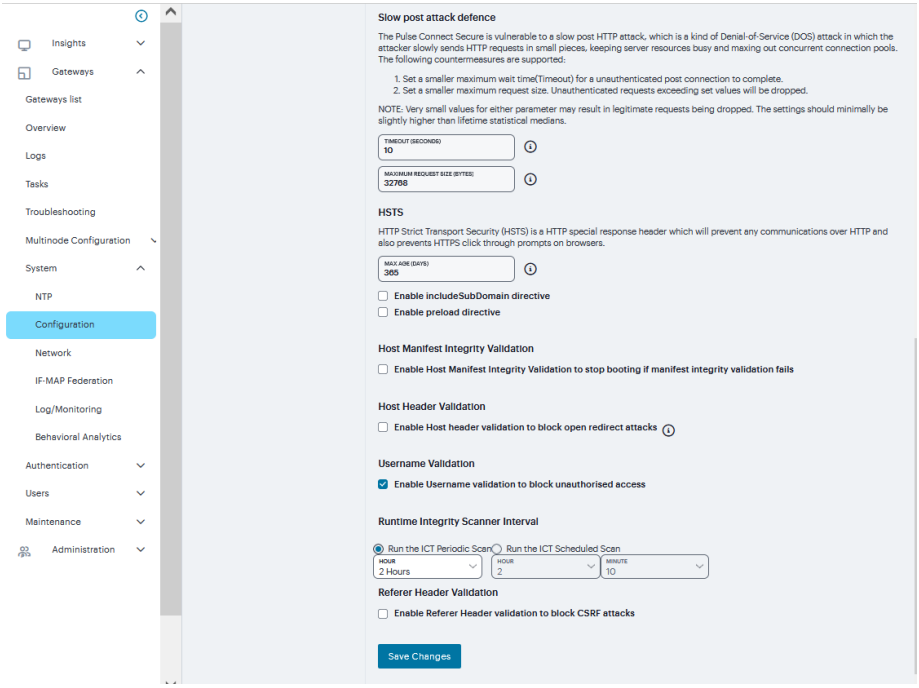


FIGURE 10.8 : Miscellaneous

Advanced Configuration

Connect Secure supports several HTTP headers, which are sent in response to the client request. There are several more headers built to improve security and prevent attacks like XSS. The Custom HTTP Headers configuration enables the administrator to add new headers that they want to enforce.

To configure custom HTTP header:

1. Navigate to **System > Configuration > Security > Advanced**
2. Click '**+**' to Add the relevant **HTTP Header** and **Header Directive**.
3. Click **Save Changes**

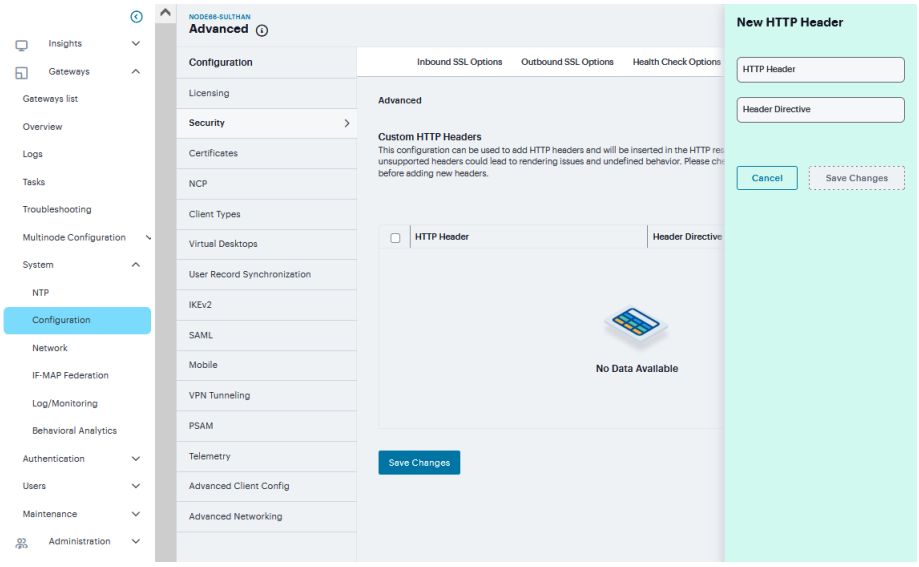


FIGURE 10.9 : Advanced

Certificates

Connect Secure uses Public Key Infrastructure (PKI) to secure the data sent to clients over the Internet. PKI is a security method that uses public and private keys to encrypt and decrypt information. These keys are enabled and stored through digital certificates. A digital certificate is an encrypted electronic file issued by a certificate authority (CA) that establishes credentials for client/server transactions.

Device Certificates

A device certificate helps to secure network traffic to and from the Ivanti Secure Access client service using elements such as your company name, a copy of your company's public key, the digital signature of the Certificate Authority (CA) that issued the certificate, a serial number, and an expiration date. When receiving the device certificate from the system, the client's browser first verifies whether the device certificate is valid and whether the user trusts the CA that issued the certificate. If the user has not already indicated that they trust the certificate issuer, the Web browser prompts the user with a warning saying connection is untrusted or there is a problem with the websites security certificate.

To import an enterprise root server certificate and private key:

1. Select **System > Configuration > Certificates > Device Certificates**.
2. Click **Import Certificate** to display the configuration page.

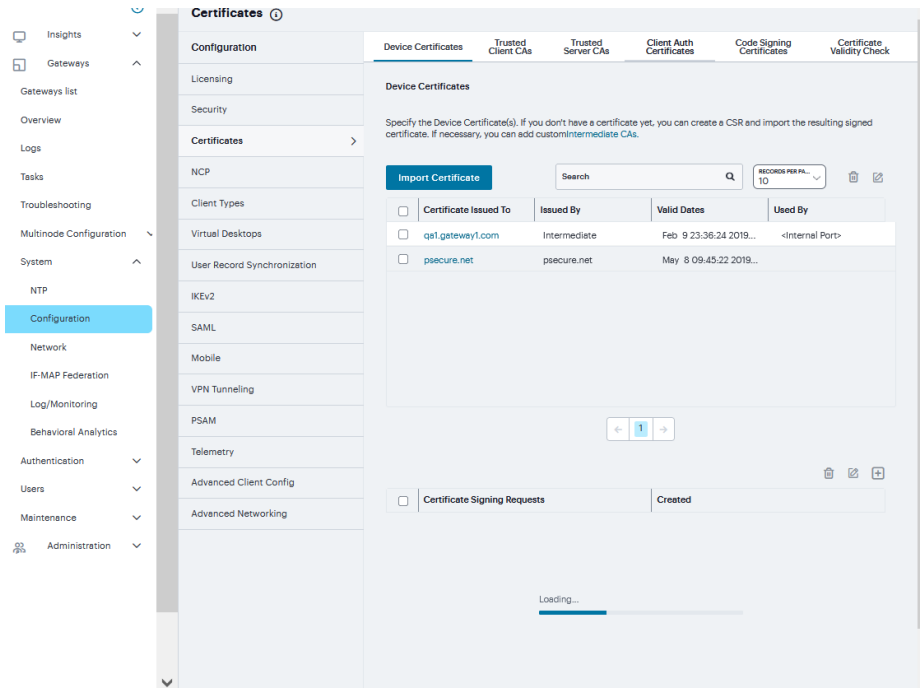


FIGURE 10.10 : Device Certificates

3. Complete the configuration described in table.
4. Click **Import**.

TABLE 10.2 : Import Certificate and Key Settings

Setting	Guidelines
If certificate and private file are separate keys	
Certificate File	Browse to the network path or local directory location of your certificate key file.
Private Key File	Browse to the network path or local directory location of your private key file.
Password Key	Enter the password key.
If certificate file includes private key	
Certificate File	Browse to the network path or local directory location of the Certificate File.
Password	Enter the password.
Import via System Configuration file	
System Configuration file	Browse to the network path or local directory location of the Certificate File. With this option, the system imports all of the certificates specified (including private keys and pending CSRs, but not the corresponding port mappings).
Password	Enter the password. If the file is password-protected, enter the password key.

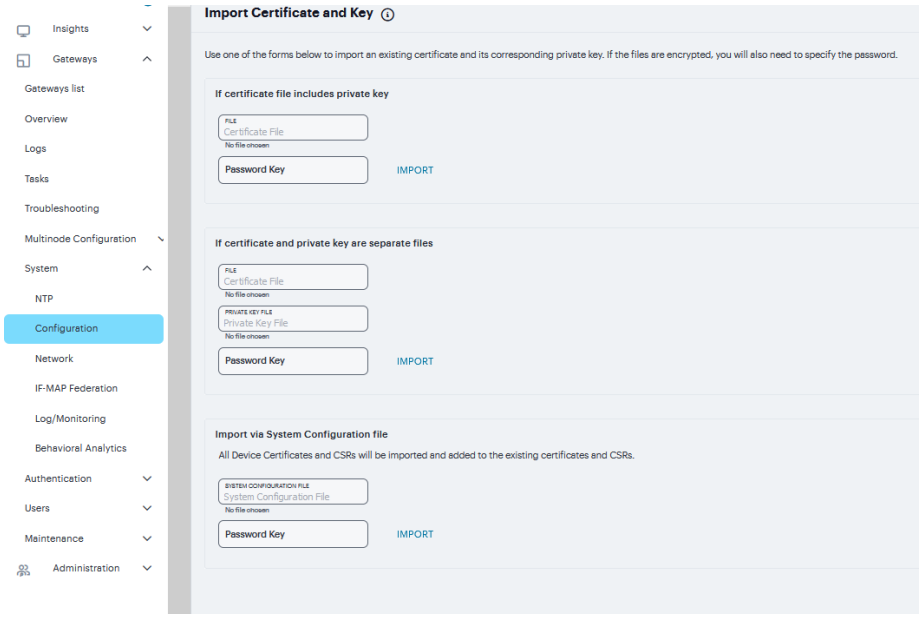


FIGURE 10.11 : Import Certificate and Key

To create Certificate Signing Request (CSR) for RSA and ECC Keys:

1. Navigate to **System > Configuration > Certificates > Client Auth Certificates**.
2. Click '**+**' on the **Certificate Signing Requests** pane.
3. Enter the required requestor information. In this example, the common name is *ecc-p256.<orgname>.net* or *pcs.<orgname>.net*.
   - If **RSA** is selected, then select **Key Length** and enter **Random characters**.
   - If **ECC** is selected, then select **ECC Curve** drop-down.
4. Click **Save Changes**.
5. The CSR is encoded and can be copied or saved to a file. The ECC certificate should be signed by an RSA/ECC CA for Suite B compliance. Follow your CA's process for sending a CSR.
6. Click the **Back to Device Certificates** link. Until you import the signed certificate from your CA, your CSR is listed as Pending.

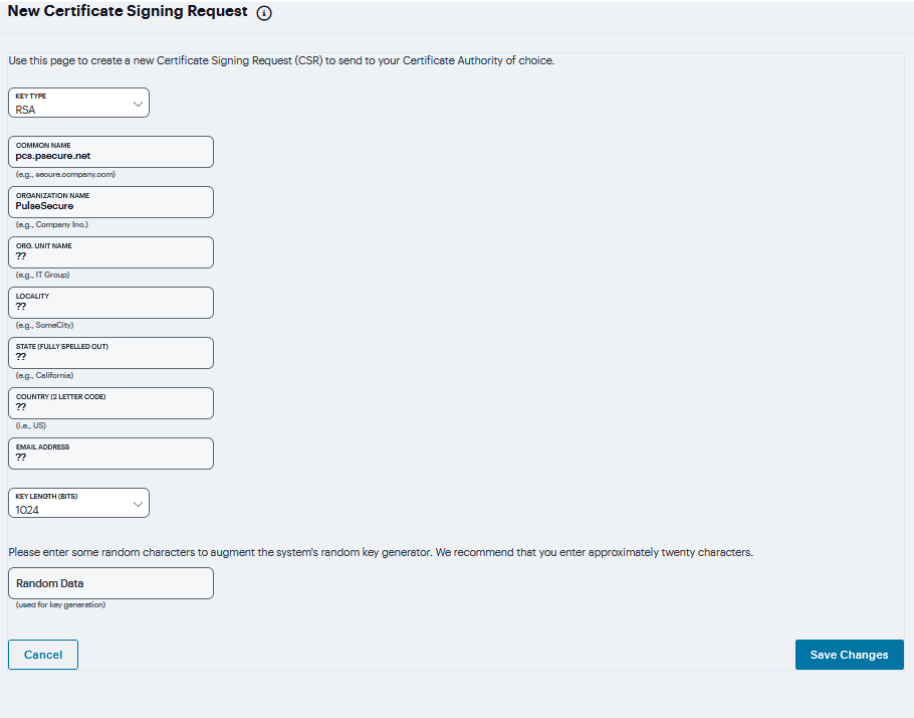


FIGURE 10.12 : Certificate Signing Request

Trusted Client CAs

A trusted client CA is a CA that you deem trusted by adding it to the trusted client CA store. The system trusts any certificate issued by that CA. To use client CA certificates, you must install and enable the proper certificates. Additionally, you must install the corresponding client-side certificates in your users' Web browsers, or you must use the MMC snap-in in your users' computer accounts (machine certificate). When validating a client-side CA certificate, the system verifies that the certificate is not expired or corrupt and that the certificate is signed by a CA that the system has been configured to recognize. If the CA certificate is chained, the system also follows the chain of issuers until it reaches the root CA, validating each issuer in turn. The system supports X.509 CA certificates in DER and PEM encode formats.

To import a trusted client CA certificate:

1. Navigate to **System > Configuration > Certificates > Trusted Client CAs** to display the configuration page.

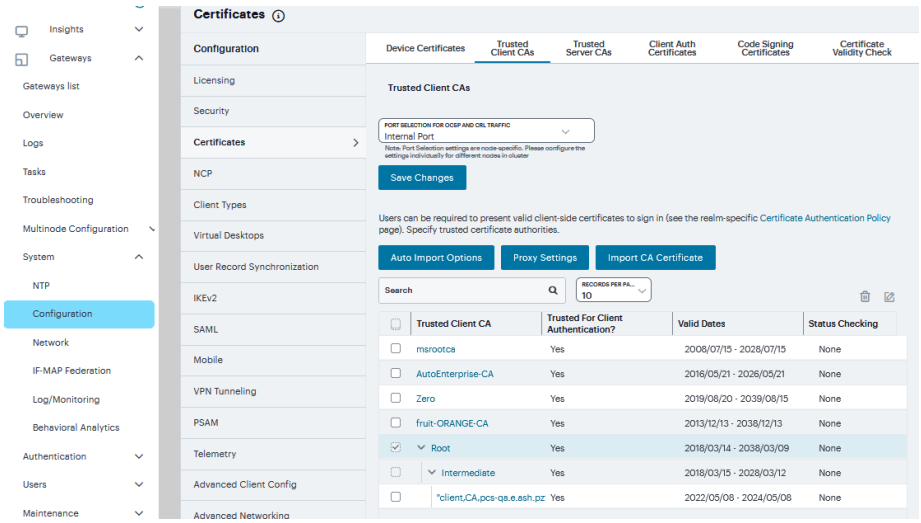


FIGURE 10.13 : Trusted Client CAs

2. Click **Import CA Certificate** to display the configuration page.
3. Browse to the *Certificate File*, select it, and click **Import** to complete the import operation.

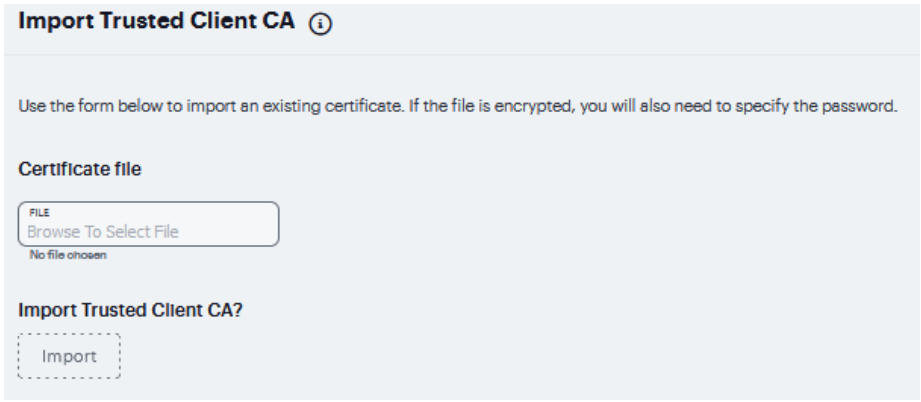


FIGURE 10.14 : Certificate File

To enable auto-importing:

1. Navigate to **System > Configuration > Certificates > Trusted Client CAs**.
2. Click the **Auto-Import Options** button to display the options.
3. Complete the configuration described in the following table.
4. Click **Save Changes**.

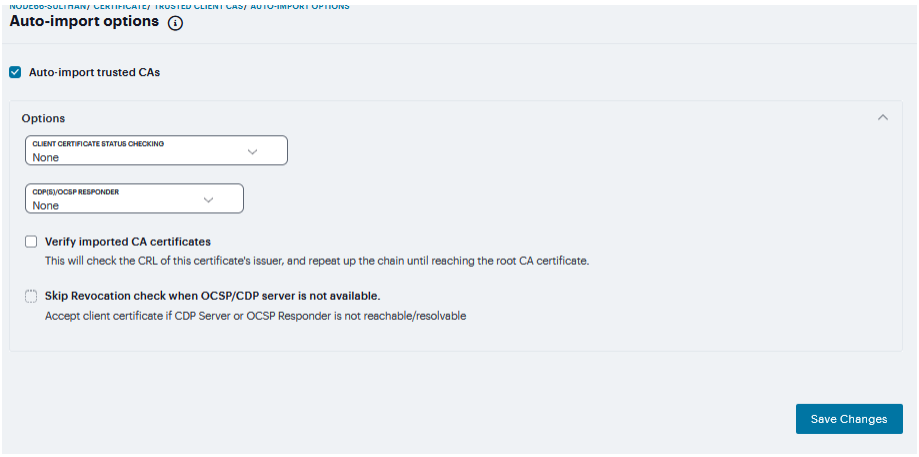


FIGURE 10.15 : Auto-Import

TABLE 10.3 : Auto-Import Options Settings

Setting	Guidelines
Auto-import trusted CAs	Select this option to enable auto-import and display its configuration settings.
Client Certificate Status Checking	**Select a method to validate the trusted client certificate:** • None-Do not validate. • Use OCSP-Use the OCSP method, validating the client certificate in real-time, as needed. After you select this option, you can specify options for OCSP. • Use CRLs-Use CRLs to validate the client certificate. After you select this option, you can specify options for CRL. • Use OCSP with CRL fallback-Use the OCSP validation method when possible, but attempt to validate client certificates using CRLs if the OCSP method fails (for example, if the link to the OCSP responder fails). After you select this option, you can specify options for OCSP and CRL. Inherit from root CA-Use the method configured for the device certificate.
CDP(s)/OCSP responder	**Select the location of the responder value:** • None-Do not use the responder. • From client certificate-Use the responder value configured in the client certificate. • From trusted CA certificate-Use the responder value configured in the trusted CA certificate that has been uploaded to the system.
Verify imported CA certificates	Select this option to verify that this trusted client CA is valid. Enabling this will check the CRL of this certificate's issuer, and repeat up the chain until reaching the root trusted client CA.
Skip Revocation check when OCSP/CDP server is not available	**Select this option to instruct ICS to skip revocation check and accept end us** The OCSP Timeout, applicable only for OCSP, is used as the maximum timeout for a network connection or data transfer operation while connecting to an OCSP Responder. An internal timeout will be used for CDP. ICS skips the revocation check in the following conditions: • Server IP is not reachable

To configure a proxy server:

1. Select **System > Configuration > Certificates > Trusted Client CAs**.
2. Click **Proxy Settings** to display the page.
3. Complete the configuration described in Proxy Settings table.
4. Click **Save Changes**.

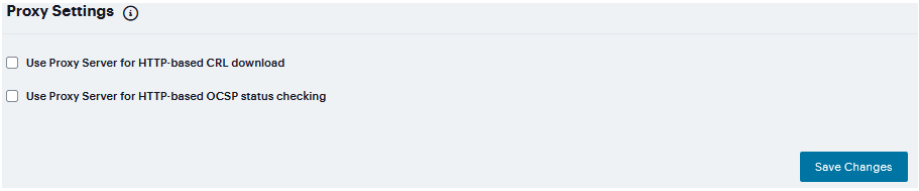


FIGURE 10.16 : Proxy Settings

TABLE 10.4 : Proxy Settings

Setting	Guidelines
Use Proxy Server for HTTP-based CRL download	Select to enable the CRL operations to use a proxy server. You can configure a proxy server for web-based URLs, not LDAP URLs.
Use Proxy Server for HTTP-based OCSP status checking	Select to enable the OCSP operations to use a proxy server.
Host Address	Specify either an IP address or a fully qualified domain name.
Port	Enter the proxy server port number if it is different from the default value of 80.
Username/password	If your proxy server required authentication, enter a username and password to log in to the proxy server.

Trusted Server CAs

All of the trusted root CAs for the Web certificates installed in Internet Explorer are preinstalled. You might need to install a trusted server CA for additional Web servers in the following situations:

- If you are using third-party integrity measurement verifiers (IMVs) that are installed on a remote server, you must upload the trusted root certificate of the CA that signed the remote server's server certificate.
- If you are using virus signature version monitoring with your own staging site for storing the current virus signatures list, you must upload the trusted root certificate of the CA that signed the staging server certificate.

You can install the trusted root CA certificate on the endpoint in any of the following ways:

- Use a CA certificate that is chained to a root certificate that is already installed on the endpoint, such as VeriSign.
- Upload the CA certificate and any intermediate CA certificates to the Ivanti Secure Access client system. During client installation, the system automatically installs the trusted root device CA certificates on the endpoint. When prompted during installation, the user must allow the installation of the CA certificate(s).
- Prompt users to import the CA certificates on the endpoint using Internet Explorer or other Microsoft Windows tools. In other words, you can use common methods organizations use to distribute root certificates.

To upload CA certificates:

1. Select **System > Configuration > Certificates > Trusted Server CAs** to display the page.
2. Click **Import Trusted Server CA** to display the page.

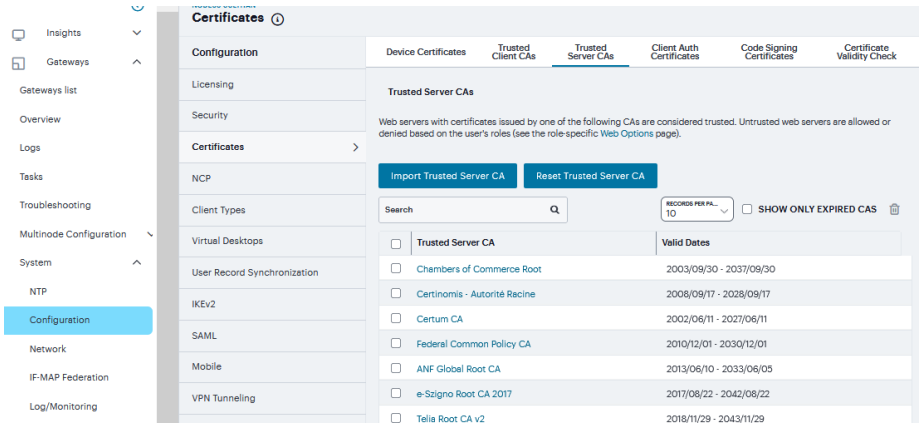


FIGURE 10.17 : Trusted Server CAs

3. Browse to the **Certificate File**, select it, and click **Import** to complete the import operation.

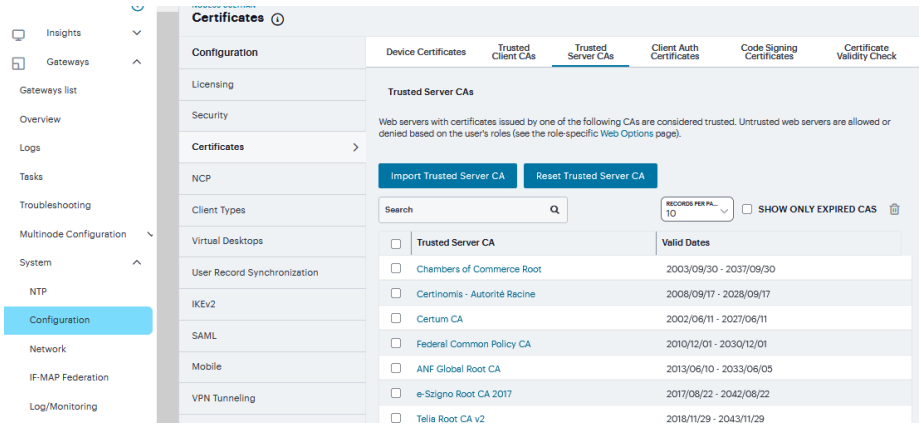


FIGURE 10.18 : Certificate File

To restore the prepopulated group of trusted CA certificates:

1. Select **System > Configuration > Certificates > Trusted Server CAs**.
2. Click **Reset Trusted Server CAs**.
3. Confirm that you want to restore the set of trusted server CAs that was installed when you upgraded.

Note: Connect Secure restores the group of pre-populated trusted server CAs that were installed upon upgrade. This operation clears all manually imported certificates.

Client Auth Certificates

In certain corporate environments, servers on the LAN are protected with two-way SSL authentication. These servers require the client to authenticate by presenting a valid certificate. In the remote access scenario, Ivanti Connect Secure is a client of these servers. You can configure Ivanti Connect Secure to present client authentication certificates to servers whenever it communicates over SSL. Note that Ivanti Connect Secure will present client certificates only when the SSL handshake requires it.

Note: This feature authenticates Ivanti Connect Secure (as a client) to back-end servers. It also authenticates end users or end-user machines to servers on the corporate LAN.

The access management framework allows certificates that include the private key and for instances where the private key is in a separate file from the certificate. In addition, if your certificates have been exported into a system configuration file, you can import the system configuration file to upload the certificates.

To import the client auth certificates files:

1. Select **System > Configuration > Certificates > Client Auth Certificates**.
2. Click **Import Certificate** to display the configuration page.

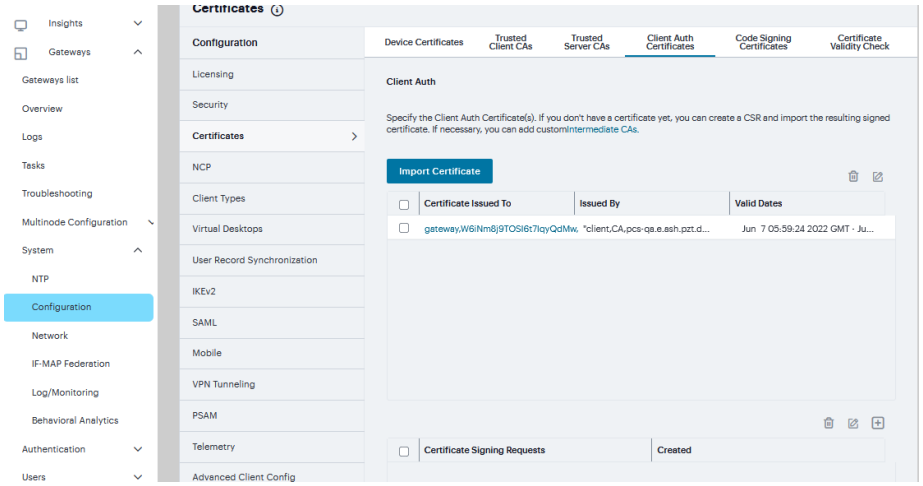


FIGURE 10.19 : Client Auth Certificates

3. Complete the configuration described in table.
4. Click **Import**.

TABLE 10.5 : Import Certificate and Key Settings

Setting	Guidelines
If certificate and private file are separate keys	
Certificate File	Browse to the network path or local directory location of your certificate key file.
Private Key File	Browse to the network path or local directory location of your private key file.
Password Key	Enter the password key.
Import via System Configuration file	
System Configuration File	Browse to the network path or local directory location of the system configuration file.
Password	Enter the password.

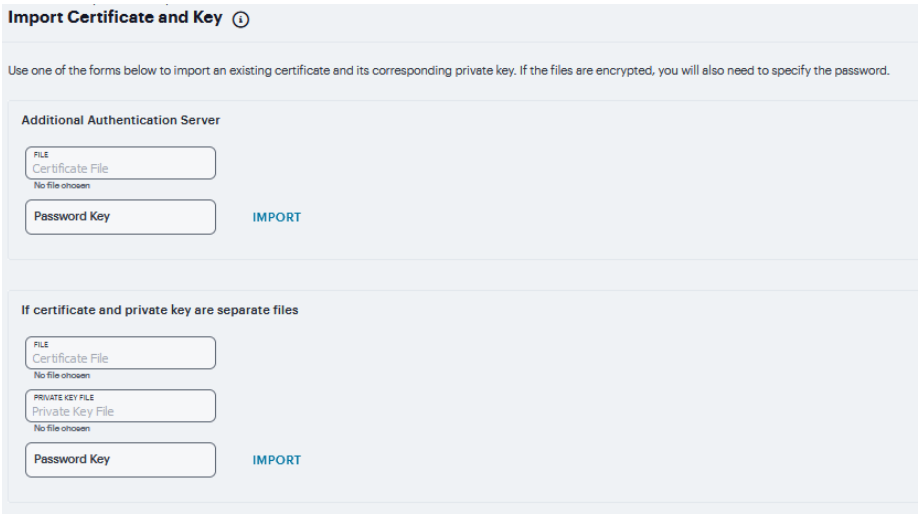


FIGURE 10.20 : Import Certificate and Key Settings

To create Certificate Signing Request (CSR) for RSA and ECC Keys:

1. Navigate to **System > Configuration > Certificates > Client Auth Certificates**.
2. Click '**+**' on the **Certificate Signing Requests** pane.
3. Enter the required requestor information. In this example, the common name is *ecc-p256.<orgname>.net* or *pcs.<orgname>.net*.
   - If **RSA** is selected then, select **Key Length** and enter **Random characters**.
   - If **ECC** is selected then, select **ECC Curve** drop down. Click **Save Changes**.
4. The CSR is encoded and can be copied or saved to a file. The ECC certificate should be signed by an RSA/ECC CA for Suite B compliance. Follow your CA's process for sending a CSR.
5. Click the **Back to Device Certificates** link. Until you import the signed certificate from your CA, your CSR is listed as Pending.

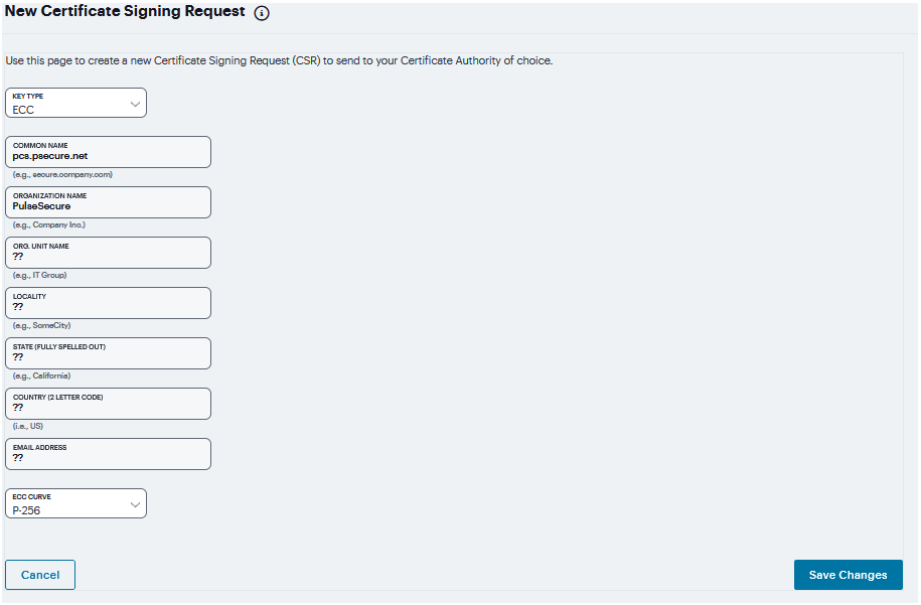


FIGURE 10.21 : Certificate Signing Request

Code-Signing Certificates

In a basic setup, the only required certificates are a device certificate and a code-signing certificate. Ivanti Connect Secure can use a single code-signing certificate to resign all Java applets and a single device certificate to intermediate all other PKI-based interactions. If the basic certificates do not meet your needs, however, you may install multiple device and applet certificates on Ivanti Connect Secure or use trusted CA certificates to validate users.

When Ivanti Connect Secure intermediates a signed Java applet, it re-signs the applet with a self-signed certificate by default. This certificate is issued by a nonstandard trusted root CA. As a result, if a user requests a potentially high-risk applet (such as an applet that accesses network servers), the user's Web browser alerts him that the root is untrusted.

To import a code-signing certificate:

1. Select **System > Configuration > Certificates > Code-Signing Certificates** to display the configuration page.
2. Click **Import Certificates** to display the configuration page.
3. Complete the configuration described in the following table.

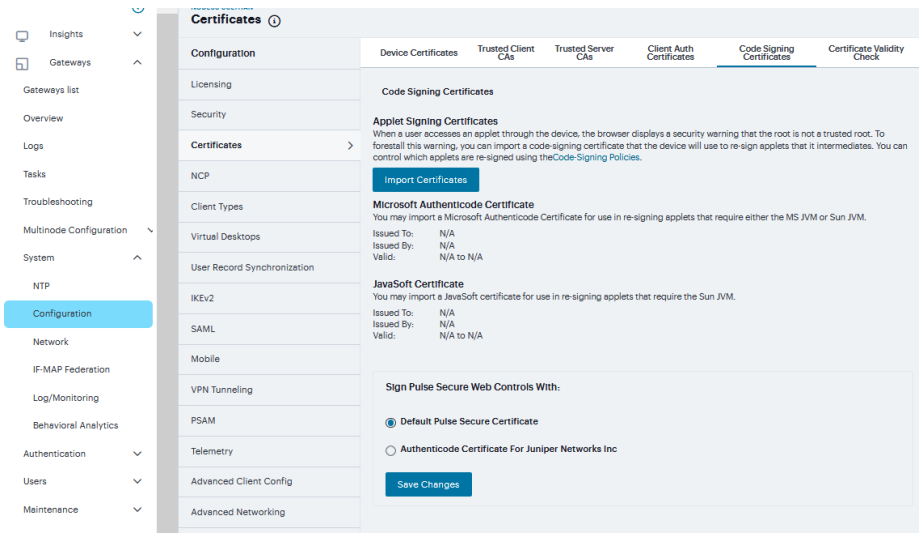


FIGURE 10.22 : Code-Signing Certificates

The following table lists the Import Certificates Configuration Guidelines:

TABLE 10.6 : Import Certificates Configuration Guidelines

Setting	Guidelines
Microsoft Authenticode or Multipurpose Certificate for Internet Explorer (Microsoft JVM)	
Certificate File	Browse to the network path or local directory location of your certificate key file.
Private Key File	Browse to the network path or local directory location of your private key file.
Password Key	Enter the password key.
Javasoft Certificate for Internet Explorer & Netscape (Sun JVM)	
Keystore File	Browse to the network path or local directory location of the keystore file.
Password key	Enter the password key.

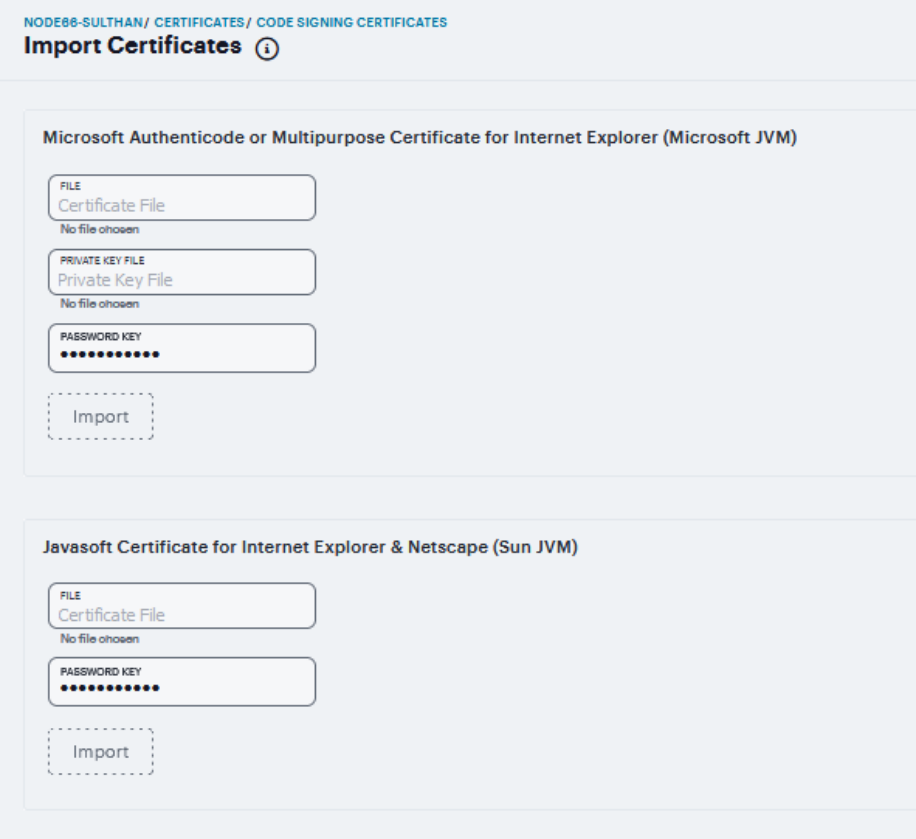


FIGURE 10.23 : Import Certificates

1. Click *Import* to complete the import operation.
2. When you have successfully imported a certificate, the system displays the Sign Ivanti Web Controls With dialog box. Specify the signing option:
   - *Default Ivanti Certificate* - Select this option to sign all ActiveX and Java applets originating from Ivanti Connect Secure using the default Ivanti certificate. If you have previously selected an imported code-signing certificate and are reverting back to this option, after you click Save, a process icon appears indicating that the system is processing the request and re-signing all of the relevant code. This process can take several minutes to complete.
   - *Authenticode Certificate* - For <Imported Certificate Name>-Select this option to sign all ActiveX and Java applets using the certificate or certificates imported in the previous step. When you click Save, a process icon appears indicating that the system is processing the request and signing all of the relevant code. This process can take several minutes to complete.
3. Click **Save Changes**.

Certificate Validity Check

Every time a certificate is added to ICS (through manual import, XML import, or upgrade), its expiration date is stored in the cache. A background process checks all certification expiration dates once in every 7 days. If any certificate is about to expire soon, the administrator is notified. Notifications to administrators include a banner message in the adminUI upon login, SNMP trap, and log messages in the event log. The administrator can configure how soon he or she wishes to be notified of the expiration. The default is 60 days in advance. It can be configured to a value starting from 7 days in advance to 999 days in advance of the expiration of the certificate. The expiration warning window is common to all types of certificates. However, the administrator can choose to enable or disable this feature for each certificate category in the user interface.

To check validity of certificates:

1. Click on **Configuration > Certificates > Certificates Validity Check**.
2. The page displays the **Certificate Expiry Notification Duration** and the **Certificate Types**.
3. Enter the number of days before which the warning must be displayed.
4. Select the type of certificate for which the expiry notification is required. By default, all types of certificates will be selected if no selection is made.
5. Click on Check Now. The Certificate Category, DN name and date of expiry are displayed.
6. When an administrator logs in, a warning sign is displayed, if there are any certificates that expire within the configured number of days.

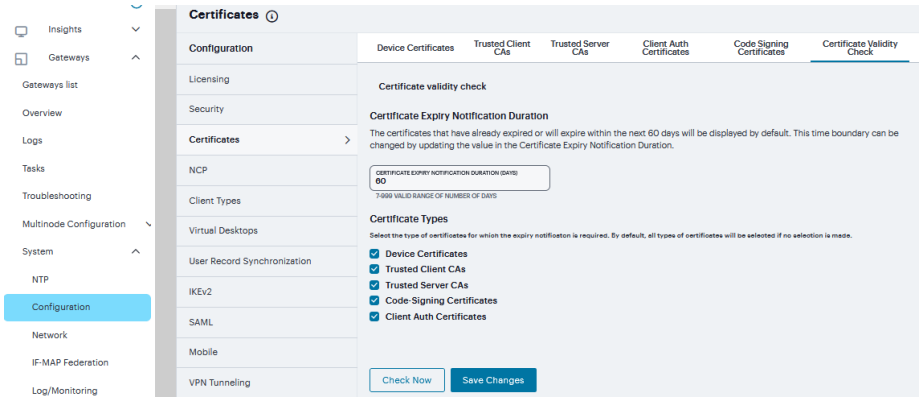


FIGURE 10.24 : Certificates Validity Check

NCP Configuration

The following types of internal protocols are used to communicate between Ivanti Connect Secure and client applications:

- *Network Communications Protocol (NCP)* - Standard NCP has been replaced with oNCP. Windows client applications, PSAM, and Terminal Services fallback to NCP if oNCP fails.
- *Optimized NCP (oNCP)* - oNCP significantly improves the throughput performance of the client applications over NCP because it contains improvements to protocol efficiency, connection handling, and data compression. Windows client applications, PSAM, and Terminal Services use oNCP by default.
- *Java Communications Protocol (JCP)* -JCP is the Java implementation of standard NCP. The system uses JCP to communicate with Java client applications, JSAM, and the Java Content Intermediation Engine.

To set NCP options:

1. Navigate to **System > Configuration > NCP**.
2. (Windows clients) Under NCP Auto-Select, select:
    - **Auto-select Enabled** (recommended) - Use the oNCP by default. If you select this option, the system uses oNCP for most client/server communications and then switches to standard NCP when necessary. The system reverts to NCP if the user is running an unsupported operating system, browser type, or combination thereof, or if the client application fails to open a direct TCP connection to the device for any reason (for instance, the presence of a proxy, timeout, disconnect).
    - **Auto-select Disabled** - Always use standard NCP. This option is primarily provided for backwards compatibility.

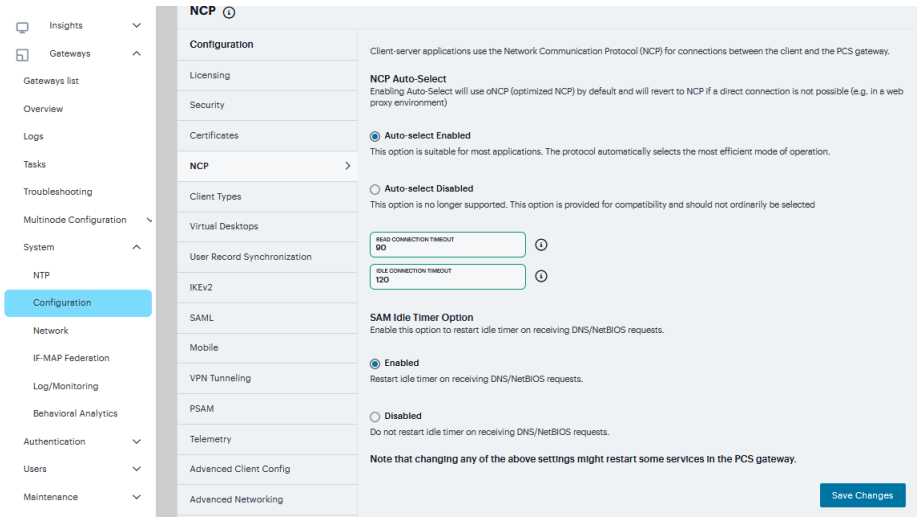


FIGURE 10.25 : NCP

Note: If you are using Network Connect to provide client access, we recommend that you exercise caution when employing the Auto-select Disabled option, as Mac and Linux clients cannot connect using the traditional NCP protocol. If you disable the oNCP/NCP auto-selection feature and a UDP-to oNCP/NCP fail-over occurs, the system disconnects Macintosh and Linux clients because it fails over from UDP to NCP (instead of oNCP), which does not support these users.

3. (Java clients) Under **Read Connection Timeout**, set the timeout interval for Java clients (15-120 seconds). If client-side secure access methods do not receive data from the system for the specified interval, they try to reestablish a connection. Note that this value does not apply to user inactivity in client applications.
4. (Windows clients) Under Idle Connection Timeout, set the idle connection interval. This timeout interval determines how long the system maintains idle connections for client-side Windows secure access methods.
5. Under **SAM Idle Timer** enable/disable idle timer to receive DNS/NetBIOS requests
6. Click **Save Changes**.

Client Types Configuration

The Client Types tab allows you to specify the types of systems your users may sign in from and the type of HTML pages to display when they do. In addition, client types are used to identify the operating system shown on the Device Management page for devices that use ActiveSync to synchronize e-mail with a Microsoft Exchange server. The user agent string used to identify a device during login may be different from the one in the ActiveSync message. For example, in the list of default user agent strings, *Apple-iPhone* and *Apple-iPad* are used only in ActiveSync messages.

To manage the client types:

1. Navigate to **System > Configuration > Client Types**.
2. In the User-agent string pattern text box, enter the user agent string for the operating system (s) that you want to support. You can specify all or part of the string. For example, you can use the default *DoCoMo* string to apply to all DoCoMo operating systems, or you can create a string such as DoCoMo/1.0/P502i/c10 to apply to a single type of DoCoMo operating system. You can use the * and ? wildcard characters in the string. Note that user agent strings on the system are case-insensitive.
3. Select the type of HTML to display to users who sign in from the operating system specified in the previous step. Options include:
   - *Standard HTML* - The system displays all standard HTML functions, including tables, full- size graphics, ActiveX components, JavaScript, Java, frames, and cookies. Ideal for standard browsers, such as Firefox, Mozilla, and Internet Explorer.
   - *Compact HTML (iMode)* - The system displays small-screen HTML-compatible pages. This mode does not support cookies or the rendering of tables, graphics, ActiveX components, JavaScript, Java, VB script, or frames. (The only difference between this option and the Smart Phone HTML Basic option is the user interface.) Ideal for iMode browsers.

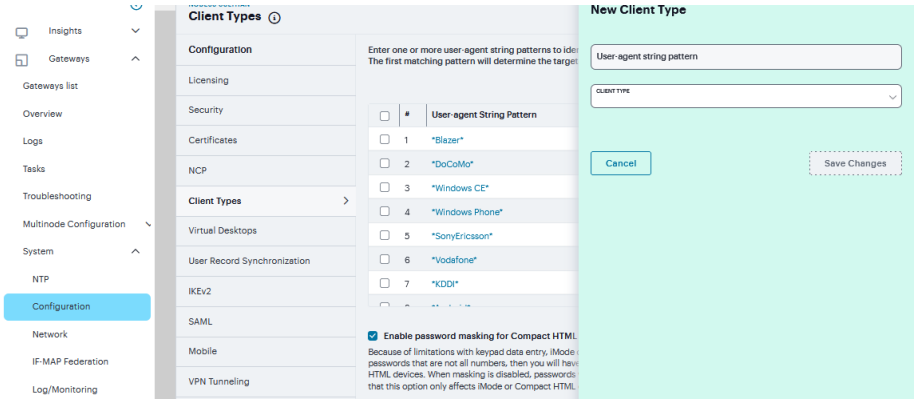


FIGURE 10.26 : Client Types

Note: Form Post SSO is not supported on iMode appliances.

- *Mobile HTML (Pocket PC)* - The system displays small-screen HTML-compatible pages that may contain tables, small graphics, JavaScript, frames, and cookies, but this mode does not facilitate the rendering of java applets or ActiveX components. Ideal for Pocket PC browsers.
- *Smart Phone HTML Advanced* - The system displays small-screen HTML-compatible pages that may contain tables, small graphics, frames, cookies, and some JavaScript, but this mode does not facilitate the

rendering of java applets, ActiveX components, or VB scripts. Ideal for Treo and Blazer browsers.

- *Smart Phone HTML Basic* - The system displays small-screen HTML-compatible pages. This mode does not support cookies or the rendering of tables, graphics, ActiveX components, JavaScript, Java, VB script, or frames. (The only difference between this option and the Compact HTML option is the user interface.) Ideal for Opera browsers on Symbian.

Note: The system rewrites hyperlinks to include the session ID in the URL instead of using cookies.

- *Mobile Safari, Android, Symbian, iPad* - The Mobile Safari (iPhone/iPod Touch), Android, and Symbian selections have Basic, Advanced, and Full HTML options.

4. Specify the order that you want to evaluate the user agents. The system applies the first rule in the list that matches the user's system. For example, you may create the following user agent string/HTML type mappings in the following order

   - User Agent String: *DoCoMo* Maps to: Compact HTML
   - User Agent String: DoCoMo/1.0/P502i/c10 Maps to: Mobile HTML

   If a user signs in from the operating system specified in the second line, the system will display compact HTML pages to him, not the more robust mobile HTML, since his user agent string matches the first item in the list. To order mappings in the list, select the check box next to an item and then use the up and down arrows to move it to the correct place in the list.

5. Select the **Enable password masking for Compact HTML** check box if you want to mask passwords entered in iMode and other devices that use compact HTML. (Devices that do not use compact HTML mask passwords regardless of whether or not you select this check box.) Note that if your iMode users' passwords contain non-numeric characters, you must disable password masking because iMode devices only allow numeric data in standard password fields. If you disable masking, passwords are still transmitted securely, but are not concealed on the user's display.

6. Click **Save Changes**.

Virtual Desktops Configuration

In addition to standard resource profiles and resource profile templates, you can configure virtual desktops as resource profiles. As with the other resource profiles, a virtual desktop profile contains all of the role assignments and end-user bookmarks required to provide access to an individual resource. Unlike other resource profile types, there is no resource policy to configure for virtual desktops due to the dynamic nature of virtual desktops. The IP address and port of the system is not known until the end user launches a session so dynamic ACLs are used.

You can use the Virtual Desktop Configuration page to define the client delivery mechanism for end-users who do not have the client. The process is similar for both Citrix XenDesktop and VMware View Manager.

1. Navigate to **System > Configuration > Virtual Desktops**.
   - For **View Client Delivery Method** Select **VMware**.
   - For **Citrix XenDesktop**, select **Citrix**.
2. Select **Download from Ivanti Connect Secure** to download the client file from the system. Click **File** to locate the client file (*.msi, .exe or .cab*) and enter the **version number**.
3. Select **Download from a URL** to download the client file from the Internet. If desired, enter a new URL to override the default.

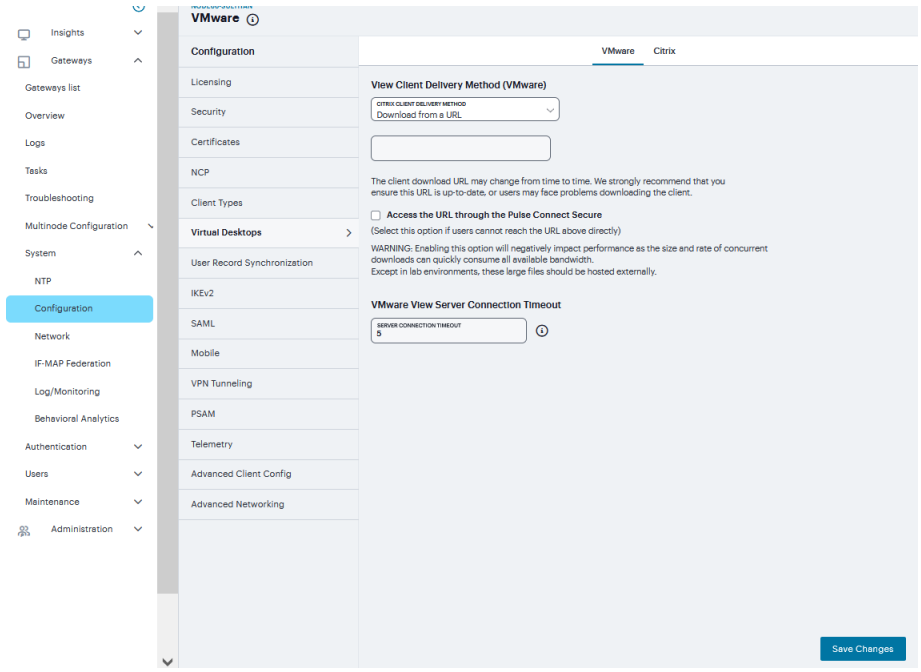


FIGURE 10.27 : Virtual Desktops

4. Check the **Access the URL through the Ivanti Connect Secure** check box if end users cannot directly access the specified Web page. Selecting this option allows users to use the secure gateway to access the URL.

5. Under **Server Connection Timeout**, enter the number of seconds to wait for the server to respond before timing out.

User Record Synchronization

The user record synchronization feature promotes a more consistent user experience by allowing users to retain their bookmarks and individual preferences regardless of which device they log in to.

User record synchronization relies on client-server pairings. The client is the device that users log in to start their remote access. Each client is associated with one primary server and one backup server to store user record data. Clients can be individual appliances or a node within a cluster.

A server in this instance is the device that stores the user data records. Each server can be configured to replicate its user record data to one or more peer servers. Servers are identified by a user-defined logical name. The same logical name can be assigned to more than one authentication server to let you associate authentication servers of different types to the same user. For example, SA1 is an ACE authentication server with user1 who creates a bookmark to www.<orgname>.net. SA2 is an Active Directory authentication server with the same user1. For the www.<orgname>.net bookmark to be transferred from SA1/ACE/user1 to SA2/AD/user1 you would assign the logical name “Logical1” to both the ACE server on SA1 and the Active Directory server on SA2.

General Setup

1. Navigate to **System > Configuration > User Record Synchronization > General**.
2. Select the **Enable User Record Synchronization** check box.
3. Enter a unique **node name**. This name is used when associating a client with a server and is different from the logical name assigned to a server. This node name is also not the same as the cluster node name.
4. Enter the **shared secret** and **confirm it**. The shared secret is the password used to authenticate the client with its servers and the primary server with its peer servers. Use the same shared secret for all clients and servers participating in user record synchronization.
5. Select whether this node is **client only** or if this node acts as both a **client and server**.
6. Click **Save Changes**.

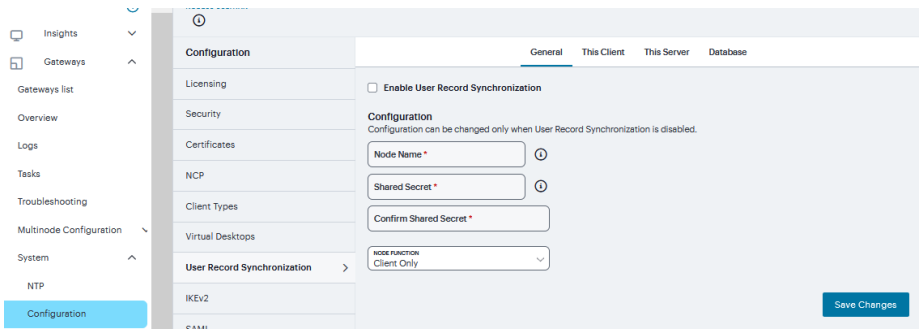


FIGURE 10.28 : General

Note:

- If you need to make any changes in this window at a later time, you must deselect the Enable User Record Synchronization check box and click Save Changes. Make your edits, select the Enable User Record Synchronization check box and save your changes.
- Once you enter a name and shared secret, you cannot clear these fields.

Client Configuration

To set up the client, you select the primary and backup server you want this client to synchronize with:

1. Navigate to **System > Configuration > User Record Synchronization > This Client**.
2. Click '**+**', Select the LAS name you want to synchronize and enter the primary IP of the user record. If you prefer to synchronize with any available server, select *Any LAS*.
3. Enter the **Primary** and optionally a **Backup server's** IP address and then click **Save Changes**.

Even if you select Any LAS, you must enter a primary server IP address. Once added, the primary and backup servers have a colored icon next to their name indicating their connection status.

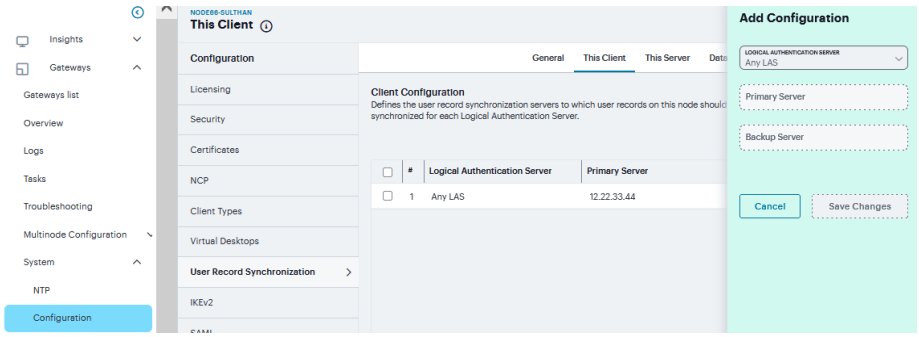


FIGURE 10.29 : Client

Server Configuration

To set up the user record synchronization server you must define its peer nodes (optional) and the clients that can access this server.

1. Navigate to **System > Configuration > User Record Synchronization > This Server**.
2. Under **Peer Server**, click '**+**'and enter the peer server's **Node name** and **IP address**, then click **Save Changes**. To specify more than one peer server, enter each server's node name and IP address individually and click **Save Changes**. There is no limit on the number of peer servers you can add.

   Data is replicated from the primary or backup server to its peer servers. If the primary is not available, user data is sent to the backup. User data is then replicated to the peer servers.
3. For each client you want synchronized with this server, Under **Client Nodes**, click '**+**'enter the **Client's name** and **IP address** and click **Save Changes**.

   Once added, peer servers will have a colored icon next to their name indicating their connection status. Node status is provided to client nodes and LAS mapping servers as well.

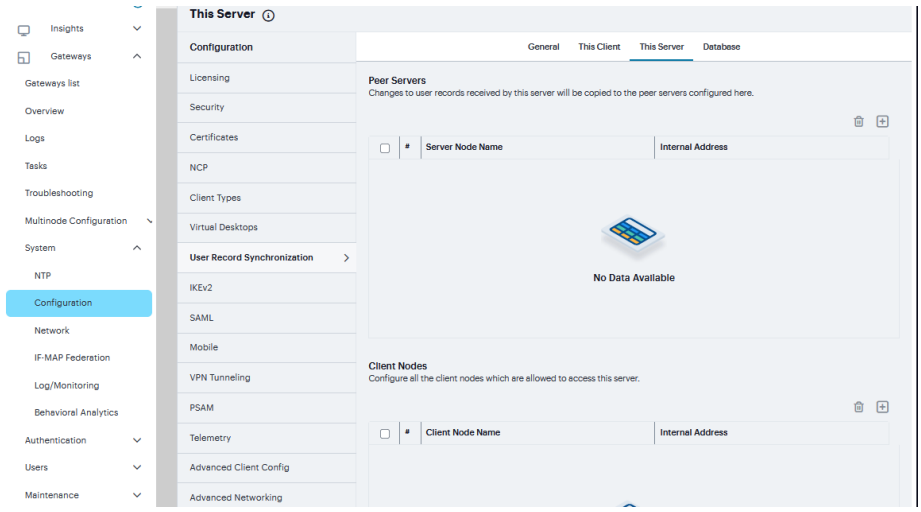


FIGURE 10.30 : Server

Database Configuration

With the Database tab, you can delete inactive records from the client cache, retrieve statistics about the database, export and import the data and remove user data from the server's database.

To configure the database:

1. Navigate to **System > Configuration > User Record Synchronization > Database**.
2. Select **Auto-delete inactive synchronized user records from the Cache** to remove inactive user records from the cache and not from the user record database.

   When this option is selected, the system performs a check every 15 minutes and deletes user records that meet all of the following criteria:

   - There are no active user sessions associated with the user record.
   - The user record does not have any custom settings, or the latest version of the user record has been synchronized with the user record database.
   - The authentication server associated with the user record database does not have type "local". For example, the "System Local" auth server that is part of the default configuration of the system has a "local" type, so any user records associated with that auth server will not be auto-deleted. However, user records associated with external authentication servers like Radius or LDAP may be deleted, depending on the two prior criteria.
3. Click **Save Changes**.
4. Under **Export**, you export user records to a file. The user records can be exported from the user record database, or from the cache. The exported file can be used to pre-populate the user record database on another node.

5. To encrypt the exported data, select the **Encrypt the exported data with password** check box and enter the **Password** and **Confirm it**.
6. Click **Export** to export the user records from the specified source (cache or database). You will be prompted where to save the file.

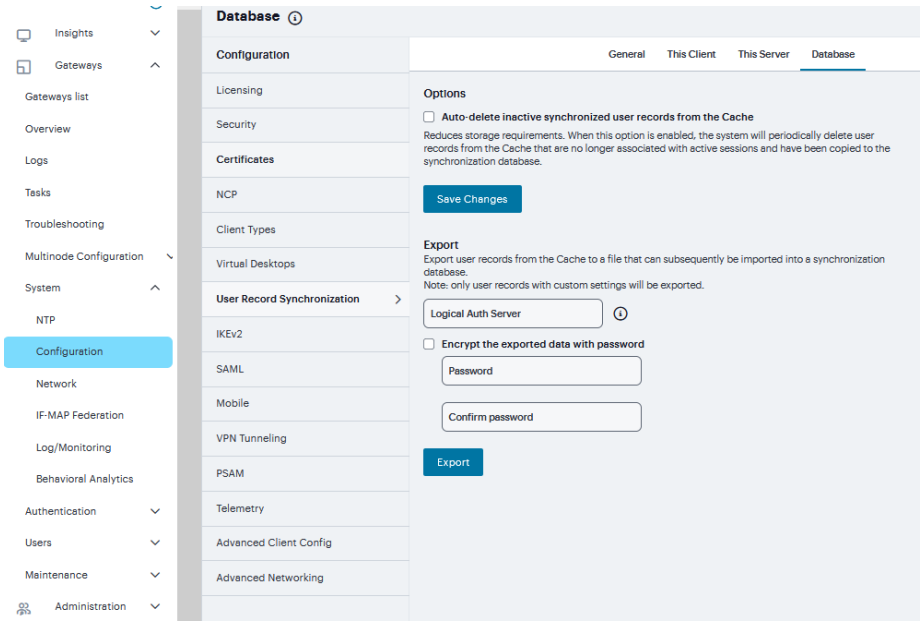


FIGURE 10.31 : Database

IKEv2 Configuration

IKE or IKEv2 (Internet Key Exchange) is the protocol used to set up a security association in the IPsec protocol suite. Microsoft Windows 7 fully supports the IKEv2 standard through Microsoft's Agile VPN functionality and can operate with a VPN gateway using these protocols. Information on IKE and IKEv2 is widely available on the Internet. It is not the intent of this guide to describe details about IKE and IKEv2.

The system supports IKEv2, enabling interoperability with clients or devices, such as smartphones, that have a standards-based IPSec VPN client. IKEv2 clients count toward the total number of sessions. Thus, the total number of sessions = number of IKEv2 sessions + number of NCP sessions. The system supports the following methods for authenticating IKEv2 clients:

- Machine certificate-based authentication
- Authentication using EAP methods

Note: IKEv2 uses port 500 exclusively. Do not configure port 500 in your VPN

Tunneling profiles.

To configure the IKEv2 ports and EAP protocol:

1. Navigate to **System > Configuration > IKEv2** to display the configuration page.
2. Enter the **DPD timeout** value in seconds. Valid values are 400-3600.

   DPD is a form of keepalive. When a tunnel is established but idle, one or both sides may send a “hello” message and the other replies with an acknowledgement. If no response is received, this continues until the DPD time value has elapsed. If there still is no traffic or acknowledgement, the peer is determined to be dead and the tunnel is closed.

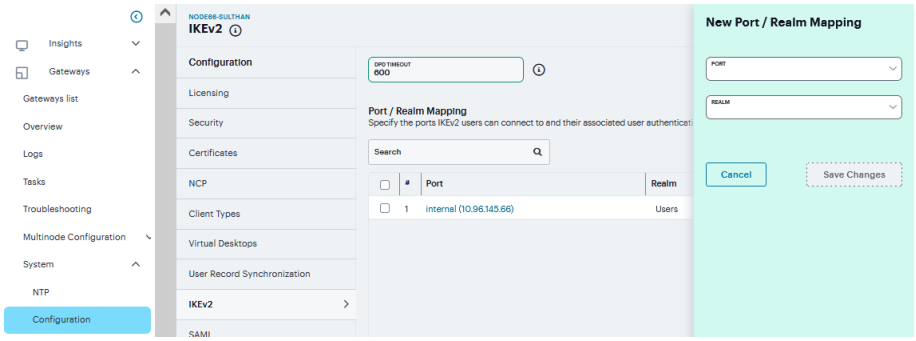


FIGURE 10.32 : Port/Realm Mapping

3. Under **Port/Realm Mapping**, click ‘**+**’ select the **Port** and the **Realm** to use that port and click **Save Changes**.
4. Under **Realm/Protocol Set Mapping**, click ‘**+**” select the **Realm** and the **EAP protocol set** to use for that realm.

   The three Protocol Set Options include EAP-MSCHAP-V2, EAP-MD5-Challenge, and EAP-TLS.

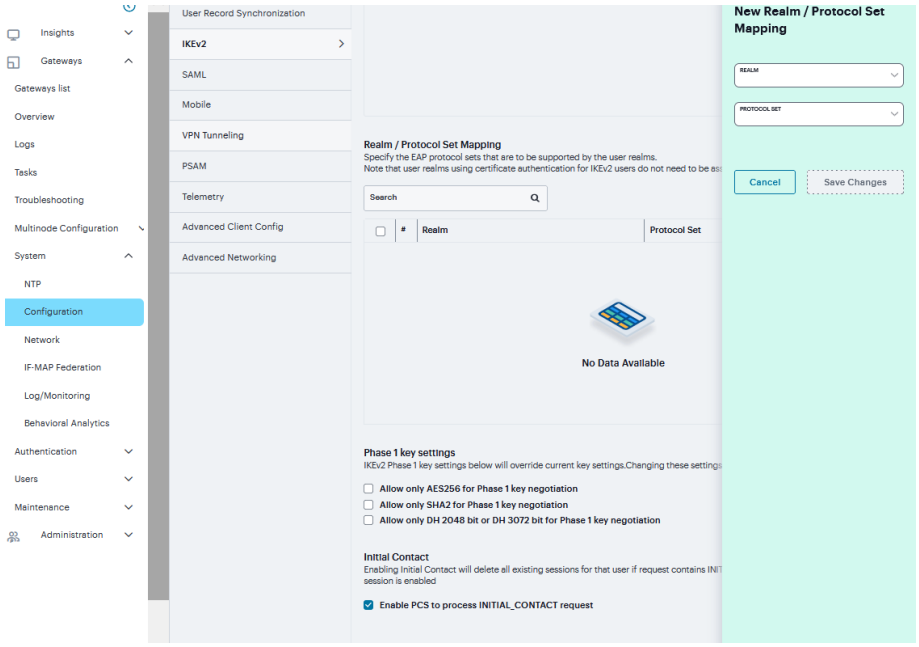


FIGURE 10.33 : Realm/Protocol Set Mapping

5. To Configure Phase-1 Key Settings, select the required Phase 1 Key Settings.

   Three new UI options are available to enforce:

   - Encryption Algorithm (AES256)
   - Integrity Algorithm (SHA256, SHA384 and SHA512)
   - Diffie-Hellman Group (DH 2048 and DH3072).

   Enabling these options mean more secured Phase 2 negotiations. When AES256 is enabled, AES256 Encryption Algorithm is preferred over AES128 or 3DES. When SHA2 is Enabled, SHA2 Integrity Algorithm is preferred over SHA1 and When DH is Enabled, DH2048 or DH3072 Diffie-Hellman Group is preferred over DH1024.

6. Click **Save Changes**.

Note: Changing IKEv2 configuration (System > Configuration > IKEv2) disconnects connections from IKEv2 clients, VPN Tunneling and Ivanti. VPN Tunneling and Ivanti will reconnect automatically.

SAML Configuration

SAML is an XML-based framework for communicating user authentication, entitlement, and attribute information. The standard defines the XML-based assertions, protocols, bindings, and profiles used in communication between SAML entities. SAML is used primarily to implement Web browser single sign-on (SSO). SAML enables businesses to leverage an identity-based security system like Ivanti Connect Secure to enforce secure access to web sites and other resources without prompting the user with more than one authentication challenge.

You use the System > Configuration > SAML pages to maintain a table of SAML metadata files for the SAML service providers and identity providers in your network. Using SAML metadata files makes configuration easier and less prone to error. You can add the metadata files to the system by:

- Uploading a metadata file.
- Retrieving the metadata file from a well-known URL.

To add metadata files:

1. Navigate to **System > Configuration > SAML**.
2. Click '**+**'' to display the configuration page.

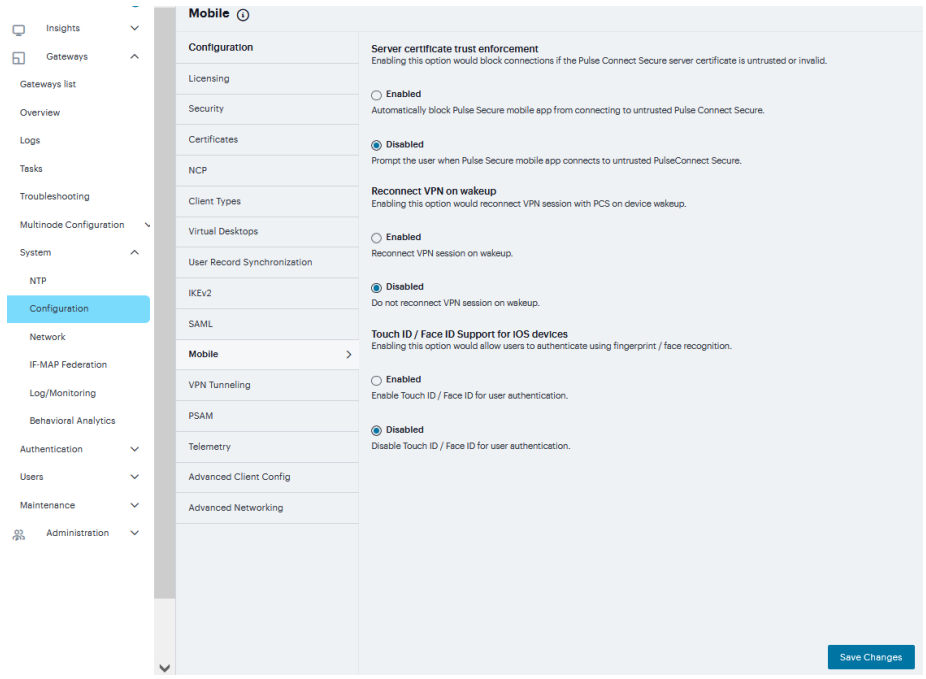


FIGURE 10.34 : SAML

3. Enter **New Metadata Provider** name.
4. Complete the settings described in the following table
5. Click **Save Changes**

TABLE 10.7 : SAML Metadata Provider Configuration Guidelines

Setting	Guidelines
Metadata Provider Location Configuration	Select one of the following methods: • **Local** Browse and locate the metadata file on your local host or file system. • **Remote** Enter the URL of the metadata file. Only http and https protocols are supported.
Upload Metadata File	You can upload the metadata file directly.
Metadata Provider Verification Configuration	
Accept Unsigned Metadata	If this option is not selected, unsigned metadata is not imported. Signed metadata is imported only after signature verification.
Signing Certificate	• Browse and locate the **certificate** that verifies the signature in the metadata file. This certificate overrides the certificate specified in the signature of the received metadata. If no certificate is uploaded here, then the certificate present in the signature of the received metadata is used. • Select the **Enable Certificate Status Checking** option to verify the certificate before using it. Certificate verification applies both to the certificate specified here and the certificate specified in the signature in the metadata file.
Metadata Provider Filter Configuration	
Roles	Select whether the metadata file includes configuration details for a SAML service provider, identity provider, or Policy Decision Point. You may select more than one. If you select a role that is not in the metadata file, it is ignored. If none of the selected roles are present in the metadata file, the system returns an error.
Entity IDs To Import	Enter the SAML Entity IDs to import from the metadata files. Enter only one ID per line. Leave this field blank to import all IDs. This option is

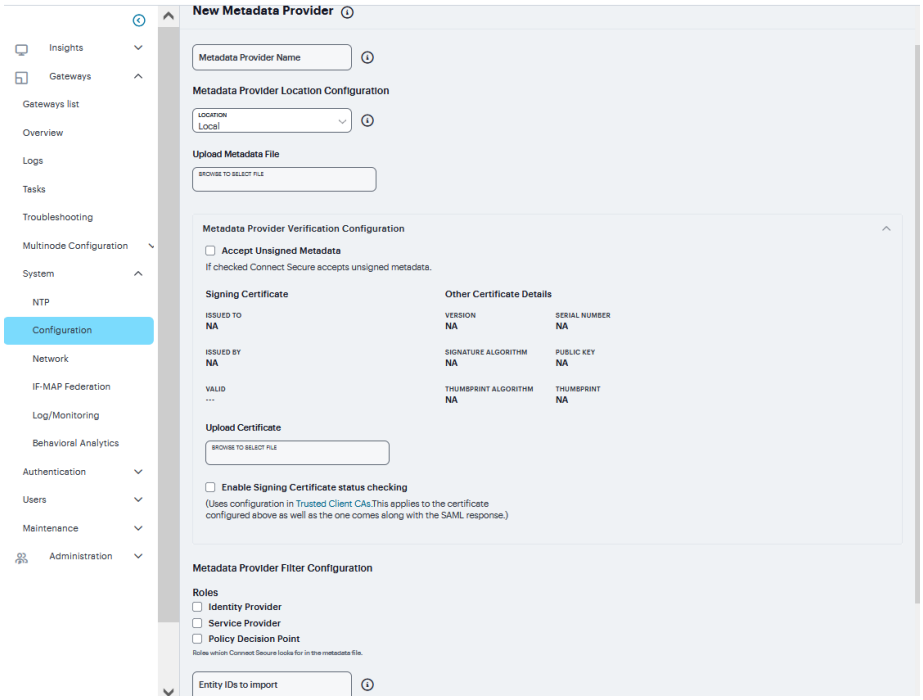


FIGURE 10.35 : SAML Metadata Provider

Mobile Configuration

This topic describes the mobile options that are available on Ivanti Connect Secure. To configure the mobile option, go to **System > Configuration > Mobile**. It includes the following information:

TABLE 10.8 : Mobile Configuration Guidelines

Setting	Guidelines
Server certificate trust enforcement	Enables you to block connections if the Ivanti Connect Secure server certificate is untrusted or invalid. When enabled, it automatically blocks the Ivanti mobile app from connecting to untrusted Ivanti Connect Secure. When disabled, it prompts when a Ivanti mobile app connects to untrusted Ivanti Connect Secure.
Reconnect VPN on wakeup	Enables you to reconnect a VPN session with ICS on device wakeup.
Touch ID / Face ID Sup-port for iOS devices	Enables you to authenticate using fingerprint / face recognition.

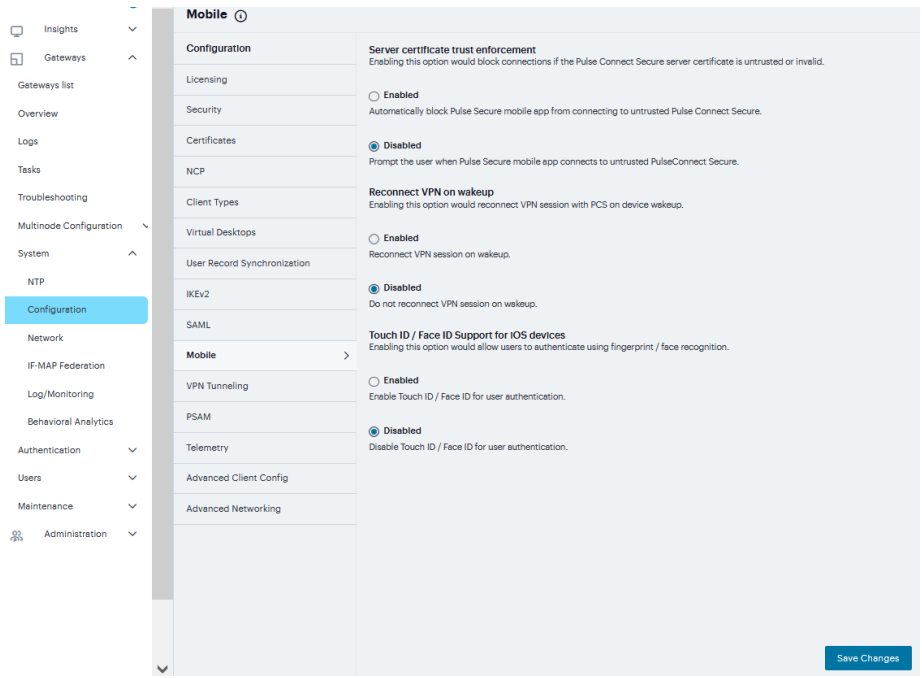


FIGURE 10.36 : Mobile

VPN Tunneling Configuration

The VPN tunneling access option (formerly called Network Connect) provides a VPN user experience, serving as an additional remote access mechanism to corporate resources using Connect Secure. This feature supports all Internet-access modes, including dial-up, broadband, and LAN scenarios, from their client machine and works through client-side proxies and firewalls that allow SSL traffic.

When a user launches VPN tunneling, the system transmits all traffic to and from the client over the secure VPN tunnel. The only exception is for traffic initiated by other system-enabled features, such as Web browsing, file browsing. If you do not want to enable other system features for certain users, create a user role for which only the VPN tunneling option is enabled and make sure that users mapped to this role are not also mapped to other roles that enable other system features.

To configure VPN tunneling:

1. Navigate to **System > Configuration > VPN Tunneling**.
2. Under **Access Control List (ACL) Count Enforcement** enable to block VPN tunneling sessions when the total number of ACL rules exceeds 60,000.
3. Under **IPv6 ESP Settings**, enter **UDP Port number** and select the **Use ESP tunnel for 6in4 and 4in6** traffic check box.
4. Under **Precedence of FQDN / IP** section, check **Prefer FQDN resources over IP resources in case of a split tunneling conflict**.

5. Under **Enable/Disable FQDN ACL**, check to Enable FQDN ACL
6. Click **Save Changes**.

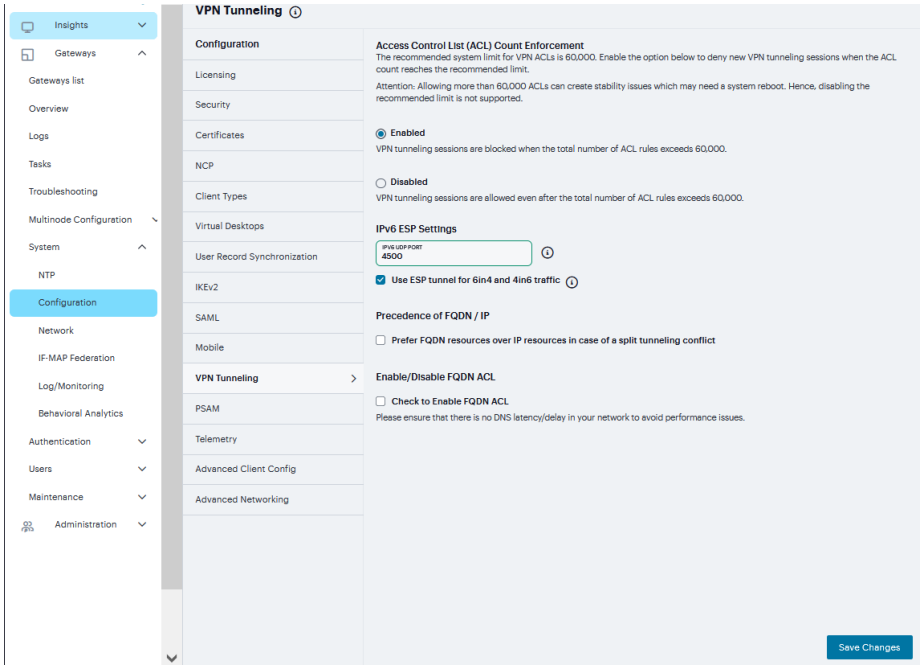


FIGURE 10.37 : VPN Tunneling

PSAM Configuration

The Secure Application Manager option provides secure, application-level remote access to enterprise servers from client applications. The Windows version of the Secure Application Manager is a Windows-based solution that enables you to secure traffic to individual client/server applications and application servers.

To Configure PSAM:

1. Navigate to **System > Configuration > PSAM**
2. Under **Precedence of FQDN / IP section**, check Prefer FQDN resources over IP resources in case of a resource ACL conflict.

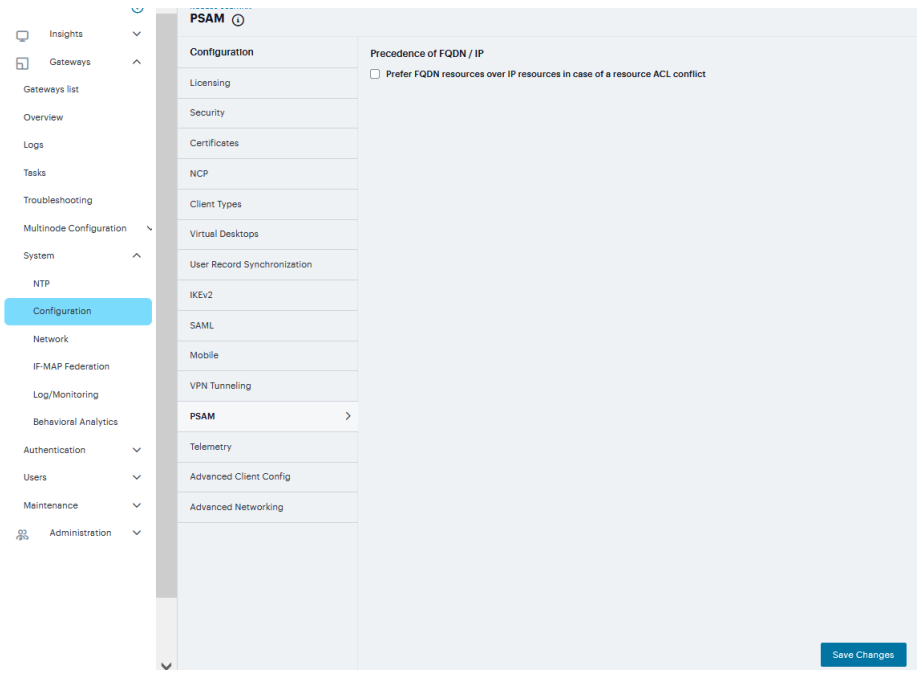


FIGURE 10.38 : PSAM

Telemetry Settings

Telemetry Settings helps you to enable Google Analytics and Crash Analytics.

To monitor the usage of customer and track the crash #. Navigate to **System > Configuration > Telemetry**

- Enable **Google Analytics** to tracking how frequently customer is using a particular feature.
- Enable **Crash Analytics** to collect logs when user faces any crash.

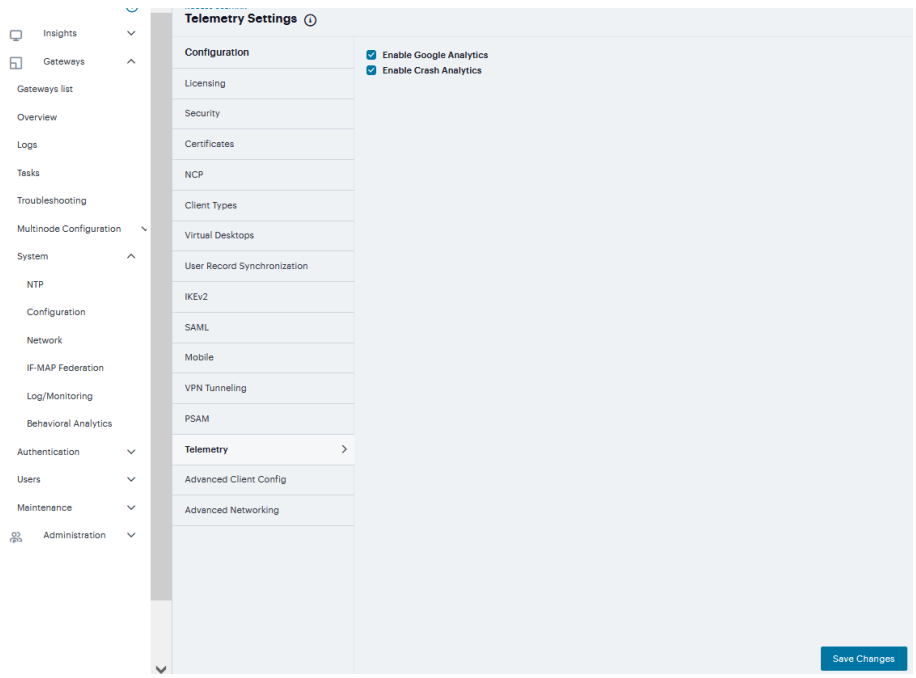


FIGURE 10.39 : Telemetry

Advanced Client Configuration

This topic describes the XML advanced client configuration that can be used by the ICS administrator to configure the custom settings, which are meant to solve a specific customer scenario without changing the ICS admin console. Admin can set these custom settings in the form of XML input through the Advanced Client Configuration UI feature. Ivanti Secure Access clients supporting these custom settings will consume them when connecting to this ICS, and the same would be applied on the client ma-chines. This feature will minimize the number of changes going into the ICS admin console, in order to fulfill a custom requirement of a specific customer.

If the administrator configures the Ivanti Connect Secure sever with the following XML input in “Advanced Client Configuration for Ivanti Secure Access Client” option, it will ignore TCP MSS options while calculating the virtual adapter MTU on client side.

To add advance client config:

1. Navigate to **System > Configuration > Advanced Client Configuration** to display the configuration page.
2. Enter the following XML input in **Advanced Configuration for Ivanti Secure Access Clients**.

```
<advanced-config>
 <version> version </version>
 <desktop-client-config>
  <layer3-connection-config>
```

(continues on next page)

(continued from previous page)

```
    <adapter-config>
     <ignore-tcp-mss>TRUE</ignore-tcp-mss>
    </adapter-config>
    </layer3-connection-config>
   </desktop-client-config>
</advanced-config>
```

3. Click **Save Changes**.

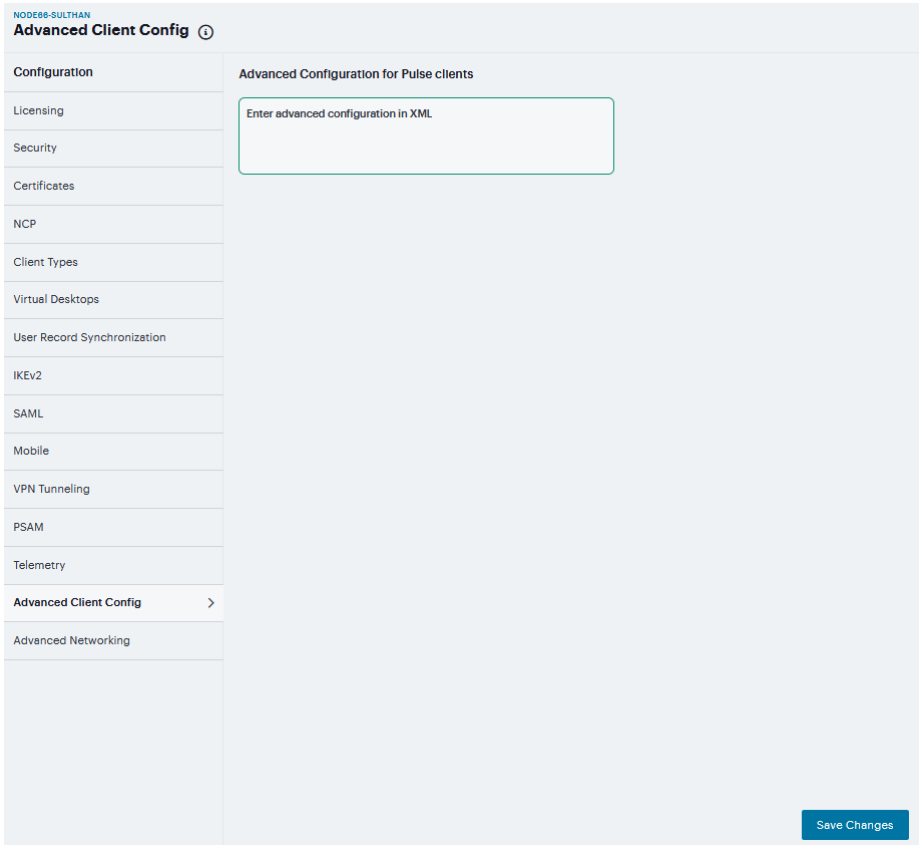


FIGURE 10.40 : Advanced Client Configuration

The advanced configuration setting “ignore-tcp-mss” is Layer3 Adapter configuration setting and this will be consumed by the Ivanti Secure Access client as part of the IpsecConfig.

Note: This “ignore-tcp-mss” setting is applicable for the virtual adapter MTU calculation only for IPv4. By default, the setting is always false, and therefore the TCP MSS options are always considered for MTU by default. Admin has to explicitly set the ignore-tcp-mss setting to TRUE (case insensitive), to ignore TCP MSS.

Advanced Networking Configuration

The NTP, SNMP, Syslog, and Log archiving services are set to send the traffic through Management port by default. In case the Management port is not available, the traffic is routed through Internal port. Now, an administrator can modify the settings of NTP and other services to any physical inter-face.

The following procedure describes the steps to configure the ports for the services. Before you proceed, ensure the External and Management ports are enabled for use in the network settings.

To configure Service Traffic Port Options

1. Navigate to **System > Configuration > Advanced Networking**.
2. For the individual service, select the required port from the drop-down list.
3. Click **Save Changes**.

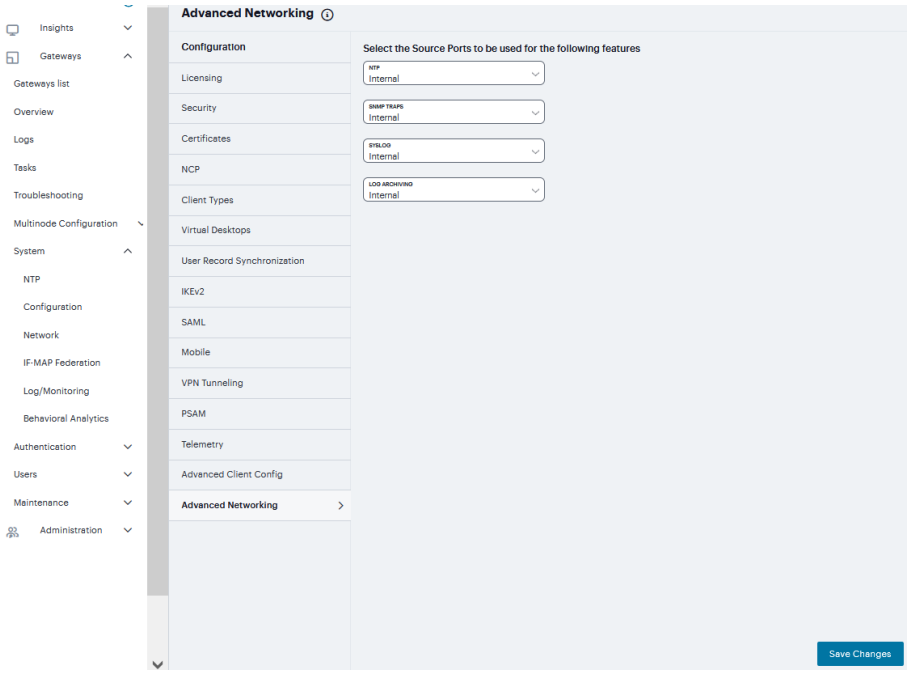


FIGURE 10.41 : Advanced Networking

In a cluster environment, when a node joins the cluster, configuration of the node is replaced with the configuration of other nodes in the cluster.

IF-MAP Federation

You can configure a Ivanti Policy Secure device to store user session information for other Ivanti Policy Secure and Ivanti Connect Secure devices. Federation allows users to authenticate to a single Ivanti Connect Secure or Ivanti Policy Secure, and then access resources that are protected by any number of Ivanti firewall devices known as Infranet Enforcers that are controlled by different Infranet Controllers. Federation enhances network performance. If a user is required to log in to multiple Ivanti Connect Secure or Ivanti Policy Secure devices during the course of a day to access different resources, each device must perform authentication and Host-Checking, often with periodic Host Checker updates throughout the day. The overhead can lead to decreased performance not only on the devices, but also on the network and the endpoint. Imported IF-MAP sessions eliminate redundant logins and Host Checks.

Federation on the device uses the standard IF-MAP (Interface for Metadata Access Point) protocol to share session information and other data between connected devices over distributed networks. IF-MAP is a protocol defined by the Trusted Network Connect Working Group (TNC-WG) as a standard interface between different network elements and devices. Federation is accomplished using an IF-MAP server and IF-MAP clients.

It is important as an administrator to understand the fundamental underlying communication method for data transmission in a Federation network over IF-MAP. Policies that you configure on the device permit this communication. In a federated network, the IF-MAP server functions as the repository, or data store for IF-MAP clients to use for publishing information regarding activity on the network. For example, IF-MAP clients can publish information about sessions on the network, and Juniper Networks IDP devices can communicate information about potential threats to the IF-MAP client for publishing. IF-MAP clients can search for information about sessions or threats, and an IF-MAP client can establish a subscription so the IF-MAP server notifies the client when other clients publish new or changed information. In addition, IF-MAP clients can purge data that is no longer valid. All transactions are initiated by the IF-MAP client.

Overview

You can configure the system as an IF-MAP client for an IF-MAP server. You configure an Infranet Controller as an IF-MAP server. Any endpoint sessions with an IP address created on an IF-MAP server are automatically published to that IF-MAP server.

You can create source IP policies for endpoints that authenticate to the device to permit access to resources behind Infranet Enforcers (ScreenOS Enforcers and Ivanti Policy Secure s). Session-Export policies that you configure on the IF-MAP clients allow the clients to publish endpoint user data to the IF-MAP server. Devices that are IF-MAP clients can subscribe to the information on an IF-MAP server. When a user accesses the device that is configured as an IF-MAP client, the client publishes basic session information, including the IP address, username and roles, to the IF-MAP server. The server stores the information as metadata. Other IF-MAP clients in the network can poll the server for metadata when session information is

needed as a result of an endpoint attempting to access protected resources behind an Infranet Enforcer.

When an authenticated user from the device that is configured as an IF-MAP client attempts to access resources that are protected by an Infranet Enforcer for an Infranet Controller that is also configured as an IF-MAP client, the Infranet Controller automatically provisions an auth table entry for the user on the Infranet Enforcer to allow access without requiring the user to authenticate to the Infranet Controller.

The Infranet Enforcer as an IF-MAP client subscribes to session information and other data for the endpoint based on the originating IP address. The authenticating device (the original IF-MAP client) publishes any changes in session parameters to the IF-MAP server. Since the Infranet Controller that is protecting the accessed resources subscribes to the metadata on the Federation server, session information is always current.

The Infranet Enforcer allows or denies traffic based on the resource access policies that are configured on the Infranet Controller to which it is connected.

You configure server settings on the Infranet Controller that will be the IF-MAP server. You configure client settings on each of the Ivanti Connect Secure and Infranet Controller devices and that will be connected in the network.

You must identify the IF-MAP server to each 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 devices that will be IF-MAP clients:

1. Log into the nSA as a Tenant Admin.
2. From the ICS menu, click the *Gateway > Gateway List* and then select any standalone ICS Gateway and Cluster node.
3. Navigate to **System > IF-MAP Federation > Overview**.
4. Select the **Enable IF-MAP Client** check box.
5. Type the Server URL for IF-MAP Web service on the IF-MAP server. Append the server URL with */dana-ws/soap/dsifmap* for all Ivanti IF-MAP servers.
6. Select the client Authentication method: **Basic** or **Certificate**.
    - If you select **Basic**, enter a **Username** and **Password**. This is the same as the information that was entered on the IF-MAP server.

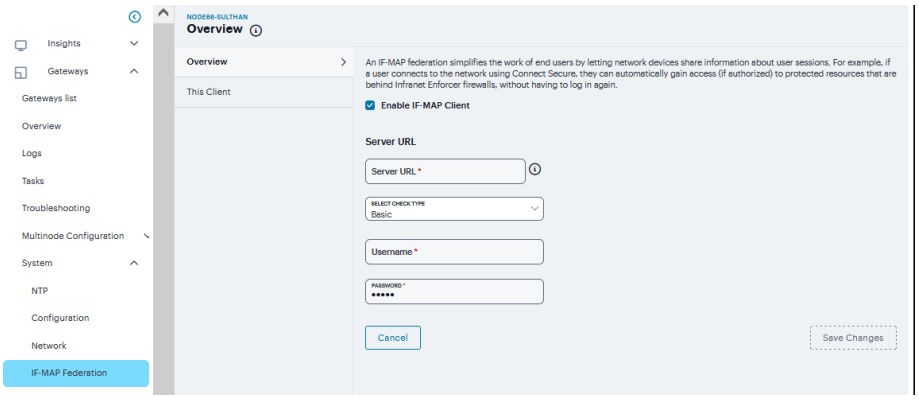


FIGURE 10.42 : Basic

- 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 CA** page.

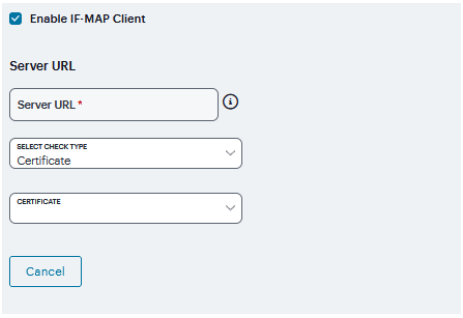


FIGURE 10.43 : Certificate

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 IFMAP server, and that the CA that signed the server certificate is configured as a trusted server CA on the IF-MAP client.

7. Click **Save Changes**.

This Client

By default, Session-Import and Session-Export IF-MAP policies are configured to allow IF-MAP capabilities (the equivalent of roles) to be published to the IF-MAP server and retrieved from the IF- MAP server, provided there are matching roles on each IF-MAP client. You can open new Session-Import and Session-Export policies on each device, and then name and close the policies. Any matching roles that the IF-MAP clients in the federated network have can be used to access resources.

By default, advanced policy actions are not visible unless you click the advanced options links on the Session-Export and Session-Import policy pages. In default mode, you configure Session-Export and Session-Import policies using IF-MAP

capabilities and roles. Device attributes, IF-MAP roles and identities can be accessed through the advanced options links. IF- MAP capabilities and Connect Secure roles should provide the functionality that most IF-MAP Federation requires.

Session-Export Policies

In a Layer 2 environment, session information on the IF-MAP server includes a MAC address. If an export policy specifies an Administrative Domain, the domain is associated with the MAC address published to the IF-MAP server (the administrative domain is also associated with the identity published to the IF-MAP server).

A DHCP server assigns an IP address to the endpoint after authentication. An IF-MAP enabled DHCPr server publishes an ip-mac link to IF-MAP, associating the endpoint's IP address with its IF-MAP session information.

Including administrative domains in MAC addresses allows the ip-mac link to be created based on the administrative domain.

If your IF-MAP Federated network spans different administrative domains, you should configure separate Session-Export policies for each domain to prevent MAC address spoofing. Each administrative domain should have an associated DHCP server and unique Session-Export policies.

Other aspects of the Session-Export policies within the IF-MAP Federated network can overlap.

To configure a Session-Export policy:

1. Log into the nSA as a Tenant Admin.
2. From the ICS menu, click the *Gateway > Gateway List* and then select any standalone ICS Gateway and Cluster node.
3. Navigate to System > IF-MAP > Session-Export Policies.
4. Click '**+**' to create a new policy.

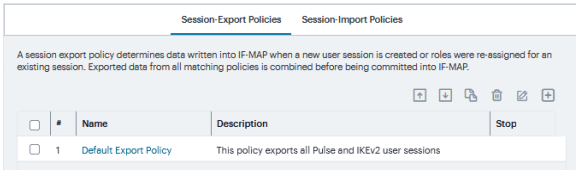


FIGURE 10.44 : Session-Export Policies

5. Type a **Policy Name**, and optionally a **Description**.
6. Optionally, add **Available Roles** to the **Selected Roles** column to determine the roles for which this policy should apply. If you do not add any roles, the policy applies to all sessions. However, if you have non-interactive devices such as printers that do not need access, you may want to manually add roles and exclude those roles with non-interactive devices.

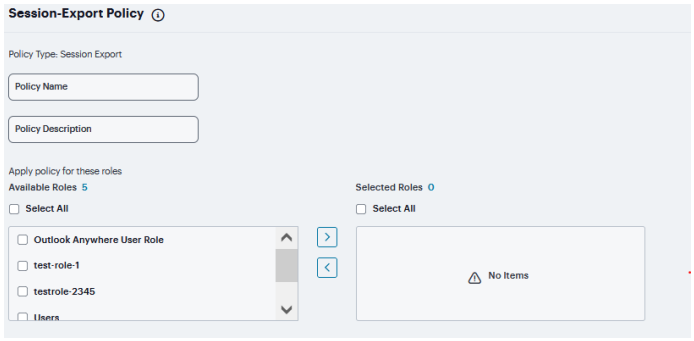


FIGURE 10.45 : Roles

7. Under **Policy Actions**, Select **Set IF-MAP Capabilities** and choose the applicable roles.
   - **Copy matching roles** - Selecting this action copies 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** - Selecting this action copies all of the roles from the user session to the IF-MAP capabilities data.
   - **Set capabilities specified below** - Enter capabilities, one per line.

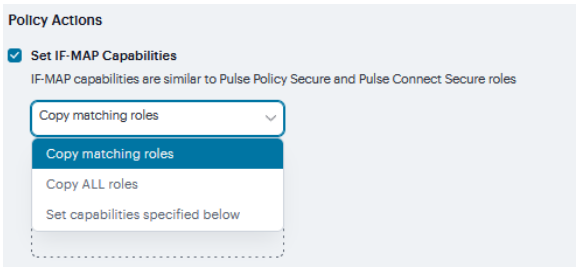


FIGURE 10.46 : Capabilities

8. Select **Stop processing policies when this policy matches** to specify that when this policy is matched, no more Session-Export policies should be applied.
9. Click **Save Changes**, or continue to configure Advanced Actions.

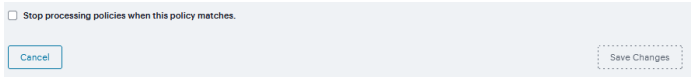


FIGURE 10.47 : Stop Processing Policies

10. Click the **View Advanced Actions** link. Additional options appear on the page.
11. **Set IF-MAP Identity** - If this action is chosen, enter the Identity and select an Identity Type from the menu. Identity is normally specified as <NAME>, which assigns the user's login name. Any combination of literal text and context variables may be specified. If you choose other for Identity Type, enter a unique Identity Type in the Other text box.

12. Optionally type the **Administrative Domain** for the Session-Export policy. This optional field is applied to identity and MAC address data. One example for using this field is in a large network environment with several domains in which a username could be duplicated. By entering the domain, you ensure that the correct user is identified.
13. **Set IF-MAP Roles** - If this action is selected, select the applicable roles.
    - **Copy matching roles** - Selecting this action copies 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** - Selecting this action copies all of the roles from the user session to the IF-MAP capabilities data.
    - **Set roles specified below** - Enter roles, one per line.
14. **Set IF-MAP Device Attributes** - **Device attributes** represent a passed Host Checker policy on the Infranet Controller or Connect Secure.
    - **Copy Host Checker policy names** - The name of each Host Checker policy that passed for the session is copied to a device attribute.
    - **Set device attributes specified below** - Type device attributes, one per line, into the text box.

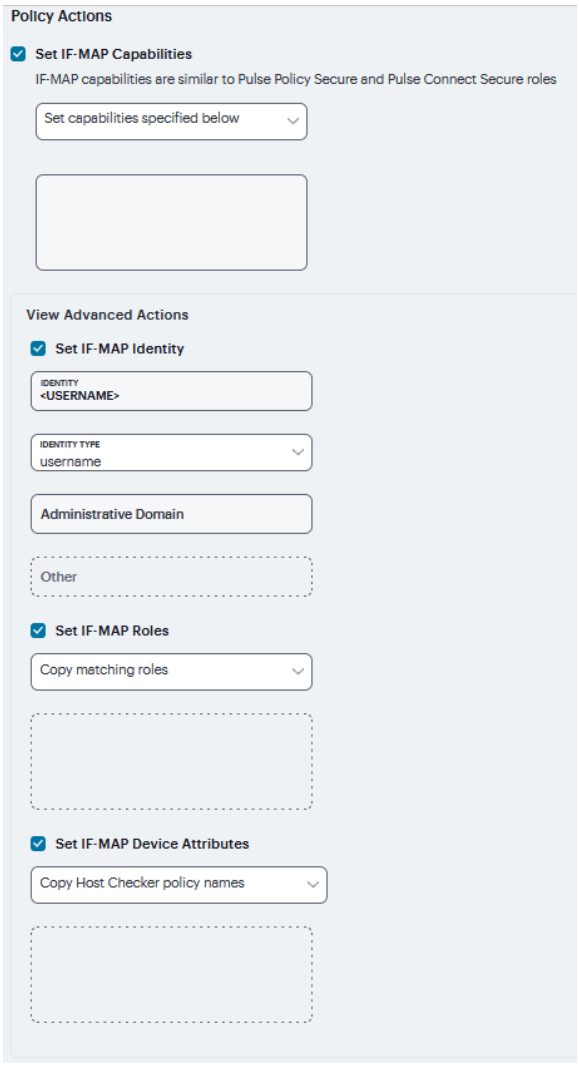


FIGURE 10.48 : View Advanced Actions

15. Click **Save Changes** to save this advanced Session-Export policy.

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.

Session-Export Policies

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 Connect Secure. 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 IVEs that are connected to an Infranet Enforcer in front of protected resources.

To configure a Session-Import policy:

1. Log into the nSA as a Tenant Admin.
2. From the ICS menu, click the *Gateway* > *Gateway List* and then select any standalone ICS Gateway and Cluster node.
3. Navigate to **System > IF-MAP > This Client > Session-Import Policies** tab.
4. Click '**+**' to create a new policy.

FIGURE 10.49 : Session-Import Policies

5. Type a **Policy Name**, and optionally a **Description**.
6. Under **Conditions when Policy Applies**, Select **Match IF-MAP Capabilities**, enter one capability per line.

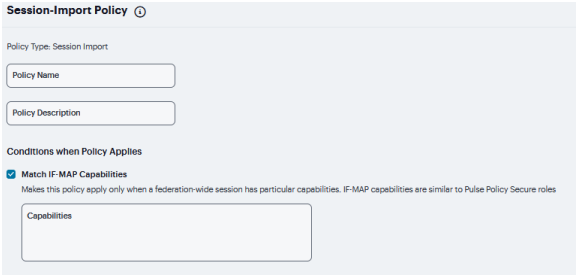


FIGURE 10.50 : Conditions When Policy Applies

7. Click the **View Advanced Conditions** link. Additional options appear on the page.
8. **Match IF-MAP Identity** - If this action is chosen, enter the **Identity** and select an **Identity Type** from the menu. Identity is normally specified as <NAME>, which assigns the user's login name. Any combination of literal text and context variables may be specified. If you choose other for Identity Type, enter a unique Identity Type in the **Other** text box.
9. Optionally select and type the **Administrative Domain** for the Session-Import policy. This optional field is applied to identity and MAC address data. One example for using this field is in a large network environment with several domains in which a username could be duplicated. By entering the domain, you ensure that the correct user is identified.

10. Match IF-MAP Roles - If this action is selected, then match then specified **Roles below** - Enter roles, one per line.
11. Match IF-MAP Device Attributes - Matches **Device attributes** passed Host Checker policy on the Infranet Controller or Connect Secure. Enter one Attribute, one per line.

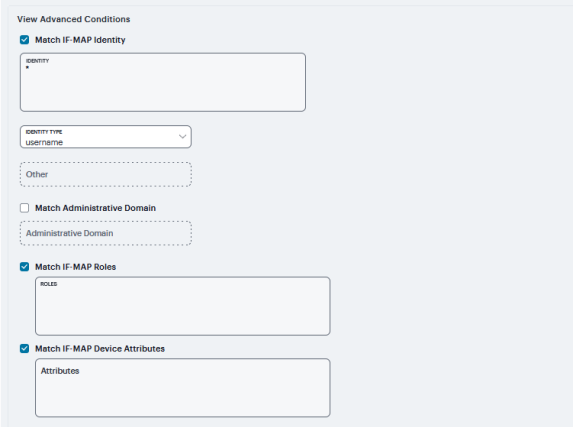


FIGURE 10.51 : View Advanced Conditions

12. Optionally, Under **Assign these roles** and Click **Use these roles** add **Available Roles** to the **Selected Roles** column to determine the roles for which this policy should apply. If you do not add any roles, the policy applies to all sessions.
13. To copy If-Map Capabilities Select Copy IF-MAP Capabilities and select the capabilities. If Specified capabilities or All capabilities other than those specified below is selected, then enter one capability per line in the text box.

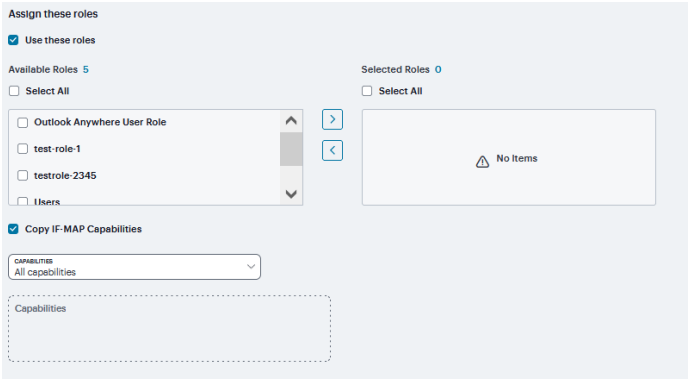


FIGURE 10.52 : Assign these roles

14. Select **Stop processing policies when this policy matches** to specify that when this policy is matched, no more Session-Import policies should be applied.
15. Click **Save Changes** or continue to configure Advanced Assignment Option.
16. Click the **View Advanced Assignment Option**. Additional options appear on the page.

17. Click **Copy IF-MAP Roles** - If this action is selected, then select the applicable roles.
18. If **Specified roles** or **All roles other than those specified below** is selected, then enter one role per line in the text box.
19. Click **Save Changes**.

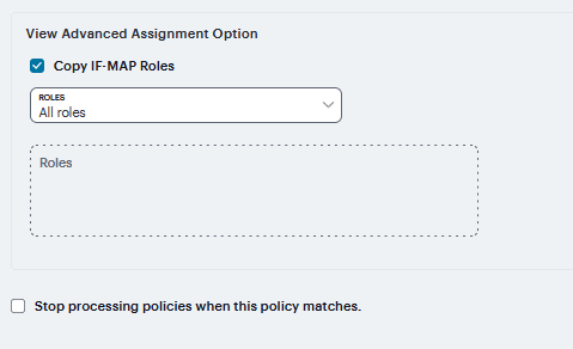


FIGURE 10.53 : View Advanced Assignment Option

Log/Monitoring

The system generates event logs related to system performance, administrator actions, network communications, access management framework results, user sessions, and so forth. The system supports the following log collection methods:

- Local log collector and log viewer.
- Reporting to syslog servers.
- Reporting to SNMP servers.

The following table lists the Event Log Severity Levels:

TABLE 10.9 : Severity Levels

Severity Level	Description
Critical (level 10)	The system cannot serve user and administrator requests or loses functionality to a majority of subsystems.
Major (levels 8-9)	The system loses functionality in one or more subsystems, but users can still access the system for other access mechanisms.
Minor (levels 5-7)	The system encounters an error that does not correspond to a major failure in a subsystem. Minor events generally correspond to individual request failures.
Info (levels 1-4)	The system writes an informational event to the log when a user makes a request or when an administrator makes a modification.

In addition to managing system logs, you can use the admin console to configure collection of client-side logs, including:

- Host checker
- Windows Secure Application Manager
- Java Secure Application Manager and Applet Rewriting
- VPN Tunneling
- Terminal Services
- Virtual Desktops

Events to Log

To configure log event categories:

1. Select **System > Log/Monitoring**.
2. Click the **Settings** tab to display the configuration page.
3. Complete the configuration as described in table.
4. Click **Save Changes**.

Note: To configure log events for each local log category, you must perform this procedure on each local log tab: Events, User Access, and Admin Access.

The following table lists the Log Events Settings:

TABLE 10.10 : Log Events

Settings	Guidelines
Maximum Log Size	

continues on next page

TABLE 10.10 – continued from previous page

Settings	Guidelines
Max Log Size	**Specify the maximum size of the local log. The default is 200 MB. The maxim** When the local log reaches the maximum log size, the current data is rolled over to a backup log file. A new, empty, file is then created for all subsequent (new) log messages. The log viewer displays the most recent 5000 log messages (the display limit). If the current log file contains fewer than 5000 log messages, older log messages from the backup log file can be displayed, up to a total of 5000 log messages. This makes the log files appear as one, even though they are stored separately. When you save the log messages or use the FTP archive function, the backup log file is appended to the current log file and is then downloaded as one log file. If the log files are not archived or saved by the time they are rolled over again, the oldest log messages (saved in the backup log file) are lost.
Archiving	Click the Archiving link to display the configuration page for Archiving jobs, including log archiving.
Select Events to Log - Events Tab	
Connection Requests	Log events related to connection requests.
System Status	Log events related to changes in system status.
Rewrite	Log events related to rewrite policies.
System Errors	Log events related to system errors.
Statistics	Log user access statistics reported on the System > Log/Monitoring > Statistics tab. If you disable the Statistics option, the statistics are not written to the log file, but are still reported on the statistics page.
License Protocol Events	Log events related to licensing.

continues on next page

TABLE 10.10 – continued from previous page

Settings	Guidelines
Reverse Proxy	Logs events related to reverse proxy information.
Select Events to Log - User Access Tab	
Login/logout	Log events related to sign in and sign out.
SAM/Java	Log events related to user access to SAM/Java in the local log file.
User Settings	Log events related to changes to user settings in the local log file.
Client Certificate	Log events related to certificate security.
IF-MAP Client User Messages	Log events related to IF-MAP.
Ivanti Secure Access Client Messages	Log events related to Ivanti Secure Access clients.
HTML5 Access	Log events related to HTML5 access.
Web Requests	Log events related to user access to web.
File Requests	Log events related to user access to files.
Secure Terminal	Log events related to user access to secure terminal.
VPN Tunneling	Log events related to user access to VPN tunneling.
SAML	Log events related to user access to SAML.
System Too Busy	Log events related to ICS overload.

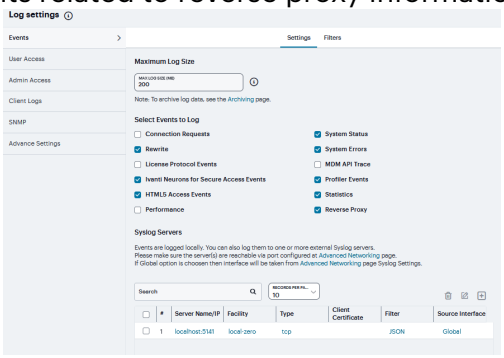
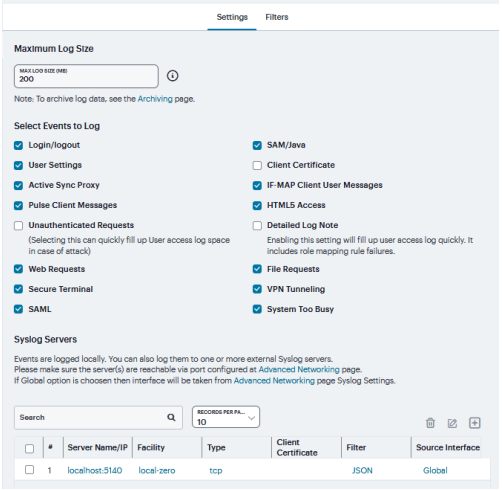
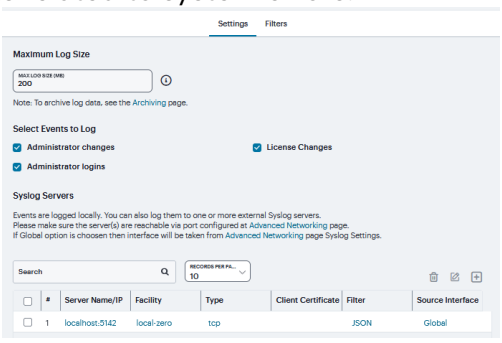


FIGURE 10.54 : Events Log

continues on next page

TABLE 10.10 – continued from previous page

Settings	Guidelines
Unauthenticated Web Requests	Log events related to web requests before authentication. By default, this check box is disabled.  FIGURE 10.55 : User Access - Events Log
Select Events to Log - Admin Access Tab	
Administrator changes	Log events related to configuration changes.
Administrator logins	Log events related to administrator access.
License changes	Log events related to licensing.
System Errors	Log events related to system errors.  FIGURE 10.56 : Admin Access - Events Log
Syslog Servers	click '**+**' to add new logs. Complete the configuration as described in below rows. You can specify multiple syslog servers.

continues on next page

TABLE 10.10 – continued from previous page

Settings	Guidelines
Server name/IP	**Specify the fully qualified domain name or IP address for the syslog se** If you select TLS from the Type list, the server name must match the CN in the subjectDN in the certificate obtained from the server.
Facility	Select a syslog server facility level (LOCAL0-LOCAL7). Your syslog server must accept messages with the following settings: facility = LOG_USER and level = LOG_INFO.
Type	**Select the connection type to the syslog server. You can select:** • UDP (User Datagram Protocol) - A simple non-secure transport model. • TCP (Transmission Control Protocol) - A core protocol of the Internet Protocol suite (IP), but lacks strong security. • TLS (Transport Layer Security) - Uses cryptographic protocols to provide a secure communication.
Client Certificate	(optional) If you select TLS from the Type menu and your remote syslog server requires client certificates, select the installed client certificate to use to authenticate to the syslog server. Client certificates are defined in the Configuration > Certificates > Client Auth Certificates page. Client certificates must be installed on the device before they can be used. There is no fallback if a connection type fails.

continues on next page

TABLE 10.10 – continued from previous page

Settings	Guidelines
Filter	Select a filter format. Any custom filter format and the following predefined filter formats are available: • **Standard (default)** - This log filter format logs the date, time, node, source IP address, user, realm, event ID, and message. • **WELF** - This customized Web Trends Enhanced Log Format (WELF) filter combines the standard WELF format with information about the system realms, roles, and messages. • **WELF-SRC-2.0-Access Report** - This filter adds access queries to the customized WELF filter. You can use this filter with NetIQ's SRC to generate reports on user access methods.
Source Interface	Select the source port type for the syslog server: • Global • External • Internal • Management Ensure the servers are reachable through port configured in the **Advanced Networking** page on the Admin UI.

Log Filters

If desired, you can create custom log collection filters to change the records displayed or exported. For example, it is common to see administrators use a filter for RADIUS accounting logs. This filter allows only the accounting log message, and it puts the entire message in a comma separated list. The order of the filtered message is: Date, Time, User, Realm, "List of Roles", NAS-ID, Acct-Status, Auth-Type, Attr-Value1, Attr-Value2, Attr-Value3.

Accounting attribute messages are different from authentication attribute messages in that the attribute name is not printed in the log message, but a comma is inserted for every attribute to be logged, even if it is not present.

To view the configuration of predefined log format filters:

1. Navigate to System > Log/Monitoring.
2. Click the **Events** / **User Access** / **Admin Access** tab.
3. Click the **Filter** tab to display the log filters page.
4. Click the hyperlinked name of the filter to display its configuration page. You cannot edit the predefined filter named Standard, but you may edit the predefined WELF filters and any other custom filters that appear in the list.

5. Click '**+**' to display the configuration page for creating new filter.
6. Complete the configuration as described in table.
7. Click **Save Changes**.

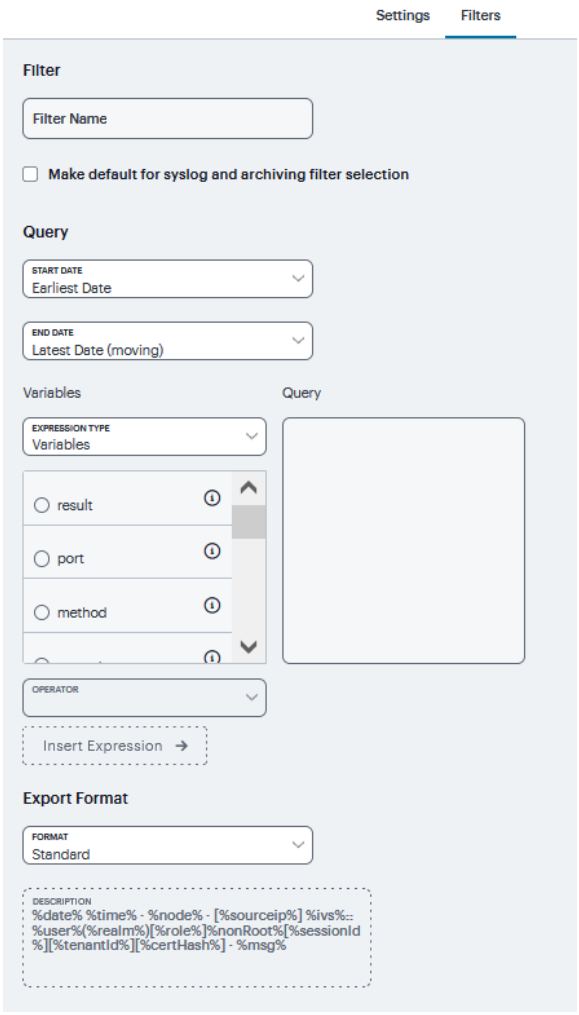


FIGURE 10.57 : Log Filter

TABLE 10.11 : Log Filters

Settings	Guidelines
Filter Name	Specify a name that is helpful to you and other administrators in understanding usage for your custom filter.
Make default	Make the filter the default on syslog and archiving configuration pages.
Query	
Start Date	Enter a start date. Click **Earliest Date** to write all logs from the first available date stored in the log file.
End Date	Enter an end date. Click **Latest Date** to write all logs up to the last available date stored in the log file.
Query	**Use the Filter Variables Dictionary to insert query expressions in the Query b** For example, insert the query expression sourceip=. Then complete the expression by adding the value '192.168.0.1'.
Export Format	Select an export format: • **Standard (default)** - This log filter format logs the date, time, node, source IP address, user, realm, and message. • **WELF** - This customized WebTrends Enhanced Log Format (WELF) filter combines the standard WELF format with information about the system realms, roles, and messages. • **Custom** - Use the Standard as a template for your custom selection of columns to be included in exports (when log collections are saved to files).

Note: Log query filters change only the data displayed (or rows exported). Log format filters change only the data displayed (or columns exported). Use of filters does not affect the log data that has been collected.

Client Side Log

Client-side logging is not enabled by default. If necessary, you can enable client-side logging to troubleshoot any client application issues.

To enable client side logging:

1. Select **System > Log/Monitoring**.
2. Click the **Client Logs** tab to display the configuration page. Complete the configuration as described in Table.
3. Click **Save Changes**.

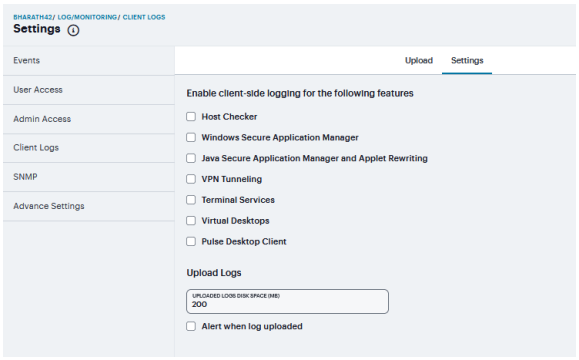


FIGURE 10.58 : Client Side Log

Upload tab displays **Uploaded Logs Details**

TABLE 10.12 : Client Side Log

Settings	Guidelines
Host Checker	Select this option to enable client-side logging of Host Checker.
Windows Secure Application Manager	Select this option to enable client-side logging of PSAM.
Java Secure Application Manager and Applet Rewriting	Select this option to enable client-side logging of JSAM and applet.
VPN Tunneling	Select this option to enable client-side logging of VPN tunneling.
Terminal Services	Select this option to enable client-side logging of terminal services.
Virtual Desktops	Select this option to enable client-side logging of virtual desktops.
Ivanti Secure Access Desktop Client	Select this option to enable client-side logging of Ivanti Secure Access desktop clients.
Upload logs	
Upload logs disk space (MB)	Specify the amount of disk space (in Megabytes) you want to allocate for uploaded client log files. You can allocate disk space from 0 to 200 MB.
Alert when log uploaded	Select this option to receive an alert message when an end user pushes a log file.

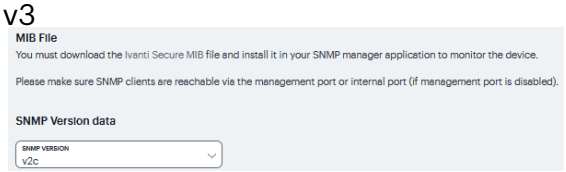
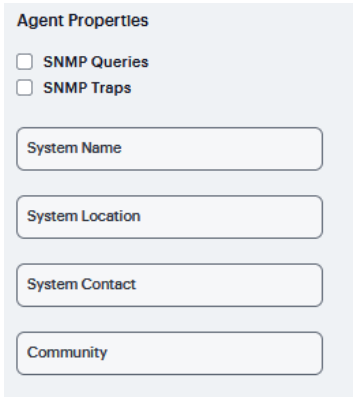
SNMP

If you prefer, you can use a third-party SNMP manager, such as HP OpenView, to monitor system health. The system supports SNMP v2c and SNMPv3. The system supports two users to be registered with an SNMP engine with different authentication and privilege settings.

To configure the SNMP agent:

1. Select **System > Log/Monitoring**.
2. Click the **SNMP** tab to display the SNMP configuration page.
3. Complete the configuration as described in Table.
4. Click **Save Changes**.

TABLE 10.13 : SNMP agent

Settings	Guidelines
MIB File	Use the Ivanti MIB file link to download the device management information base MIB file. You add this file to your SNMP manager configuration.
SNMP Version	**Select your SNMP server version:** • v2c • v3  FIGURE 10.59 : SNMP server version
Agent Properties	
SNMP Queries	Select to support SNMP queries. Selecting this option enables the SNMP Diagnostic Log utility in the Troubleshooting > Monitoring > Diagnostic Logs page.
SNMP Traps	Select to send SNMP traps. Selecting this option enables the SNMP Diagnostic Log utility in the Troubleshooting > Monitoring > Diagnostic Logs page.
System Name	Specify a system name.
System Location	Specify a location.
System Contact	Specify a system contact
Community String	**Required only for SNMPv2c.** To query the system, your network management station must send it the community string. To stop the SNMP system, clear the community field.  FIGURE 10.60 : Agent Properties
SNMPv3 Configuration	

Keep the following configuration tips in mind when you configure your SNMP manager to listen for this SNMP agent:

- Add the Ivanti MIB file to the SNMP manager configuration.
- If using SNMPv2c, the community string configuration for the SNMP manager and SNMP agent must match.
- If using SNMPv3, the SNMPv3 user configuration for the SNMP manager and the SNMP agent must match.
- If using SNMPv3, you must specify the Authoritative Engine ID for SNMPv3 traps that was generated when you saved the SNMP agent configuration.

Advanced Settings

This option helps to configure fault tolerance on each configured TCP and TLS syslog server available. Fault tolerance is supported only for TCP and TLS syslog servers. UDP syslog servers cannot be configured for fault-tolerance. This functionality helps the syslog server to recover the logs lost during a disconnect. The administrator can configure fault-tolerance on syslog servers by enabling this option from the admin UI. ICS/IPS reads the lost pending logs during a disconnect from the log disk and transports them to the syslog server on a reconnect. Fault tolerance is supported only for the syslog servers configured under the following log-types:

- Events
- User Access
- Admin Access

Note: Fault tolerance is node-specific. In case of clusters, the setting needs to be enabled/disabled by logging into each of the cluster members. Fault tolerance is supported only for TCP and TLS syslog servers. UDP syslog servers cannot be configured for fault tolerance.

To configure advance settings to a TCP and TLS syslog server:

1. Navigate to **System > Log/Monitoring**.
2. Click the **Advance Settings** tab to display the configuration page.
3. Complete the configuration as described in Table.
4. Click **Save changes**.

Note: This feature is limited to configuring fault tolerance settings of an existing syslog server; and cannot be used to create or delete a new syslog

server.

TABLE 10.14 : Advance Settings

Settings	Guidelines
Syslog Server Fault Tolerance	
Syslog Server	Lists the existing Syslog servers.
Type	Specifies if the Syslog server is a TLS or TCP type.
Fault Tolerance	Tolerates the loss of network connection to a TCP/TLS syslog server for a brief period (maximum of 4 hours) by sending the logs missed during the disconnect time. Click the check box to enable this option. Fault-tolerance is disabled by default on any syslog server.

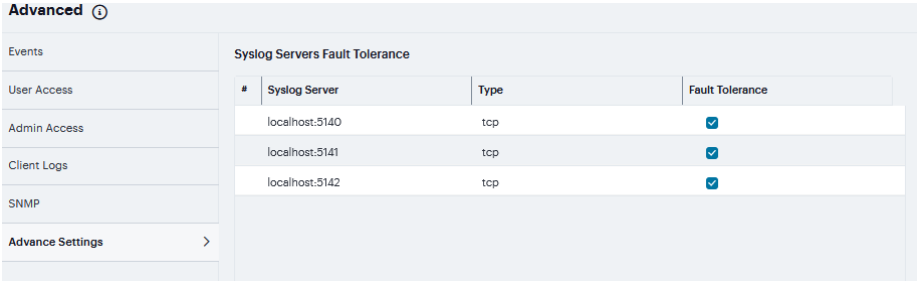


FIGURE 10.64 : Advanced Settings

Behavioral Analytics

Behavioral Analytics feature analyzes user's action along with other context data to derive conclusions about any anomalous activities. It provides information/visibility based on real time user or device context thus helping in advanced attack detection and helps in proactive policy-based enforcement.

The Behavioral Analytics feature addresses the following types of anomaly detection:

- **User/device is prompted for second level of authentication based on the threat profile det**
  Below are some scenarios where second level of authentication is required:

- User authenticating from new device: This is detected by using the device MAC address.
- User authenticating from new location: Location details are obtained by using the location configurations.

Benefits

- **ICS monitors the traffic from users and helps in determining the possible anomalous activities su**
  - If the user is authenticating from a new device / new location.
  - If the device traffic is different from previous instances.
- Data collected as part of Behavior Analytics is stored so that it can be used later for determining the anomalies.

To enable behavioral analytics:

1. Log into the nSA as a Tenant Admin.
2. From the ICS menu, click the *Gateways* > *Gateways List* and then select any standalone ICS Gateway or Cluster node.
3. Navigate to **System > Behavioral Analytics > Configuration**.
4. Under Configurations, select **Enable Behavioral Analytics**.
5. For enabling Adaptive Authentication, select **Enable data collection during authentication of devices and users**.
6. Click **Save Changes**.

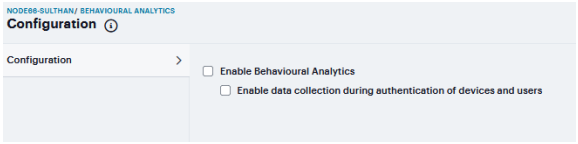


FIGURE 10.65 : Behavioral Analytics

In case you have a Fresh Installation of ICS, then it will NOT have UEBA package by default with it. Please add the UEBA package before using Adaptive Authentication.

Network and Host Administration

Introduction

When you install and initially set up the device, you use the serial port console to set basic network and host settings. To get started, you must use the serial console to configure these settings for the internal interface. You have the option to use the serial console to configure network and host settings for the external interface and the management interface. The network and host settings you configure with the serial port console include:

Once the internal interface has been configured, you can use the admin console Network Settings pages to modify settings for the internal interface, to enable and configure the external interface and the management interface, and to configure or manage advanced networking features, including:

- Hostname
- IPv6 addresses
- VLAN ports
- Virtual ports
- Route table entries

- Host mapping table entries
- ARP cache entries
- Neighbor discovery cache entries
- System date and time (manual configuration) or NTP

Internal Port Configuration

The internal port, also known as the internal interface, handles all LAN requests to resources, listening for Web browsing, file browsing, authentication, and outbound mail requests.

To configure the internal port configuration:

Settings

1. Log in to the Ivanti Neurons for Secure Access portal as a Tenant Admin. See *Logging in to Ivanti Neurons for Secure Access* (page 5).
2. Use the Gateway Switcher and select **Ivanti Connect Secure**.
3. From the Ivanti Connect Secure menu, click the **Gateways** icon, then select **Gateways > Gateways List**.

   The All Gateways page is displayed showing a list of standalone ICS Gateways and Cluster nodes.
4. From the **Standalone ICS Gateways** list, click on the gateway link that you want to configure.
5. On the Ivanti Connect Secure menu, select **System > Network > Internal Port > Settings** to display the configuration page.
6. Under IPV4 Settings, assign an IP address, assign a Netmask, and specify the IPv4 address for the default Gateway.

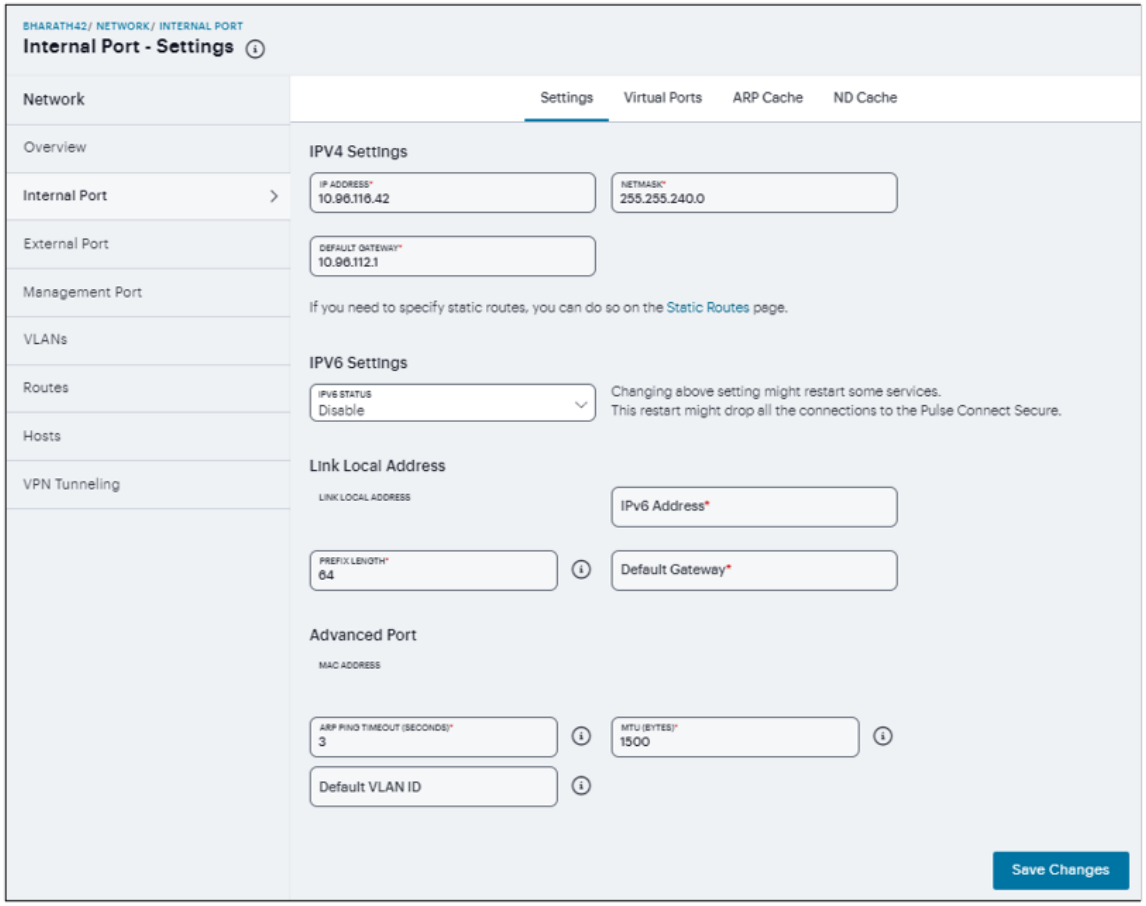


FIGURE 11.1 : Internal Port Configuration

7. Under IPV6 Settings, select IPV6 Status.
8. Under Link Local Address, you can see the auto-configured link local address. Specify a routable IPv6 address, Prefix Length, and IPv6 address for the default Gateway.
9. Under Advanced Port, specify the ARP Ping Timeout, maximum transmission unit, and default VLAN ID for the traffic of this port.
10. Click **Save Changes**.

Virtual port - You can use virtual ports to provide different groups of users access to the same system using different IP aliases and domains.

To configure a virtual port:

1. Select **Internal Port > Virtual Ports**. Port is Internal Port or External Port.
2. Click '+' to display the configuration page.
3. Enter a name for the virtual port.
4. Enter the IPv4 address and the IPv6 address.
5. Click **Save Changes**.

ARP Cache - In IPv4 networking, network nodes use ARP to maintain information about peer network nodes.

To manage the ARP table:

1. Select **Internal Port > ARP Cache**. Port is Internal Port, External Port, or Management Port.
2. Click '+' to display the configuration page.
3. Enter an IP address, and a MAC address.
4. Click **Save Changes** to add an entry.
5. You can delete all dynamically discovered entries.

ND Cache - In IPv6 networking, network nodes use the Neighbor Discovery Protocol (NDP) to determine the Layer 2 MAC addresses for neighboring hosts and routers.

To manage the neighbor discovery table:

1. Select **Internal Port > ND Cache**. Port is Internal Port, External Port, or Management Port.
2. The **Flush NDP Entries** deletes all dynamically discovered entries.

External Port Configuration

The external port, also known as the external interface, handles all requests from users signed into Ivanti Connect Secure from outside the customer LAN, for example, from the Internet. Before sending a packet, Ivanti Connect Secure determines if the packet is associated with a TCP connection that was initiated by a user through the external interface. If that is the case, Ivanti Connect Secure sends the packet to the external interface. All other packets go to the internal interface.

To configure the external port configuration:

Settings

1. Log in to the Ivanti Neurons for Secure Access portal as a Tenant Admin. See *Logging in to Ivanti Neurons for Secure Access* (page 5).
2. Use the Gateway Switcher and select **Ivanti Connect Secure**.
3. From the Ivanti Connect Secure menu, click the **Gateways** icon, then select **Gateways > Gateways List**.

   The All Gateways page is displayed showing a list of standalone ICS Gateways and Cluster nodes.
4. From the **Standalone ICS Gateways** list, click on the gateway link that you want to configure.
5. On the Ivanti Connect Secure menu, select **System > Network > External Port > Settings** to display the configuration page.

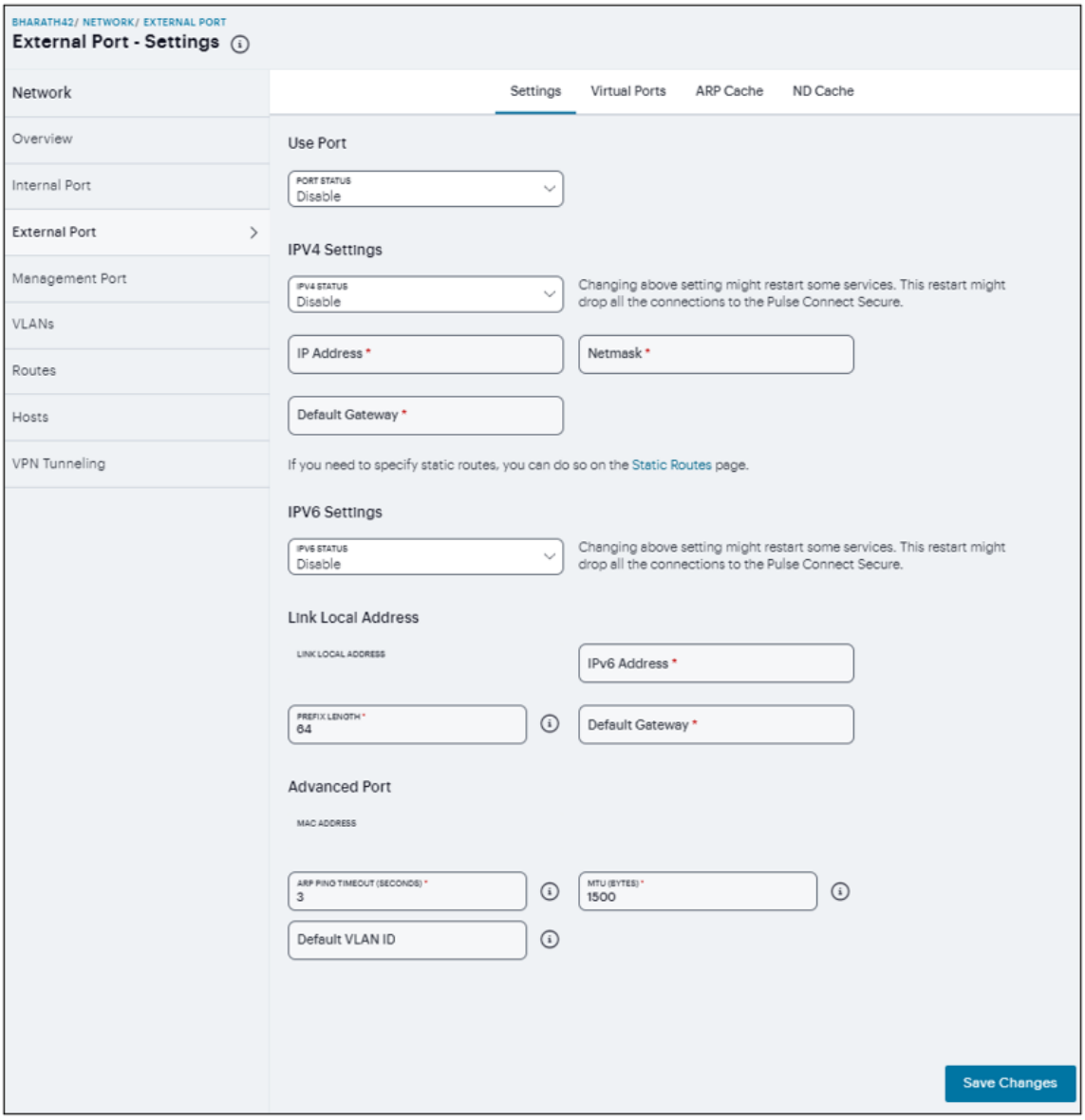


FIGURE 11.2 : External Port Configuration

6. Enable the **Port Status**.
7. Under IPV4 Settings, assign an IP address, a Netmask, and the IPv4 address for the default Gateway.
8. Under IPV6 Settings, select **IPV6 Status**.
9. Under Link Local Address, you can see the auto-configured link local address. Specify a routable IPv6 address, Prefix Length, and IPv6 address for the default Gateway.
10. Under Advanced Port, specify the ARP Ping Timeout, maximum transmission unit, and default VLAN ID for the traffic of this port.
11. Click **Save Changes**.

Virtual Ports - You can use virtual ports to provide different groups of users access

to the same system using different IP aliases and domains.

To configure a virtual port:

1. Select **External Port > Virtual Ports**. Port is Internal Port or External Port.
2. Click '+' to display the configuration page. Specify a name for the virtual port, an IPv4 address, and an IPv6 address.
3. Click **Save Changes**.

ARP Cache - In IPv4 networking, network nodes use ARP to maintain information about peer network nodes.

To manage the ARP table:

1. Select **External Port > ARP Cache**. Port is Internal Port, External Port, or Management Port.
2. Click '+' and specify an IP address, a MAC address.
3. Click **Save Changes** to add an entry.
4. You can delete all dynamically discovered entries.

ND Cache - In IPv6 networking, network nodes use the Neighbor Discovery Protocol (NDP) to determine the Layer 2 MAC addresses for neighboring hosts and routers.

To manage the neighbor discovery table:

1. Select **External Port > ND Cache**. Port is Internal Port, External Port, or Management Port.
2. The **Flush NDP Entries** deletes all dynamically discovered entries.

Management Port Configuration

You connect the management port to an Ethernet switch or router that is part of your internal local area network (LAN) and that can connect to your network management infrastructure. When the management port is enabled, the following traffic is directed out the management port: archiving (FTP/SCP), NTP, push config, SNMP, syslog. When the management port is not enabled, that traffic uses the internal port.

To configure the management port:

1. Log in to the Ivanti Neurons for Secure Access portal as a Tenant Admin. See *Logging in to Ivanti Neurons for Secure Access* (page 5).
2. Use the Gateway Switcher and select **Ivanti Connect Secure**.
3. From the Ivanti Connect Secure menu, click the **Gateways** icon, then select **Gateways > Gateways List**.

   The All Gateways page is displayed showing a list of standalone ICS Gateways and Cluster nodes.

4. From the **Standalone ICS Gateways** list, click on the gateway link that you want to configure.
5. On the Ivanti Connect Secure menu, select **System > Network > Management Port > Settings** to display the configuration page.

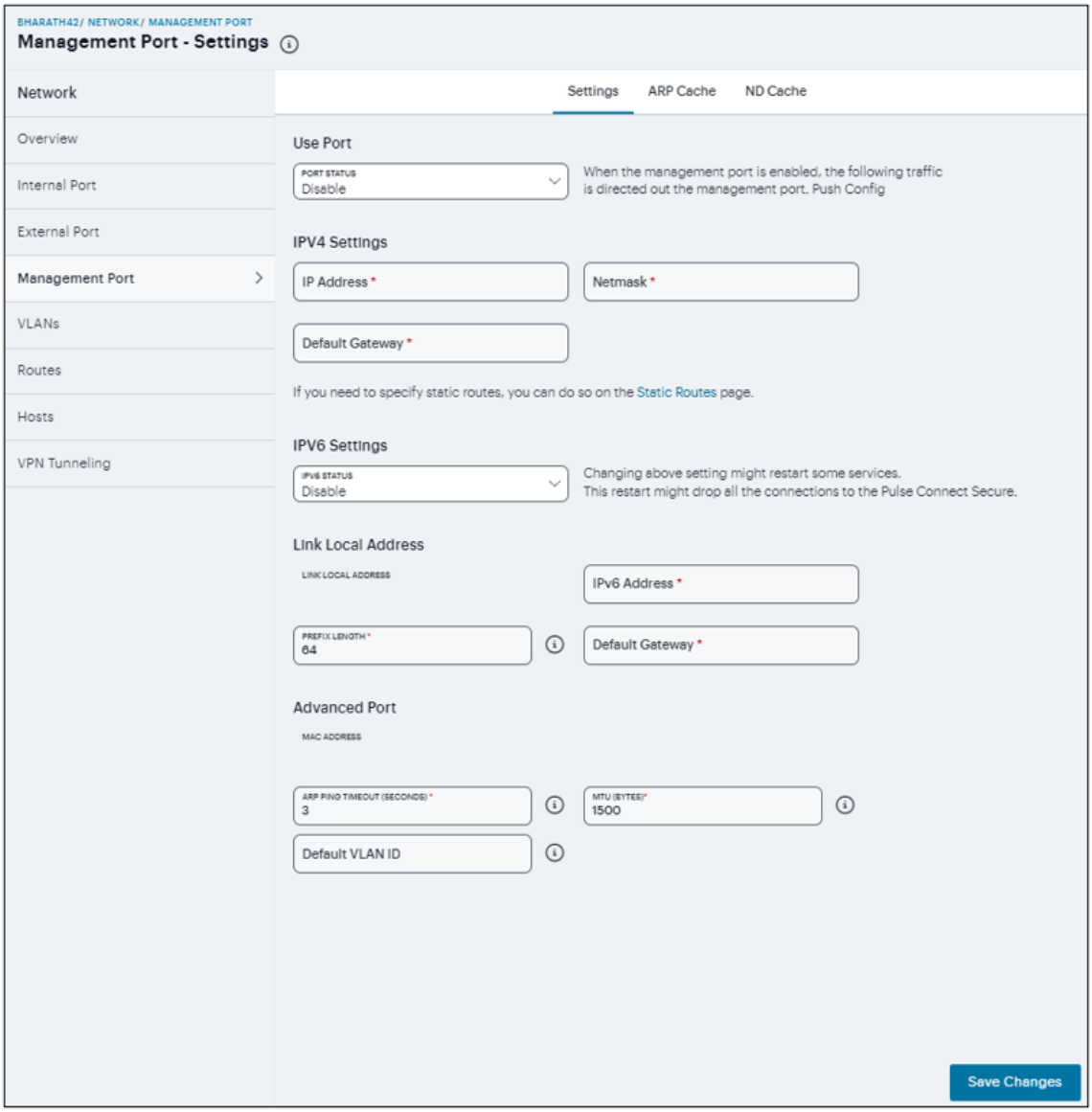


FIGURE 11.3 : Management Port Configuration

6. Enable the **Port Status**.
7. Under IPV4 Settings, Assign an IP address, a Netmask, and specify the IPv4 address for the default Gateway.
8. Under IPV6 Settings, select **IPV6 Status**.
9. Under Link Local Address, you can see the auto-configured link local address. Specify a routable IPv6 address, Prefix Length, and IPv6 address for the default Gateway.

10. Under Advanced Port, specify the ARP Ping Timeout, maximum transmission unit, and default VLAN ID for the traffic of this port.
11. Click **Save Changes**.

ARP Cache - In IPv4 networking, network nodes use ARP to maintain information about peer network nodes.

To manage the ARP table:

1. Select **Management Port > ARP Cache**. Port is Internal Port, External Port, or Management Port.
2. Click '+' and specify an IP address and a MAC address.
3. Click **Save Changes** to add an entry.
4. You can delete all dynamically discovered entries.

ND Cache - In IPv6 networking, network nodes use the Neighbor Discovery Protocol (NDP) to determine the Layer 2 MAC addresses for neighboring hosts and routers.

To manage the neighbor discovery table:

1. Select **Management Port > ND Cache**. Port is Internal Port, External Port, or Management Port.
2. The **Flush NDP Entries** deletes all dynamically discovered entries.

VLAN Ports Configuration

Your network design might include VLANs to provide network segmentation. When connected to a trunk port on a VLAN-enabled switch, the system encounters traffic from all VLANs. This is useful for network designs with separate VLANs for separate classes of users or endpoints, and for making the system accessible from all VLANs. You can use RADIUS attributes to place different users in different network segments.

The system supports IEEE 802.1Q VLAN tagging. You must define a VLAN port for each VLAN. The internal port must be assigned to the root system and must be marked as the default VLAN. Routes to servers reachable from the VLAN interfaces must have the next-hop gateway set to the configured gateway for the VLAN interface, and must have the output port defined as the VLAN port.

When you save the configuration for a new VLAN port, the system creates two static routes by default:

- The default route for the VLAN pointing to the default gateway.
- The interface route to the directly connected network.

To configure an internal VLAN port:

1. Log in to the Ivanti Neurons for Secure Access portal as a Tenant Admin. See *Logging in to Ivanti Neurons for Secure Access* (page 5).
2. Use the Gateway Switcher and select **Ivanti Connect Secure**.

3. From the Ivanti Connect Secure menu, click the **Gateways** icon, then select **Gateways > Gateways List**.

   The All Gateways page is displayed showing a list of standalone ICS Gateways and Cluster nodes.

4. From the **Standalone ICS Gateways** list, click on the gateway link that you want to configure.
5. On the Ivanti Connect Secure menu, select **System > Network > VLANs > Internal Port** to display the configuration page.
6. Select **VLANs > Internal Port**.
7. Click '+', a New VLAN Port -Settings opens.

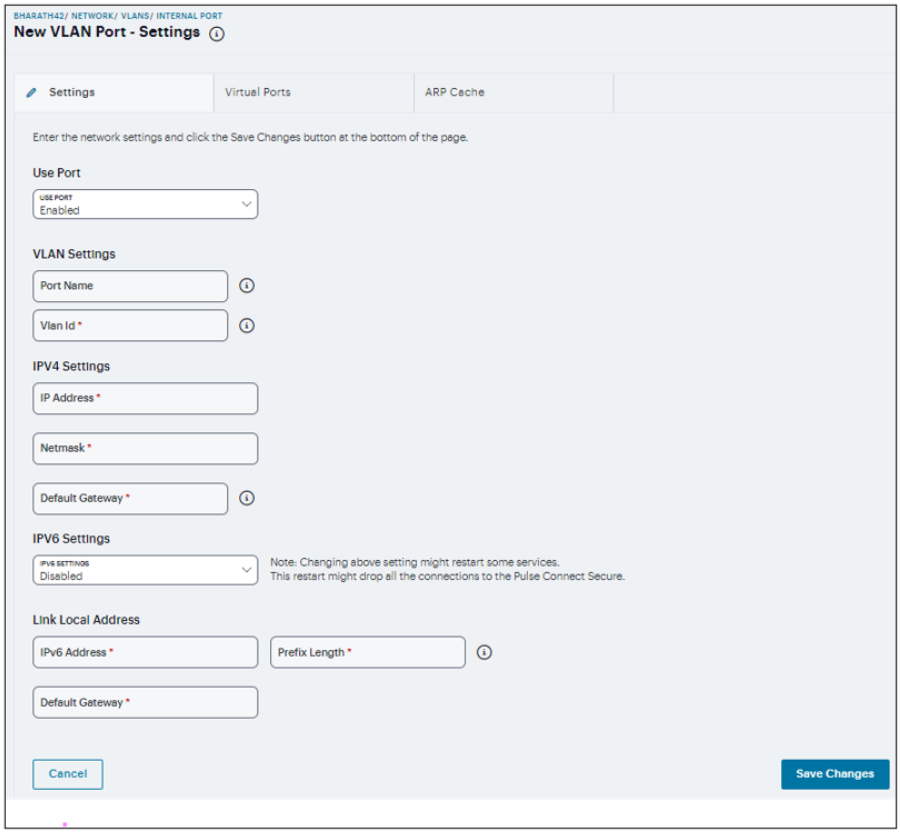


FIGURE 11.4 : VLANS Internal Port Configuration

8. Enable the **Use Port**.
9. Under VLAN Settings, specify a Name that is unique across all VLAN ports and specify a VLAN ID between 1 and 4094.
10. Under IPV4 Settings, assign an IP address, a Netmask, and specify the IPv4 address for the default Gateway.
11. Under IPV6 Settings, select the **IPV6 Status**.
12. Under Link Local Address, specify a Routable IPv6 address, Prefix Length, and IPv6 address for the default Gateway.

13. Click **Save Changes**.

To configure an External VLAN port:

1. Select **VLANs > External Port**.
2. Click '+', a New VLAN Port -Settings opens.

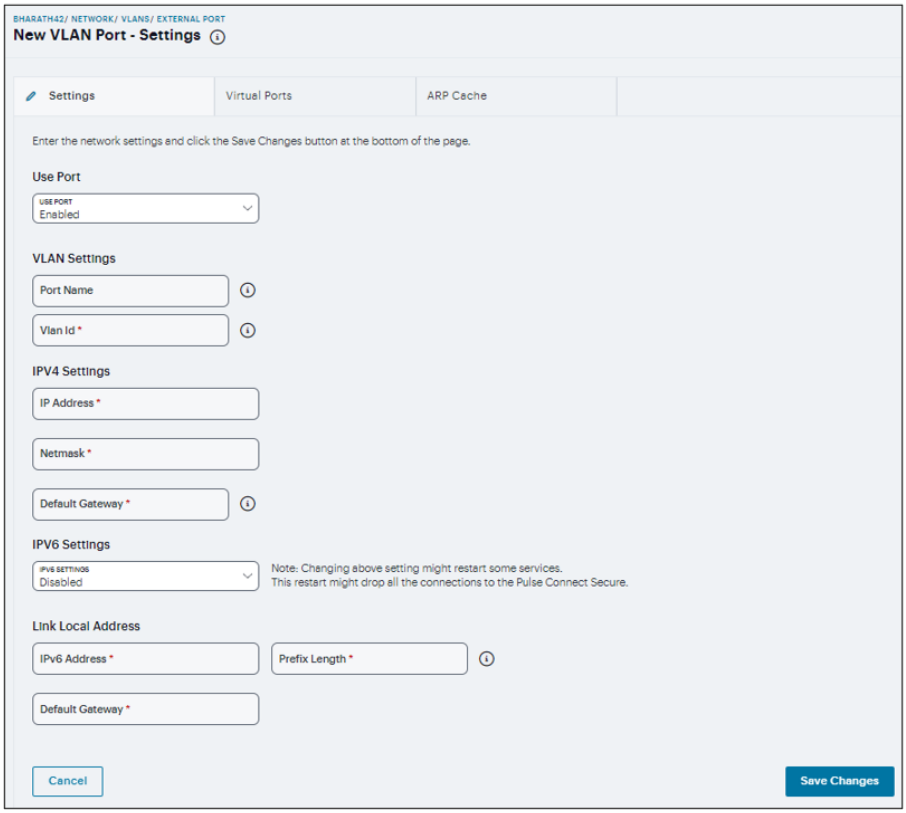


FIGURE 11.5 : VLANS External Port Configuration

3. Enable the **Use Port**.
4. Under VLAN Settings, specify a Name that is unique across all VLAN ports and specify a VLAN ID between 1 and 4094.
5. Under IPV4 Settings, assign an IP address, a Netmask, and specify the IPv4 address for the default Gateway.
6. Under IPV6 Settings, select the **IPV6 Status**.
7. Under Link Local Address, specify a Routable IPv6 address, Prefix Length, and IPv6 address for the default Gateway.
8. Click **Save Changes**.

To configure a Management VLAN port:

1. Select **VLANs > Management Port**.
2. Click '+', a New VLAN Port -Settings opens.

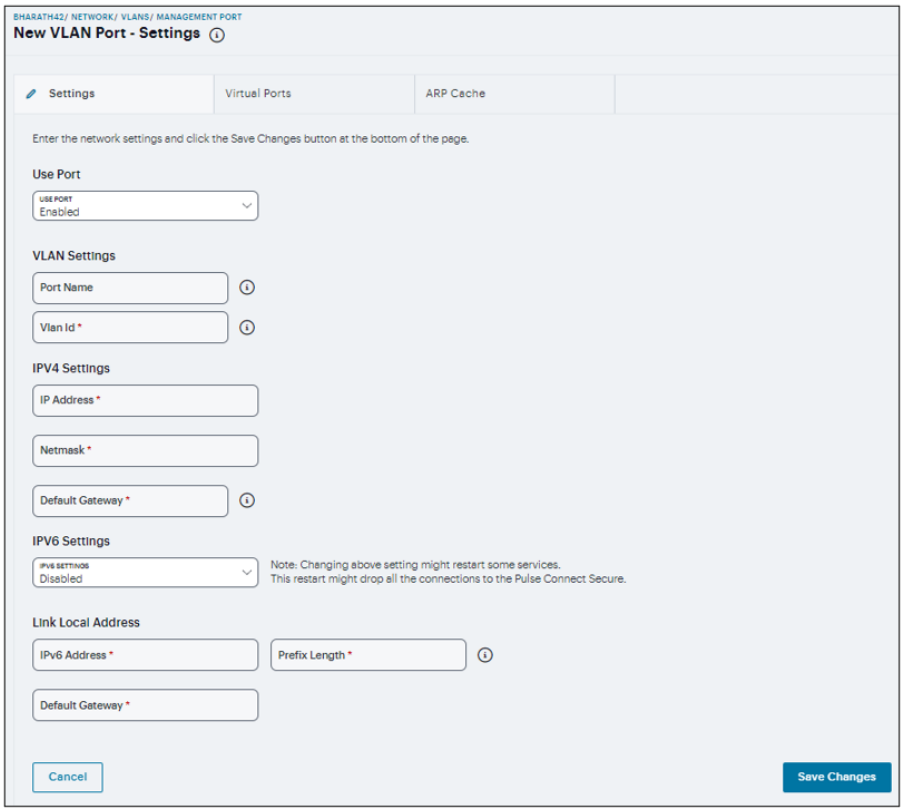


FIGURE 11.6 : VLANS Management Port Configuration

3. Enable the **Use Port**.
4. Under VLAN Settings, specify a **Name** that is unique across all VLAN ports and specify a **VLAN ID** between 1 and 4094.
5. Under IPV4 Settings, assign an IP address, a Netmask, and specify the IPv4 address for the default Gateway.
6. Under IPV6 Settings, select the **IPV6 Status**.
7. Under Link Local Address, specify a Routable IPv6 address, Prefix Length, and IPv6 address for the default Gateway.
8. Click **Save Changes**.

Routes Configuration

The system populates the routes table with dynamic, auto-discovered routes. Many networks will not require changes to this routing table. If necessary, you can delete routes or add static routes.

To manage the routes table:

1. In the Routes page, use the controls to change the display to show the route table for internal, external, or management interfaces; and for IPv4 or IPv6 routes.

2. Click '+' and complete the configuration to add a route to the table.

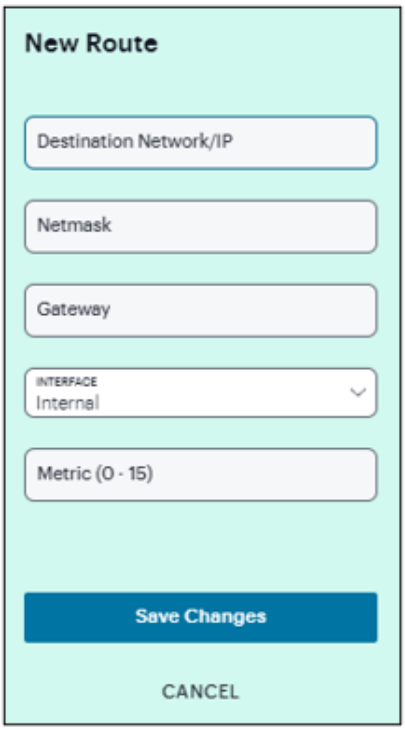


FIGURE 11.7 : Network Routes Configuration

3. Specify a valid IP address, Gateway, DNS address, and select the Interface and metric.
4. Click **Save Changes**.

Hosts Configuration

In general, the system uses the configured DNS servers to resolve hostnames, but it also maintains a local hosts table that can be used for name resolution. The system populates some entries from host-IP address pair settings in your configuration. You can add host-IP address mappings for other hosts that might not be known to the DNS servers used by the system, or in cases where DNS is not reachable.

To configure hosts table:

1. In the Hosts page, click '+'.

FIGURE 11.8 : Network Hosts Configuration

2. Specify an IP address, hostname, and comment (a description for the benefit of system administrators).
3. Click **Save Changes**.

VPN Tunnel Configuration

The VPN tunneling access option (formerly called Network Connect) provides a VPN user experience, serving as an additional remote access mechanism to corporate resources using Connect Secure. The VPN Tunneling Server uses the filter list to assign IP addresses to clients requesting a VPN client session. A filter is an IP address/netmask combination. For example: 10.11.0.0/255.255.0.0 or 10.11.0.0/16.

To add an IP address to the VPN tunneling filter list:

1. In the VPN tunneling page, click +, and enter an IP address/netmask combination.

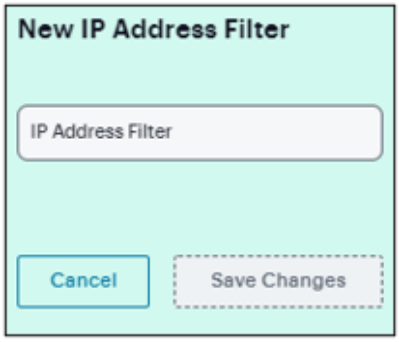


FIGURE 11.9 : Specifying IP Address Filter

2. In the **VPN Tunnel Server IP Address** text box, enter the base IP address used by the VPN tunneling server to assign IP addresses to the tunnel interfaces created for VPN Tunneling sessions.
3. Click **Save Changes**.

Note: Only change the VPN tunneling server base IP address when instructed to do so by the Ivanti Support team.

Authentication and Directory Servers

Introduction

The access management framework supports the following types of AAA servers: Local, External (standards-based), and External (other).

- Local includes “Local Authentication Server”, “Certificate Server”.
- External (standards-based) includes “LDAP Server”, “RADIUS Server”.
- External (other) includes “MDM Server”, “RSA ACE Server”, “TOTP Server”.

Configuring Authentication Servers

To add an authentication server:

1. Log into the nSA as a Tenant Admin.
2. From the ICS menu, click **Gateways > Gateways List**. In the Gateways list page, select the standalone ICS Gateway or Cluster node that you want to configure.
3. From the ICS menu, click **Authentication > Authentication Servers**.
4. Click the Add icon and select the Authentication server type from the list.

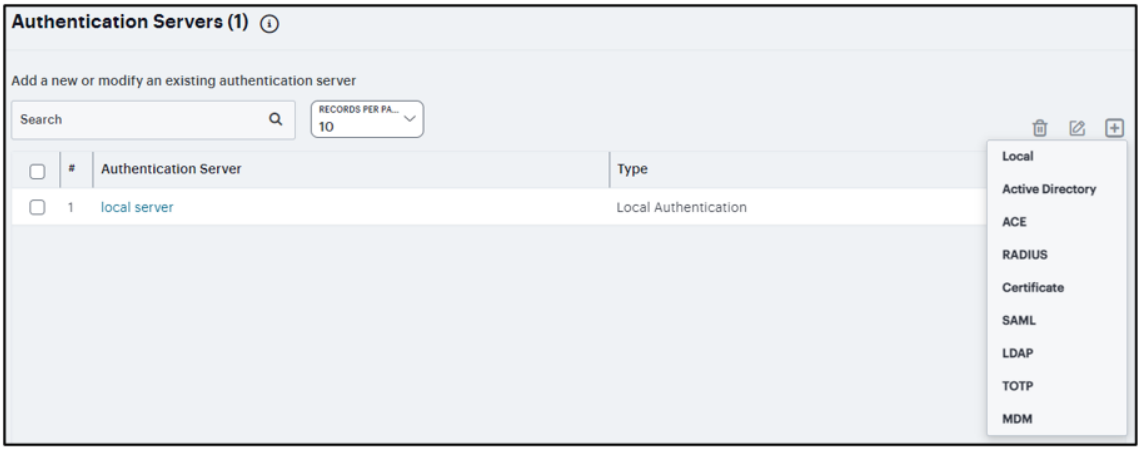


FIGURE 12.1 : Configuring Authentication Servers

Configuring Local Authentication Server

You can create multiple local authentication server instances. When you define a new local authentication server, you must give the server a unique name and configure options for passwords.

To create a local authentication server:

1. Select **Authentication > Authentication Servers**.
2. Click the Add icon and select **Local** from the list to display the configuration page.
3. Complete the configuration and save changes.
    - Enter a Server Name.
    - Select **Password Options**.
    - Select the **Allow users to change passwords** option if you want users to be able to change their passwords.
    - Select the **Force password change after** option to specify the number of days after which a password expires. The default is 64 days.

- Select the **Prompt users to change password** option to specify when to prompt the user to change passwords.
- Select the **Enable account lockout for users** option to manage user authentication failures for admin users of local authentication server.
- Enter the number of consecutive wrong password attempts after which the admin user account will be locked. The default value is 3 retries.
- Enter the time in minutes for which admin user account will remain locked. The default value is 10 minutes.

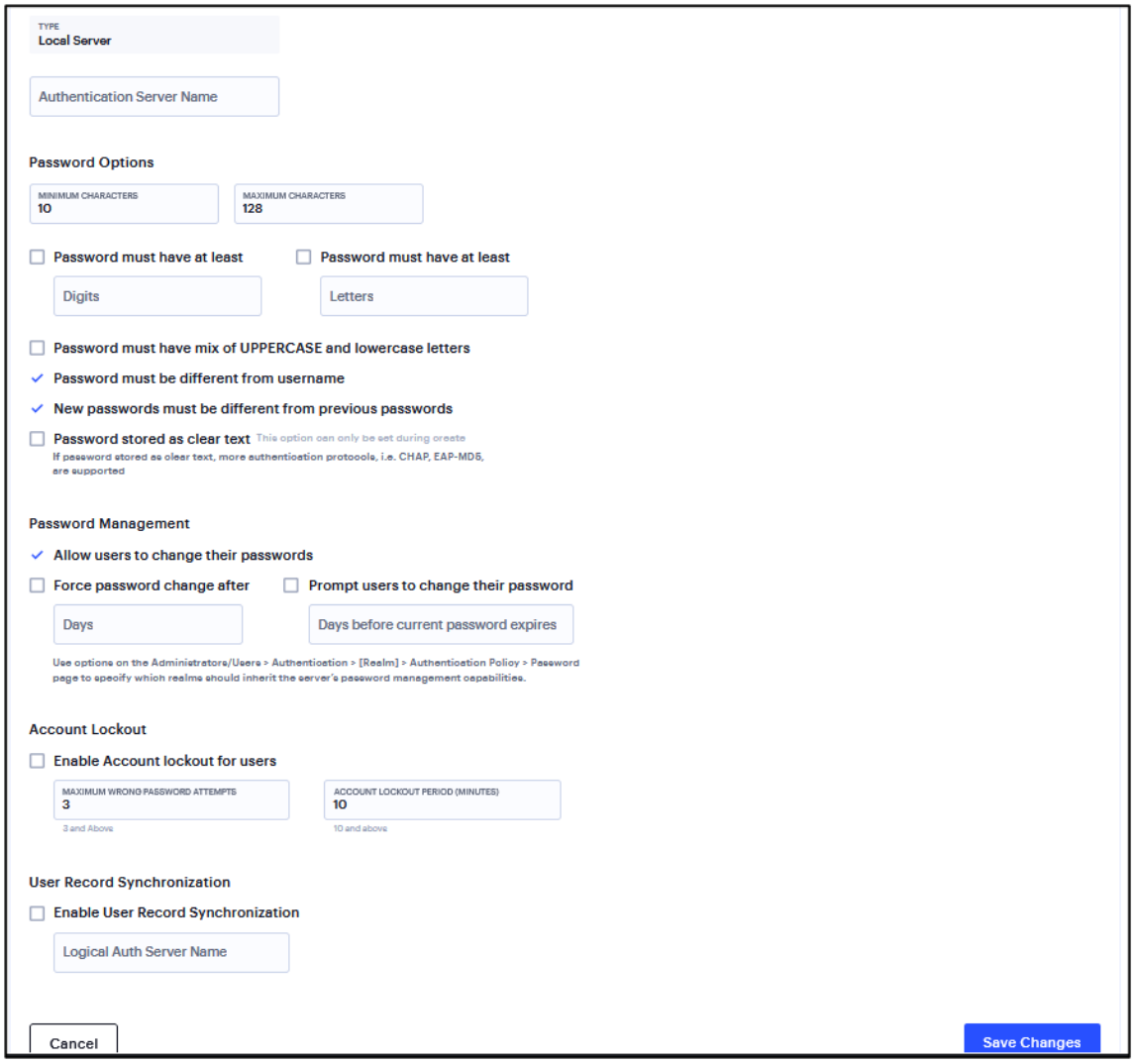


FIGURE 12.2 : Local Authentication Server

Configuring ACE Authentication Server

RSA Authentication Manager (formerly known as ACE/Server) is an authentication and authorization server that allows user authentication based on credentials from the RSA SecurID® product from RSA Security Inc.

To configure authentication with the ACE server:

1. Select **Authentication > Authentication Servers**.
2. Click the Add icon and select **ACE** from the list to display the configuration page.
3. Complete the configuration and save changes.
    - Enter a Server Name.
    - Enter the default port of the authentication server.
    - Click and browse **Import New Config File** to upload the sdconf.rec configuration file.
    - Select the **Enable User Record Synchronization** option to retain the bookmarks and individual preferences regardless of which system you log in to.
    - Enter a logical authentication server name.

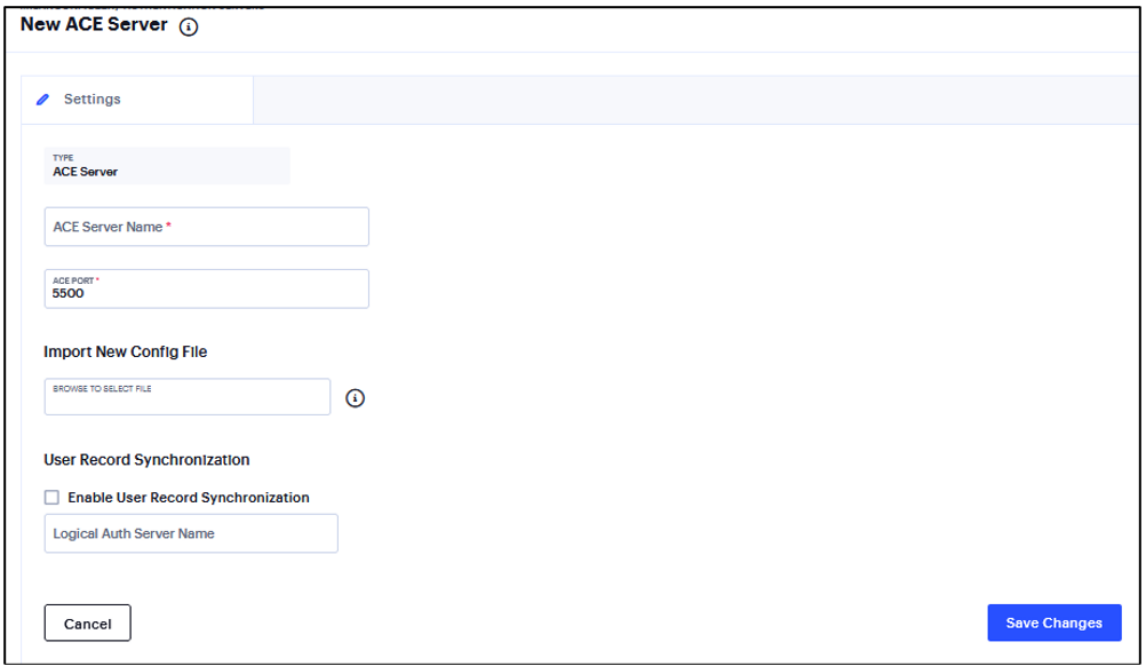


FIGURE 12.3 : ACE Authentication Server

Configuring RADIUS Authentication Server

To configure authentication with the RADIUS server:

1. Select **Authentication > Authentication Servers**.
2. Click the Add icon and select **RADIUS** from the list to display the configuration page.
3. Complete the configuration and save changes.

   Settings page

   - Enter a Server Name.
   - Enter the name that identifies the Network Access Server (NAS) client to the RADIUS server.
   - Enter the name or IP address of the RADIUS server.
   - Enter the authentication port value for the RADIUS server. Default port number: 1812, 1645 (legacy servers).
   - Enter the NAS IP address. If you leave this field empty, the internal IP address is passed to RADIUS requests. You can also fill this field with IPv6 address.
   - Enter the interval of time in seconds to wait for a response from the RADIUS server before timing out the connection.
   - Enter the number of times to try to make a connection after the first attempt fails.
   - Select the **Users authenticate using tokens or one-time passwords** option to prompt the user for a token instead of a password.
   - Click **Next**.

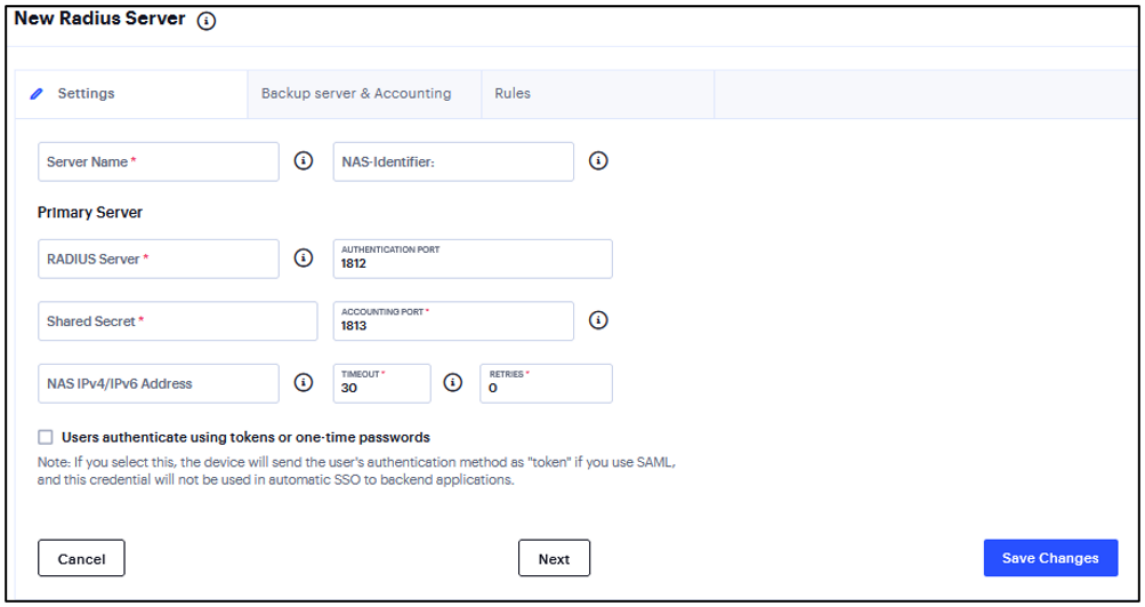


FIGURE 12.4 : RADIUS Authentication Server

Backup server & Accounting page (required only if Backup server exists)

- Enter the secondary RADIUS server.
- Enter the Authentication Port.
- Enter the Shared Secret.
- Enter the Accounting Port.
- Enter the user information to the RADIUS accounting server.
- Enter **Interim Update Interval** in minutes to achieve more precise billing for long-lived session clients and during network failure.
- Select the **Use VPN Tunnel assigned IP Address for FRAMED-IP-ADDRESS/FRAMED-IPV6-ADDRESS attribute value in RADIUS Accounting** option to use the VPN Tunneling IP address for the FRAMED-IP-ADDRESS/FRAMED-IPV6-ADDRESS attribute instead of the pre-authenticated (original) IP address. Framed IPv6 addresses based attribute fetching and parsing:
  - NAS-IPv6-Address
  - Login-IPv6-Host
- Enable the **Send Interim Updates for sub sessions created inside parent sessions** check box to send interim updates for sub sessions (child sessions) created inside parent sessions.
- Click **Next**.

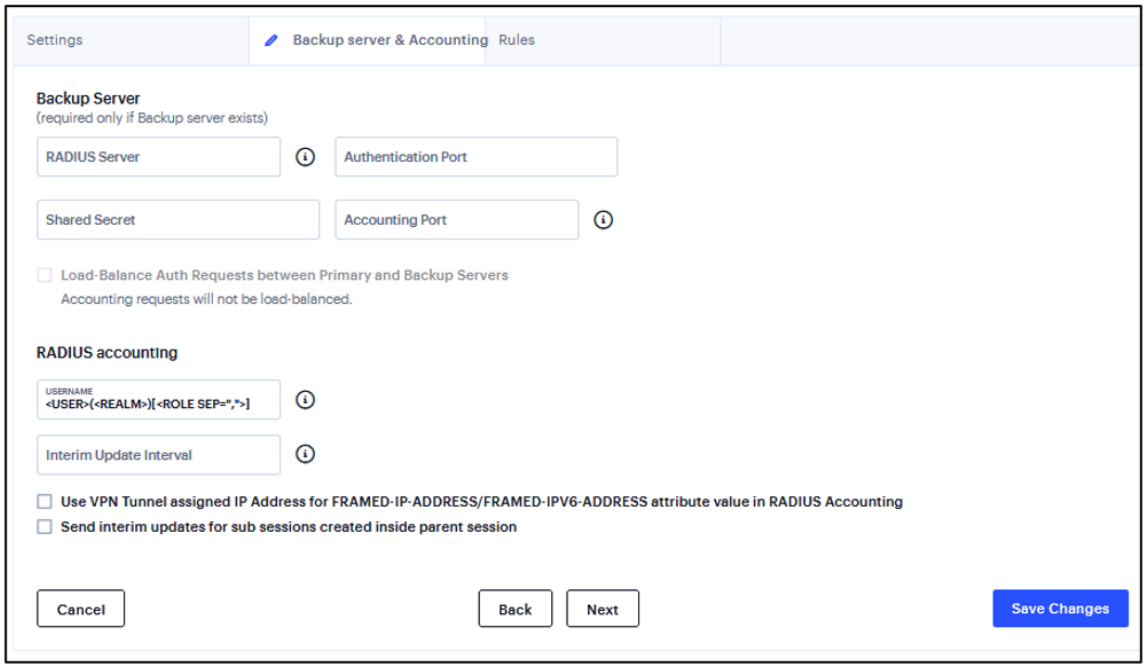


FIGURE 12.5 : RADIUS Authentication Server

Rules page

- Select the **Enable processing of Radius Disconnect Requests** check box. The Radius Disconnect requests received from the backend Radius server will terminate sessions that match the attributes in the request.
- Select the **Enable User Record Synchronization** option to retain the bookmarks and individual preferences regardless of which system you log in to.
- Enter a logical authentication server name.

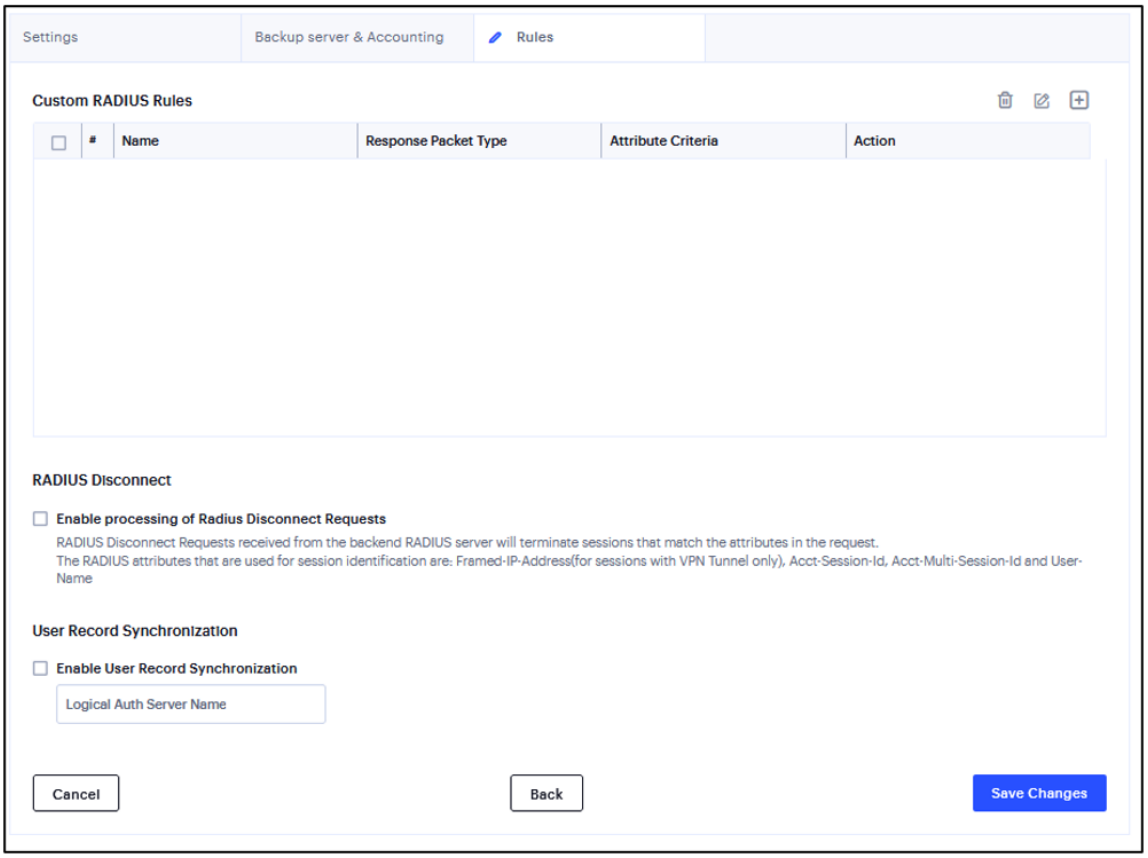


FIGURE 12.6 : RADIUS Authentication Server

Configuring Certificate Authentication Server

The certificate server is a local server that allows user authentication based on the digital certificate presented by the user without any other user credentials.

To configure authentication with the Certificate server:

1. Select **Authentication > Authentication Servers**.
2. Click the Add icon and select **Certificate** from the list to display the configuration page.
3. Complete the configuration and save changes.
    - Enter a Server Name.

- Enter a username template. Specify how the system should construct a username. You may use any combination of certificate variables contained in angle brackets and plain text.
- Select the **Enable User Record Synchronization** option to retain the bookmarks and individual preferences regardless of which system you log in to.
- Enter a logical authentication server name.

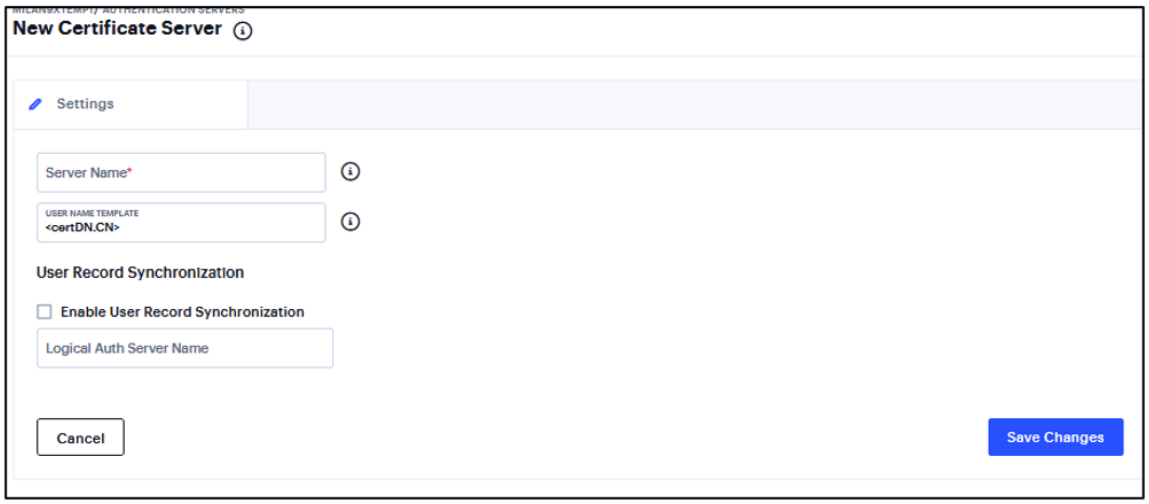


FIGURE 12.7 : Certificate Authentication Server

Configuring LDAP Authentication Server

Lightweight Directory Access Protocol (LDAP) facilitates the access of online directory services. LDAP directory consists of a collection of attributes with a name, known as a distinguished name (DN). Each of the entry's attributes, known as a relative distinguished name (RDN), has a type and one or more values. The types are typically mnemonic strings, such as CN for common name. The valid values for each field depend on the types.

To configure authentication with the LDAP server:

1. Select **Authentication > Authentication Servers**.
2. Click the Add icon and select **LDAP** from the list to display the configuration page.
3. Complete the configuration and save changes.

   Settings page

   - Enter a Server Name.
   - Select the **Enable Domain Name** option if you want to fetch a list of servers from the DNS server. Clear this option if you want to manually enter all the domain controllers host names.
   - Enter the LDAP server name or the IP address.

- (Optional) Enter the parameters for backup LDAP server1. Default port number: 389
- Enter the parameters for backup LDAP port1.
- (Optional) Specify the parameters for backup LDAP server2.
- Enter the parameters for backup LDAP port2.
- Select the backend LDAP server type from the following choices: Generic, Active Directory, iPlanet, Novell eDirectory.
- Select one of the following options for the connection to the LDAP server:
  - Unencrypted - The device sends the username and password to the LDAP Directory Service in cleartext.
  - LDAPS - The device encrypts the data in the LDAP authentication session using the Secure Socket Layer (SSL) protocol before sending it to the LDAP Directory Service.
  - Start TLS - The device allows both secure and plain requests against an LDAP server on a single connection.
- Enter the time (in seconds) to wait for connection to the primary LDAP server, and then to each backup LDAP server. Default: 15 seconds
- Enter the time (in seconds) to wait for search results from a connected LDAP server.

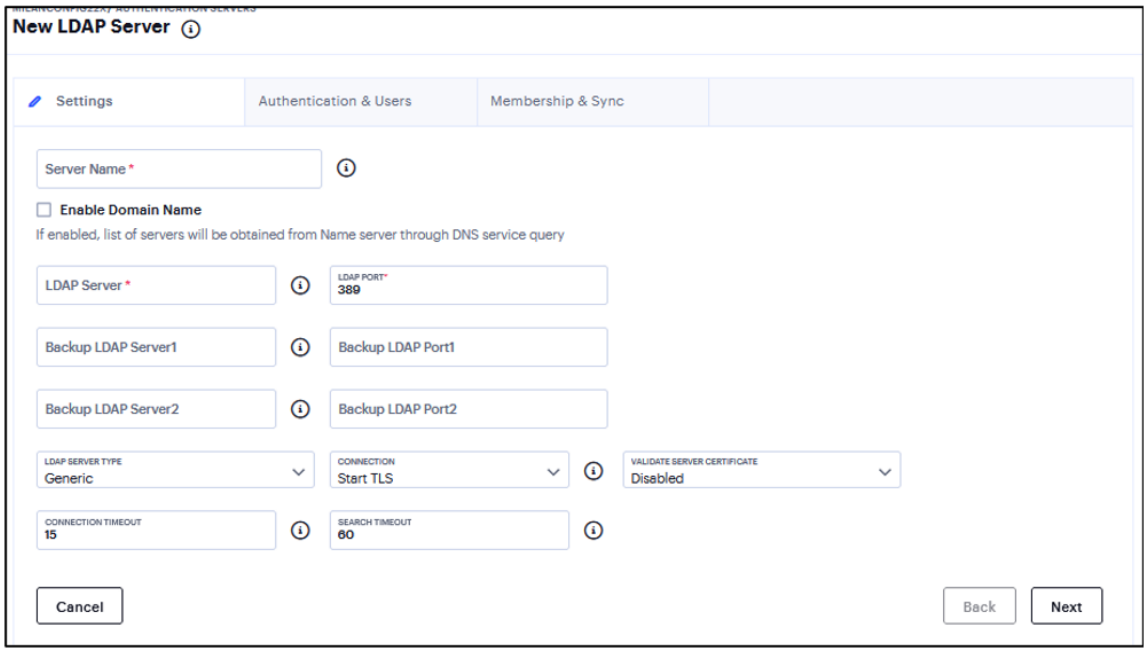


FIGURE 12.8 : LDAP Authentication Server

- Click **Next**.

Authentication & Users page

- Select the **Authentication required to search LDAP** option to require authentication when performing search or password management operations.
- Enter the administrator DN for queries to the LDAP directory.
- Enter the password for the LDAP server.
- Enter the backup administrator DN for queries to the LDAP directory, as a fallback when primary Admin DN fails (due to account expiration).
- Enter the backup administrator password for the LDAP server.

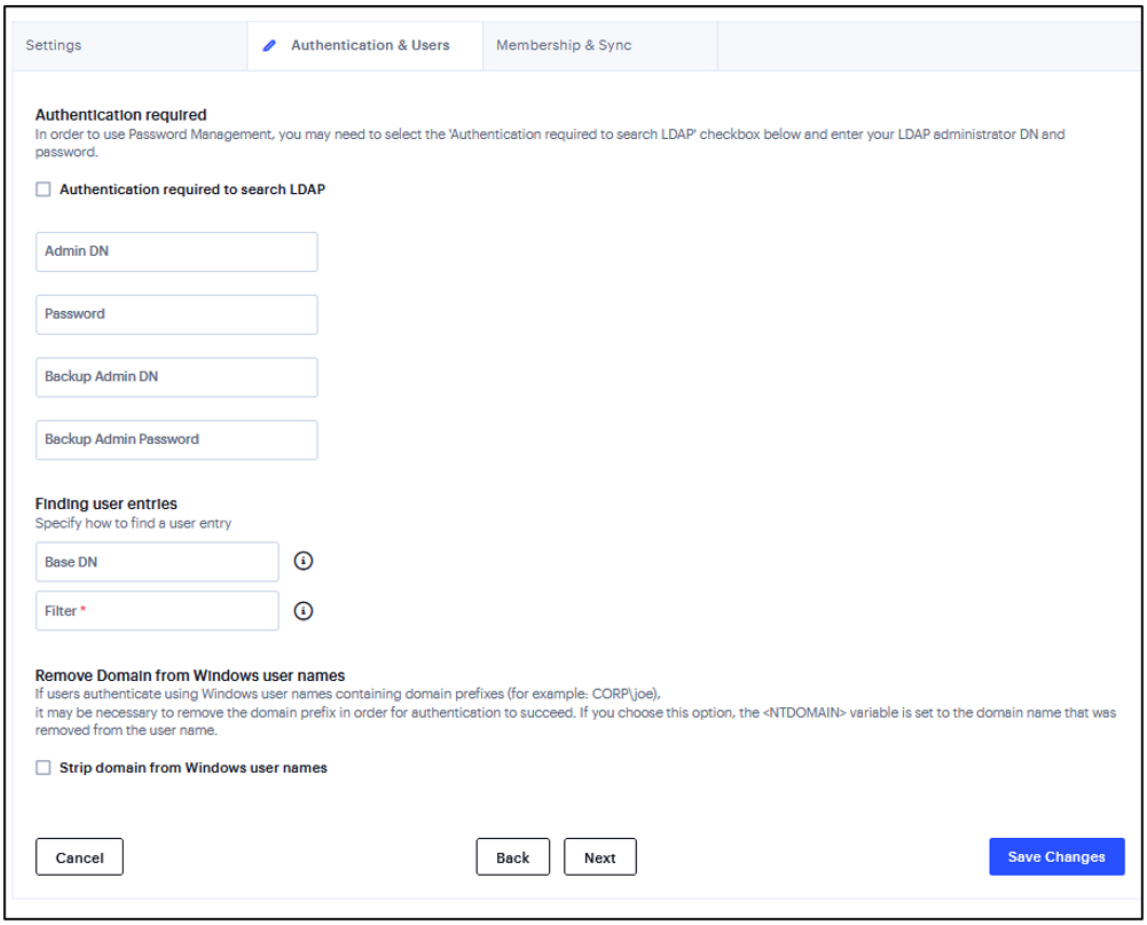


FIGURE 12.9 : Finding user entries

- Under **Finding user entries**:
  - Enter the base DN under which the users are located. For example, dc=sales,dc=acme, dc=com.
  - Enter a unique variable that can be used to do a fine search in the tree. For example, samAccountname=<username> or cn=<username>.
  - Select the **Strip domain from Windows username** option to pass the username without the domain name to the LDAP server.
- Click **Next**.

Membership & Sync page

- Enter the base DN to search for user groups.
- Enter a unique variable which can be used to do a fine search in the tree. For example, samAccountname=<username> or cn=<GROUPNAME>.
- Enter all the members of a static group. For example, member or uniquemember (iPlanet specific Deprecated for 21.x).
- Select the **Reverse group search** option to start the search from the member instead of the group. This option is available only for Active Directory server types.
- Enter an LDAP query that returns the members of a dynamic group. For example, memberURL.
- Enter how many levels within a group to search for the user. The higher the number, the longer the query time, so we recommend that you specify to perform the search no more than two levels deep.
- Select one of the following options: Nested groups in Server Catalog, Search all nested groups.

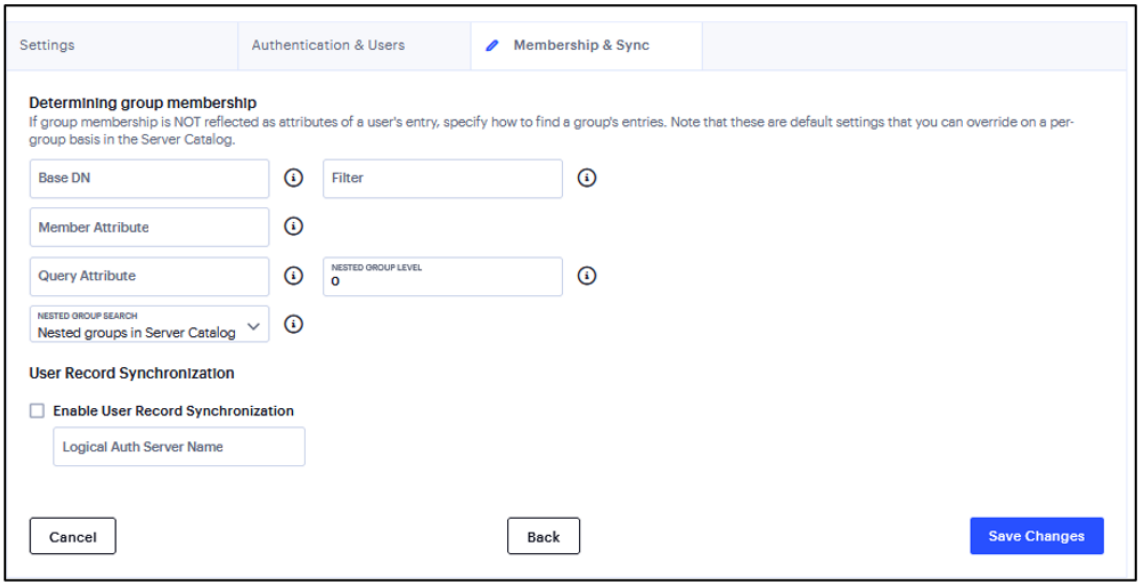


FIGURE 12.10 : Determining group membership

Configuring SAML Authentication Server

SAML is an XML-based framework for communicating user authentication, entitlement, and attribute information. The standard defines the XML-based assertions, protocols, bindings, and profiles used in communication between SAML entities. SAML is used primarily to implement Web browser single sign-on (SSO). SAML enables businesses to leverage an identity-based security system like Ivanti Connect Secure to enforce secure access to web sites and other resources without prompting the user with more than one authentication challenge.

For complete details on the SAML standard, see the OASIS web site:

To configure authentication with the SAML server:

1. Select **Authentication > Authentication Servers**.
2. Click the Add icon and select **SAML** from the list to display the configuration page.
3. Complete the configuration and save changes.

   Settings

   - Enter a name to identify the server instance.
   - Select SAML version used by the SAML IdP.
   - Select to override the Host FQDN for the SAML server. Host FQDN is used to update the Unique SAML Identifier and ACS URL of the SAML Authentication Server.
   - Select Manual or Metadata for Configuration Mode. If a metadata file or location is available from the SAML identity provider, use the metadata option to make configuration simpler and less prone to error.
   - Enter **Identity Provider Entity ID**. The identity provider entity ID is sent as the Issuer value in the assertion generated by the SAML identity provider.
   - Enter **Identity Provider Single Sign On Service URL**. The identity provider SSO service URL is a URL provisioned by the SAML identity provider. The setting is required to support service-provider-initiated SSO.
   - Specify **User Name Template** to derive the username from the assertion.
   - Specify the maximum allowed difference in time between the system clock and the SAML identity provider server clock.
   - Select **Support Single Logout**. Single logout is a mechanism provided by SAML for logging out a particular user from all the sessions created by the identity provider. Select this option if the system must receive and send a single logout request for the peer SAML identity provider.

- Click **Save Changes**. The SAML Authentication Server gets listed in the Authentication Servers page.

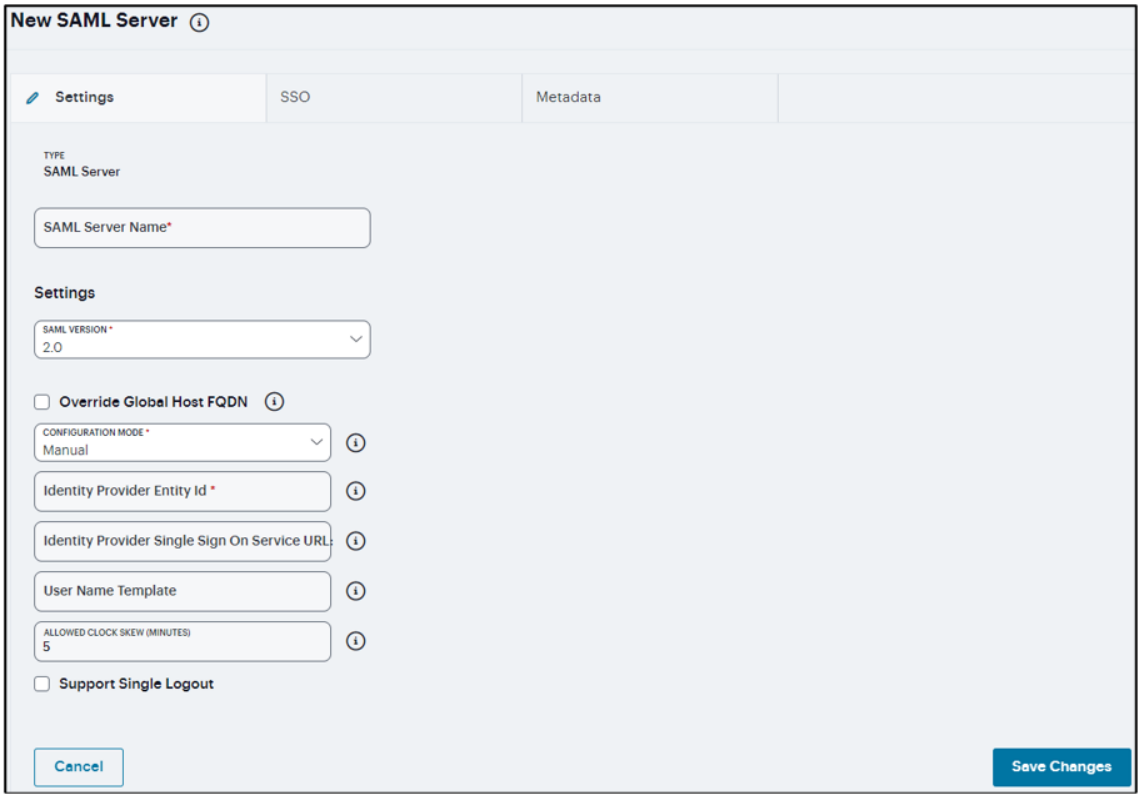


FIGURE 12.11 : SAML Authentication Server Settings

SSO

- Select the **SSO** tab.
- Select **Artifact** to use the Artifact binding. The system then contacts the Artifact Resolution Service (ARS) to fetch the assertion using SOAP protocol. If the ARS is hosted on a HTTPS URL, then the certificate presented by the ARS is verified by the system.
- Select **POST** to use the POST binding, the system uses a response signing certificate to verify the signature in the incoming response or assertion. The certificate file must be in PEM or DER format. The certificate you select should be the same certificate used by the identity provider to sign SAML responses.
- Use the **Add** and **Remove** buttons to select authentication context classes to be sent in the authentication requests to the SAML identity provider. These are included in the RequestedAuthnContext element.
- Click **Save Changes**.

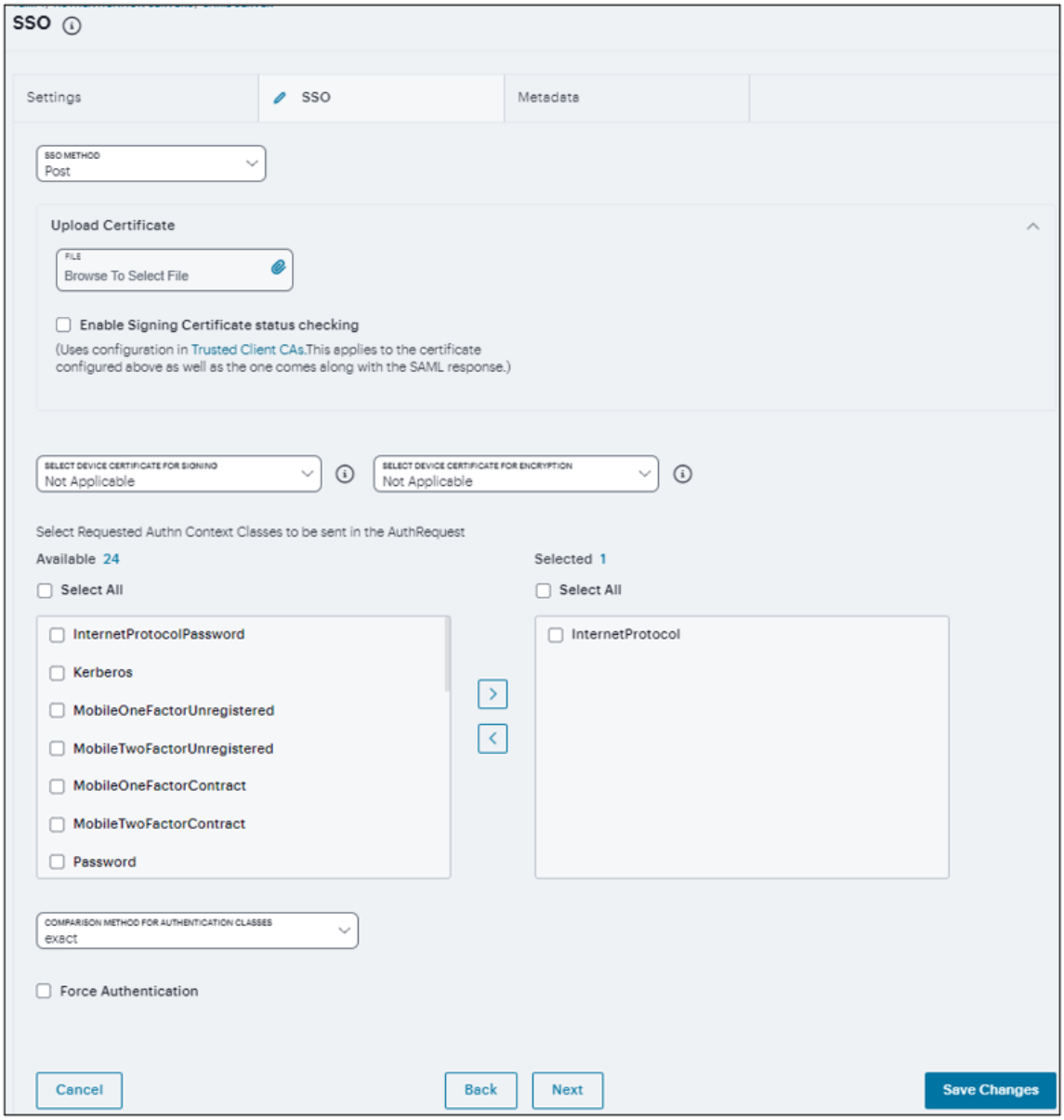


FIGURE 12.12 : SSO Settings

Metadata Settings

- Select the **Metadata** tab.
- Enter the number of days the metadata is valid. Valid values are 0 to 9999. 0 specifies the metadata does not expire.
- Select **Do Not Publish SA Metadata** if you do not want to publish the metadata at the location specified by the **Entity ID** field.
- Select **Download Metadata**. This button appears only after you have saved the authentication server configuration. Use this button to download the metadata of the current SAML service provider.
- Click **Save Changes**.

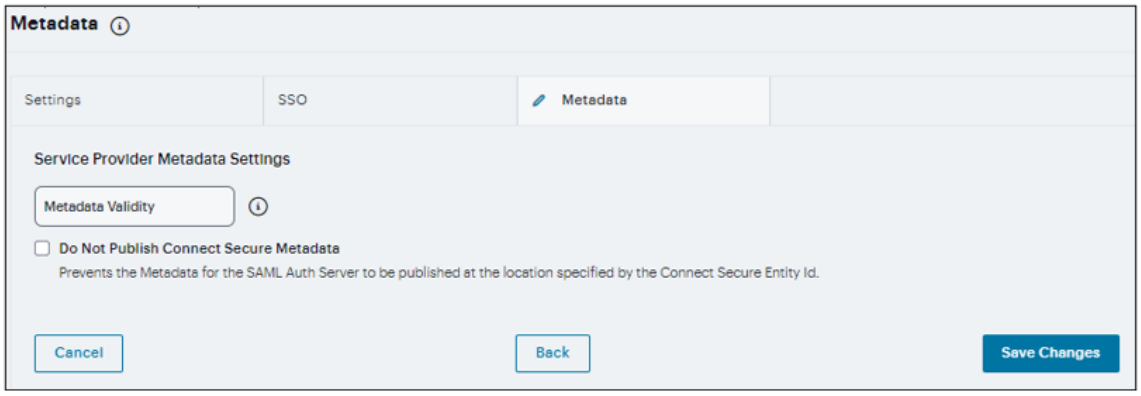


FIGURE 12.13 : Metadata Settings

Configuring TOTP Authentication Server

Time-based One-Time Password (TOTP) algorithm as defined in RFC6238 is an authentication mechanism where a one-time password (a.k.a token) is generated by the authentication server and client from a shared secret key and the current time. ICS can act as TOTP authentication server. Any third-party TOTP applications (for example, Windows Authenticator or Google Authenticator) available on the mobile and desktop client platforms generate TOTP tokens.

To configure the TOTP server as Local:

1. Select **Authentication > Authentication Servers**.
2. Click the Add icon and select **TOTP** from the list to display the configuration page.
3. Complete the configuration and save changes.

   TOTP Auth Server Settings - Local

   - Select **Local** as Server Type. TOTP context is created locally and user database is maintained locally on the same device.
   - Time Skew - Specify maximum time difference between Ivanti Connect Secure and end user device while authenticating a user's token. (minimum: 1 minute, maximum: 5 minutes).
   - Number of attempts allowed - Specify maximum number of consecutive wrong attempts allowed after which account will be locked (minimum: 1 attempt, maximum: 5 attempts).
   - Custom message for registration page - Specify a custom message which can be shown on new TOTP user registration web-page.
   - Allow Auto Unlock - When checked, locked account will be automatically unlocked after specified period. (minimum: 10 minutes, maximum: 90 days).
   - Allow new TOTP user registration to happen via external port - When unchecked (default), new TOTP user registrations will happen only via internal port.

- Accept TOTP authentication from remote ICS devices - When checked, REST access to this TOTP server is allowed from other Ivanti Connect Secure devices.
- Display QR code during user registration - When checked, displays QR code during user registration.
- Disable generation of backup codes - When unchecked, generates backup codes.

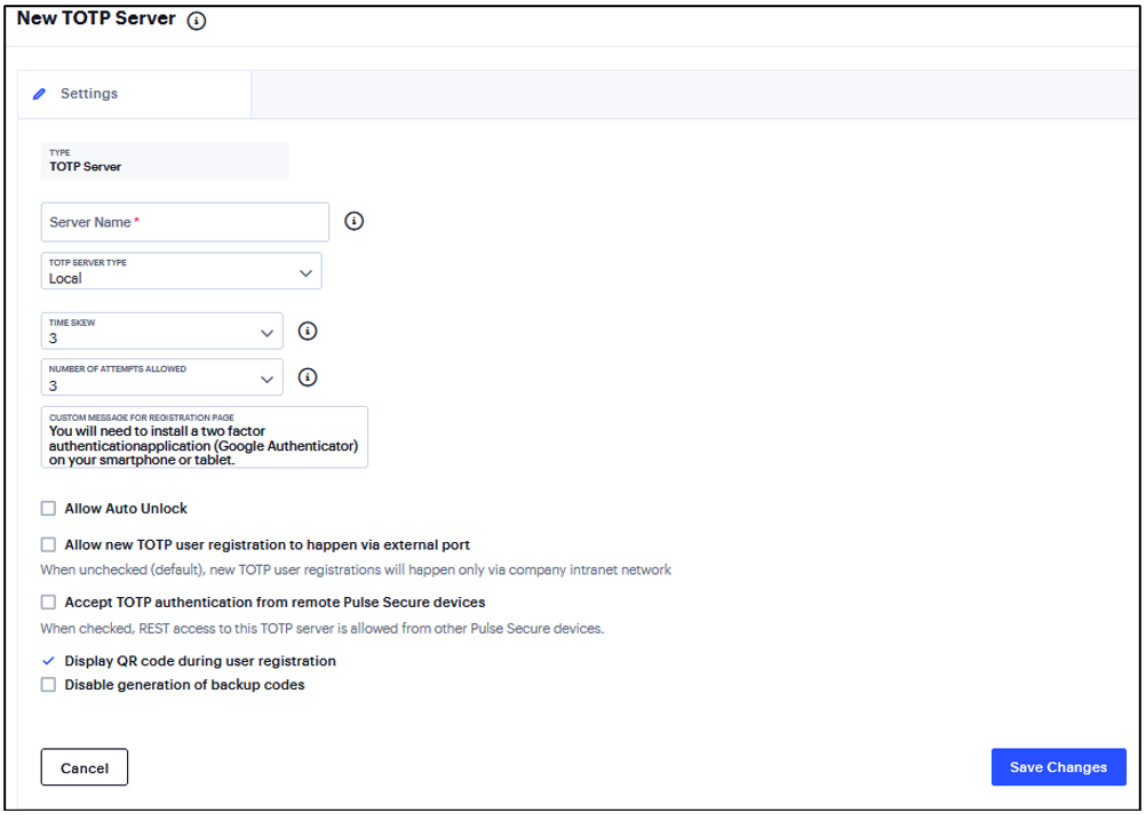


FIGURE 12.14 : TOTP Authentication Server

TOTP Auth Server Settings - Remote

- Select **Remote** as Server Type. In this configuration, authentication checks take place on the remote TOTP server.
- If the **Allow new TOTP user registration to happen via external port** option is not selected, new TOTP user registrations happen only via company intranet network.
- Enter remote host name or IP address where the TOTP server is configured. The IP address or host name must match the common name mentioned in the remote TOTP server certificate.
- Enter TOTP Server Name configured on the Remote TOTP server.
- Enter the REST API login name.
- Enter the REST API password.

- Enter the realm name, which refers to the realm that should be used for authenticating the REST user (using the auth. server mapped to the Realm).
- Use the Test Connection button to validate the connection to the remote TOTP server.

Configuring MDM Authentication Server

The access management framework MDM authentication server configuration includes details on how the system communicates with the MDM Web RESTful API service and how it derives the device identifier from the certificates presented by endpoints.

To configure authentication with the MDM server:

1. Select **Authentication > Authentication Servers**.
2. Click the Add icon and select **MDM** from the list to display the configuration page.
3. Complete the configuration and save changes.
   - Type - Select one of the following options: AirWatch, MobileIron, Microsoft Intune

   Applicable to AirWatch and MobileIron

   - Enter the URL for the MDM server. This is the URL the MDM has instructed you to use to access its RESTful Web API (also called a RESTful Web service).
   - Enter the URL for the MDM report viewer. This URL is used for links from the Active Users page to the MDM report viewer.
   - Enter a timeout period (5-60 seconds) for queries to the MDM server. The default is 15 seconds.
   - Enter the username and password for an account that has privileges to access the MDM RESTful Web API.
   - (AirWatch only) Copy and paste the AirWatch API tenant code.

   Applicable to Microsoft Intune

   - Enter Azure AD Tenant ID.
   - Enter Web application ID that has been registered in Azure AD.
   - Enter Secret key of the web application registered in azure AD.
   - Enter a timeout period (5-60 seconds) for queries to the MDM server. The default is 15 seconds.

   Device Identifier

   - Construct a template to derive the device identifier from the certificate attributes. The template can contain textual characters as well as variables for substitution.

- Select the device identifier type that matches the selection in the MDM SCEP certificate configuration:
  - UUID - The device Universal Unique Identifier. This is the key device identifier supported by MobileIron MDM.
  - Serial Number - The device serial number.
  - UDID - The device Unique Device Identifier. This is the key device identifier supported by AirWatch MDM.
  - IMEI - The device unique identifier. IMEI (15 decimal digits: 14 digits plus a check digit) or IMEISV (16 digits) includes information on the origin, model, and serial number of the device. This is the key device identifier supported by Microsoft Intune.

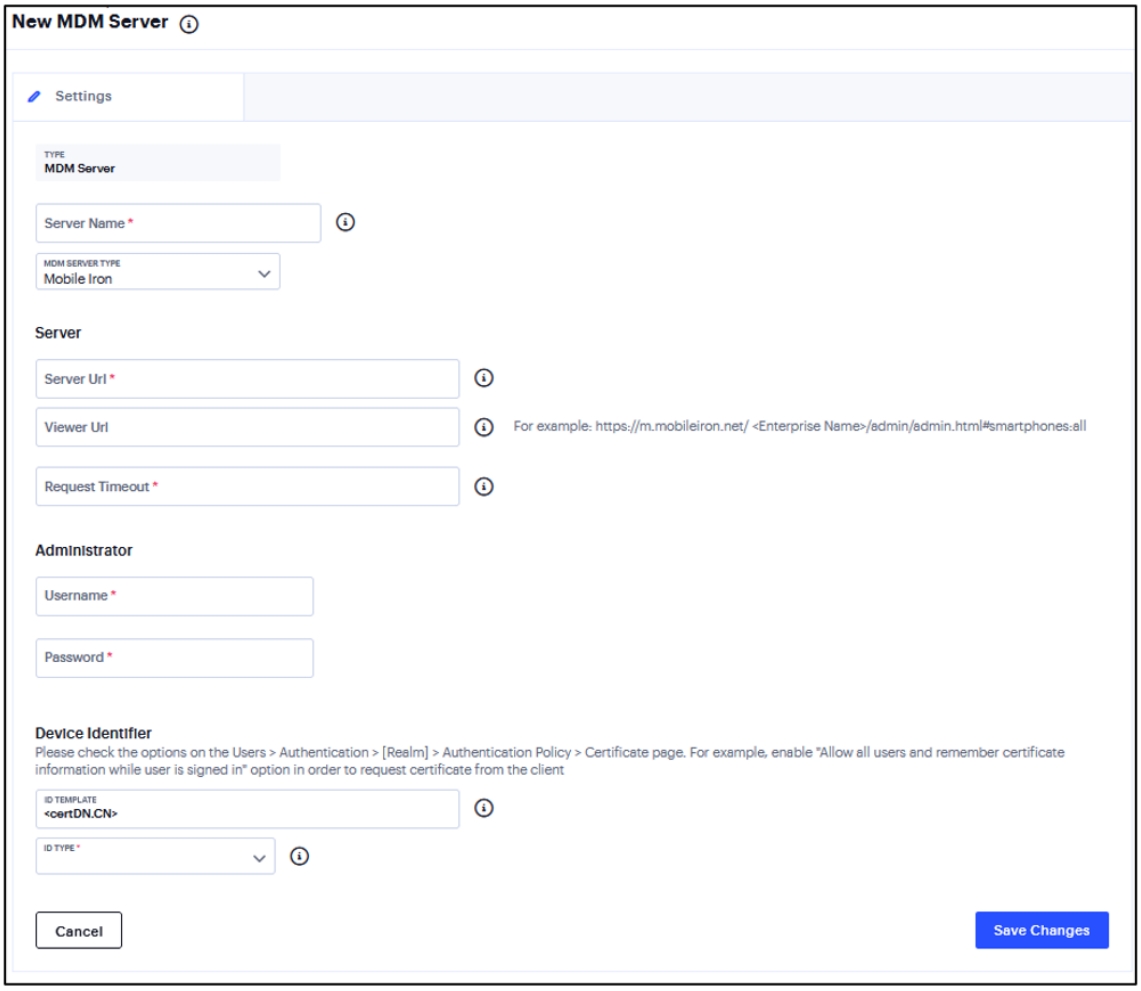


FIGURE 12.15 : MDM Authentication Server

Configuring Active Directory Authentication Server

Active Directory is a directory service used in Windows domain networks. It is included in most Windows server operating systems. Enterprise servers that run Active Directory are called domain controllers. An Active Directory domain controller authenticates and authorizes users and computers in a Windows domain network.

When you use Active Directory as the authentication and authorization service for your Ivanti access management framework, users can sign in to Ivanti Connect Secure using the same username and password they use to access their Windows desktops. You can also use Active Directory group information in role mapping rules.

To configure authentication with the MDM server:

1. Select **Authentication > Authentication Servers**.
2. Click the Add icon and select **Active Directory** from the list to display the configuration page.
3. Complete the configuration and save changes.

- Specify a name to identify the server within the system.
- Specify the NetBIOS domain name for the Active Directory domain.
- Specify the FQDN of the Active Directory domain.
- Specify a username that has permission to join computers to the Active Directory domain.
- Specify the password for the special user.
- Select **Save Credentials**. If this setting is not enabled, the credentials entered will be destroyed after successfully joining the domain.
- Specify the machine account name. The default computer name is derived from the license hardware in the following format: 0161MT2L00K2C0. We recommend the Computer Name string contain no more than 14 characters to avoid potential issues with the AD/NT server. Do not include the '$' character.
- Specify the protocol to use during authentication. The system attempts authentication using the protocols you have enabled in the order shown on the configuration page. For example, if you have selected the check boxes for Kerberos and NTLMv2, the system sends the credentials to Kerberos. If Kerberos succeeds, the system does not send the credentials to NTLMv2. If Kerberos is not supported or fails, the system uses NTLMv2 as the next protocol in order.
- Contact trusted domains. Select this option to contact domain controllers of trusted domains directly without proxying authentication requests and group membership checks through the domain controller.
- Enter the maximum number of simultaneous domain connections (1 to 10).
- Enable periodic password change of machine account. Select this option to change the domain machine account password for this configuration.

- Click **Save Changes**.

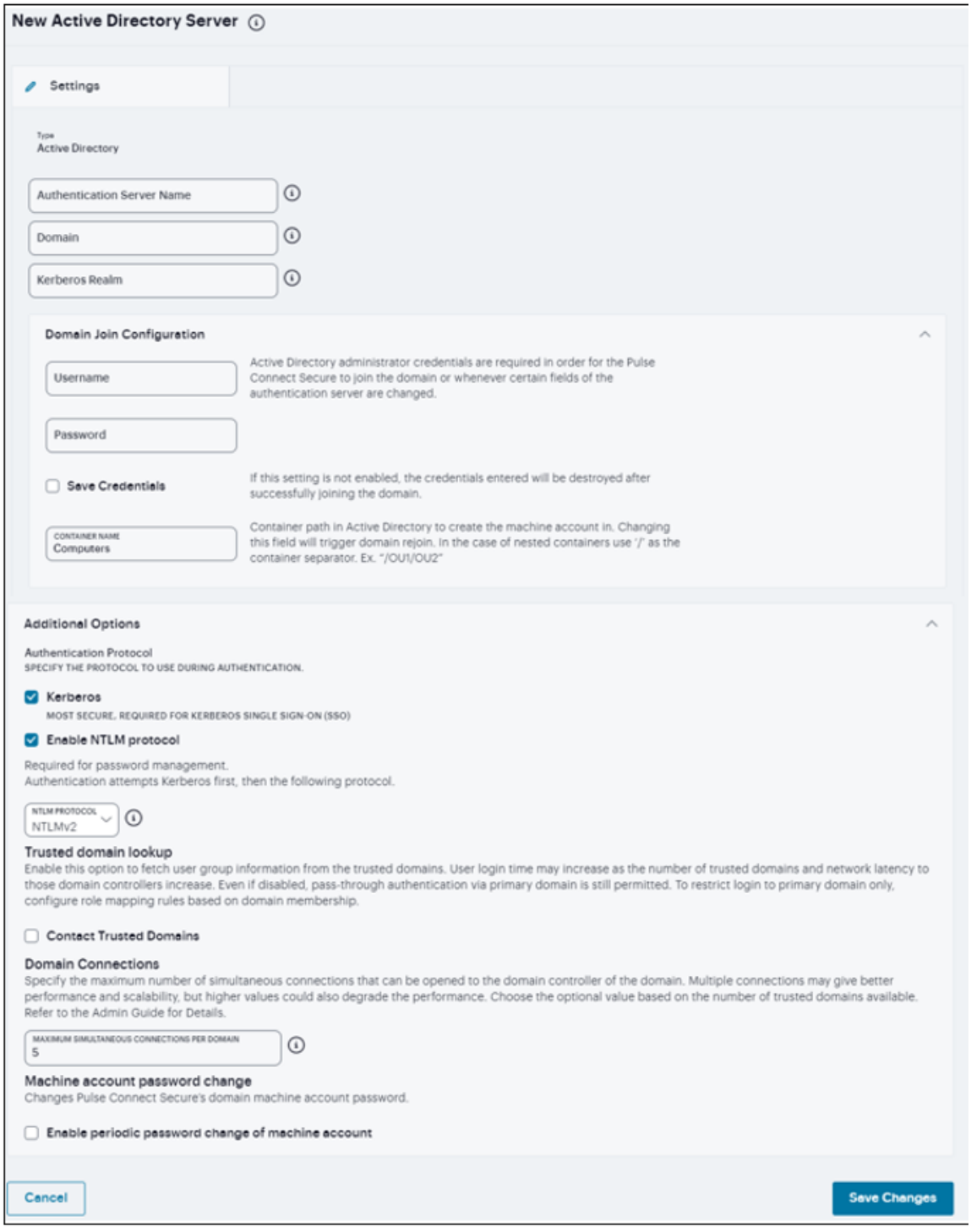


FIGURE 12.16 : Active Directory Authentication Server

Sign-in Policies

Introduction

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

For example, in order to allow all users to sign in to the device, you must add all user authentication realms to the user sign-in policy. You may also choose to modify the standard URL that the end-users use to access the system and the sign-in page that they see. Or, if you have the proper license, you can create multiple user sign-in policies, enabling different users to sign into different URLs and pages.

You can create multiple sign-in policies, associating different sign-in pages with different URLs. When configuring a sign-in policy, you must associate it with a realm or realms. Then, only members of the specified authentication realm(s) may sign in using the URL defined in the policy. Within the sign-in policy, you may also define different sign-in pages to associate with different URLs.

For example, you can create sign-in policies that specify:

- Members of the “Partners” realm can sign in to the device using the URLs: partner1.yourcompany.com and partner2.yourcompany.com. Users who sign into the first URL see the “partners1” sign-in page; users who sign into the second URL see the “partners2” sign-in page.

- Members of the “Local” and “Remote” realms can sign into the device using the URL: employees.yourcompany.com. When they do, they see the “Employees” sign-in page.
- Members of the “Admin Users” realm can sign into the device using the URL: access.yourcompany.com/super. When they do, they see the “Administrators” sign-in page.

When defining sign-in policies, you may use different hostnames (such as partners.yourcompany.com and employees.yourcompany.com) or different paths (such as yourcompany.com/partners and yourcompany.com/employees) to differentiate between URLs.

To create or configure user sign-in policies:

1. Navigate to **Authentication > Signing In > Sign-in Policies**.
2. Select the **Enable multiple user sessions** check box to allow users to have multiple concurrent sessions, and specify whether the user can log in when the maximum number of sessions is reached:
   - **Deny any more session from the user** - Displays a message saying the login is denied because it would exceed the maximum number of concurrent sessions.
   - **Allow the user to login** - Allows the user to log in. If the Display open user session[s] warning notification option is enabled, the user can select which session to close; otherwise the session that has been idle the longest is closed automatically.
3. Select the **Display open user session[s] warning notification** check box to allow users who have met the maximum session count to close one of their existing sessions before continuing with the current log in. If this option is disabled, the system terminates the session that has been idle the longest. This option applies only if Enable multiple user sessions is enabled along with Allow the user to log in. Specify when the user is warned about concurrent sessions:
   - Select **Always** to notify users each time they log in when they already have another active session
   - Select **If the maximum session limit per user for the realm has been reached** to display the warning message only when the user’s maximum session count has been met.
4. To enable or disable an individual policy, select the check box next to the policy that you want to change, and then click **Enable** or **Disable**.

   Note: If you select this option, all user sessions are immediately terminated. If this device is part of a cluster, all user sessions across all nodes in the cluster are immediately terminated.

5. To create a new sign-in policy, click ‘**+**’. Or, to edit an existing policy, click a URL in the Administrator URLs or User URLs column.
6. Select **Users** to specify which type of user can sign in using the access policy.

7. In the **Sign-in URL** field, enter the URL that you want to associate with the policy. Use the format <host>/<path> where <host> is the hostname of the device, and <path> is any string you want users to enter. For example: partner1.yourcompany.com/outside. To specify multiple hosts, use the * wildcard character.

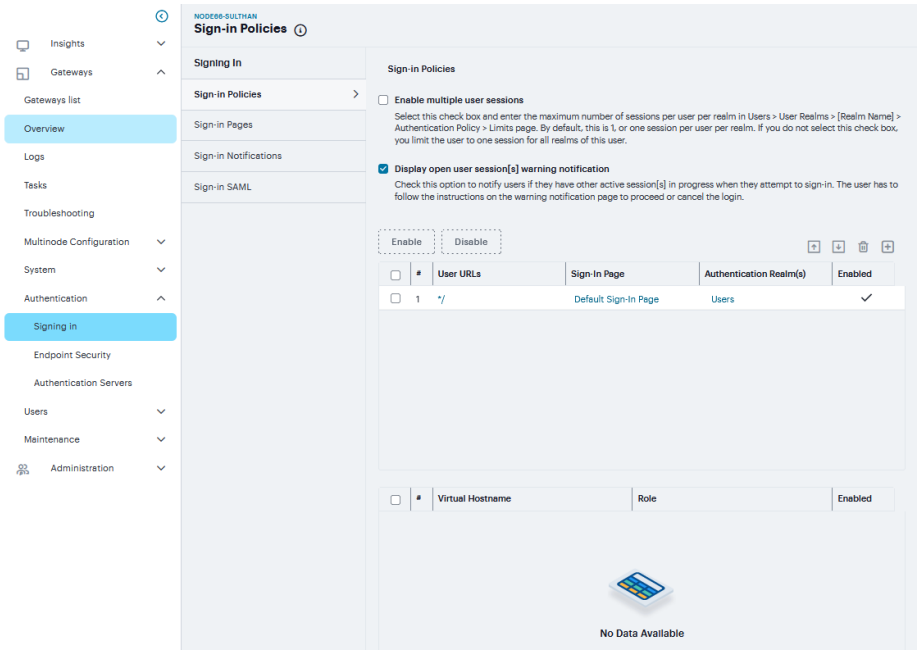


FIGURE 13.1 : Sign-in Policies

To specify that all administrator URLs should use the sign-in page, enter (/admin)*.

- You may only use wildcard characters (*) in the beginning of the hostname portion of the URL. The system does not recognize wildcards in the URL path.
- SAML authentication does not support sign-in URLs that contain multiple realms. Instead, map each sign-in URL to a single realm.

8. (optional) Enter a **Description** for the policy.
9. From the **Sign-in Page** list, select the sign-in page that you want to associate with the policy. You may select the default page that comes with the system, a variation of the standard sign-in page, or a custom page that you create using the customizable UI feature.
10. Under **Authentication realm**, specify which realm(s) map to the policy, and how users and administrators should pick from amongst realms. If you select:
    - **User types the realm name** - The system maps the sign-in policy to all authentication realms, but does not provide a list of realms from which the user or administrator can choose. Instead, the user or administrator must manually enter his realm name into the sign-in page.
    - **User picks from a list of authentication realms** - The system only maps the sign-in policy to the authentication realms that you choose. The

system presents this list of realms to the user or administrator when he signs-in to a device and allows him to choose a realm from the list. (Note that the system does not display a drop-down list of authentication realms if the URL is only mapped to one realm. Instead, it automatically uses the realm you specify.)

11. To move **Available realms** to **Selected realms** use the arrows. Similarly use arrows to move vice versa.
12. Under **Configure Sign-in Notifications**, select the check box for **Pre-Auth Sign-in Notification**, **Post-Auth Sign-in Notification**, or both.
    - After Pre-Auth Sign-in Notification, select a previously configured sign-in notification from the drop-down menu.
    - After Post-Auth Sign-in Notification, select the option for Use a common Sign-in Notification for all roles or Use the Sign-in Notification associated to the assigned role.
13. Click **Save Changes**.

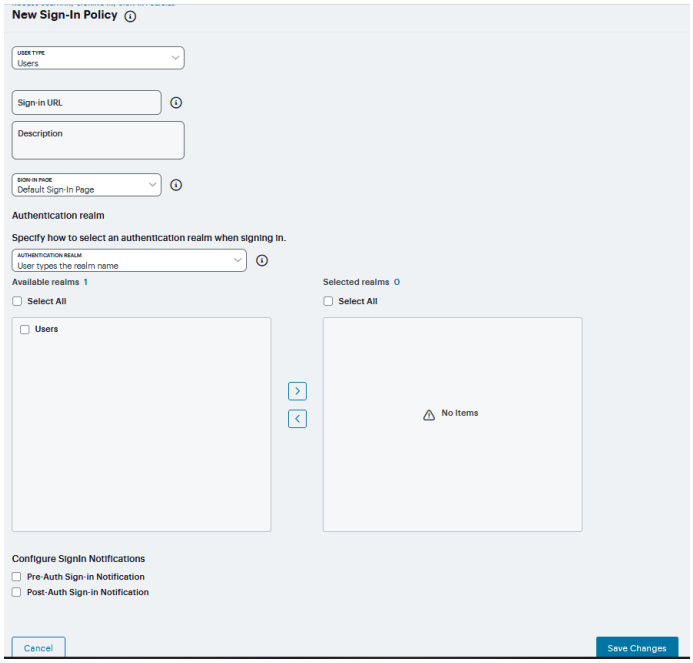


FIGURE 13.2 : Users

Defining Authorization-Only Access Policies

Authorization-only access is similar to a reverse proxy. Typically, a reverse proxy is a proxy server that is installed in front of webservers. All connections coming from the Internet addressed to one of the webservers are routed through the proxy server, which may either deal with the request itself or pass the request wholly or partially to the main webserver.

With an authorization-only access, you select a user role. the system then acts as reverse proxy server and performs authorization against the server for each request.

For example, the authorization-only access feature satisfies the following business needs:

- If you have a third-party AAA policy management server, the system acts as an authorization-only agent.
- If your user sessions are managed by a third-part session management system, there is no need to duplicate the user session management in the system.

With authorization-only access, there is no SSO from the system. SSO is controlled by your third-party AAA infrastructure.

To create or configure authorization-only access policies:

1. In the admin console, choose **Authentication > Signing In > Sign-in Policies**.
2. To create a new authorization only access policy, click '**+**' and select authorization only access. Or, to edit an existing policy, click a URL in the Virtual Hostname column.
3. In the **Virtual Hostname** field, enter the name that maps to the system's IP address. The name must be unique among all virtual hostnames used in pass-through proxy's hostname mode. The hostname is used to access backend application entered in the Backend URL field. Do not include the protocol (for example, http:) in this field.

   For example, if the virtual hostname is myapp.ivehostname.com, and the backend URL is http://www.example.com:8080/, a request to https://myapp.ivehostname.com/test1 via the system is converted to a request to http://www.example.com:8080/test1. The response of the converted request is sent to the original requesting web browser.
4. In the **Backend URL** field, enter the URL for the remote server. You must specify the protocol, hostname and port of the server. For example, *(http://www.mydomain.com:8080/)*.

   When requests match the hostname in the Virtual Hostname field, the request is transformed to the URL specified in the Backend URL field. The client is directed to the backend URL unaware of the redirect.

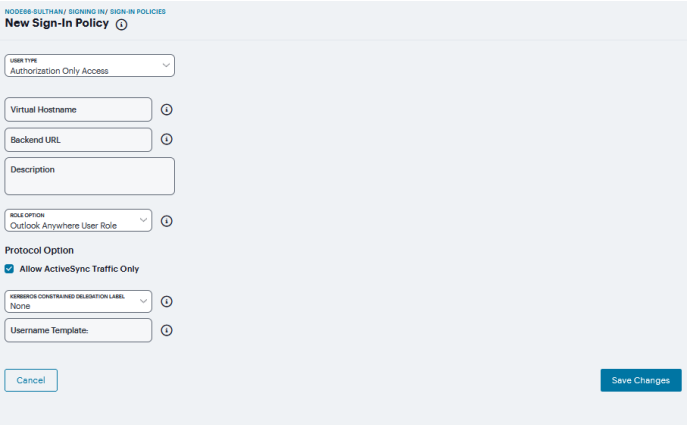


FIGURE 13.3 : Authorization-Only Access Policies

5. (optional) Enter a Description for this policy.

6. Select a user role from the Role Option drop-down menu. Only the following user role options are applicable for authorization-only access.
   - Allow browsing un-trusted SSL web sites (Users > User Roles > RoleName > Web > Options > View advanced options)
   - HTTP Connection Timeout (Users > User Roles > RoleName > Web > Options > View advanced options)
   - Source IP restrictions (Users > User Roles > RoleName > General > Restrictions)
   - Browser restrictions (Users > User Roles > RoleName > General > Restrictions)

   Ensure the user role you select has an associated Web Access policy.
7. Select the **Allow ActiveSync Traffic only** option to perform a basic of validation of the HTTP header to ensure the request is consistent with ActiveSync protocol. If you select this option only ActiveSync protocol requests can be processed. If validation fails, a message is created in the user's event log. If you do not select this option, both ActiveSync and non-ActiveSync requests are processed.
8. Select the **Kerberos Constrained Delegation Label** option to configure a KCD policy for Active Sync. This would list the existing configured Constrained Delegation labels. Selecting any one of the valid Constrained Delegation labels would force to use KCD for the Exchange Active Sync traffic. Also, this option is applicable only for Active Sync traffic.

   This option also has the following dependencies:
   - Enforce client certificate requirement on virtual ports which are used for Active Sync.
   - Appropriate CA certificate should be imported under Trusted Client CAs.
   - The role configured to use for Active Sync should be configured to have Certificate Restrictions to Only allow users with a client-side certificate signed by Certification Authority to sign in.
   - Appropriate Constrained Delegation policy should be configured. Please refer to the section "Constrained Delegation" under configuring SSO policies

   ---

   Note: External configurations should be appropriately configured to support Constrained Delegation SSO; Exchange server should be configured to allow Kerberos authentication, i.e., Windows Authentication.

   ---
9. If Kerberos Constrained Delegation Label policy is chosen, enter the appropriate **Username Template** from certificate attributes.
10. Click **Save Changes**.

Configuring Sign-In Pages

A sign-in page defines the customized properties in the end-user's welcome page such as the welcome text, help text, logo, header, and footer. The system allows you to create two types of sign-in pages to present to users and administrators: * **Standard sign-in pages** - Standard sign-in pages are produced by Ivanti and are included with all versions of the Ivanti Connect Secure software. You can modify standard sign-in pages through the Authentication > Signing In > Sign-in Pages tab of the admin console. * **Customized sign-in pages** - Customized sign-in pages are THTML pages that you produce using the Template Toolkit and upload to the system in the form of an archived ZIP file. The customized sign-in pages feature enables you to use your own pages rather than having to modify the sign-in page included with the system.

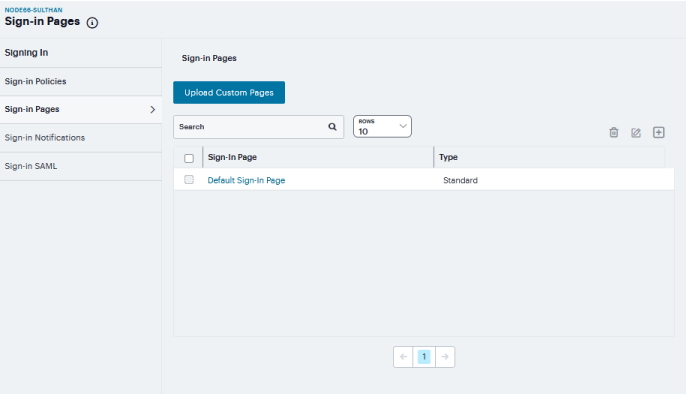


FIGURE 13.4 : Sign-In Pages

Configuring Standard Sign-In Pages

Standard sign-in pages that come with the system include:

- Default Sign-In Page - the system displays this page to users when they sign into the device.

  You can modify the default sign-in page that the system displays to users when they sign into the device. You can also create new standard sign-in pages that contain custom text, logo, colors, and error message text using settings in the Authentication > Signing In > Sign-in Pages tab of the admin console.

To create or modify a standard sign-in page:

1. In the admin console, select **Authentication > Signing In > Sign-in Pages.**
2. If you are:
   - Creating a new page, Click '**+**'.
   - Modifying an existing page, select the link corresponding to the page you want to modify.

3. Enter a **Name** to identify the page.
4. In the **Custom text** section, revise the default text used for the various screen labels as desired. When adding text to the **Instructions** field, note that you may format text and add links using the following HTML tags: <i>, <b>,
, <font>, and <a href>. However, the system does not rewrite links on the sign-in page (since the user has not yet authenticated), so you should only point to external sites. Links to sites behind a firewall will fail.

   If you use unsupported HTML tags in your custom message, the system may display the end user's home page incorrectly.

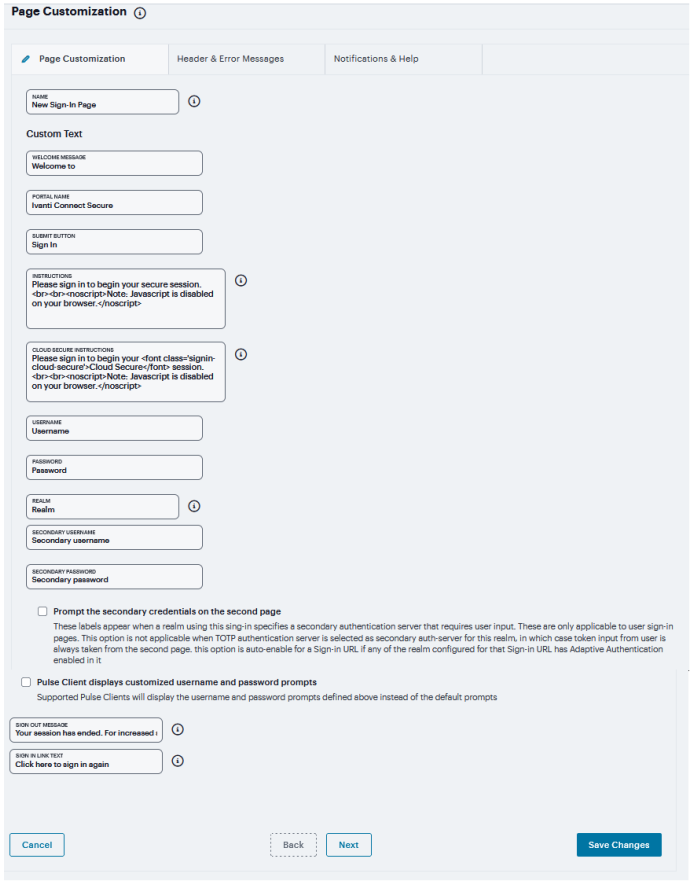


FIGURE 13.5 : Page Customization

5. In the Header appearance section, specify a **Custom logo** image file for the header and a different **Background color**.
6. In the **Custom error messages** section, revise the default text that is displayed to users if they encounter certificate errors.

   You can include <<host>>, <<port>>, <<protocol>>, and <<request>> variables and user attribute variables, such as <<userAttr.cn>> in the custom error messages. Note that these variables must follow the format <variable> to distinguish them from HTML tags which have the format <tag>.

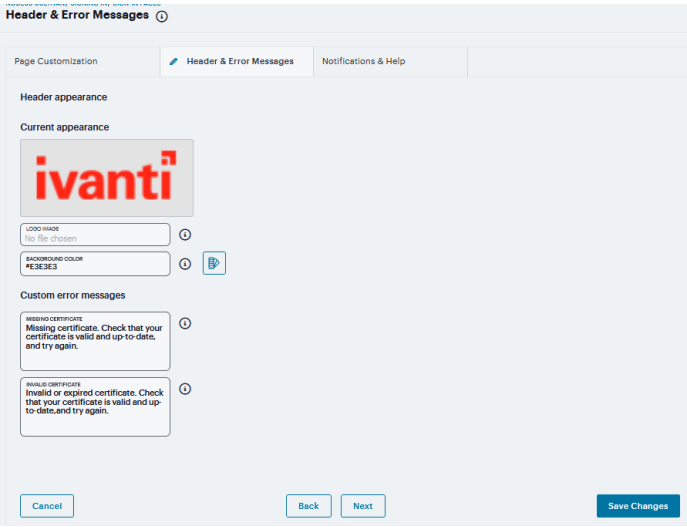


FIGURE 13.6 : Header & Error Messages

7. The user is expected to read the content of the sign-in notification message and acknowledge by clicking a Proceed button. The user may indicate disagreement by clicking a Decline button, which ends the login attempt. To configure this provide **Notification title**, **Proceed Button** label, **Decline Button** label and **Message on Decline**. Select **Display 'Decline' button** check box to make the button visible to user. Perform the step for **Pre-Auth Notification** and **Post-Auth Notification**.
8. To provide custom help or additional instructions for your users, select **Show Help button**, enter a label to display on the button, and specify an HTML file to upload to the system. Note that the system does not display images and other content referenced in this HTML page.
9. Click **Save Changes**. The changes take effect immediately, but users with active sessions might need to refresh their Web browsers.

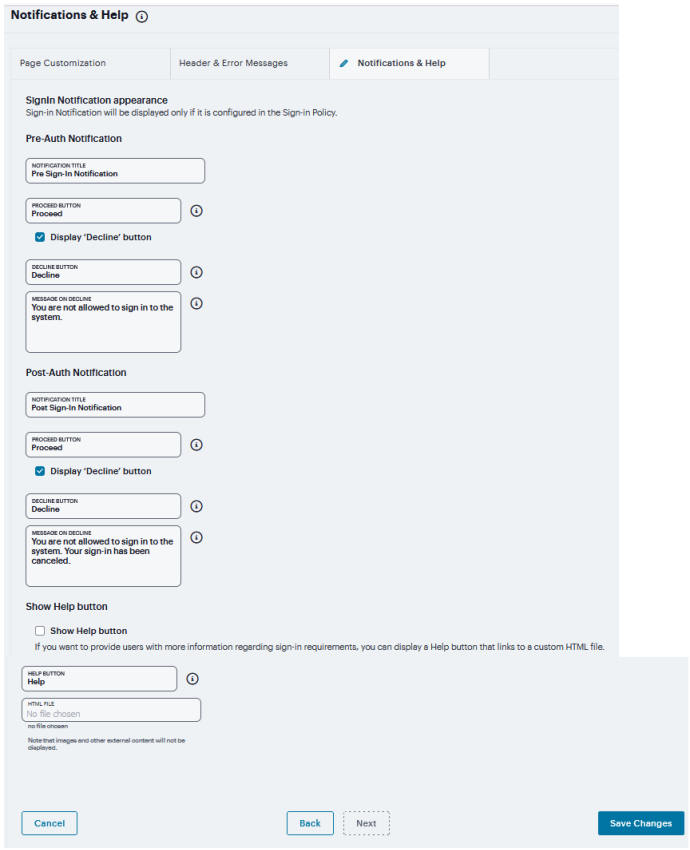


FIGURE 13.7 : Notifications & Help

You can use **Back** and **Next** button to switch between tabs

Custom Sign-In Pages

Downloadable Zip Files

Although each zip file contains all the templates, each zip file is for a particular set of features:

- Sample.zip — This zip file is for standard IPS/ICS pages, including standard pre- and post-authentication pages, ACE pre-authentication pages, ACE pre-authentication pages for use with eTrust SiteMinder, and password management pages.
- SoftID.zip — This zip file is for use with the RSA Soft ID client.
- Kiosk.zip — This zip file is for use by kiosk users or for any system in which you want to lock out keyboard-based login.

To upload custom sign-in Pages into ICS:

1. Download new "**Sample Custom Page**" from new Admin UI after login as Admin. (**Authentication > Sign-In Pages > Upload Custom Sign-In Pages**. Click on **Sample** It will download the Sample Folder as ZIP & save it on Local disk)

2. Copy the following files after unzip the folder (locally saved in previous step):
    - Logout.thtml
    - PleaseWait.thtml
3. Open pre-downloaded Sample Custom Sign-in folder as unzipped and replace all those files here.
4. Now select all the files and create (*.ZIP*) file to uploading custom sign-in page on latest build.
5. Log into ICS as admin which is running on latest build and follow the steps to upload new Custom Sign-In Page In new Admin UI Authentication > Sign-In Pages > Upload Custom Pages > Put the **Name** of Custom Sign-In Page > Click **Template file** field and select previously saved (*.ZIP*) file from local storage in step 4.
6. Select **Use Custom Page for the Ivanti Desktop Client Logon** check box will open a web browser and use custom pages for authentication instead of standard login prompts.
7. Select **Prompt the secondary credentials on the second page** check box to specifies a secondary authentication server that requires user input.
8. Now click on **Upload Custom Pages**. After successful upload, click **Save Changes**.
9. Once all the above steps are successful, we can see the new sign-in page added under Authentication -> Sign-In Pages.
10. Old variable names may change and new variables may be added. It is recommended that you convert old variable names to their new counterparts as the default values for the old variables may no longer exist. If you do not want to update your variable names, you can select the **Skip validation checks during upload** option in the Upload Custom Sign-In Pages page. If you select this option, you should review all your custom pages to ensure that they are still functioning correctly.

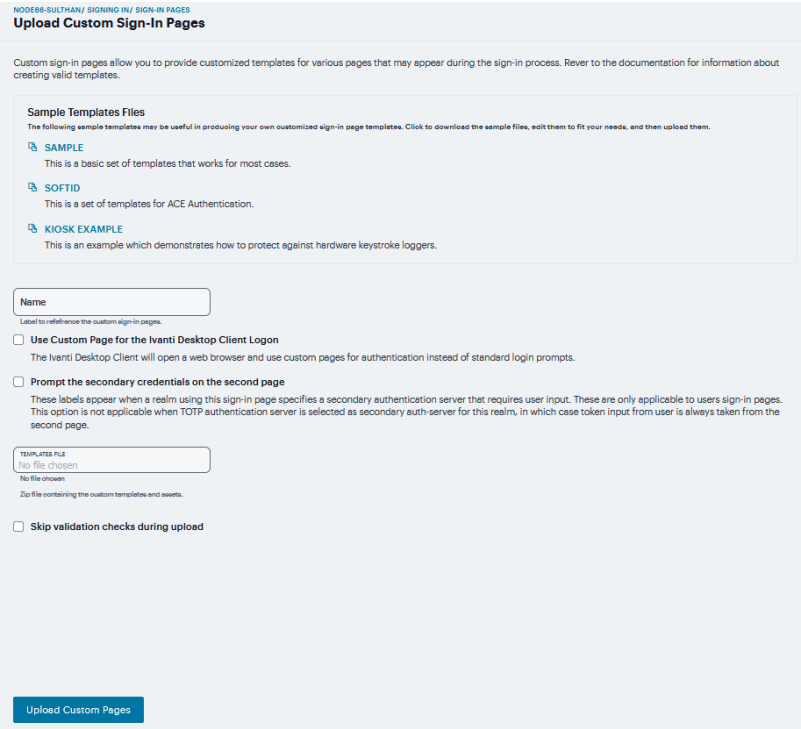


FIGURE 13.8 : Custom Sign-In Pages

Sign-in Notifications

With sign-in notifications, you can create and configure detailed notification messages that appear for Ivanti Secure Access clients and for agentless access endpoints when the user attempts to sign in. For example, you could configure a notification message that explains terms of use, company-specific policies, a welcome page, an end user license agreement (EULA), or a message of the day (MOTD).

For a browser-based (agentless) login, the notification message appears in a separate page either before (pre-auth) or after (post-auth) user authentication during the sign-in process. For a Ivanti Secure Access client login, the notification messages appear in a Ivanti message box. The user is expected to read the content of the sign-in notification message and acknowledge by clicking a Proceed button. The user may indicate disagreement by clicking a Decline button, which ends the login attempt.

You can configure a sign-in policy to use a sign-in notification either as pre-auth or post-auth (or both). In the case of post-auth configuration, you can either use a common message for all roles or use separate messages for each role.

You can create a multi-language sign-in notification package that relies on the language setting of the endpoint. You can customize the sign-in notification page appearance for browser-based logins by modifying the related fields in a sign-in page in the Admin UI or by using a custom sign-in page.

- Sign-in notifications are supported on Windows, Mac, and for browser-based

access on mobile devices. However, sign-in notifications might not work well with all mobile devices due to device limitations.

- Sign-in notifications (including uploaded packages) are included in XML exports.
- If a Ivanti session is resumed or extended, the pre-auth notification message is not shown again. However, if the user switches roles when resuming a session, and that role change results in a new notification, Ivanti displays the message. You can configure the post-auth message to be skipped if it has already been seen. If the post-auth message is not marked to be skipped, then it always appears.

Sign-in notifications appear for Ivanti Secure Access client and for browser-based logins when the user attempts to sign in.

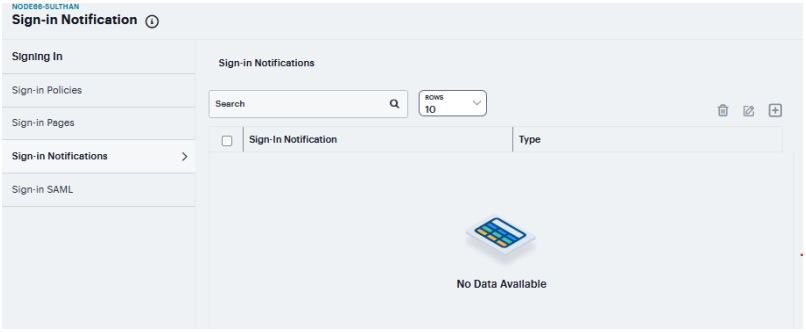


FIGURE 13.9 : Sign-in Notifications

To configure and implement sign-in notifications:

1. In the admin console, select **Authentication > Signing In > Sign-in Notifications**.
2. Click '**+**'. Specify a **Name** for the notification. This name appears in the sign-in policies page, and in the UI Options page for a selected role.
3. Select **Text** or **Package** in the Type box.

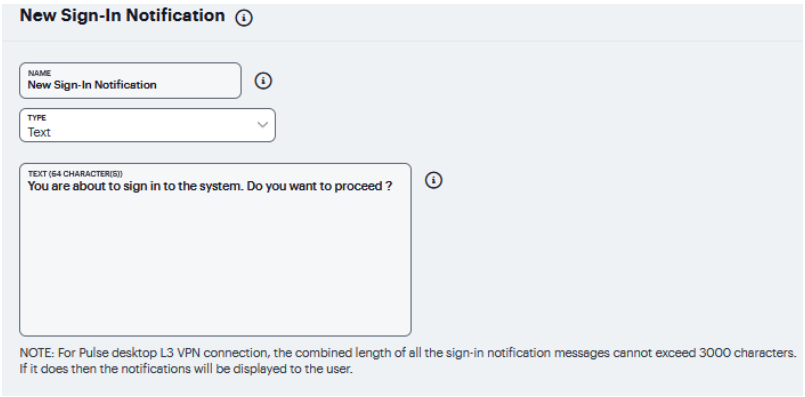


FIGURE 13.10 : Custom Sign-In Pages Text

- If you select **Text**, type the desired sign-in notification message, or copy and paste the relevant text into the Text field.
- If you select **Package**, click the **Package** filed and navigate to a previously prepared .zip file. A package is typically used to provide different language versions of the notification message.
- The zip file should include a default.txt file and one or more <language>.txt files (Example: en.txt).
- Language-abbreviations should be strings that can appear in Accept-Language header of an HTTP request. For example:
  1. Upload a zip file containing files with name format: <language-abbreviation>.txt (Example: en.txt).
  2. Include 'default.txt' and one file for each language you want to support.
  3. Language-abbreviations should be strings that can appear in Accept-Language header of an HTTP request.
- The character encoding supported is UTF-8.

Note: When you create a zip file, do not add the folder containing the files, but add the files directly.

4. Click **Save Changes**.

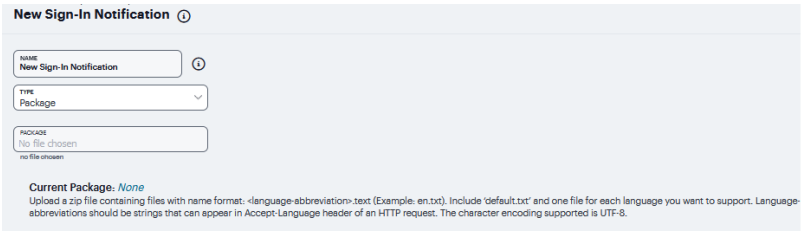


FIGURE 13.11 : Custom Sign-In Pages Package

Sign-in SAML

SAML is an XML-based framework for communicating user authentication, entitlement, and attribute information. The standard defines the XML-based assertions, protocols, bindings, and profiles used in communication between SAML entities. SAML is used primarily to implement Web browser single sign- on (SSO). SAML enables businesses to leverage an identity-based security system like Ivanti Connect Secure to enforce secure access to web sites and other resources without prompting the user with more than one authentication challenge.

SAML Metadata Provider

Sign-in SAML metadata provider settings determine how the system identity provider metadata is published. To configure the identity provider metadata publication settings:

1. Select **Authentication > Signing In > Sign-In SAML > Metadata Provider** to display the configuration page.
2. Complete the settings described in the following table.
3. Click **Save Metadata Provider** to save your changes.

The following table lists the Sign-in SAML Metadata Provider Configuration Guidelines:

TABLE 13.1 : Sign-in SAML Metadata Provider

Setting	Guidelines
Entity ID	This value is prepopulated. It is generated by the system, based on the value for the Host FQDN for SAML setting on the System > Configuration > SAML > Settings page.
Metadata Validity	Specify the maximum duration for which a peer SAML entity can cache the system SAML metadata file. Valid values are 1 to 9999. The default is 365 days.
Do Not Publish SA Metadata	Select this option if you do not want the system to publish the metadata at the location specified by the system Entity ID field. You can use this option to toggle off publication without deleting your settings.
Download Metadata	Use this button to download the system SAML identity provider metadata.

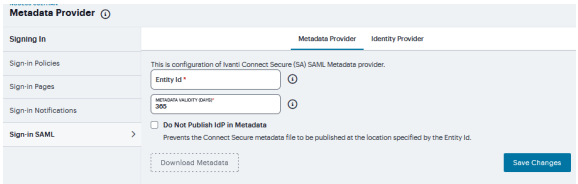


FIGURE 13.12 : SAML Metadata Provider

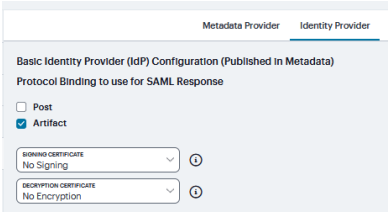
SAML Identity Provider

The settings defined in this procedure are the default settings for the system SAML identity provider communication with all SAML service providers. If necessary, you can use the peer service provider configuration to override these settings for particular service providers. To configure sign-in SAML identity provider settings:

1. Select **Authentication > Signing In > Sign-In SAML > Identity Provider** to display the configuration page.
2. Complete the settings described in the following table.
3. Save the configuration.

The following table lists the Sign-in SAML Identity Provider Configuration Guidelines:

TABLE 13.2 : Sign-in SAML Identity Provider

Setting	Guidelines
Basic Identity Provider (IdP) Configuration (Published in Metadata)	
Protocol Binding to use for SAML Response	Select **POST**, **Artifact**, or both, depending on your total requirements.
Signing Certificate	Select the **Certificate** used to sign the SAML messages sent by the system. The certificates listed here are configured on the *System > Configuration > Certificate > Device Certificates* page.
Decryption Certificate	Select the **Certificate** used to decrypt the SAML messages sent by peer service providers. The public key associated with this certificate is used by the peer service provider to encrypt SAML messages exchanged with this identity provider. The decryption certificate must be configured if the peer service provider encrypts the SAML messages sent to the system. The certificates listed here are configured on the *System > Configuration > Certificate > Device Certificates* page.  FIGURE 13.13 : Basic Identity Provider (IdP) Configuration
Other Configurations	**Reuse Existing NC (Ivanti Secure) Session**. This feature applies to a service- provider-initiated SSO scenario - that is, when a user clicks a link to log into the service provider site. The service provider redirects the user to the identity provider SSO Service URL. If this option is selected, a user with an active NC/Ivanti Secure session is not prompted to authenticate. The system uses information from the existing session to form the SAML response. • **Accept unsigned AuthnRequest**. In a service-provider-initiated SSO scenario, the SP sends an AuthnRequest to the identity provider. This AuthnRequest could be either signed or unsigned. If this option is unchecked, the system

Configuring Peer SAML Service Provider Settings

The peer service provider list defines the set of service providers configured to communicate with he system SAML identity provider. When you add a peer service provider to the list, you can customize the SAML identity provider settings used to communicate with the individual service provider. If the service provider provides a SAML metadata file, you can use it to simplify configuration, or you can complete more detailed manual steps. If available, we recommend you use metadata so that configuration is simpler and less prone to error.

To configure peer SAML service provider settings:

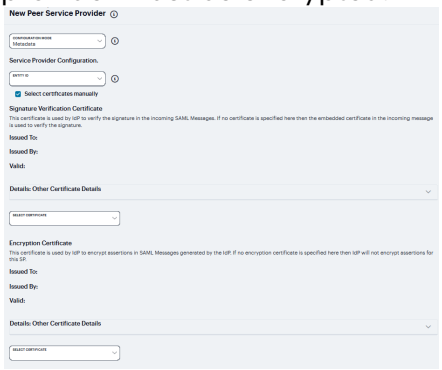
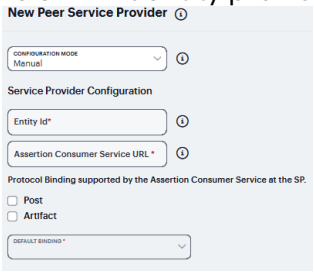
1. Select **Authentication > Signing In > Sign-In SAML > Identity Provider**.
2. Under **Peer Service Provider Configuration**, create a list of service providers that are SAML peers to the system **SAML identity provider**. To add a service provider to the list, click '**+**' to display the configuration page
3. Complete the settings described in the following table.
4. Click **Save Changes**.

TABLE 13.3 : Sign-in SAML Identity Provider

Setting	Guidelines
Configuration Mode	Select Manual or Metadata.
Service Provider Configuration - Metadata	
Entity Id	If you use metadata, select the SAML entity ID of the service provider. This list contains all the service providers specified in all the metadata files added to the System > Configuration > SAML page.
Select certificates manually	When you use the metadata configuration, the system SAML identity provider iterates through all the signature verification certificates specified when verifying the incoming SAML messages coming from the service provider. Similarly, when encrypting the SAML messages going out, the system SAML identity provider encrypts the messages with the first valid encryption certificate encountered in the metadata. Select this option to override this default behavior and select certificates manually.
Signature Verification Certificate	If you select the Select certificates manually option, select the certificate to be used by the identity provider to verify the signature of incoming SAML messages..

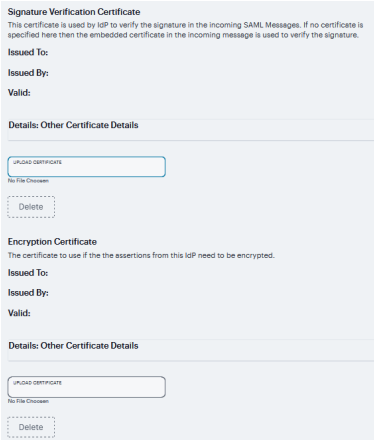
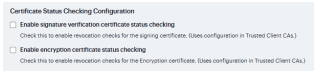
continues on next page

TABLE 13.3 – continued from previous page

Setting	Guidelines
Encryption Certificate	If you select the Select certificates manually option, select the certificate to be used if the assertions sent by the identity provider must be encrypted.  FIGURE 13.19 : Service Provider Configuration - Metadata*
Service Provider Configuration - Manual	
Entity Id	If you are completing a manual configuration, ask the SAML service provider administrator for this setting.
Assertion Consumer Service URL	SAML service provider URL that receives the assertion or artifact sent by the identity provider.
Protocol Binding supported by the Assertion Consumer Service at the SP	Select POST, Artifact, or both. This setting must be consistent with the SAML identity provider configuration.
Default Binding	If both POST and Artifact bindings are supported, which is the default? Post Artifact This setting must be consistent with the SAML identity provider configuration.  FIGURE 13.20 : Service Provider Configuration - Manual

continues on next page

TABLE 13.3 – continued from previous page

Setting	Guidelines
Signature Verification Certificate	Upload the certificate to be used by the identity provider to verify the signature of incoming SAML messages. If no certificate is specified, the certificate embedded in the incoming SAML message is used for signature verification.
Encryption Certificate	Upload the certificate to be used if the assertions sent by the identity provider must be encrypted. If not certificate is specified, the assertions sent by the identity provider are not encrypted.  FIGURE 13.21 : Certificates
Certificate Status Checking Configuration	
Enable signature verification certificate status checking	Select this option to enable revocation checks for the signing certificate. Uses the configuration on the System > Configuration > Certificates > Trusted Client CAs page.
Enable encryption certificate status checking	Select this option to enable revocation checks for the encryption certificate. Uses the configuration on the System > Configuration > Certificates > Trusted Client CAs page.  FIGURE 13.22 : Certificate Status Checking Configuration
Customize identity provider Behavior	

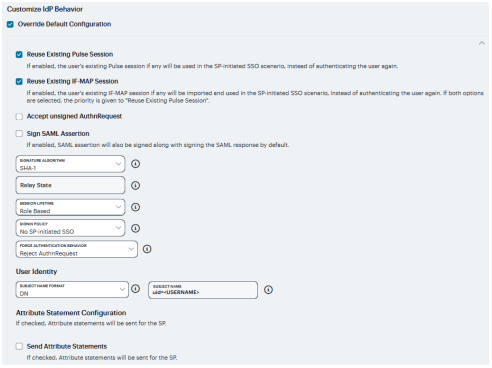
continues on next page

TABLE 13.3 – continued from previous page

Setting	Guidelines
Override Default Configuration	Select this option to set custom behavior of the system SAML identity provider for this SP instance. If you select this option, the user interface displays the additional options listed next.
Reuse Existing NC (Ivanti Secure) Session	This option cannot be enabled here if it is not selected for the sign-in SAML identity provider default settings.
Reuse Existing IF-MAP Session	If enabled, the user's existing IF-MAP session if any will be imported and used in the SP-initiated SSO scenario, instead of authenticating the user again. If both options are selected, the priority is given to "Reuse Existing Ivanti Secure Session".
Accept unsigned AuthnRequest	**Individual service providers can choose to accept unsigned AuthnRequest.** • **Sign SAML Assertion**. If enabled, SAML assertion will also be signed along with signing the SAML response by default.Individual SPs can choose to accept only signed SAML assertion. • **Signature Algorithm**, select the algorithm from drop down.
Relay State	SAML RelayState attribute sent to the service provider in an identity- provider-initiated SSO scenario. If left blank, the RelayState value is the URL identifier of the resource being accessed.
Session Lifetime	Suggest a maximum duration of the session at the service provider created as a result of the SAML SSO. Select one of the following options: None. The identity provider does not suggest a session duration. Role Based. Suggest the value of the session lifetime configured for the user role. Customized. If you select this option, the user interface displays a text box in which you specify a maximum in minutes.
Sign-In Policy	Select the sign-in URL to which the user is redirected in a service-provider - initiated scenario. The list is populated by the sign-in pages configured on the Authentication > Signing In > Sign-in Policies page. The user is not redirected if he or she already has a session with the system and had authenticated through this sign-in policy.

continues on next page

TABLE 13.3 – continued from previous page

Setting	Guidelines
Force Authentication Behavior	**In an service-provider-initiated scenario, the service provider sends a** • Reject AuthnRequest. Do not honor the SAML SSO request. • Re-Authenticate User. Invalidate the user session and prompt for reauthentication. This setting prevails over the Ivanti session reuse setting.  FIGURE 13.23 : Customize identity provider Behavior
User Identity	
Subject Name Format	**Format of the NameIdentifier field in the generated assertion. Select** • DN - Username in the format of DN (distinguished name). • Email address - Username in the format of an e-mail address. • Windows - Username in the format of a Windows domain qualified username. • Other - Username in an unspecified format.
Subject Name	Template for generating the username that is sent as the value of the NameIdentifier field in the assertion. You may use any combination of available system or custom variables contained in angle brackets and plain text.
Attribute Statement Configuration	

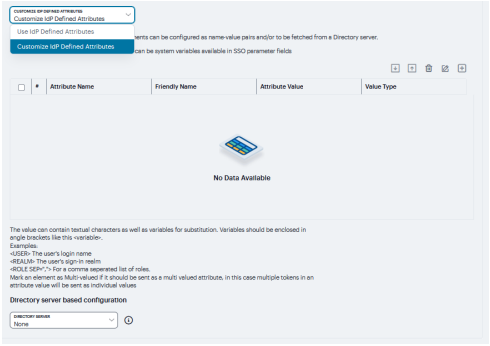
continues on next page

TABLE 13.3 – continued from previous page

Setting	Guidelines
Send Attribute Statements	**Select this option if the SAML SP requires additional attributes to be sent wit** • Use IdP Defined Attributes-Send attributes based on the default settings for the system SAML identity provider communication with all SAML service providers. • Customize IdP Defined Attributes-Selectively configure the attributes that are sent for this particular peer SAML SP. Attributes to be sent in SAML Attribute statements can be specified manually as name-value pairs, or you can configure an option to fetch name-value pairs from an LDAP server (or you can specify both manual entries and LDAP entries). If you select this option, configure the settings described next.
Attribute Name	An ASCII string.
Friendly Name	A more readable friendly name for the attribute. This is optional (an option included in the SAML standard).
Attribute Value	**The attribute value can be specified as a hard-coded string, a custom variabl** • The value can be a combination of a string and a user or custom variable. For example: Email::<customVar.email>. • The value can also be a combination of user and custom variables and hardcoded text. For example: mydata=<USER><REALM><customVar.email>.

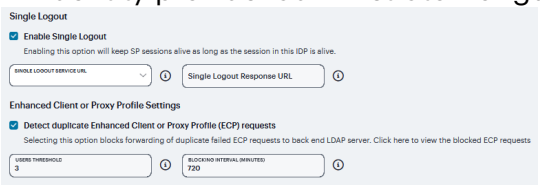
continues on next page

TABLE 13.3 – continued from previous page

Setting	Guidelines
Value Type	**Select Single-Valued or Multivalued.** • A single-valued attribute can be a combination of a string and a user or custom variable. • If there are multiple single-valued attributes configured with the same attribute names, they are combined and sent as a multivalued attribute. Select Multivalue if you want every individual token defined in the Attribute Value column to be sent as a separate AttributeValue. For example: <element ref="saml:AttributeValue" minOccurs="0" maxOccurs="unbounded"/> • If the Attribute value is given as <USER>mars<REALM><orgname><ROLE> and the value type is marked as Multivalued, then the values sent as part of attribute statement are sent as follows: – Username – Realmname – Role Note that only the tokens ['<>'] will be considered when processing a Multivalued attribute marked. The remaining data (for example mars, jupiter) is discarded.  FIGURE 13.24 : Attribute Statement Configuration Specifying the token <ROLE> will send only one role. To send all roles, specify the Attribute value with the syntax <ROLE SEP=",">. If you specify <ROLE SEP=","> as a single-valued attribute, it is sent as a single string with "," separated roles. If you specify <ROLE SEP=","> as a multi-valued attribute, each role is sent in a separate <AttributeValue> element. Encryption is set at the assertion level. You cannot encrypt individual attributes.

continues on next page

TABLE 13.3 – continued from previous page

Setting	Guidelines
Directory Server	**To fetch attribute name-value pairs from an LDAP server, complete the follow** • **Directory Server** - Select the LDAP server from the list. You must add the LDAP server to the Authentication > Auth. Servers list before it can be selected.
Single Logout	Single logout is a mechanism provided by SAML for logging out a particular user from all the sessions created by the identity provider. Select this option if the system must receive and send a single logout request for the peer SAML identity provider.
Enable Single Logout	• If you use the metadata option, the Single Logout Service URL setting can be completed by selecting the SLO service URL from the list. The list is populated by the identity provider entities defined in metadata files added to the System > Configuration > SAML page. The system sends Single Logout requests to this URL. • In addition, if you use the metadata option, the Single Logout Response URL setting is completed based on your selection for Single Logout Service URL. If the identity provider has left this setting empty in its metadata file, the system sends the Single Logout response to the SLO service URL. If you complete these settings manually, ask the SAML identity provider administrator for guidance.  FIGURE 13.25 : Single Logout
Enhanced Client or Proxy Profile Settings	Select **Detect duplicate Enhanced Client or Proxy Profile (ECP) requests** option to block forwarding of duplicate failed ECP requests to back end LDAP server.
Users Threshold	Number of duplicate ECP requests that can be detected and blocked per user
Blocking Interval	In Minutes

continues on next page

TABLE 13.3 – continued from previous page

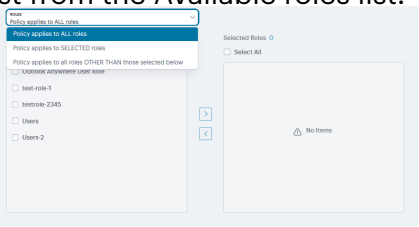
Setting	Guidelines
Roles	**Select one of the following options:** • Policy applies to ALL roles. To apply this policy to all users. • Policy applies to SELECTED roles. To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list. • Policy applies to all roles OTHER THAN those selected below. To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.  FIGURE 13.26 : Roles

FIGURE 13.18 : Peer SAML Service Provider

Using Endpoint Security

Managing ESAP Versions

The Endpoint Security Assessment Plug-in (ESAP) on Ivanti Connect Secure checks third-party applications on endpoints for compliance with the predefined rules you configure in a Host Checker policy. This plug-in is included in the system software package.

Ivanti frequently adds enhancements, bug fixes, and support for new third-party applications to the plug-in. New plug-in releases are available independently and more frequently than new releases of the system software package. If necessary, you can upgrade the plug-in independently of upgrading the system software package.

You can upload up to four versions of the plug-in to your system, but it uses only one version at a time (called the active version). If necessary, you can roll back to a previously active version of the plug-in.

The default SDK version used is v3, but it can be reconfigured based on your requirement. The product/vendor names used by v3 and v4 SDK might differ. Due to the product/vendor names mismatch, there is a possibility that the rules become empty while creating Host Checker rule with v3 SDK activated and upon enabling v4 SDK. To avoid this, a migration page is added to help the administrators in migrating the policies from v3 to v4 SDK.

To migrate from v3 to v4 version:

1. Navigate to **Manage Endpoint Security Assessment PlugIn Versions** section on the **Authentication > Endpoint Security > Host Checker** page.
2. Select the **Enable migration of Opswat SDK from old to new version (V3 to V4)** option.

3. Click **Save Changes**.

   On enabling this option, the clients start downloading the V4 SDK and migrate to newer SDK.

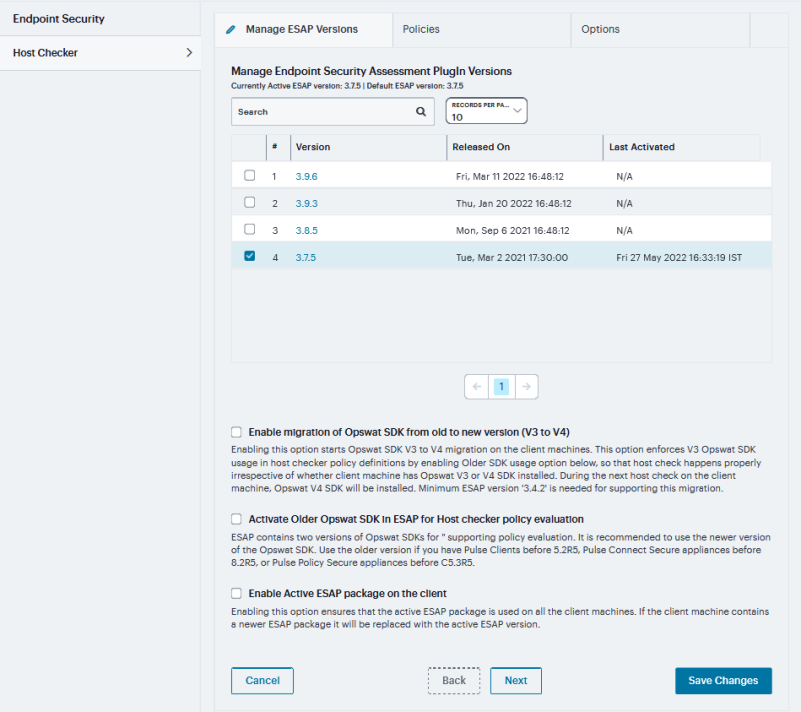


FIGURE 14.1 : Endpoint Security Assessment PlugIn Versions

4. Clear the Enable migration of Opswat SDK from old to new version (V3 to V4) option once the migration is complete.
5. Verify the migration status. In the confirmation message box, click Confirm.

To roll back to previous version of OPSWAT SDK:

1. Navigate to **Manage Endpoint Security Assessment PlugIn Versions** section on **Authentication > Endpoint Security > Host Checker** page.
2. Clear the **Enable migration of Opswat SDK from old to new version (V3 to V4)** check box.
3. Enable **Activate Older Opswat SDK in ESAP for Host Checker policy evaluation**.
4. Click **Save Changes**.

Enabling the Active ESAP Package

Administrator can enable “Enable Active ESAP package on the client” check box to ensure that client machine always uses the active ESAP package, even if the active ESAP package is older than the version installed on the client system. In case client machine has newer ESAP package installed, it will be replaced with the older Active ESAP version with this option enabled.

To enable the active ESAP package:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Under Manage Endpoint Security Assessment Plugin Versions, select the **Enable Active ESAP package on the client** check box.
3. Click **Save Changes**.

Configuring Host Checker Policy

Host Checker is a software component that performs endpoint compliance checks on hosts that connect to Ivanti Connect Secure. It supports two types of rules within a policy; predefined and custom. The pre-defined inspection capabilities consist of health and security checks including antivirus versions, antispyware, OS versions, hard disk encryption status and patch checks. The pre-defined rules are provided by OPSWAT and it uses the ESAP plug-in for pre-defined checks.

To configure a Host Checker policy, perform these tasks:

1. Log into the nSA as a Tenant Admin.
2. From the ICS menu, click **Gateways > Gateways List**. In the Gateways list page, select the standalone ICS Gateway or Cluster node that you want to configure.
3. From the ICS menu, select **Authentication > Endpoint Security > Host Checker**.

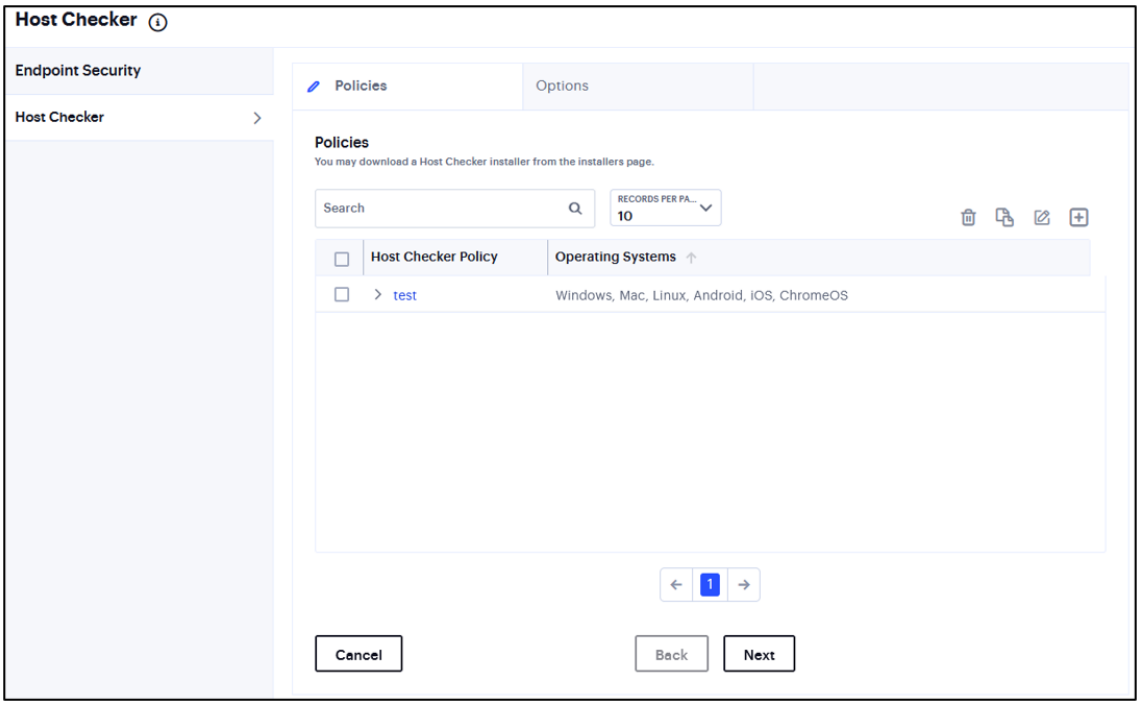


FIGURE 14.2 : Host Checker

4. Under Policies, click the '**+**' icon.
5. Enter a name for the policy and then click **Save Changes**.

   A list of all the added policies is displayed.
6. Create one or more rules to associate with the policy.

   In the **Options** tab, enter time limit for performance check and logout time if the device is inactive.

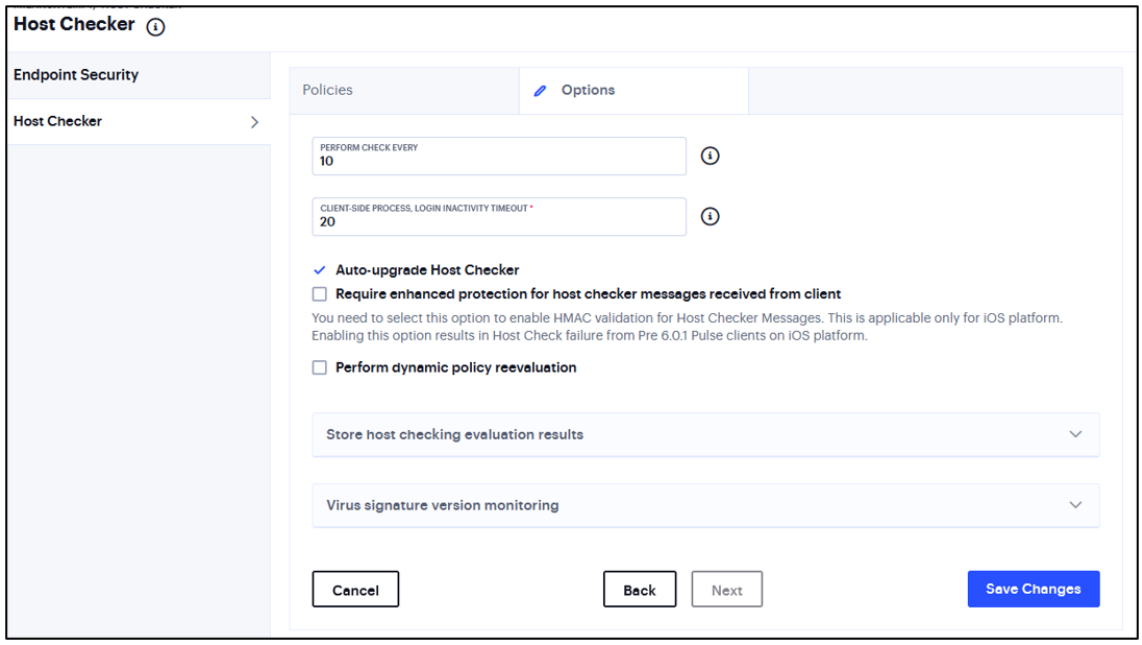


FIGURE 14.3 : Host Checker Options

7. You can select Auto-upgrade Host Checker, Require enhanced protection for host checker messages received from client, and Perform dynamic policy reevaluation.

Note: You need to select this option to enable HMAC validation for Host Checker messages. This is applicable only for iOS platform. Enabling this option results in Host Check failure from Pre 6.0.1 Ivanti Secure Access clients on iOS platform.

---

8. Select **Store Host Checking evaluation results** to cache the result for the certain number of days.
9. Select **Cache results if any of the roles is assigned** or **Cache results only if any of the selected roles are assigned** and select the roles from **Available Roles**.

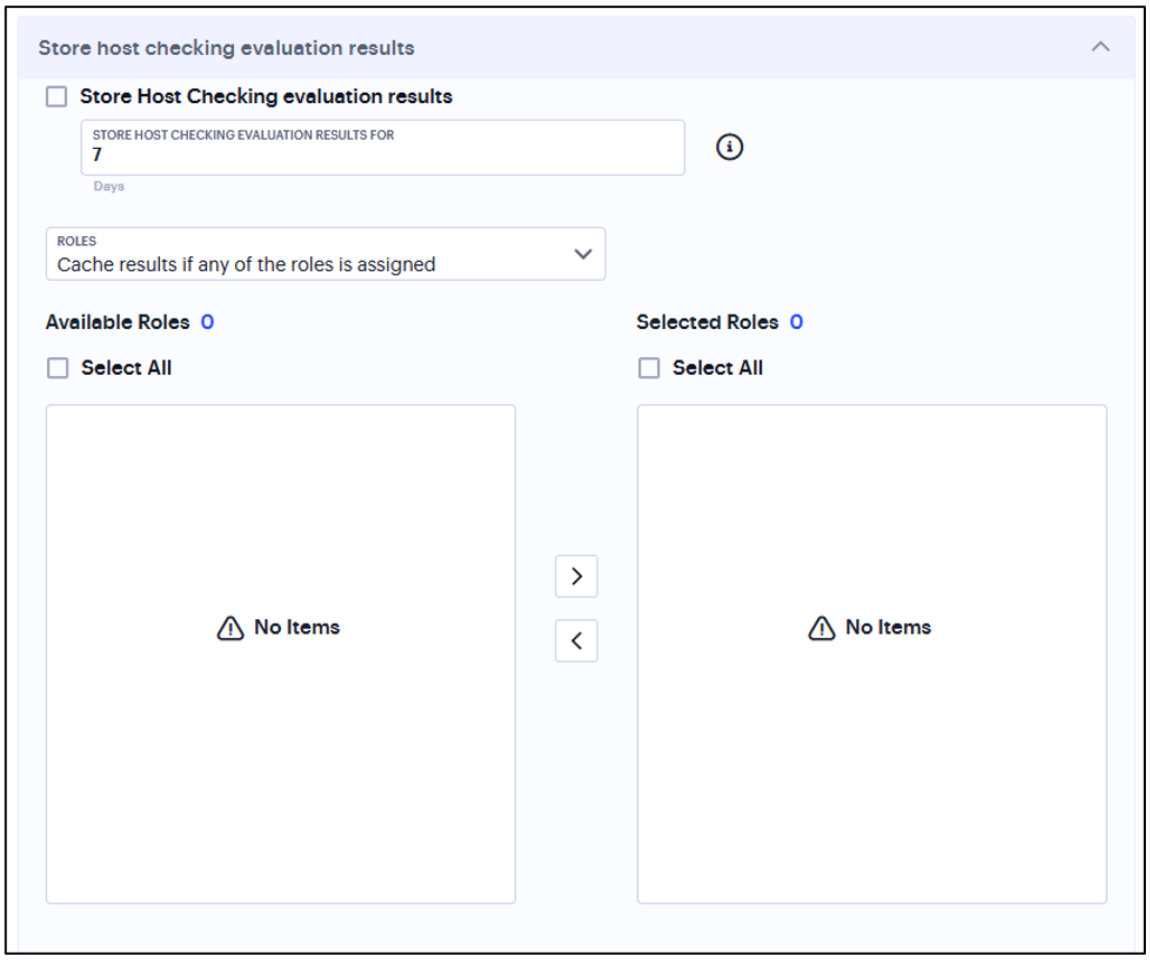


FIGURE 14.4 : Store Host Checking Evaluation Results

10. In Virus signature version monitoring, select **Auto-update virus signatures list**.
    - For Download path, leave the existing URL(s) of the staging site(s) where the current list(s) are stored.
    - For Download interval, specify how often you want the system to automatically import the current list(s).
    - For Username and Password, enter your Connect Secure credentials.
    - To use a proxy server as the auto-update server, select **Use Proxy Server** and provide the proxy server details.

Note: You can also import the virus signatures manually by importing signature list.

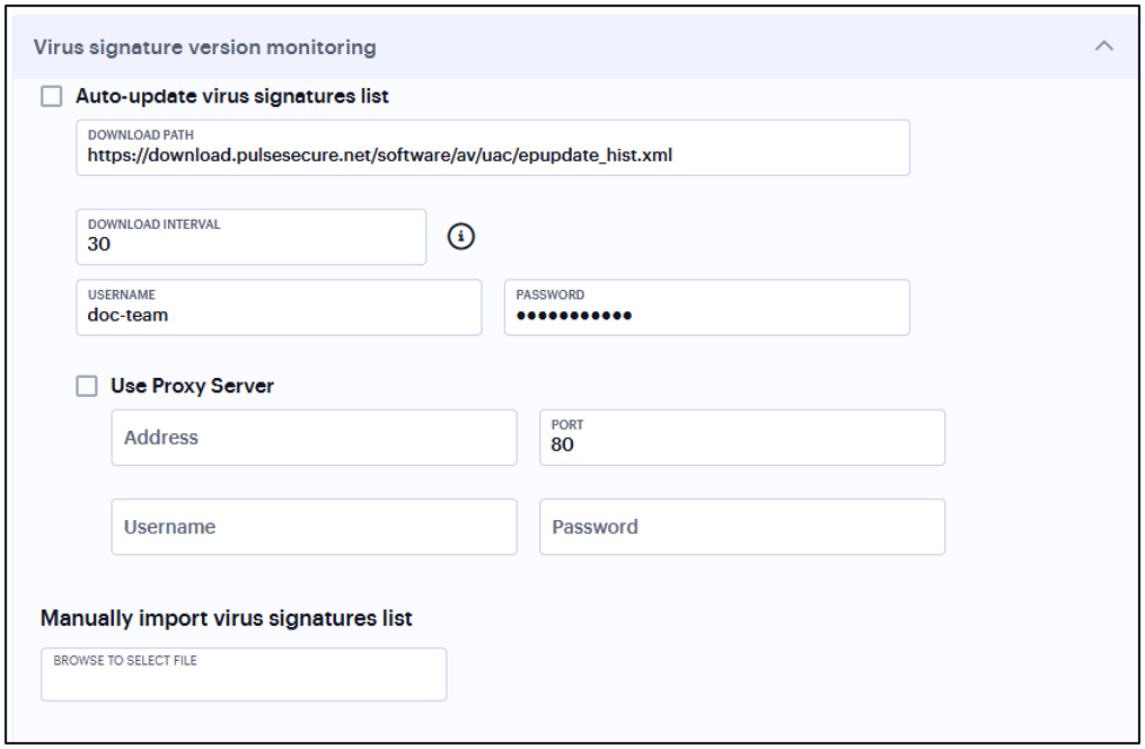


FIGURE 14.5 : Virus Signature Version Monitoring

11. To edit an existing policy, select the corresponding check box and click the Edit icon.
12. To delete one or more policies, select the corresponding check boxes and click the Delete icon.

Checking for Third-Party Applications Using Predefined Rules

Host Checker comes pre-equipped with a vast 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 users' computers in accordance with your specifications. For firewall and antivirus rules, you can specify remediation actions to automatically bring the endpoint into compliance.

Add Rule: Antivirus Rule with Remediation Options

To configure a Predefined Antivirus rule:

1. Select one of the following supported platforms:
   - Windows
   - Mac
2. Enter a Rule Name.
3. Under Criteria, click **Require specific products/vendors**. A new window will open with a list of all of the products that support the feature.
4. Select your vendor(s) and product(s) by using either the **Require any supported product from a specific vendor** or **Require specific products** check box.
5. If your product is supported, select the check box for any or all of the remediation actions that you want to apply.
6. (Optional) Select or clear the check box next to **Successful System Scan must have been performed in the last**, and enter the number of days in the field.
   - If you select this check box, a new option appears. If the remediation action to start an antivirus scan has been successfully begun, you can override the previous check.
7. (Optional) Select or clear the check box next to **Check for the Virus Definition files**. Enter a number between 1 and 20. If you enter 1, the client must have the latest update.
8. (Optional) Select **Monitor this rule for change in result** to continuously monitor the policy compliance of endpoints.

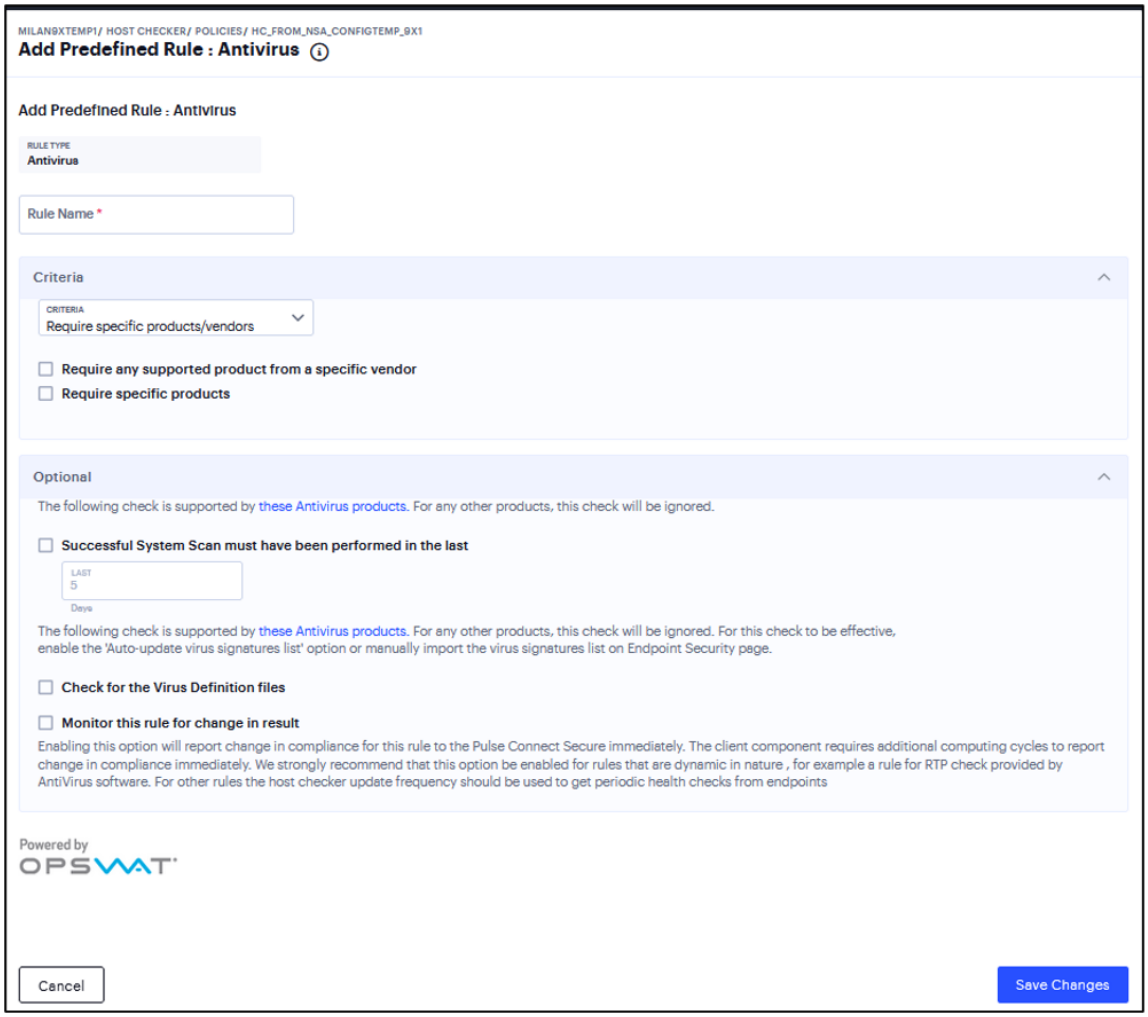


FIGURE 14.6 : Antivirus Rule

Note:

- Use this option only for dynamic rules, such as checking whether Real Time Protection is enabled on the antivirus software. Use the host checker update frequency to monitor other rules periodically.
- Monitor this rule for change in result for port check is applicable only for Windows and not for Linux or MAC machines.

Add Rule: Firewall Rule with Remediation Options

When you enforce the Host Checker rule with firewall remediation actions, if an endpoint attempts to log in without the required firewall running, Host Checker can attempt to enable the firewall on the client machine.

1. Select one of the following supported platforms:
   - Windows
   - Mac
2. Enter a Rule Name.
3. Under Criteria, click **Require specific products/vendors**. A new window will open with a list of all of the products that support the feature.
4. Select your vendor(s) and product(s) by using either the **Require any supported product from a specific vendor** or **Require specific products** check box.
5. (Optional) Select **Monitor this rule for change in result** to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, the system initiates a new handshake to re-evaluate realm or role assignments.

FIGURE 14.7 : Firewall Rule

Note: Monitor this rule for change in result for port check is applicable only for Windows and not for Linux or MAC machines.

Add Rule: AntiSpyware

You can configure Host Checker to check for installed antispyware on endpoints.

To configure a Host Checker Predefined Spyware rule:

1. Select one of the following supported platforms:
   - Windows
   - Mac
2. Enter a Rule Name.
3. Under Criteria, click **Require specific products/vendors**. A new window will open with a list of all of the products that support the feature.
4. Select your vendor(s) and product(s) by using either the **Require any supported product from a specific vendor** or **Require specific products** check box.
5. (Optional) Select **Monitor this rule for change in result** to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, the system initiates a new handshake to re-evaluate realm or role assignments.

FIGURE 14.8 : AntiSpyware

Note: Monitor this rule for change in result for port check is applicable only for Windows and not for Linux or Mac machines.

Add Rule: Hard Disk Encryption

You can configure Host Checker to check for installed Hard Disk Encryption on endpoints and specify the drives which needs to be encrypted using these software.

To configure a predefined hard disk encryption rule:

1. Select one of the following supported platforms:
   - Windows
   - Mac
2. Enter a Rule Name.
3. Under Criteria, click **Require specific products/vendors**. A new window will open with a list of all of the products that support the feature.
4. Select your vendor(s) and product(s) by using either the **Require any supported product from a specific vendor** or **Require specific products** check box.

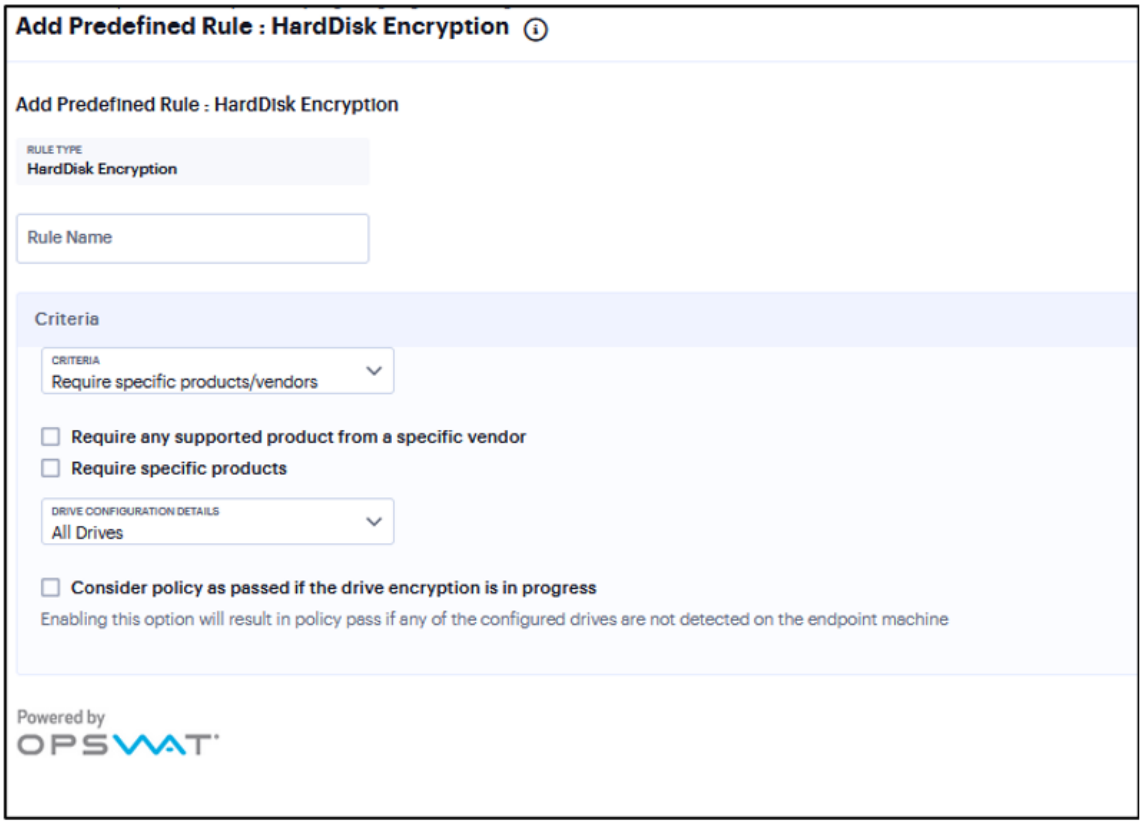


FIGURE 14.9 : HardDisk Encryption

5. Under Drive Configuration Details, select the required option:
   - All Drives - (Default) Select this option to check if all the drives on the client machine are encrypted.

- Specific Drives - Select this option to check if only specific drives on the client machine are encrypted.
  - Drive Letters - Enter the drive name. For example, C, D, E.
- Select the **Consider policy as passed if the drive Encryption is in progress** option to allow the Host Checker policy to pass if the encryption process is in progress and the drive is not fully encrypted.

Note:

- The drive encryption process takes time to complete depending up on the drive size and contents.
- For multiple drives, the Host Checker policy passes only if the encryption process is in progress in all the drives.

Add Rule: Patch Management

You can configure Host Checker to check for installed Patch management Software on endpoints.

To configure a predefined patch management rule:

1. Select one of the following supported platform options:
   - Windows
   - Mac
2. Enter a Rule Name.
3. Under Criteria, select the product name.
4. Default “Severity” options selected in policy are Critical, Important.
5. Default “Category” options selected in policy are Security Update, Critical Update, Regular Update, Driver Update.
6. To automatically enable patch deployment, select **Enable Automatic Patch Deployment**.

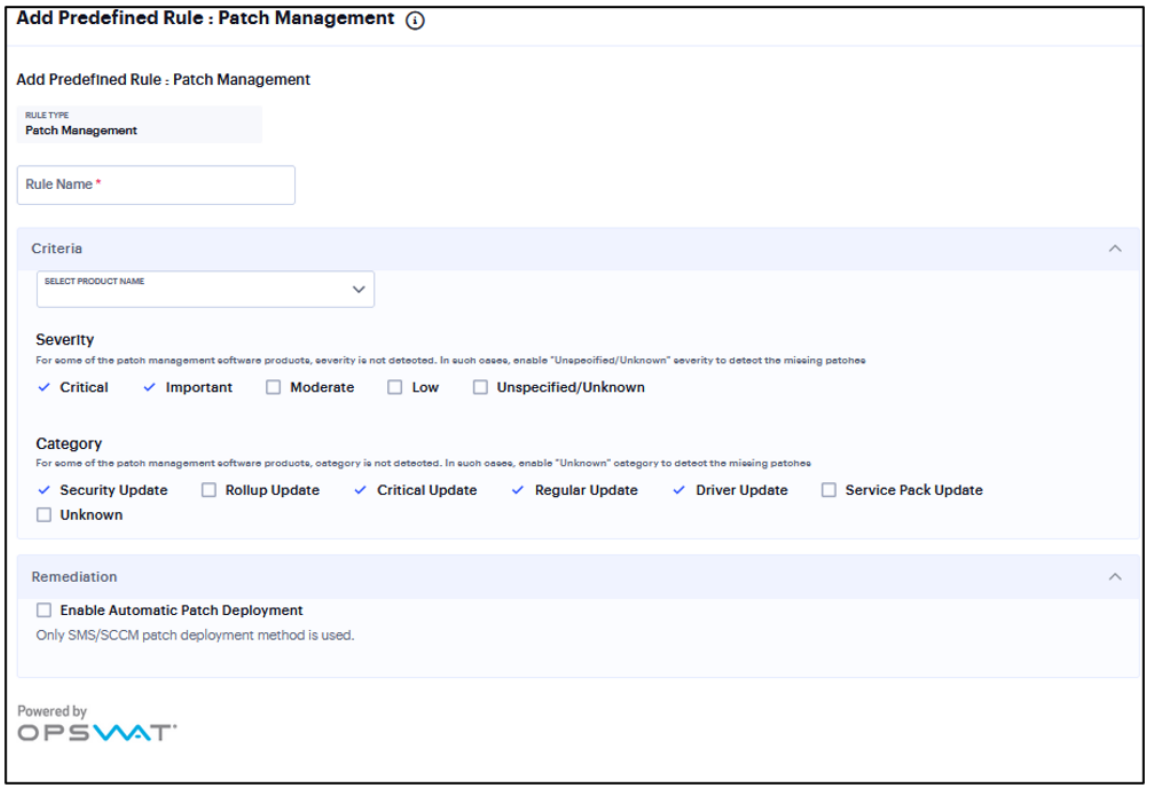


FIGURE 14.10 : Patch Management

Add Rule: Common Vulnerability and Exposure (CVE)

The CVE check rule helps in identifying the endpoints which are vulnerable using the OPSWAT library.

This rule is applicable only to Windows platform.

To configure a predefined CVE check rule:

1. Enter a Rule Name.
2. From the Criteria, select if you require all the CVE checks from OPSWAT or choose the specific CVE checks from the available CVE checks list.

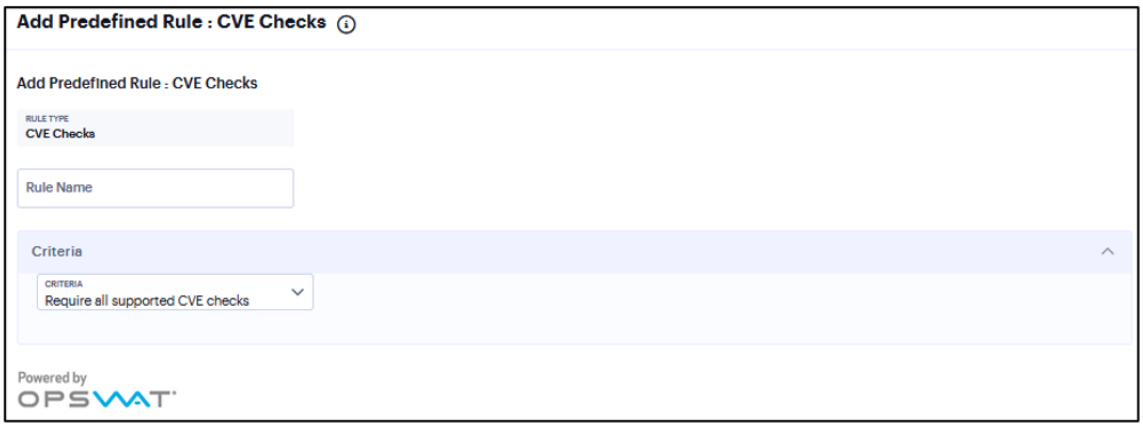


FIGURE 14.11 : CVE Checks

Add Rule: OS Checks

You can configure Host Checker to check the version of the windows operating systems and minimum service packs.

This rule is applicable only to Windows platform.

To configure a Host Checker Predefined OS Checks rule:

1. Enter a rule name.
2. Under Criteria, select the service pack/version to ignore.

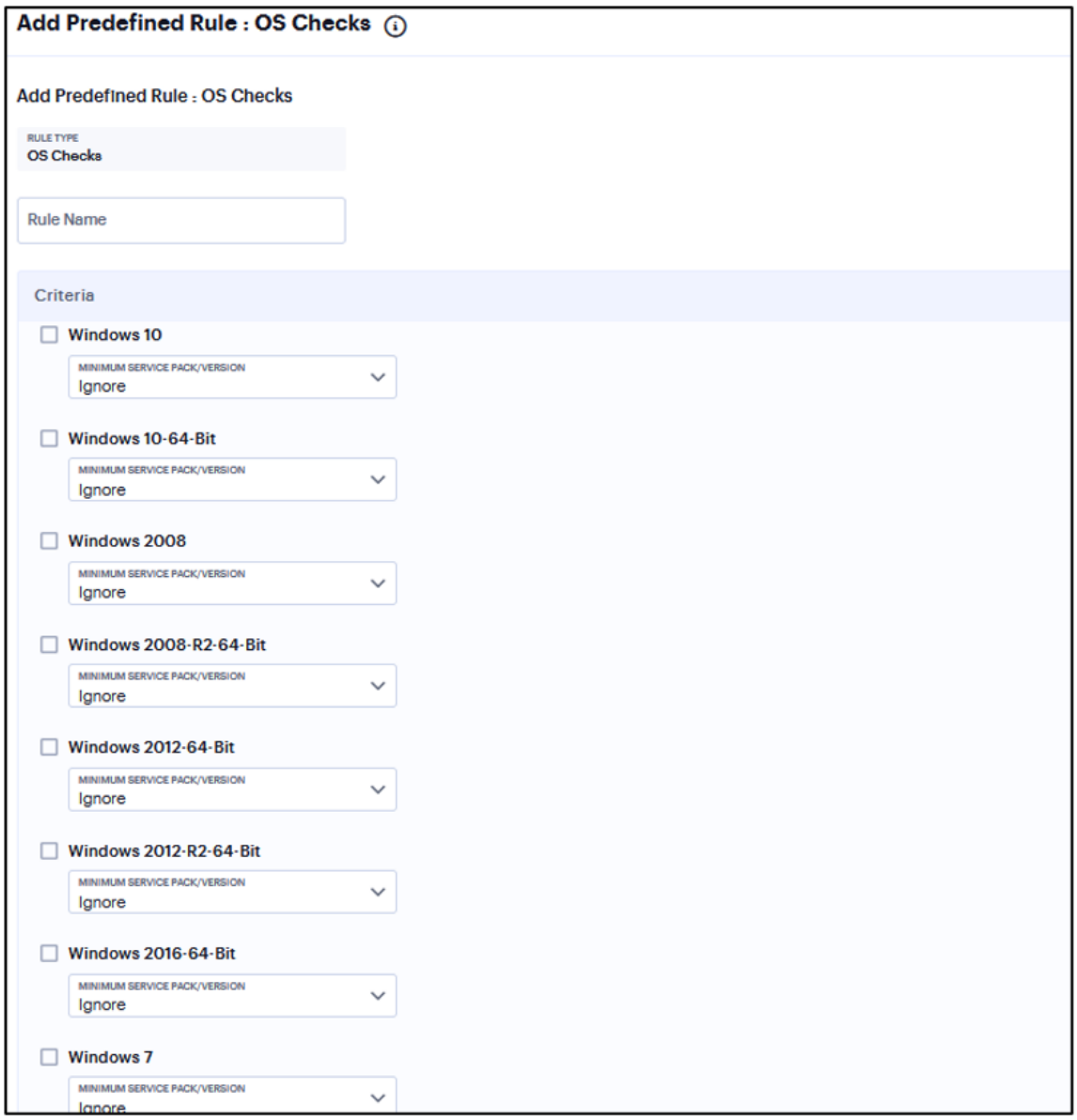


FIGURE 14.12 : CVE Checks

Specifying Customized Requirements Using Custom Rules

In addition to the predefined policies and rules that come with the system, you can create custom rules within a Host Checker policy to define requirements that your users' computers must meet.

Add Rule: Ports

Use this rule type to control 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 device.

To configure the Ports rule:

1. Select one of the following supported platform options:
    - Windows
    - Mac
    - Linux
2. Enter the rule name.
3. Under Criteria, enter the Port list.
4. Click Status and select Required/Deny.
    - Required: Select this to enable access from a listed port.
    - Deny: Select this to disallow access from a listed port.

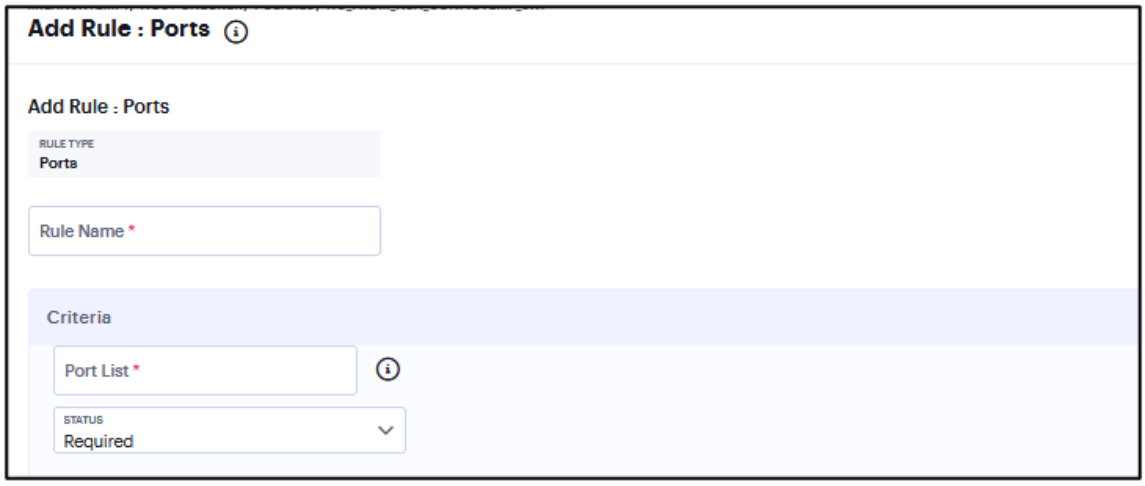


FIGURE 14.13 : Ports

Add Rule: Process

To configure the Process rule:

1. Select one of the following supported platform options:
    - Windows
    - Mac
    - Linux
2. Enter the rule name.
3. Under Criteria, enter the Process name. For example, explorer.exe.

4. Click **Status** and select **Required/Deny**.
    - Required: Select this to allow access if the process exists.
    - Deny: Select this to deny access if the process does not exist.
5. (Optional) Enter the MD5 Checksums/SHA256 Checksums.
6. Select Monitor this rule for change in result to check if there is any change in compliance result.

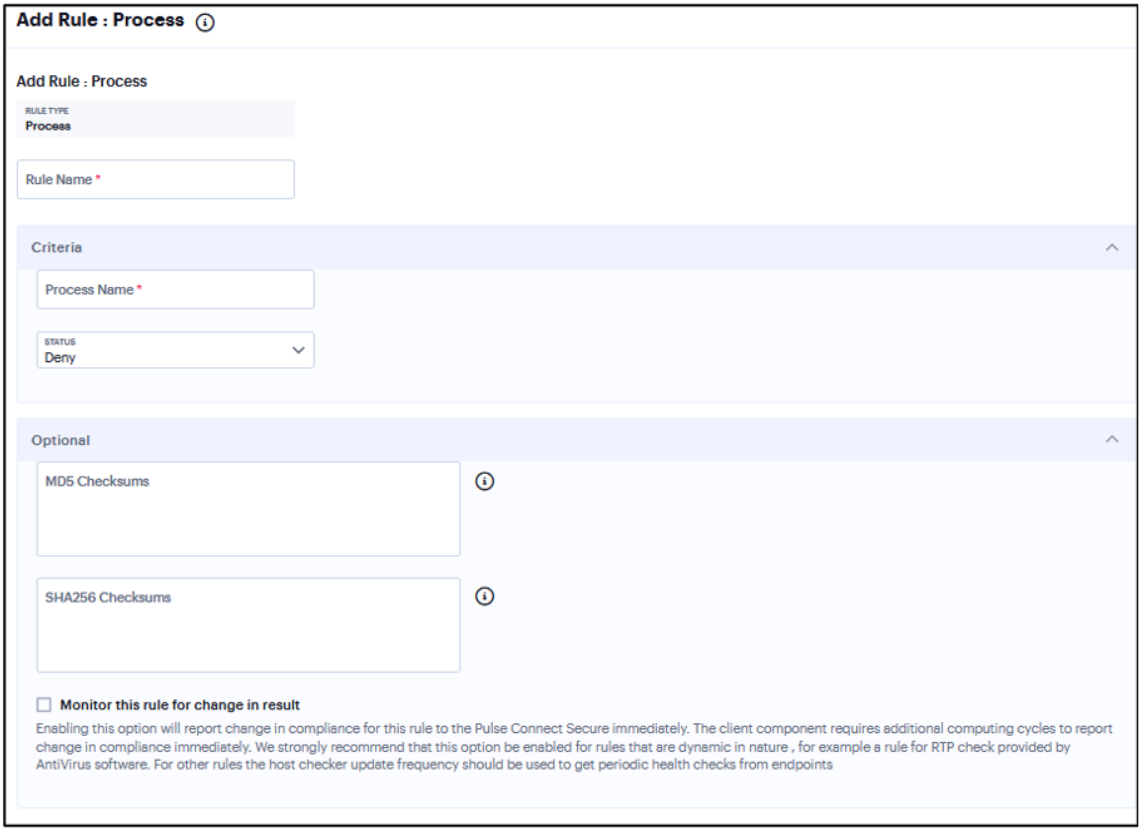


FIGURE 14.14 : Process Rule

Add Rule: File

To configure the File rule:

1. Select one of the following supported platform options:
    - Windows
    - Mac
    - Linux
2. Enter the rule name.
3. Enter a full file name and path in File Name. For example, “c:test.txt” or “/Users/exampleuser/Downloads/test.txt”.
4. Under Criteria, click **Status** and select **Required/Deny**.

- Required: Select this to allow access where the file exists and is valid.
- Deny: Select this to deny access if the file does not exist or is invalid.

5. (Optional) Enter the MD5 Checksums/SHA256 Checksums value for the file.
6. Select Monitor this rule for change in result to check if there is any change in compliance result.

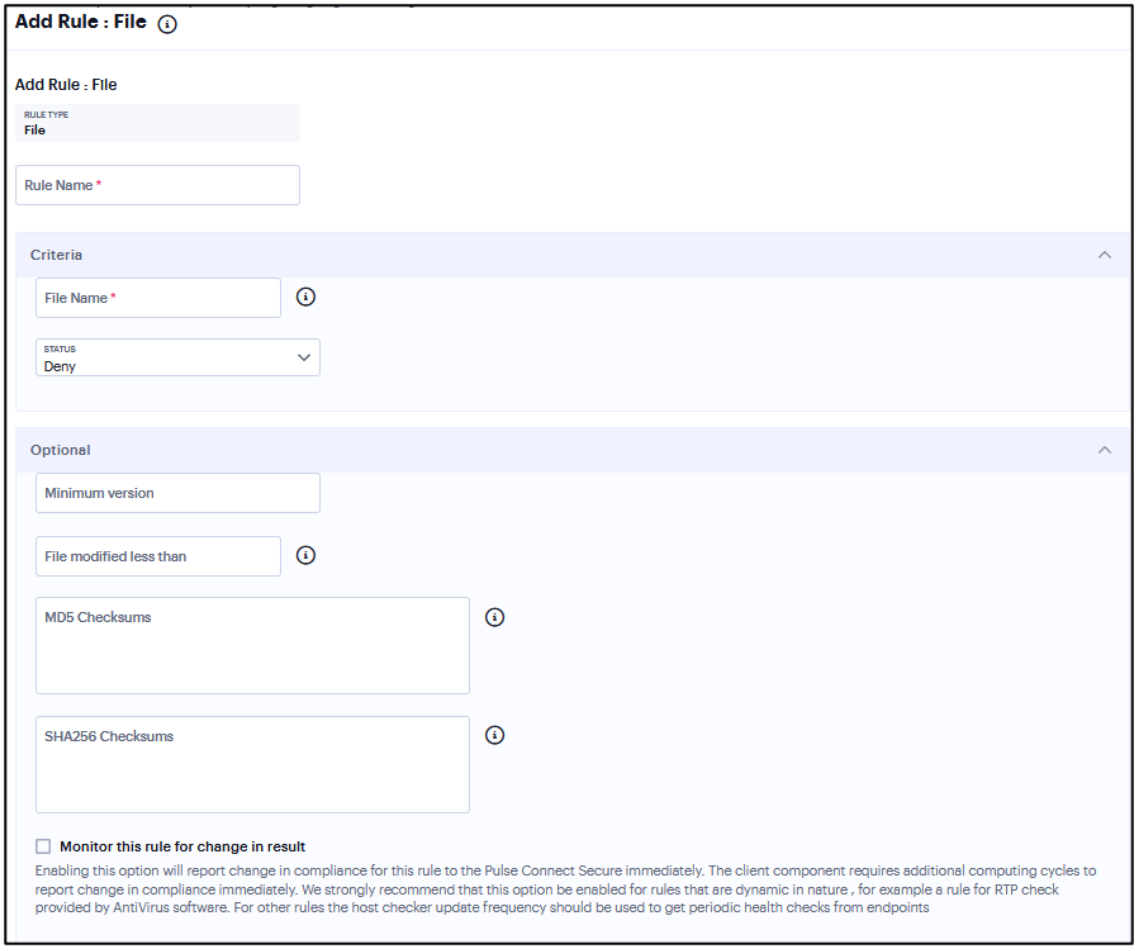


FIGURE 14.15 : File Rule

Add Rule: NetBIOS

To configure the NetBios rule:

1. Select one of the following supported platform options:
   - Windows
   - Mac
2. Enter the rule name.
3. Enter the Netbios domain Names as a comma-separated list (without spaces) of domain names. Each name can be 15 characters. Duplicate names are not supported. For example, WINDOWS-PC,WIN*-PC,*-PC,WINDOWS*

4. Under Criteria, click **Status** and select **Required/Deny**.
    - Required: Select this to allow access from a listed Netbios domain name.
    - Deny: Select this to deny access from a listed Netbios domain name.

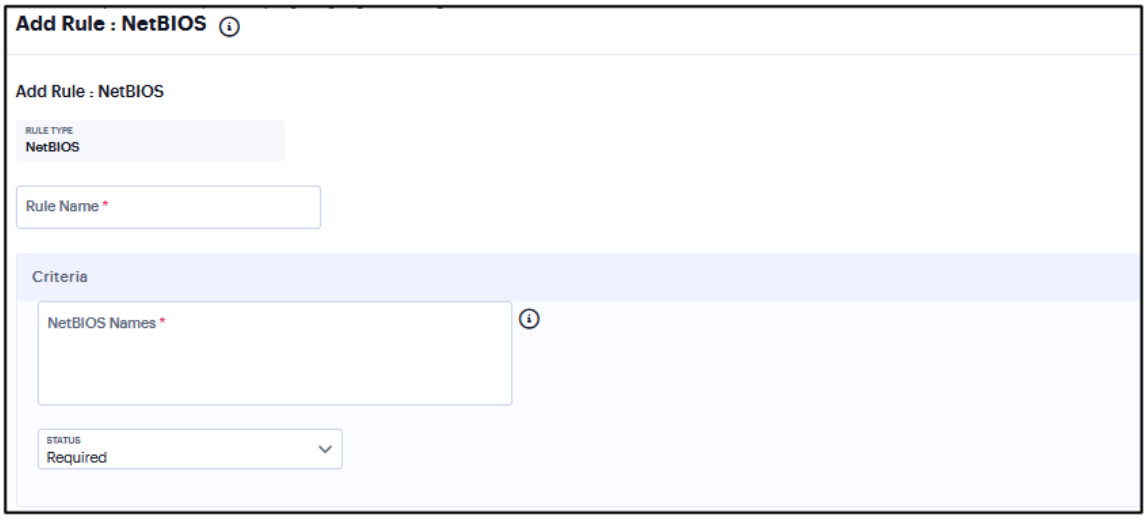


FIGURE 14.16 : NetBIOS Rule

Add Rule: MAC Address

To configure the MAC Address rule:

1. Select one of the following supported platform options:
    - Windows
    - Mac
2. Enter the rule name.
3. Under Criteria, Enter the MAC address as a comma-separated list (without spaces) of MAC addresses in the form HH:HH:HH:HH:HH:HH where the HH is a two-digit hexadecimal number. Duplicate MAC addresses are not supported.
4. Click **Status** and select **Required/Deny**.
    - Required: Select this to enable access from a listed MAC address.
    - Deny: Select this to disallow access from a listed MAC address.

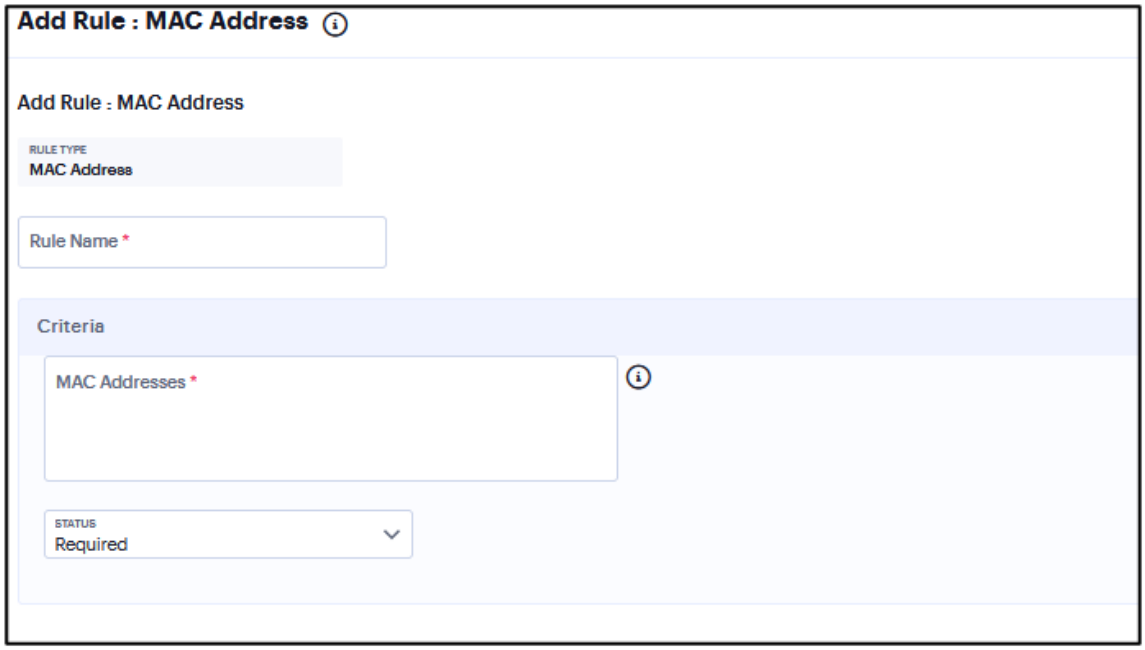


FIGURE 14.17 : MAC Address Rule

Add Rule: Machine Certificate

To configure the Machine Certificate rule:

1. Select one of the following supported platform options:
   - Windows
   - Mac
2. Enter the rule name.
3. Under Criteria, select Any certificate to allow access with any certificate.
4. (Optional) Enter specific values in the machine certificate.

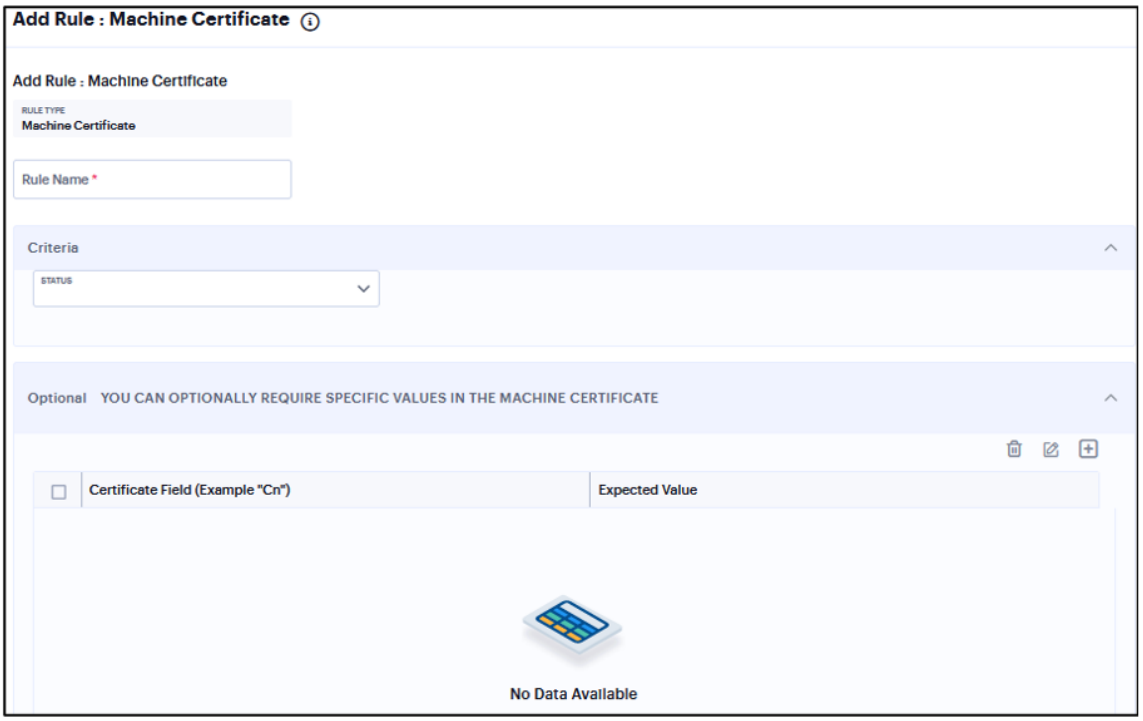


FIGURE 14.18 : Machine Certificate

Add Rule: Registry Setting

Note that Registry Setting rule is applicable only to Windows platform.

To configure the Registry Setting rule:

1. Enter the rule name.
2. Under Criteria, select one of the following options:
   - HKEY_LOCAL_MACHINE
   - HKEY_USERS
   - HKEY_CURRENT_USER
   - HKEY_CURRENT_CONFIG
   - HKEY_CLASSES_ROOT
3. Enter a Subkey for the registry path.
4. Under Key Type, select one of the following key types:
   - string
   - dword
   - binary
5. Enter a Key name.
6. Enter a Value for the registry key.

7. Select the 64-bit check box to use the 64-bit registry store. Clear this check box to use the 32-bit registry store.
8. (Optional) Select Monitor this rule for change in result to check if there is any change in compliance result.
9. Under Optional, select Monitor this rule for change in result to continuously monitor the policy compliance of endpoints.

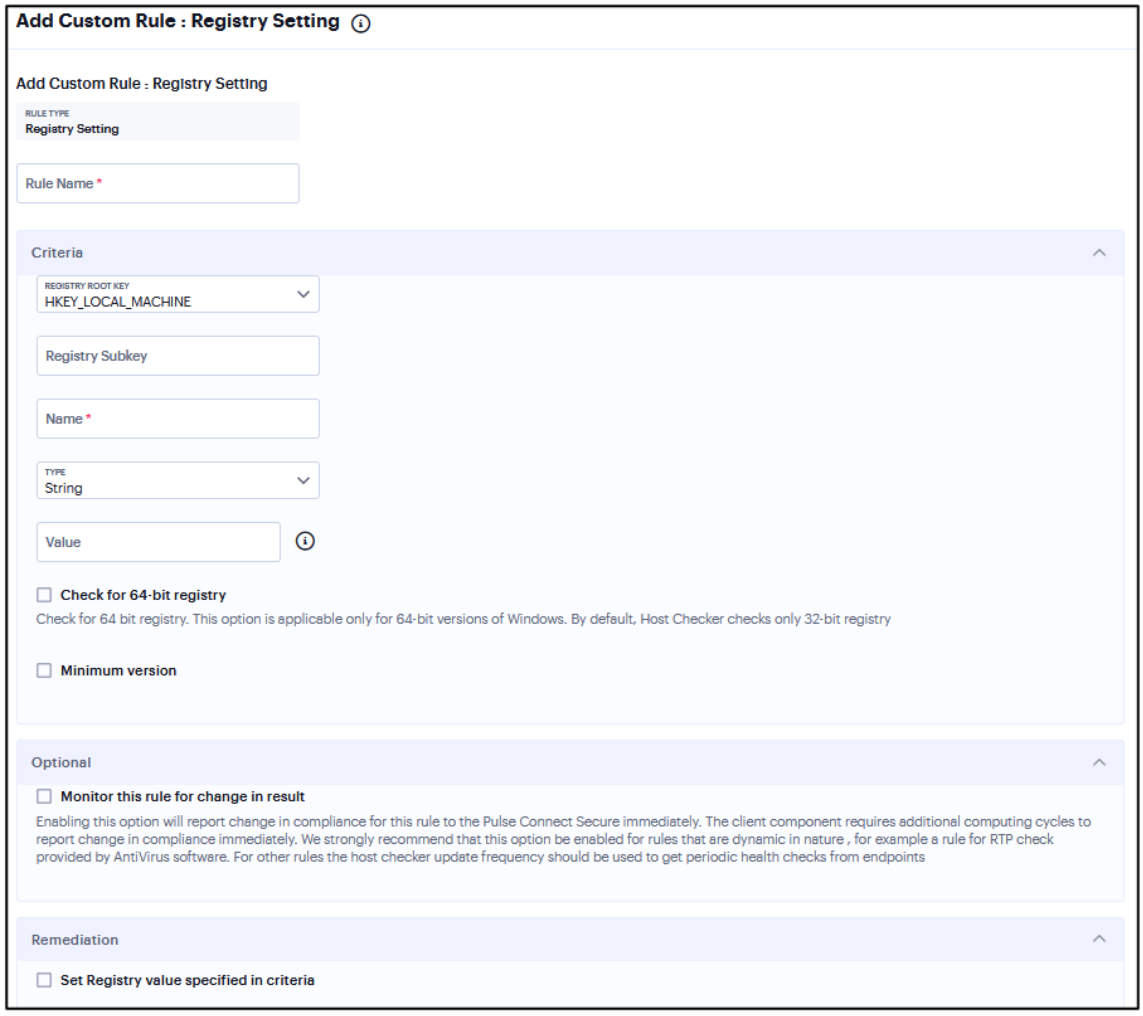


FIGURE 14.19 : Registry Setting

Add Rule: Advanced Host Checking

Note that Advanced Host Checking rule is applicable only to Windows platform.

To configure the Advanced Host Checking rule:

1. Enter the rule name.
2. Under Criteria, select one of the following options:
    - ports
    - process

- File
- NETBIOS
- MAC Address

3. Enable Required/Deny.
4. Select the registry root key- HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_USER, HKEY_CURRENT_CONFIG, or HKEY_CLASSES_ROOT.
5. Enter the registry subkey.
6. Enter the name of the registry.
7. Select the type of the registry- String, Binary, or DWORD.
8. Select “Check for 64-bit registry” to check the 64 bit registry on Windows. The default is 32 bit registry.

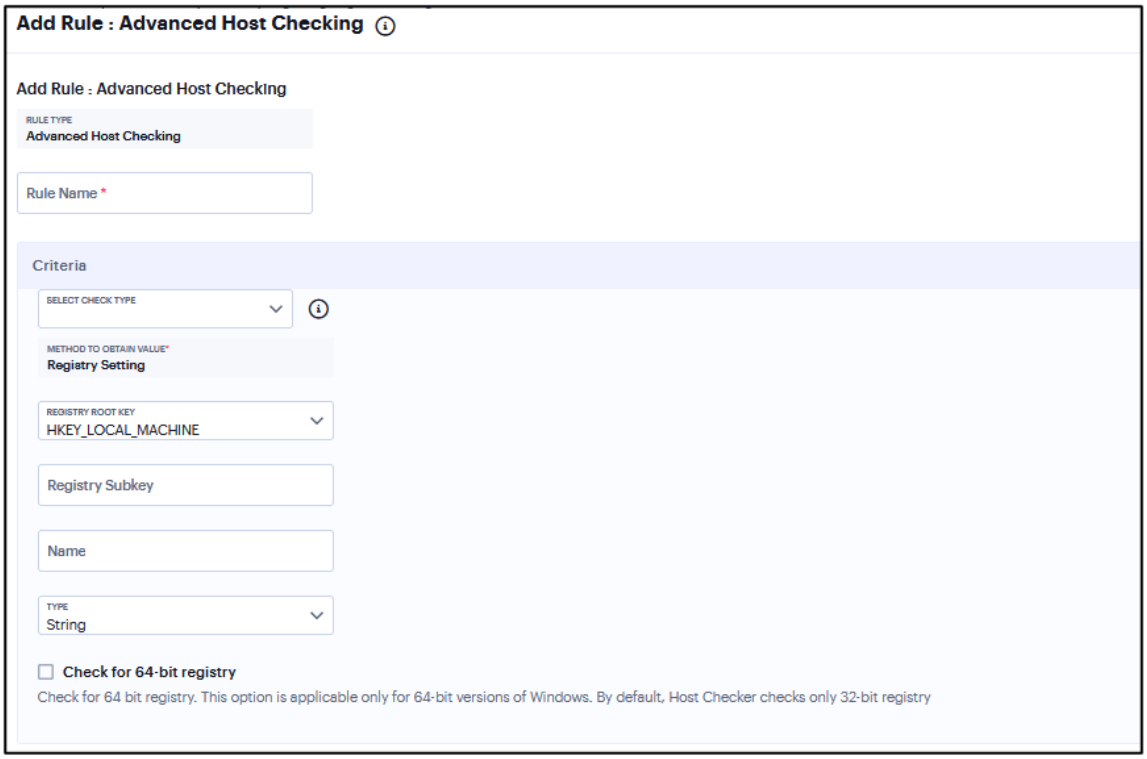


FIGURE 14.20 : Advanced Host Checking

Add Rule: Jail Breaking Detection

Note that Jail Breaking Detection rule is applicable only to iOS platform.

To configure the Jail Breaking Detection rule:

1. Select one of the supported iOS platform options.
2. Enter the rule name.
3. Under Criteria, select **Don’t allow Jail Broken devices**

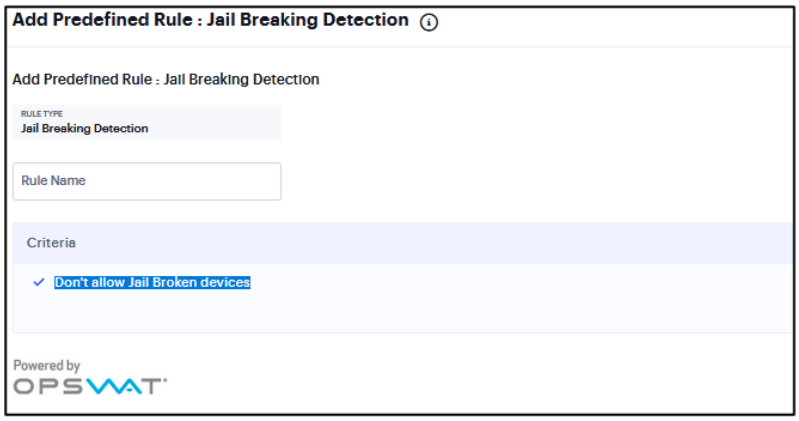


FIGURE 14.21 : Jail Breaking Detection

Add Rule: Rooting Detection

To configure the Rooting Detection rule:

1. Select one of the supported android platform options.
2. Enter the rule name.
3. Under Criteria, select **Don't allow Rooted devices**.

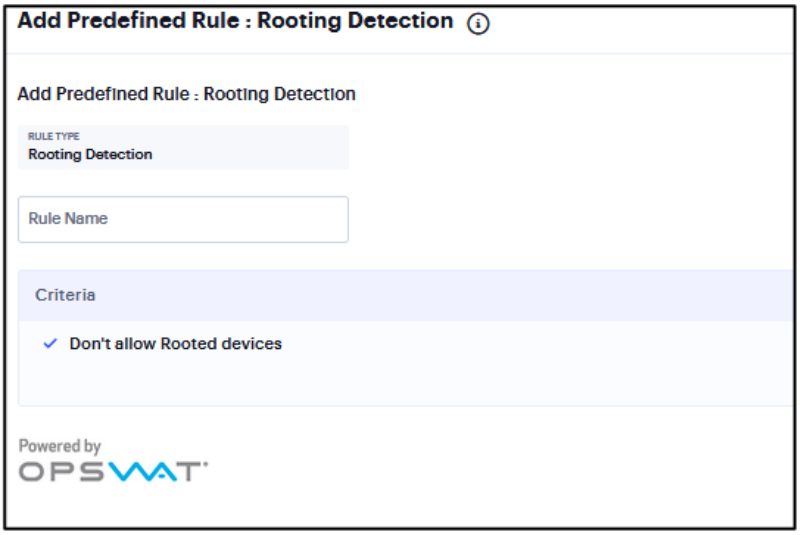


FIGURE 14.22 : Rooting Detection

Users Configuration

Configuring User Realm

The user realm configuration associates the authentication server data and MDM server data with user roles.

To configure user realm:

1. Log into the nSA as a Tenant Admin.
2. From the ICS menu, click the **Gateway > Gateway List** and then select any standalone ICS Gateway and Cluster node.
3. Navigate to **Users > User Realms**.
4. In the User Realms page, click the Add icon.

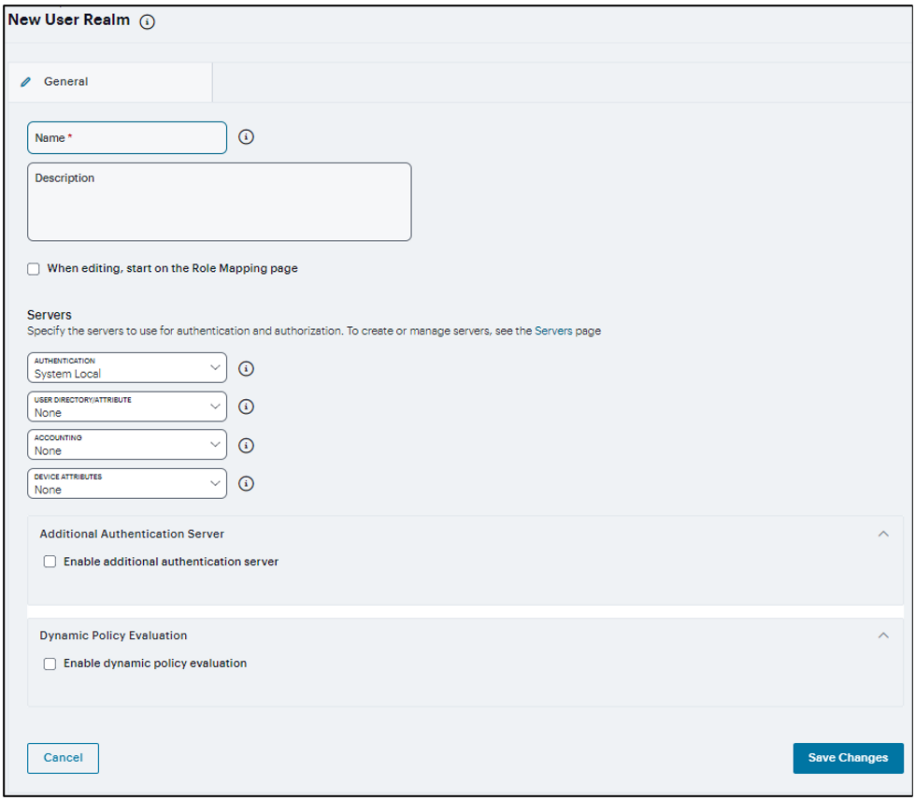


FIGURE 15.1 : Configure User Realm

1. Enter a name and description for the realm.
2. Under Servers, select the user authentication server for this realm's users.
3. If you want to use dynamic policy evaluation for this realm, select **Dynamic policy evaluation** to enable an automatic timer for dynamic policy evaluation of this realm's authentication policy, role mapping rules, and role restrictions:
   - Use the **Refresh interval** option to specify how often you want Connect Secure to perform an automatic policy evaluation of all currently signed-in realm users.
   - Select **Refresh roles** to also refresh the roles of all users in this realm.
   - Select **Refresh resource policies** to also refresh the resource policies for all users in this realm.
   - Click **Refresh Now** to manually evaluate the realm's authentication policy, role mapping rules, role restrictions, user roles, and resource policies of all currently signed-in realm users.
4. Click **Save Changes** to create the realm.

Configuring User Role

A user role is an entity that defines user session parameters, personalization settings, and enabled access features. You can customize a user role by enabling specific access features, defining Web, application, and session bookmarks, and configuring session settings for the enabled access features.

To add a new user role:

1. Log into the nSA as a Tenant Admin.
2. From the ICS menu, click the **Gateway > Gateway List** and then select any standalone ICS Gateway and Cluster node.
3. Navigate to **Users > User Roles**.
4. In the User Roles page, click the Add icon.

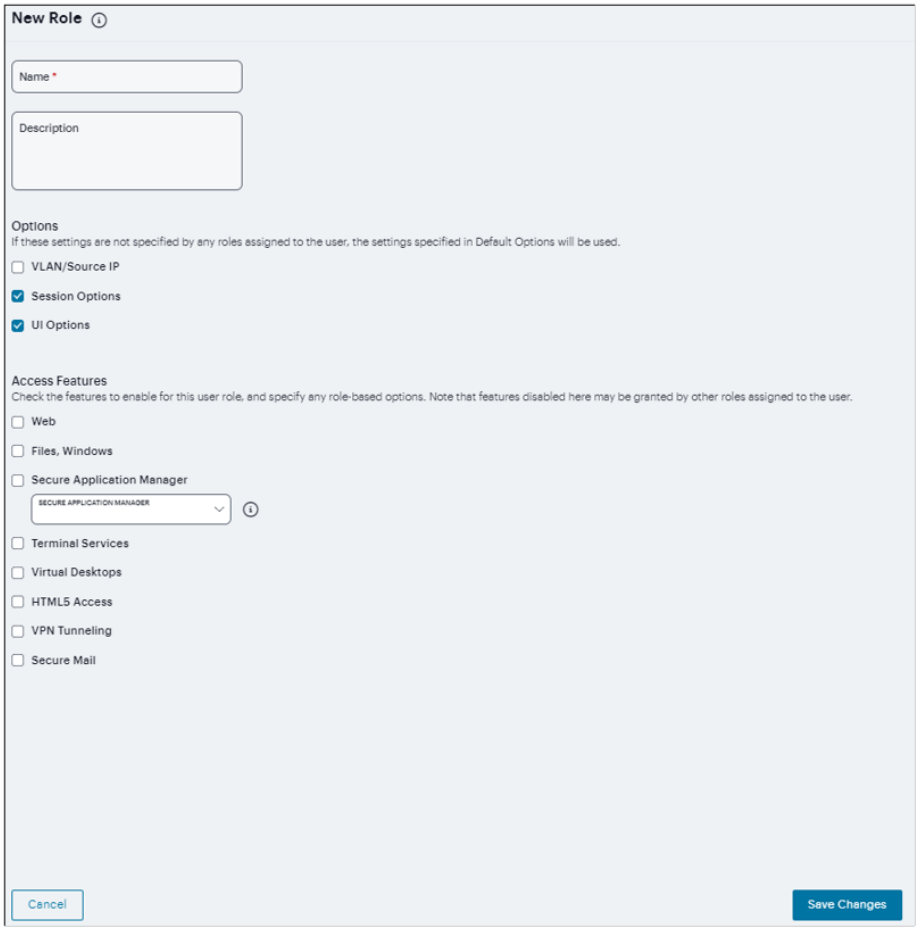


FIGURE 15.2 : Configure User Role

5. Enter a name and optionally a description.
6. Under Options:
   - Select the **VLAN/Source IP** option to apply the role settings configured on the General > VLAN/Source IP page.

- Select the **Session Options** option to apply the role settings in the General > Session Options page to the role.
- Select the **UI Options** option to apply the role settings in the General > UI Options page to the role.

7. Under Access features, select the features you want to enable for the role. Options include:
   - Web - intermediate Web URLs through the Content Intermediation Engine.
   - Files, Windows - resource profile that controls access to resources on Windows server shares.
   - Secure Application Manager (Windows version or Java version) - provides secure, application-level remote access to enterprise servers from client applications.
   - Terminal Services - enable terminal emulation sessions on a Windows terminal server, Citrix NFuse server, or Citrix Metaframe server.
   - Virtual Desktops - enable virtual desktop session using the VDI architecture.
   - HTML5 Access - enable HTML5 session for RDP connection, telnet connection, SSH session or VNC connection.
   - VPN Tunneling - provides secure, SSL-based network-level remote access to all enterprise application resources using the system.
   - Secure Mail - enables automatic synchronization with an Exchange server (ActiveSync) and e-mail encryption for iOS devices that have the Ivanti Secure Access Client.
8. Click **Save Changes** to apply the settings to the role.

Resource Profiles

A resource profile contains all of the resource policies, role assignments, and end-user bookmarks required to provide access to an individual resource. Resource profiles simplify resource configuration by consolidating the relevant settings for an individual resource into a single page within the admin console.

The system comes with two types of resource profiles:

- Standard resource profiles enable you to configure settings for a variety of resource types, such as web sites, client/server applications, directory servers, and terminal servers. When you use this method, you choose a profile type that corresponds to your individual resource and then provide details about the resource.
- Resource profile templates enable you to configure settings for specific applications. When you use this method, you choose a specific application (such as the Citrix NFuse version 4.0). Then, the system pre-populates a

variety of values for you based on your chosen application and prompts you to configure additional settings as necessary.

Resource profiles are an integral part of the access management framework, and therefore are available on all Ivanti Connect Secure products. However, you can only access resource profile types that correspond to your licensed features.

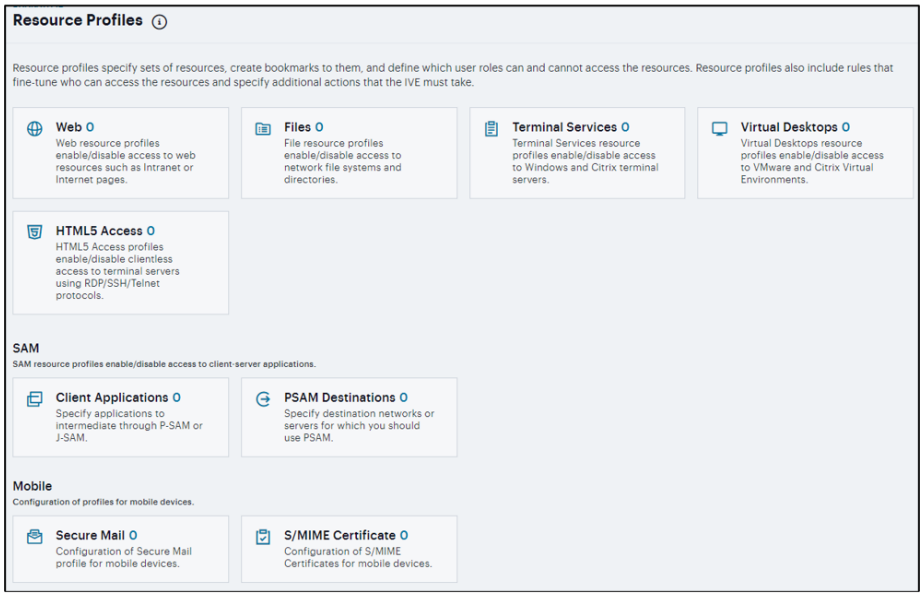


FIGURE 15.3 : Resource Profiles

Web Resource Profile

To Create new Web Application Resource Profiles:

1. Log into the nSA as a Tenant Admin.
2. From the ICS menu, click the **Gateway > Gateway List** and then select any standalone ICS Gateway and Cluster node.
3. Navigate to **Users > Resource Profiles > Web**.
4. Click '**+**' and select the Profile Template from drop down.

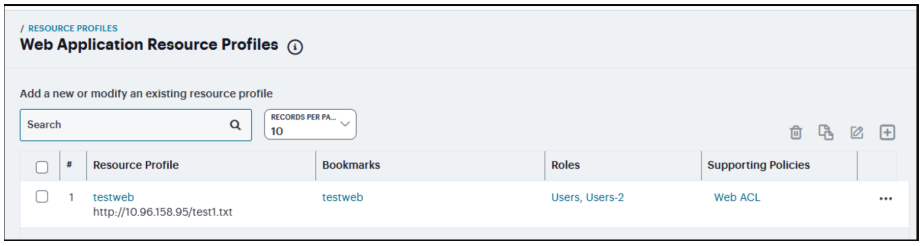


FIGURE 15.4 : Web Application

5. Enter a unique **Name** and optionally a **Description** for the profile.

Citrix Storefront Server

If you have the Citrix StoreFront 31. and above, you can create a Web template to allow users to access Citrix applications without the need for a Citrix client. Users must have one of the following browser versions (or later) to support HTML5 and Websockets:

- Internet Explorer 10
- Safari 6
- Google Chrome 23
- Mozilla Firefox 17

If **Citrix resource profile** selected as Profile Template, then

1. Enter the URL of the **Citrix StoreFront Web** server in the **Base URL** field. Use the format: [protocol://]host[:port][/path]. The system uses the specified URL to define the default bookmark for the Citrix resource profile.
2. Under **Citrix Settings**, select the **ICA Client Access** option. Admin can either choose to go with the HTML5 way of delivery or can choose to deliver ICA over CTS/PSAM/HTML5 Access clients. If admin chooses the ICA over CTS/PSAM/HMTL5 Access, the corresponding ACL should be created and when ICS rewrites ICA content it should launch the appropriate client. Add the Number of servers/applications and Citrix Ports which require ICA client access.

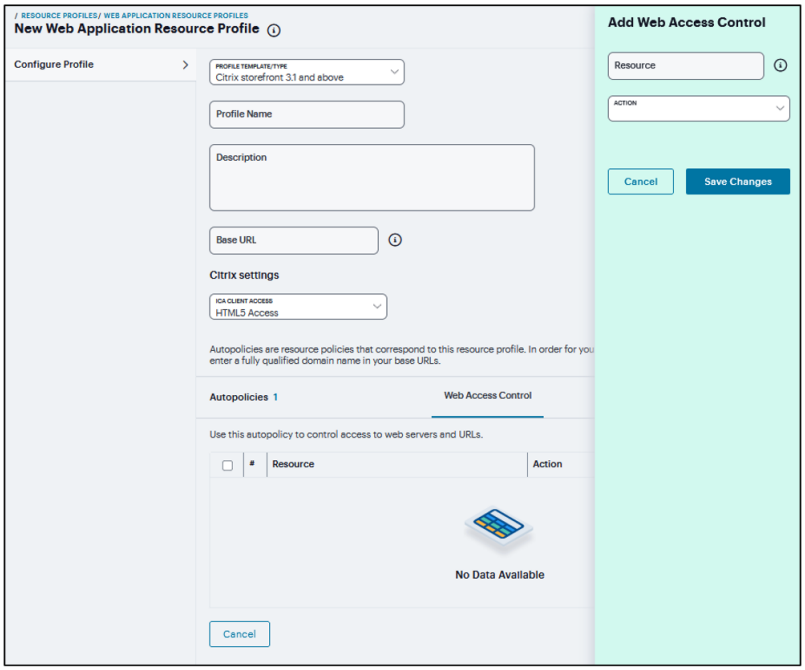


FIGURE 15.5 : Citrix Resource Profile

3. Click **Add Autopolicy**, **Web Access Control** or **Single Sign-on** check box to create a policy and click **Add Selected**.

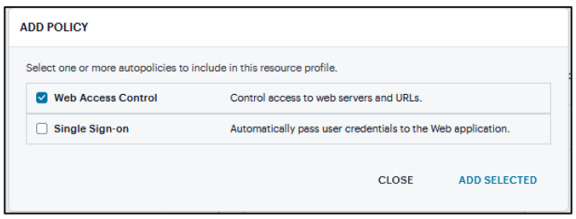


FIGURE 15.6 : Autopolicy

4. Under **Web Access Control**, click '**+**' specific Resource under the Base URL. Enter the full URL of the resource, select **Allow** or **Deny**, and click **Save Changes**. By default, the system automatically creates a policy that enables access to the resource and all of its subdirectories.

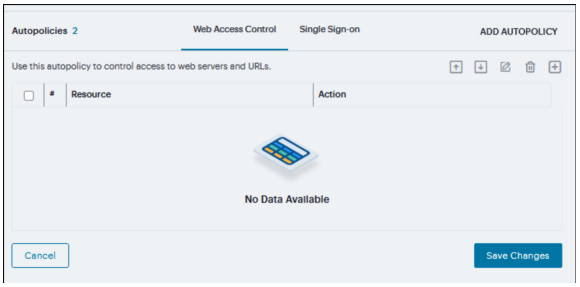


FIGURE 15.7 : Web Access Control

5. Under **Single Sign-on**, select the **POST the following data** check box and specify the application's sign-in page in **Resource** field and In **Post URL** field, specify the absolute URL where the application posts the user's credentials.
    - In the Resource field, specify the application's sign-in page, such as: http://my.domain.com/public/login.cgi. Wildcard characters are not supported in this field.
    - In the Post URL field, specify the absolute URL where the application posts the user's credentials, such as: http://yourcompany.com/login.cgi.
6. Select the **Deny direct login for this resource** check box if you do not want to allow users to manually enter their credentials in a sign-in page. Users may see a sign-in page if the form POST fails.
7. Select the **Allow multiple POSTs to this resource** check box if you want to send POST and cookie values to the resource multiple times if required.
8. Optionally, click '+' specify the **Label, Name, Value, and select User modifiable, click **Save Changes**.**
    - Label - The name used to identify the data.
    - Name - The name used to identify the data in the Value field. The back-end application should expect this name.
    - Value - The value to post to the form for the specified Name. You can enter static data, a system variable, or system session variables containing username and password values.

- User modifiable? - Select Not modifiable to prevent users from changing the information in the Value field. Select User CAN change value to allow users to specify data for a back-end application. Select User MUST change value if users must enter additional data to access a back-end application.

9. To post header data to the specified URL select the **Send the following data as request headers** check box.
10. Specify the **Resources** to which this policy applies.
11. Optionally, click '**+**' specify the **Header name** and **Value** and click **Save Changes**.

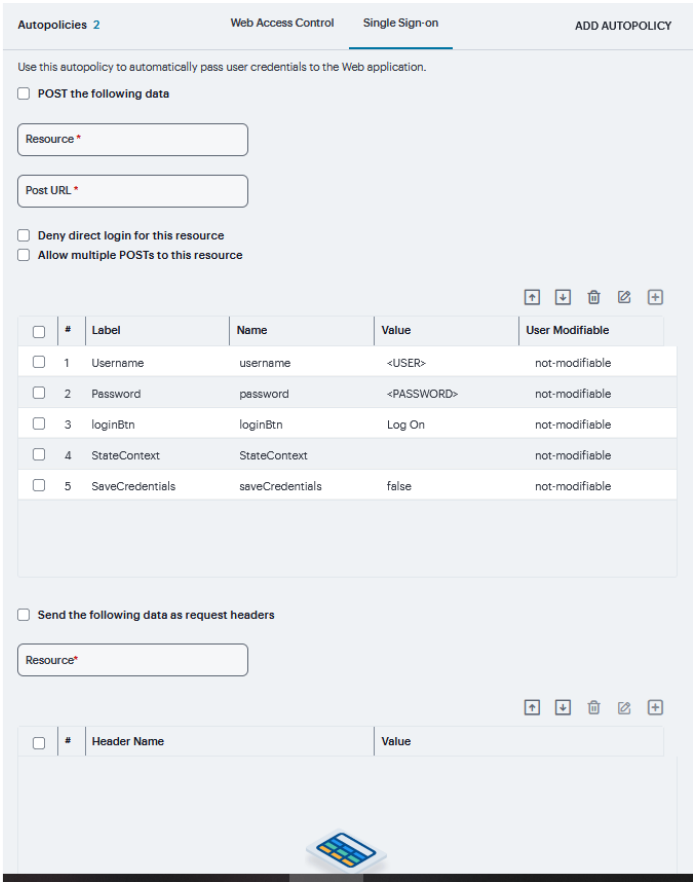


FIGURE 15.8 : Web Access Control

Hosted Java Applet

The Java applet upload feature enables you to store the Java applets of your choice directly on the device without employing a separate Web server to host them. When you use this feature, you simply upload the applets to the device (along with additional files that the applets reference) and create a simple Web page through the system that references the files. Then, the system intermediates the Web page and Java applet content using its Content Intermediation Engine.

For example, you might want to use the system to intermediate traffic between an IBM AS/400 system on your network and individual 5250 terminal emulators on your

users' computers. To configure the system to intermediate this traffic, obtain the 5250 terminal emulator's Java applet. Then you can upload this applet to the system and create a simple Web page that references the applet. After you create the Web page through the system, it creates a corresponding bookmark that users can access through their home pages.

If **Hosted Java applet** is selected as Profile Template, then

1. Select the Java applet that you want to associate with the resource profile from the **Applet to use** list. Or, if the applet that you want to use is not currently available in the list, click **Edit list**.

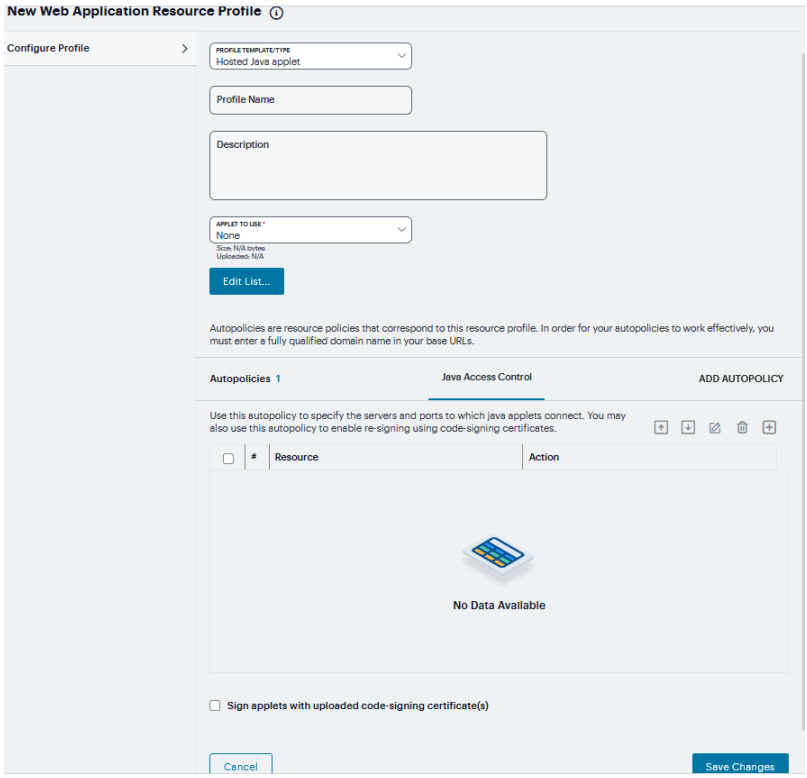


FIGURE 15.9 : Hosted Java Applet

1. Click '**+**' to add an applet to this list.

Note: If you replace an existing archive, make sure that the new applet archive contains all of the necessary files for the applet to successfully launch and run. If the associated HTML for the applet refers to files that do not exist in the new archive, then the applet will not function correctly.

---

2. Enter **Name** to identify the applet.
3. Click the text field to browse to the applet that you want to upload.
4. Select the **Uncompress archive file** check box if the file that you selected is an archive that contains the applet. Click **OK**.

FIGURE 15.10 : New Applet

Note: When you select an applet in the Java Applets dialog box, you are loading third-party software onto the Ivanti product. By clicking OK, you are agreeing to the following terms on behalf of yourself (as purchaser of the equipment) or the organization that purchased the Ivanti product, as applicable.

2. Click **Add Autopolicy**, select **Java Access Control to enable access** if your Java applets need to make socket connections.

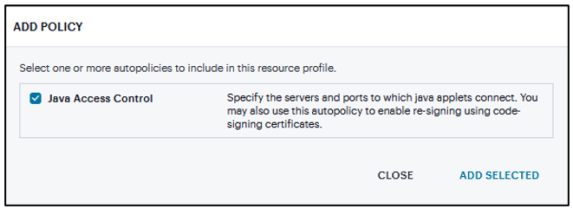


FIGURE 15.11 : Hosted Java Applet

3. Click '**+**' specific **Resource** under the Base URL. Enter the full URL of the resource, select **Allow** or **Deny**, and click **Save Changes**.

FIGURE 15.12 : Java Access Conytrol

4. Select the **Sign applets with uploaded code-signing certificate(s)** to use a single code-signing certificate to resign all Java applets.
5. Click **Save Changes**.

Microsoft RDWeb

A Microsoft RDWeb template is a resource profile that controls access to the published desktops and applications based on HTML5. Microsoft RDWeb templates significantly reduce the configuration time by consolidating configuration settings into one place and by pre-populating a variety of resource policy settings.

If **Microsoft RDWeb** resource profile selected as Profile Template, then

1. Enter the URL of the Microsoft RDWeb server in the **Base URL** field.
2. Click **Add Autopolicy**, **Web Access Control** check box to create a policy and click **Add Selected**.

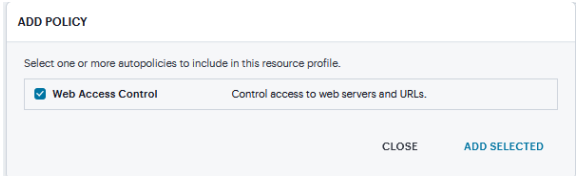


FIGURE 15.13 : Web Access Control

3. Under **Web Access Control**, click '**+**' specific **Resource** under the Base URL. Enter the full URL of the resource, select **Allow** or **Deny**, and click **Save Changes**.

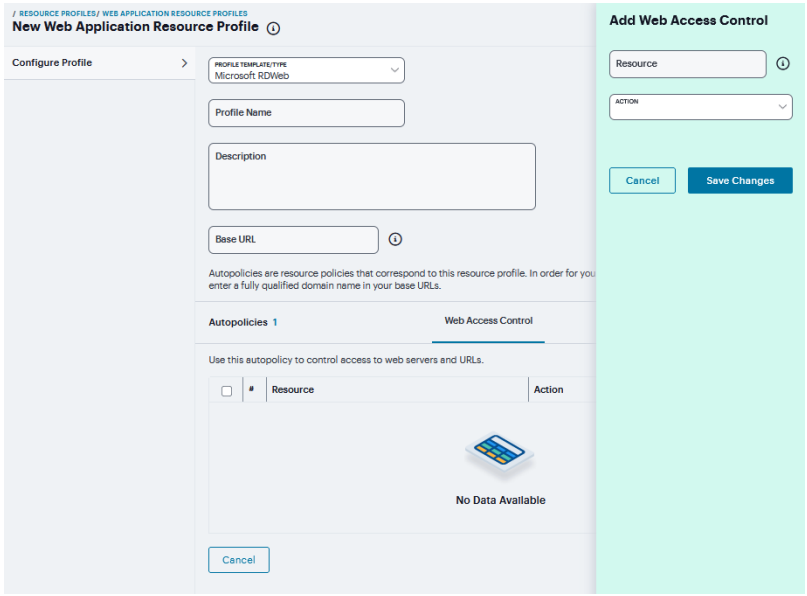


FIGURE 15.14 : Microsoft RDWeb

Microsoft OWA Versions

A Microsoft Outlook Web Access (OWA) template is a resource profile that controls access to the application and configures OWA settings as necessary. OWA templates significantly reduce your configuration time by consolidating configuration settings into one place and by prepopulating a variety of resource policy settings for you depending on the type of setup you select. The system supports intermediating traffic to Microsoft OWA through a Web rewriting resource profile template, JSAM, PSAM, and VPN Tunneling. This topic describes how to configure access using the Web rewriting template. The prepopulated values vary depending on the version of OWA you select and are based on the most common deployment of the servers.

If any of the **Microsoft OWA** Versions are selected as Profile Template, then

1. Enter the URL of the OWA resource to which you want to control access In the **Base URL** box.
2. Under **OWA settings**, select **Security Settings** and Select **Prevent download of attachments** to prohibit users from downloading attachments to their systems.
3. Select **Prevent upload of attachments** to prevent users from transmitting (uploading) attachments to the system.

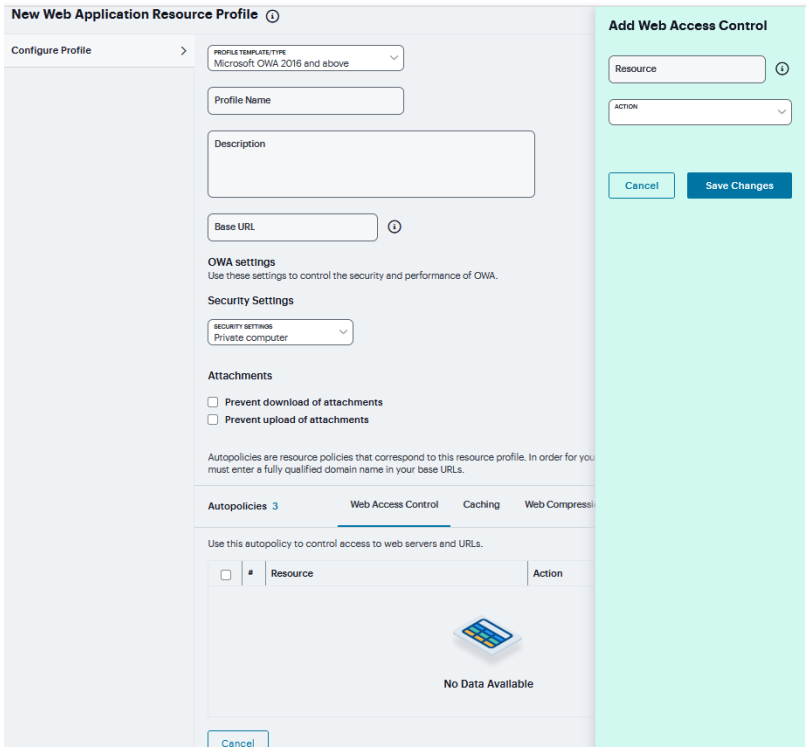


FIGURE 15.15 : Microsoft OWA

4. Click **Add Autopolicy**, check box to create a policy and click **Add Selected**.

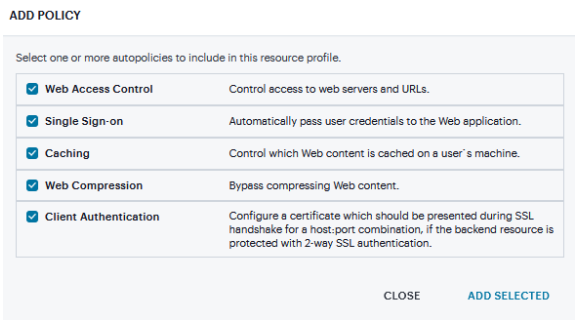


FIGURE 15.16 : Autopolicy

5. Under **Web Access Control**, click '**+**' specific **Resource** under the Base URL. Enter the full **URL** of the resource, select **Allow** or **Deny**, and click **Save Changes**.

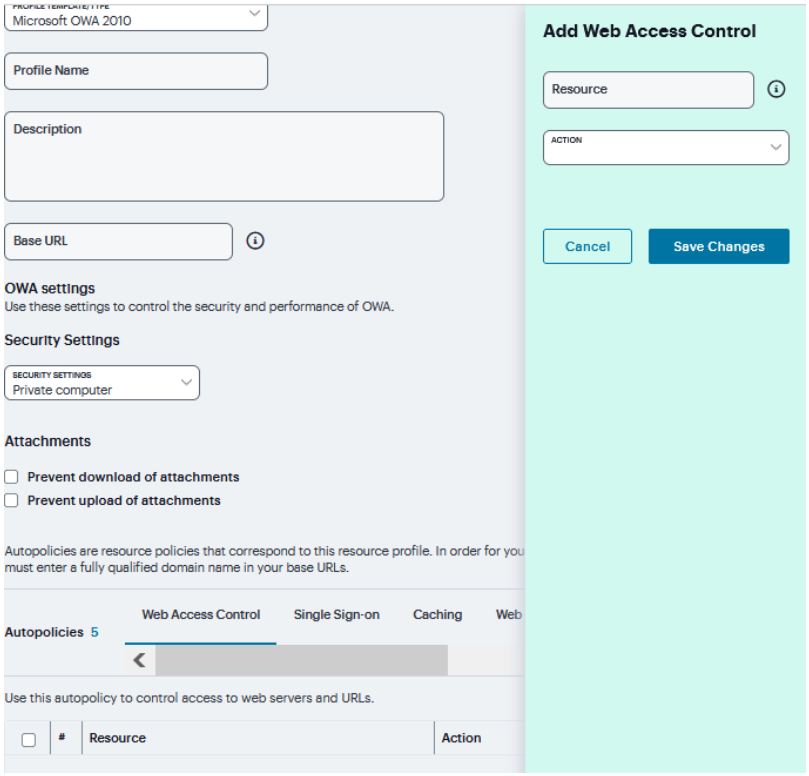


FIGURE 15.17 : Web Access Control

6. Under **Single Sign-on**, **select the SSO** from drop down and specify the application's sign-in page in **Resource** field and select user's **credentials**.
7. Check **Fallback to NTLM V1** to enable fallback option and click **Save Changes**.

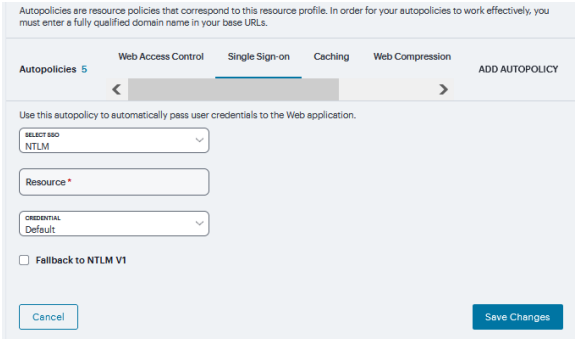


FIGURE 15.18 : Single Sign-on

8. Under **Caching**, click '**+**' and specify the resources to which this policy applies in the **Resource** filed and select the **Action** from drop down and click **Save Changes**.

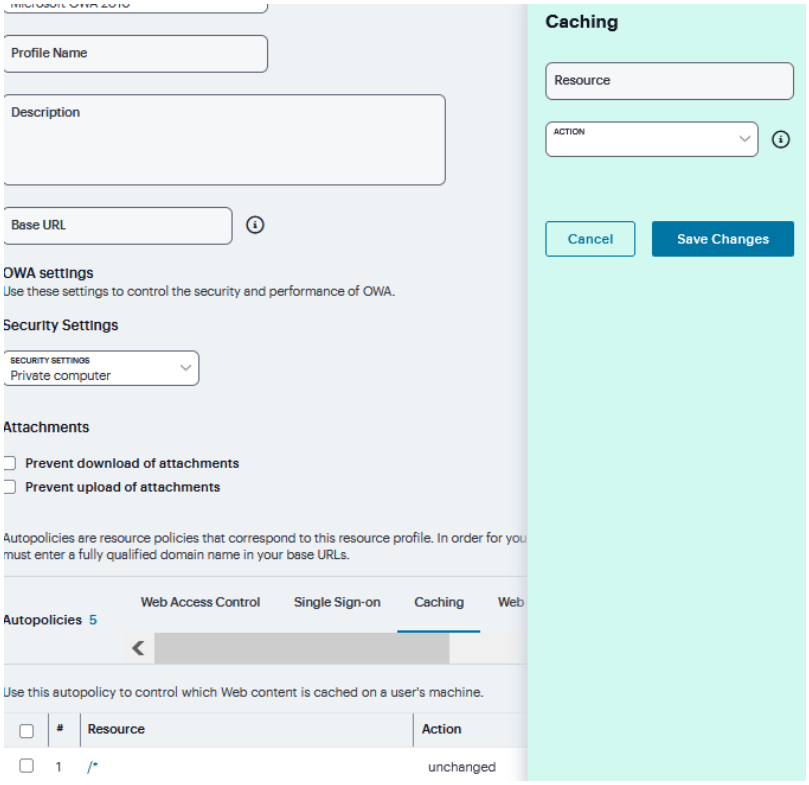


FIGURE 15.19 : Caching

9. Under **Web Compression**, click '**+**' and specify the resources to which this policy applies in the **Resource** filed and select the **Action** from drop-down and click **Save Changes**.

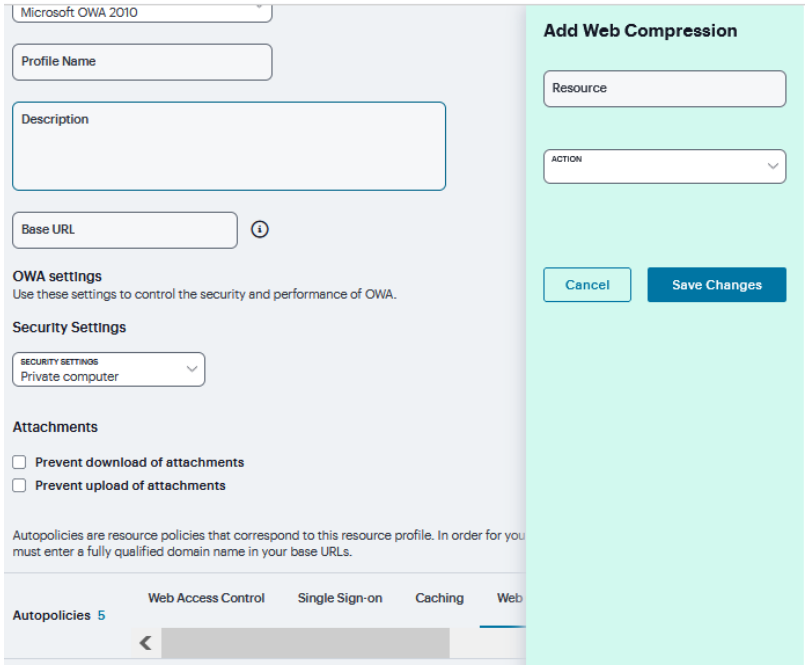


FIGURE 15.20 : Web Compression

10. Under **Client Authentication**, click '**+**' and specify the resources to which this policy applies in the **Resource** filed and select the **Certificate** from drop down and click **Save Changes**.

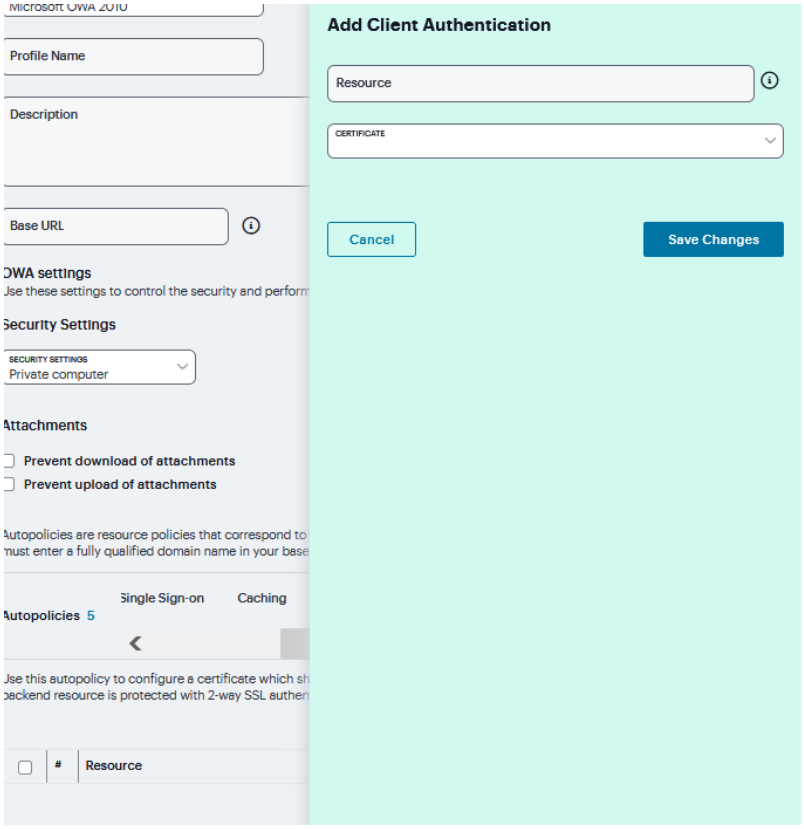


FIGURE 15.21 : Client Authentication

Lotus iNotes Versions

A Lotus iNotes template is a resource profile that controls access to the Web application and configures iNotes settings as necessary. Lotus iNotes templates significantly reduce your configuration time by consolidating settings into one place and by prepopulating a variety of resource policy settings for you depending on the type of setup you select.

The system supports intermediating traffic to Lotus iNotes through a Web rewriting resource profile template, JSAM, PSAM, and VPN Tunneling. This topic describes how to configure access using the Web rewriting template. The prepopulated values vary depending on the version of iNotes you select and are based on the most common deployment of the servers.

If any of the **Lotus iNotes** versions resource profile are selected as Profile Template, then

1. Enter the **URL** of the Lotus iNotes resource to which you want to control access In the Base URL box.
2. Under **iNotes settings**, select **Caching Settings**, select **Allow caching on client** to let Web browsers store non-user data, such as Javascript and CSS files, on a user's machine. Select **Minimize caching on client to allow** the system to send a cache-control:no-store header or a cache-control:no-cache header based on the user's Web browser and content type. This is the same as smart caching.

   The Allow caching on client option caches content that the backend iNotes server typically caches. This caching option improves performance by using the cached content instead of retrieving the content from the server the next time the page displays. The Minimize caching on client option provides security by sending a cache-control:no-store header or a cache-control:no-cache header to either not store content or to re-validate the cached content each time it is requested. With both caching option, you can choose to either allow or prevent the uploading or downloading of attachments.
3. Select **Prevent download of attachments** to prohibit users from downloading attachments to their systems.
4. Select **Prevent upload of attachments** to prevent users from transmitting (uploading) attachments to the system.

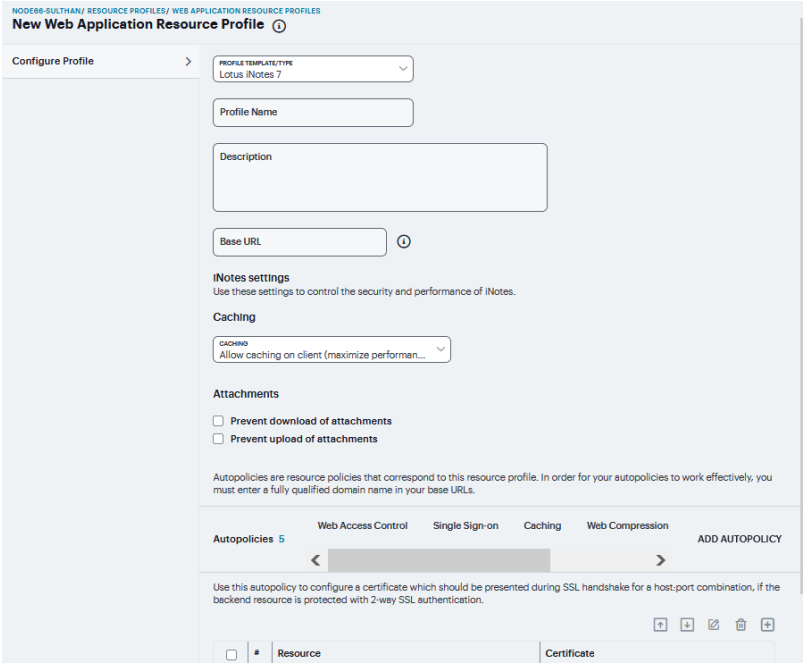


FIGURE 15.22 : Lotus iNotes

5. Click **Add Autopolicy**, check box to create a policy and click **Add Selected**.

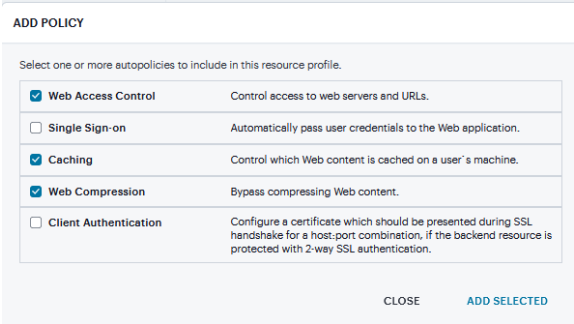


FIGURE 15.23 : Autopolicy

6. Under **Web Access Control**, click '**+**' specific **Resource** under the Base URL. Enter the full URL of the resource, select **Allow** or **Deny**, and click **Save Changes**.

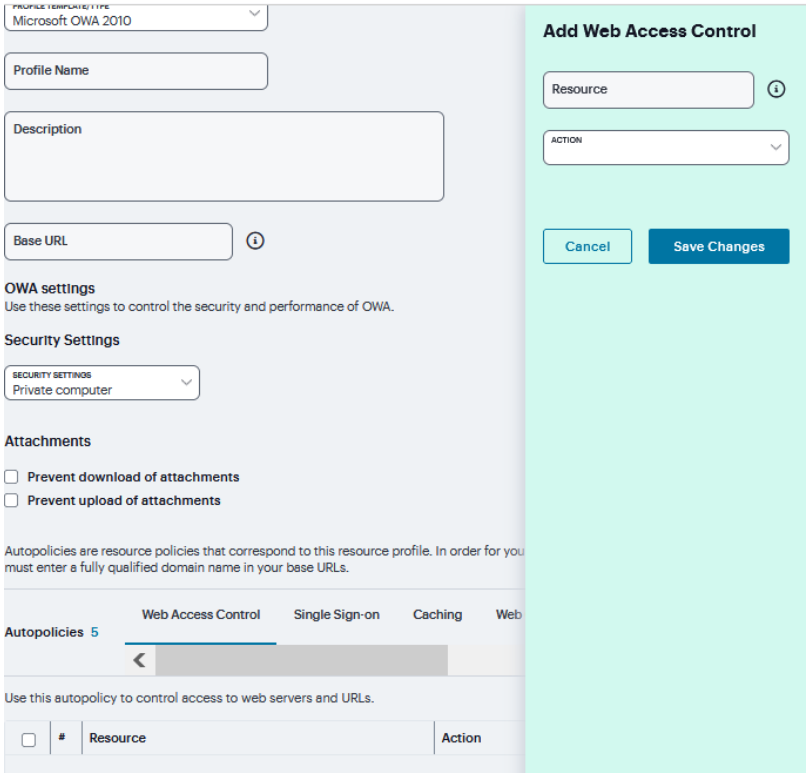


FIGURE 15.24 : Web Access Control

7. Under **Single Sign-on**, select the **SSO** from drop down and specify the application's sign-in page in **Resource** field and select user's **Credentials** and click **Save Changes**.

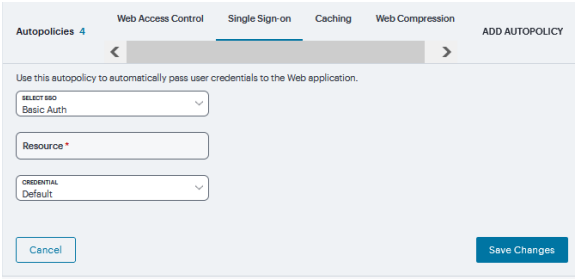


FIGURE 15.25 : Single Sign-on

8. Under **Caching**, click '**+**' and specify the resources to which this policy applies in the **Resource** filed and select the **Action** from drop down and click **Save Changes**.

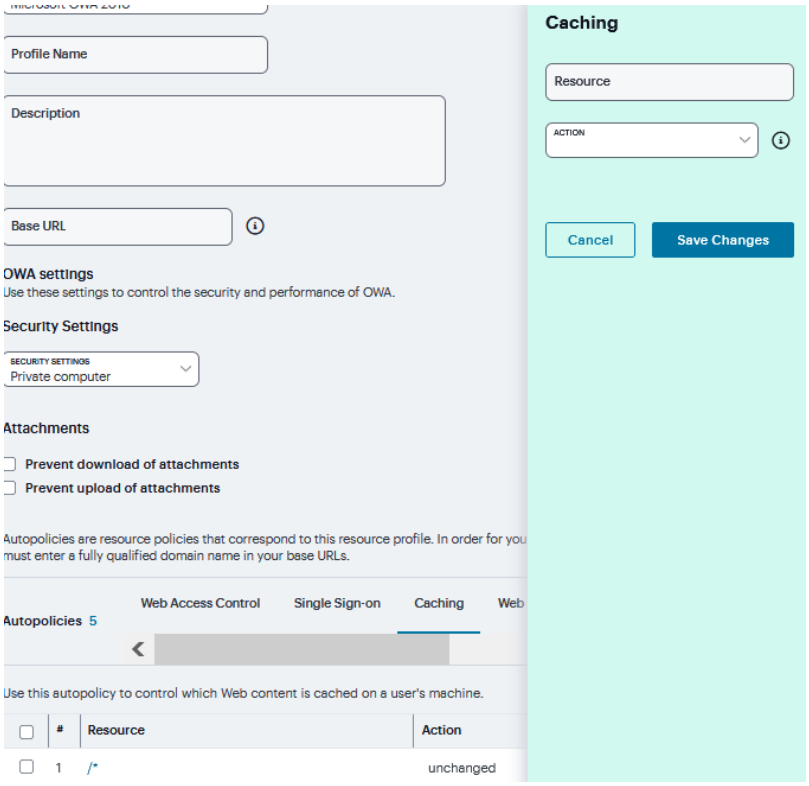


FIGURE 15.26 : Caching

9. Under **Web Compression**, click '**+**' and specify the resources to which this policy applies in the **Resource** filed and select the **Action** from drop down and click **Save Changes**.

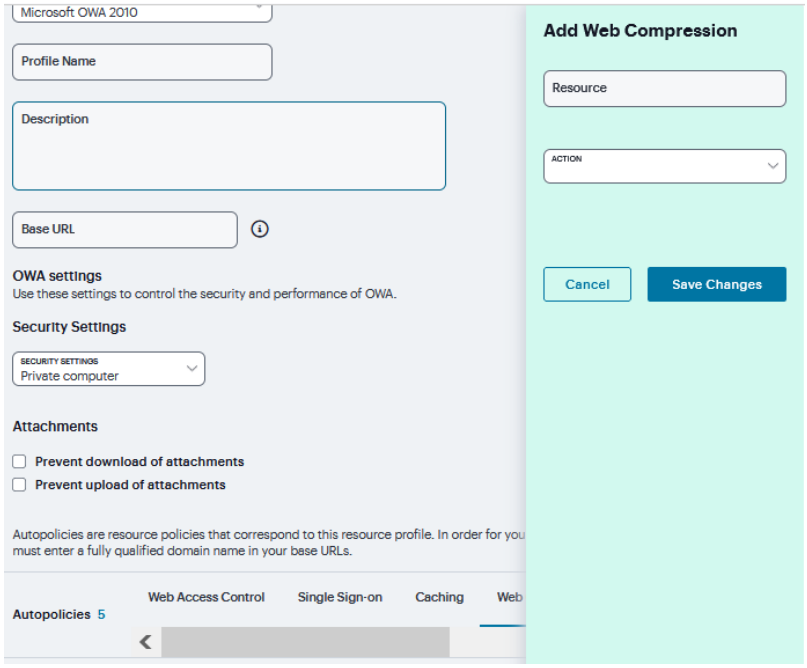


FIGURE 15.27 : Web Compression

10. Under **Client Authentication**, click '**+**' and specify the resources to which this policy applies in the **Resource** filed and select the **Certificate** from drop down and click **Save Changes**.

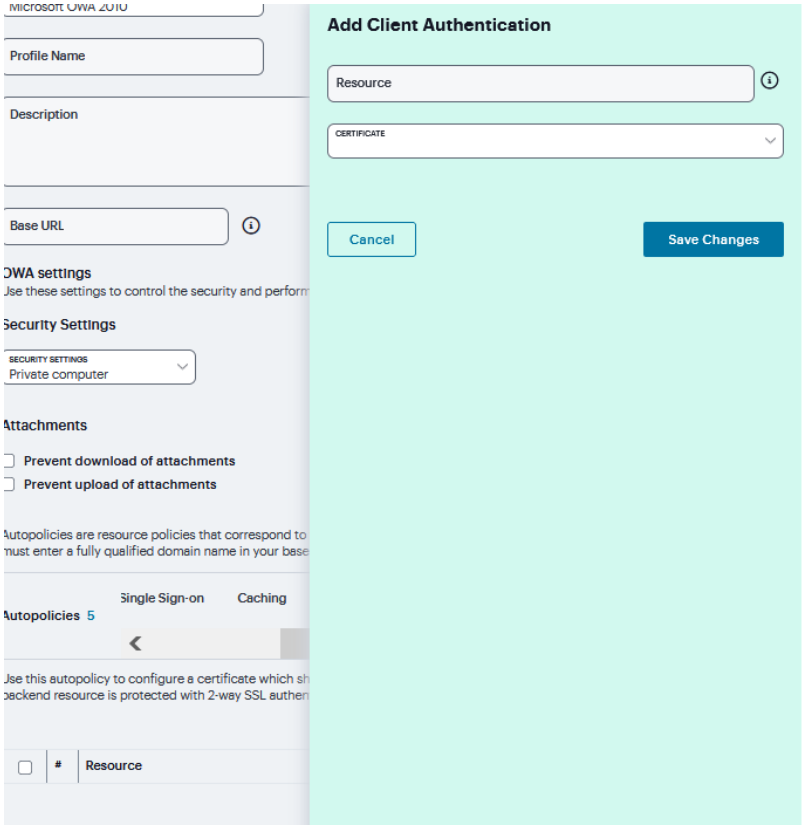


FIGURE 15.28 : Client Authentication

Microsoft Sharepoint

A Microsoft Sharepoint template is a resource profile that controls access to the application and configures Sharepoint settings as necessary. Microsoft Sharepoint templates significantly reduce your configuration time by consolidating configuration settings into one place and by pre-populating a variety of resource policy settings for you depending on the type of setup you select.

The system supports intermediating traffic to Microsoft Sharepoint through a Web rewriting resource profile template, JSAM, PSAM, and VPN Tunneling. This topic describes how to configure access using the Web rewriting template.

If **Microsoft Sharepoint** resource profile selected as Profile Template, then

1. Enter the URL of the Sharepoint resource to which you want to control access In the Base URL box.Use the format: *[protocol://]host[:port][/path]*.
2. Under Sharepoint Settings, select **Allow in-line editing of documents within explorer view** to allow users to modify files displayed in the explorer view.
3. Click '**+**' to add the Resource and click **Save Resource**.

4. Enter the number of minutes a persistent cookie resides on a user's computer before it expires in the **Persistent cookie** timeout box.

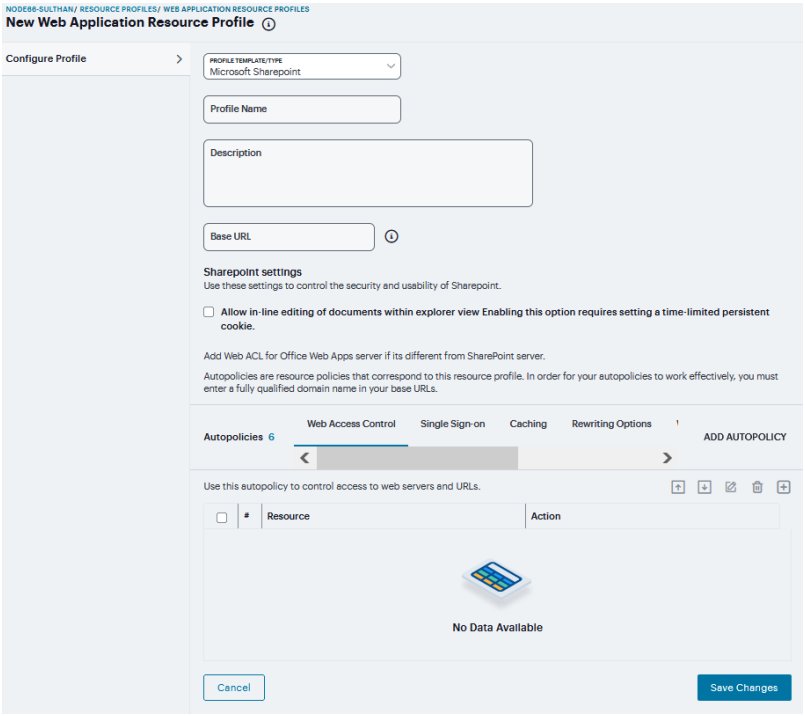


FIGURE 15.29 : Microsoft Sharepoint

5. Click **Add Autopolicy**, check box to create a policy and click **Add Selected**.

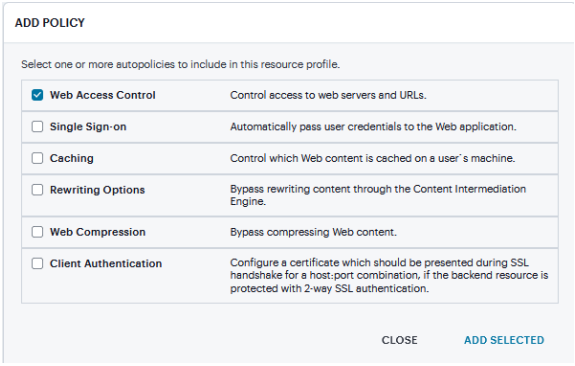


FIGURE 15.30 : Autopolicy

6. Under **Web Access Control**, click '**+**' specific **Resource** under the Base URL. Enter the full URL of the resource, select **Allow** or **Deny**, and click **Save Changes**.

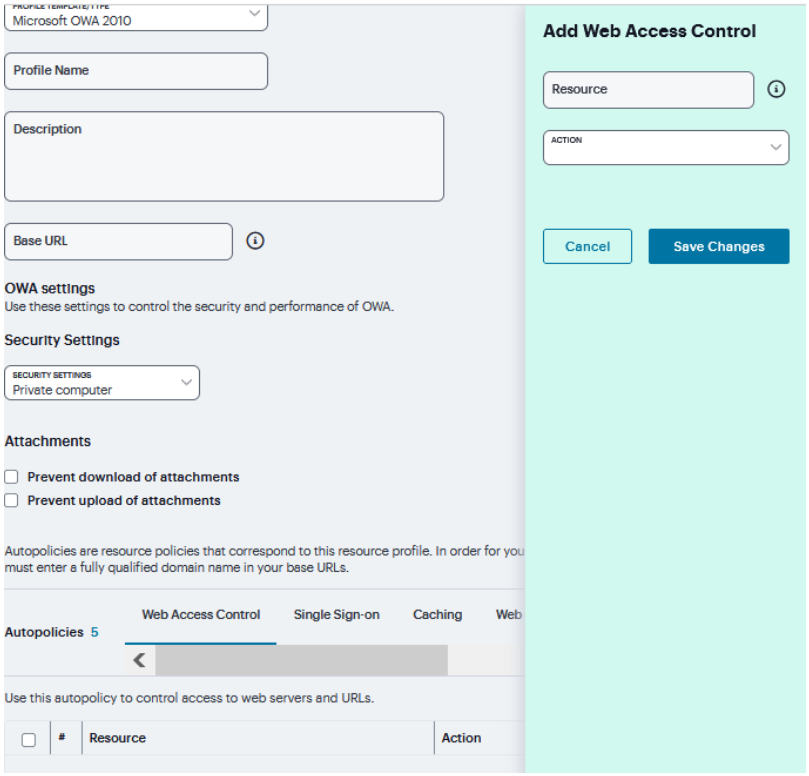


FIGURE 15.31 : Web Access Control

7. Under **Single Sign-on**, select the **SSO** from drop down and specify the application's sign-in page in **Resource** field and click **Save Changes**.

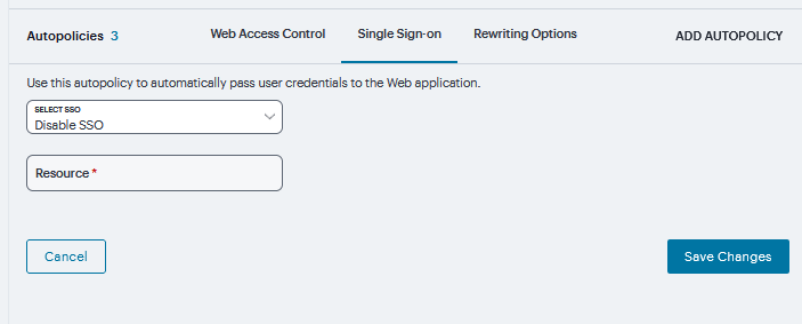


FIGURE 15.32 : Single Sign-on

8. Under **Caching**, click '**+**' and specify the resources to which this policy applies in the **Resource** filed and select the **Action** from drop down and click **Save Changes**.

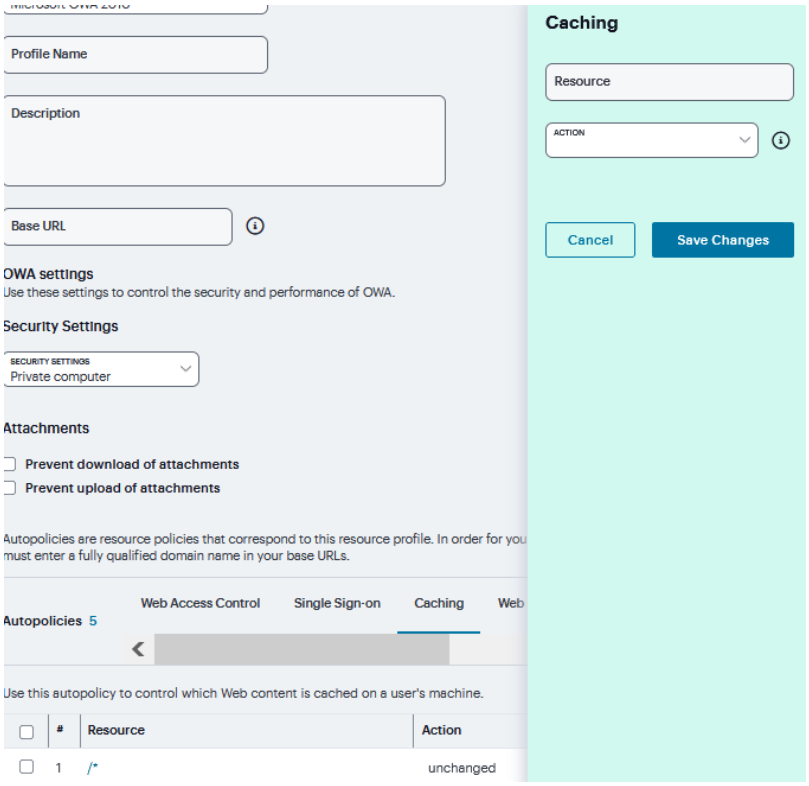


FIGURE 15.33 : Caching

9. Under Rewriting Options, select the Rewriting Options:

   - **Passthrough Proxy** - Select this option to specify Web applications for which the Content Intermediation Engine performs minimal intermediation.
   - **No rewriting (use WSAM)** - Select this option to intermediate content using PSAM instead of the Content Intermediation Engine. Then, specify the application server for which you want to intermediate content. (At minimum, you need to click Add in order to intermediate content to and from the server that the system extracts from the Web access control policy).
   - **No rewriting (use JSAM)** - Select this option to intermediate content using JSAM instead of the Content Intermediation Engine. Then, specify the application server for which you want to intermediate content. (At minimum, you need to click Add in order to intermediate content to and from the server that the system extracts from the Web access control policy).
   - **No rewriting** - Select this option to automatically create a selective rewriting policy for the autopolicy's URL, thereby configuring the system to not intermediate any content to and from the resource. For example, you may choose this option if you do not want the system to intermediate traffic from web sites that reside outside of the corporate network, such as yahoo.com. If you select this option, you do not have to configure any additional rewriting settings.

If **Passthrough Proxy** is selected:

1. Choose the way in which you want to enable the passthrough proxy feature:
   - **Use virtual hostname** - If you choose this option, specify a hostname alias for the application server. When the system receives a client request for the application server hostname alias, it forwards the request to the specified application server port in the Base URL field.
   - **Use IVE port** - If you choose this option, specify a unique port in the range 11000-11099. The system listens for client requests to the application server on the specified port and forwards any requests to the application server port specified in the Base URL field.
2. Select the **Rewrite XML** check box if you want to rewrite URLs contained within XML content. If this option is disabled, the system passes the XML content "as is" to the server.
3. Select the **Rewrite external links** check box if you want to rewrite all the URLs presented to the proxy. If this option is disabled, the system rewrites only those URLs where the hostname is configured as part of the passthrough proxy policy.
4. Select the **Block cookies from being sent to the browser** check box if you want to block cookies destined for the client's browser. The system stores the cookies locally and sends them to applications whenever they are requested.
5. Select the **Host-Header forwarding** check box if you want to pass the hostname as part of the host header instead of the actual host identifier. click **Save Changes**.

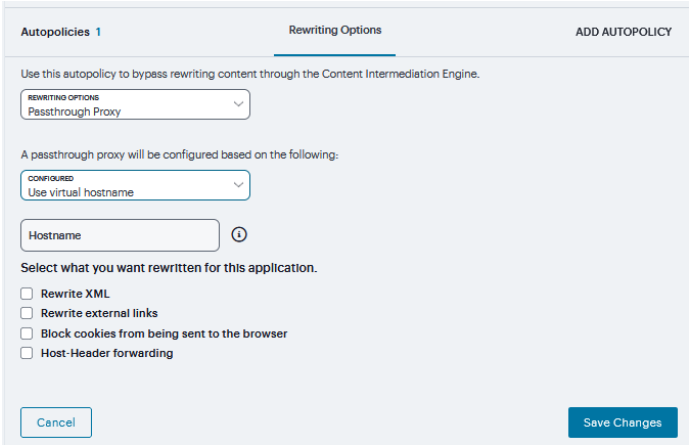


FIGURE 15.34 : Passthrough Proxy

If **No rewriting (use WSAM)** is selected

1. Create a rewriting autopolicy and select No rewriting (use WSAM).
2. In the **Destination** field, specify resources for which PSAM secures client/server traffic between the client and the system. By default, the

system extracts the correct server from the Web access control policy. You may choose to use this server as-is, modify it, and/or add new servers to the list.

When specifying a server, specify the hostname (the wild cards '*' or '?' are accepted) or an IP/netmask pair. Specify multiple ports for a host as separate entries.

3. Click **Save Changes**.

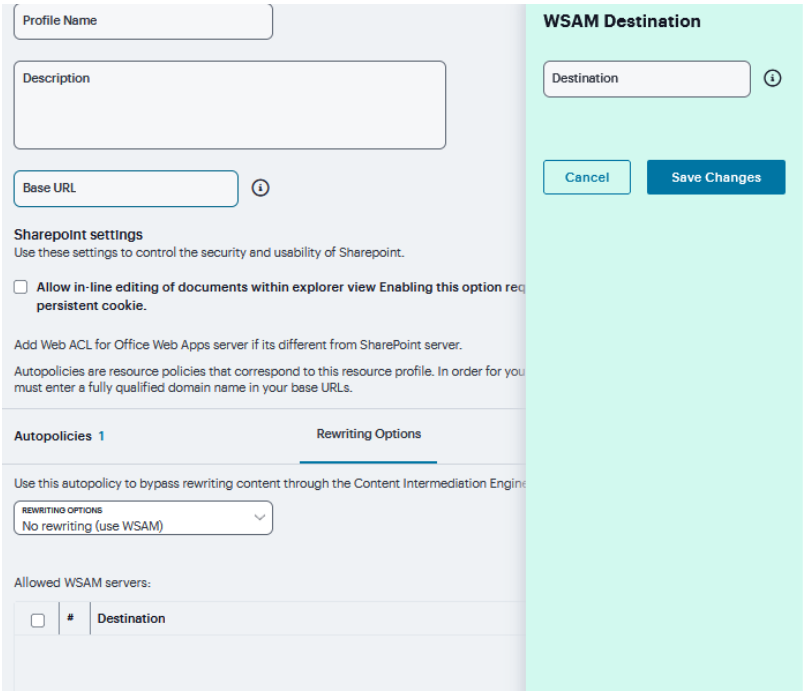


FIGURE 15.35 : No rewriting (use WSAM)

If **No rewriting (use JSAM)** options is selected:

1. In the **Server Name** field, enter the DNS name of the application server or the server IP address.
2. In the **Server Port** field, enter the port on which the remote server listens for client connections.
   - For example, to forward Telnet traffic from a remote machine, specify port 23 for both the client port (on which JSAM listens) and the server port (on which the Telnet server listens).
   - To enable drive mapping to this resource, enter 139 as the server port.
3. In the **Client Loopback IP** field, provide a static loopback address. If you do not provide a static IP loopback address, the system assigns an IP loopback address dynamically.
4. In the **Client Port** field, enter the port on which JSAM should listen for client application connections.

   Typically, the local port value is the same value as the server port; the

local port value usually only differs for Linux or Macintosh users who want to add applications for port forwarding that use ports under 1024.

To enable drive mapping to this resource, enter 139 as the server port.

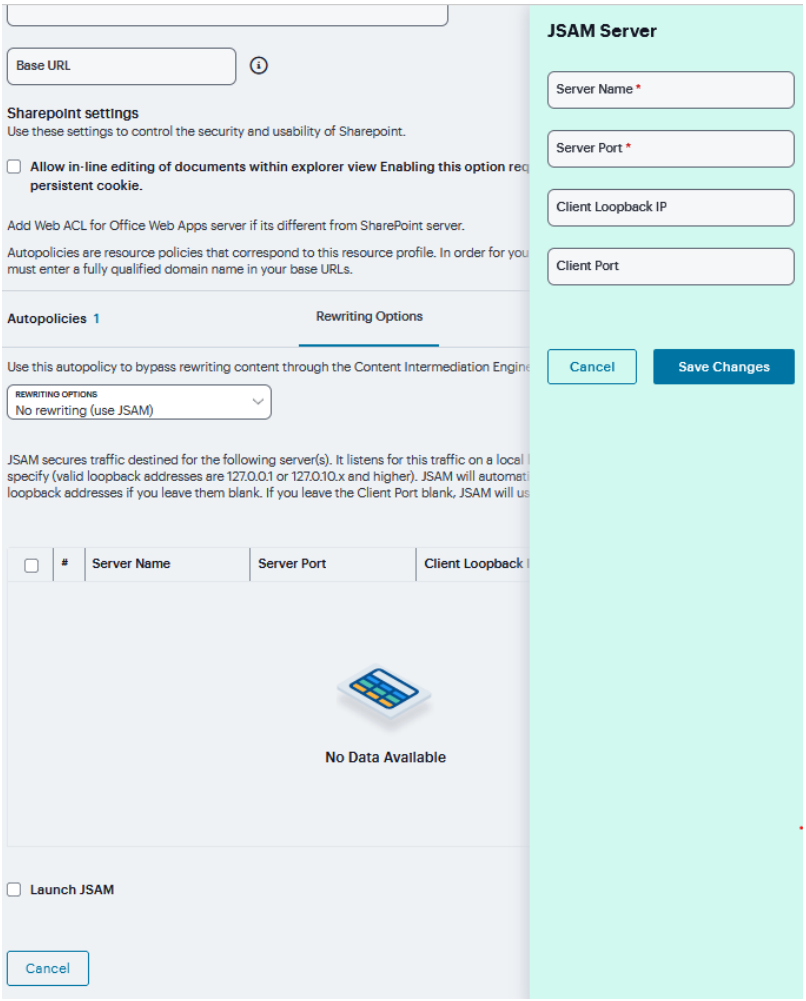


FIGURE 15.36 : No rewriting (use JSAM)

10. Select **Launch JSAM** to automatically start JSAM when the system encounters the Base URL.
11. Click **Save Changes**.

    If **No rewriting** options is selected, then only selective rewriting resource policy is created.

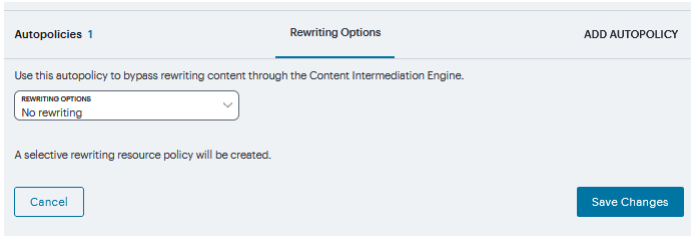


FIGURE 15.37 : No rewriting

12. Under **Web Compression**, click '**+**' and specify the resources to which this policy applies in the **Resource** filed and select the **Action** from drop down and click **Save Changes**.

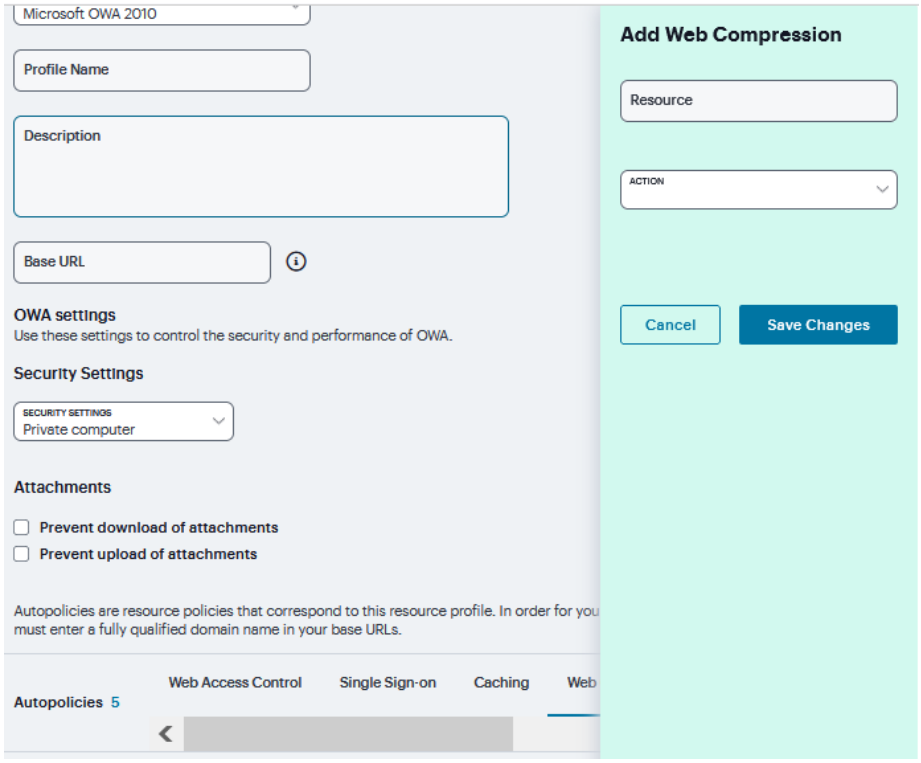


FIGURE 15.38 : Web Compression

13. Under **Client Authentication**, click '**+**' and specify the resources to which this policy applies in the **Resource** filed and select the **Certificate** from drop down and click **Save Changes**.

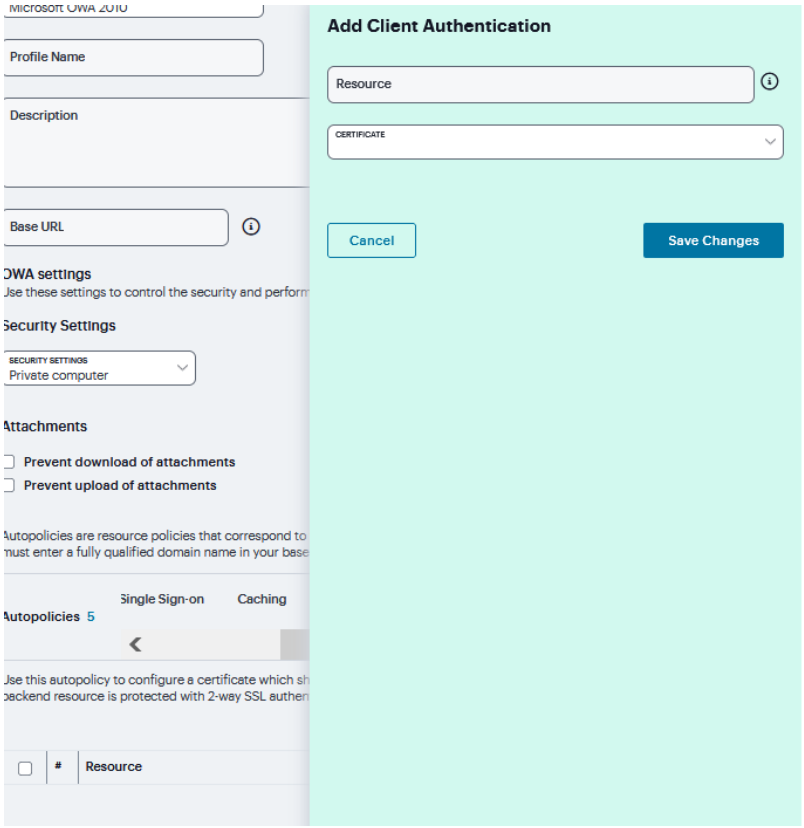


FIGURE 15.39 : Client Authentication

File Browsing

To create a Windows file browsing resource profile:

1. Navigate to **Users > Resource Profiles > Files**.
2. Click '**+**'. Or select an existing profile from the list.

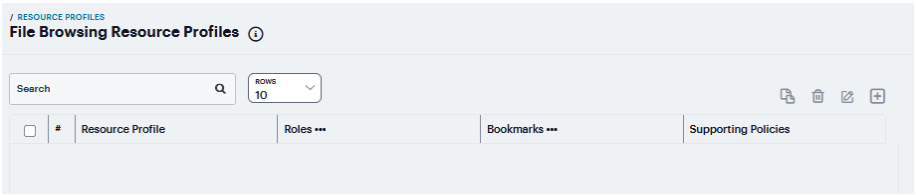


FIGURE 15.40 : File Browsing

3. Select **Windows** from the Type list.
4. Enter a unique **Name** and optionally a **Description** for the resource profile. (This name becomes the default session bookmark's name.)
5. Enter the **Server name** to share.
6. If required, select to **show All AutoPolicy** types.

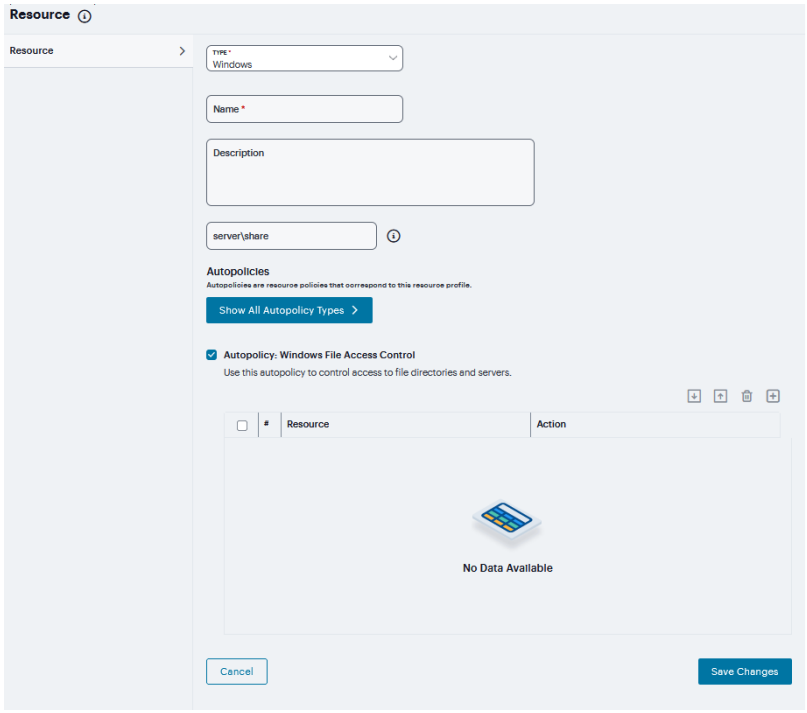


FIGURE 15.41 : File Resourcing

7. Check **Autopolicy Windows File Access Control** to set the file access control.
8. Click '**+**' to add specific **Resource**. Enter the full URL of the resource, select **Allow**, **Deny** or **Read Only**, and click **Save Changes**.

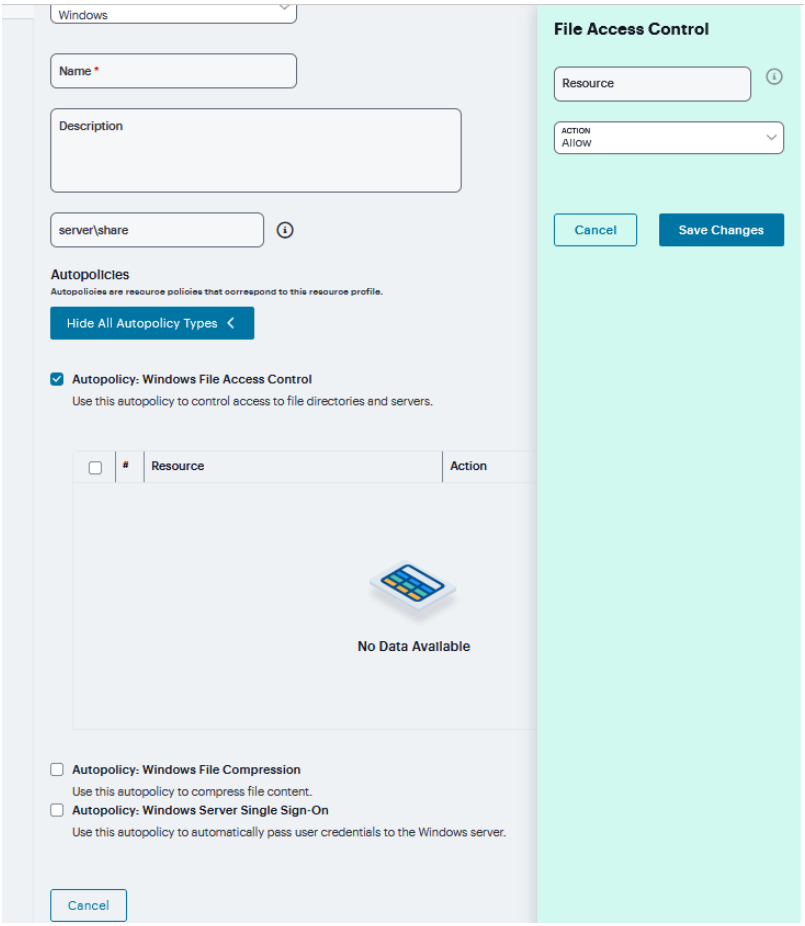


FIGURE 15.42 : Windows File Access

9. Check **Autopolicy: Windows File Compression** to set the file access control.
10. Click '**+**' to add specific resource. Enter the full URL of the resource, select **Compress** or **Do not Compress**, and click **Save Changes**.

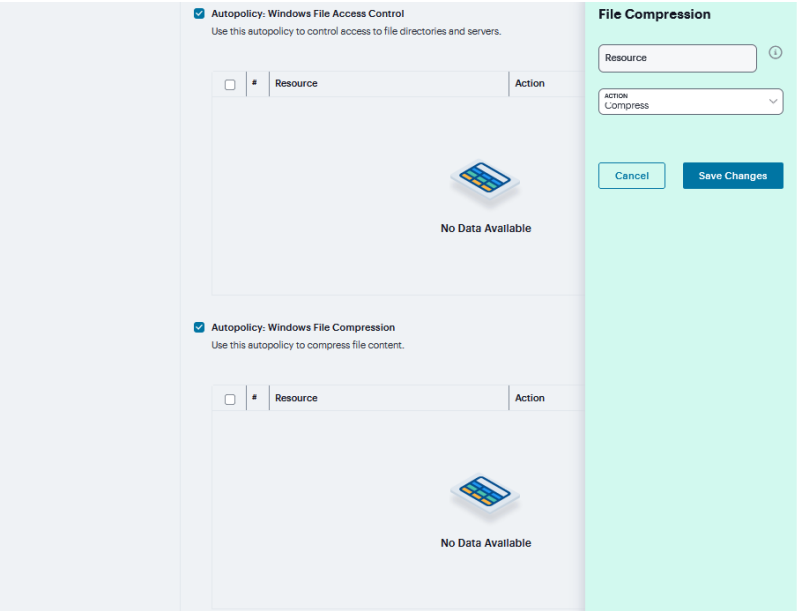


FIGURE 15.43 : Windows File Compression

11. Under **Autopolicy: Windows Server Single Sign-On**, select the **SSO** from drop down and specify the application's sign-in page in **Resource** field and click **Save Changes**.

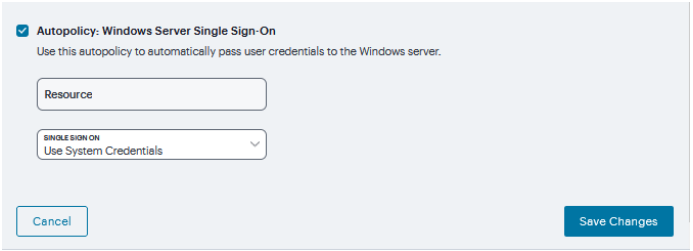


FIGURE 15.44 : Windows Single Sign-on

Terminal Services

Terminal Services resource profile configuration instructions vary depending on whether you want to configure access to a Windows terminal server (which requires an RDP client) or Citrix terminal server (which requires an ICA client). Furthermore, if you choose to configure access to a Citrix server using a custom ICA file, you include many of your configuration settings in the ICA file itself and therefore do not need to configure them through the system.

If you configure access to a Citrix server using the default ICA file on the system, however, you must configure additional settings. You may want to create multiple bookmarks for the same terminal services resource in order to provide easy access to multiple applications. For instance, the server defined in your resource profile may provide access to multiple applications (such as Siebel and Outlook). To easily provide access to each of these applications, you can create resource profile

bookmarks to each. Or, you may want to use multiple bookmarks to configure single sign-on to one application, but not another.

To create a terminal services resource profile:

1. Navigate to **Users > Resource Profiles > Terminal Services**.
2. Click '**+**'. Or select an existing profile from the list.

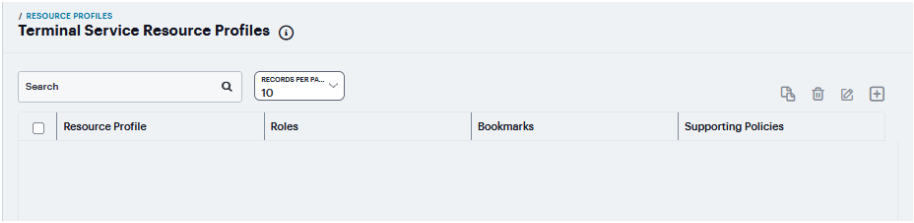


FIGURE 15.45 : Terminal Services

3. If **Windows Terminal Services** is selected from the Type list.
    1. Enter a unique Name and optionally a description for the resource profile. (This name becomes the default session bookmark's name.)
    2. Specify the server and port to which this resource profile should connect in the Host field. When entering the server, you may enter a hostname or IP address.
    3. Enter the port on which the terminal server listens in the Server port box. (By default, the system populates this box with port number 3389.)
    4. Select the **Create an access control policy allowing Terminal Service access to this server** check box to enable access to the server specified in the Server Port box (enabled by default).
    5. If you want to enable intermediation using a Java client, select **Enable Java support** and then specify which Java client the system should use.

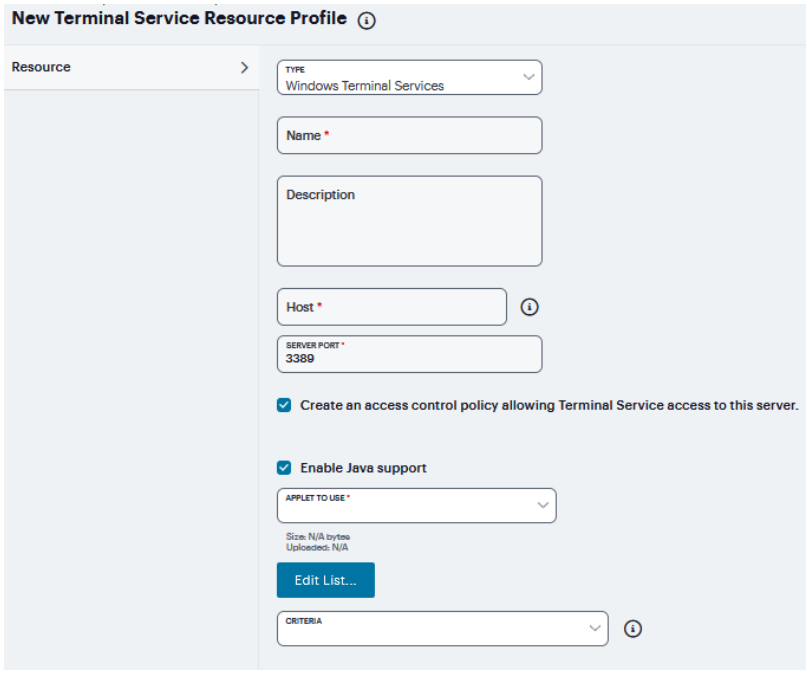


FIGURE 15.46 : Windows Terminal Services

6. Select the Java applet that you want to associate with the resource profile from the **Applet to use** list. Or, if the applet that you want to use is not currently available in the list, click **Edit list**.
7. Click '**+**' to add an applet to this list.
8. Enter **Name** to identify the applet.

FIGURE 15.47 : Java Applet

9. Click the text field to browse to the applet that you want to upload.
10. Select the **Uncompress archive file** check box if the file that you selected is an archive that contains the applet. Click **OK**.
11. Select the **Criteria** from the drop down. If the Windows client launches, then this Java applet will not be used.
12. Click **Save Changes**.

Note: When you select an applet in the Java Applets dialog box, you are loading third-party software onto the Ivanti product. By clicking OK, you are agreeing to the following terms on behalf of yourself (as purchaser of the equipment) or the organization that purchased the Ivanti product, as applicable.

---

4. If **Citrix using default ICA** is selected from the Type list.
    1. Enter a unique Name and optionally a description for the resource profile. (This name becomes the default session bookmark's name).
    2. Specify the server and port to which this resource profile should connect in the Host field. When entering the server, you may enter a hostname or IP address.
    3. Enter the port on which the terminal server listens in the Server port box. (By default, the system populates this box with port number 3389).
    4. Select the **Create an access control policy allowing Terminal Service access to this server** check box to enable access to the server specified in the Server Port box (enabled by default).
    5. If you want to enable intermediation using a Java client, select **Enable Java support** and then specify which Java client the system should use.

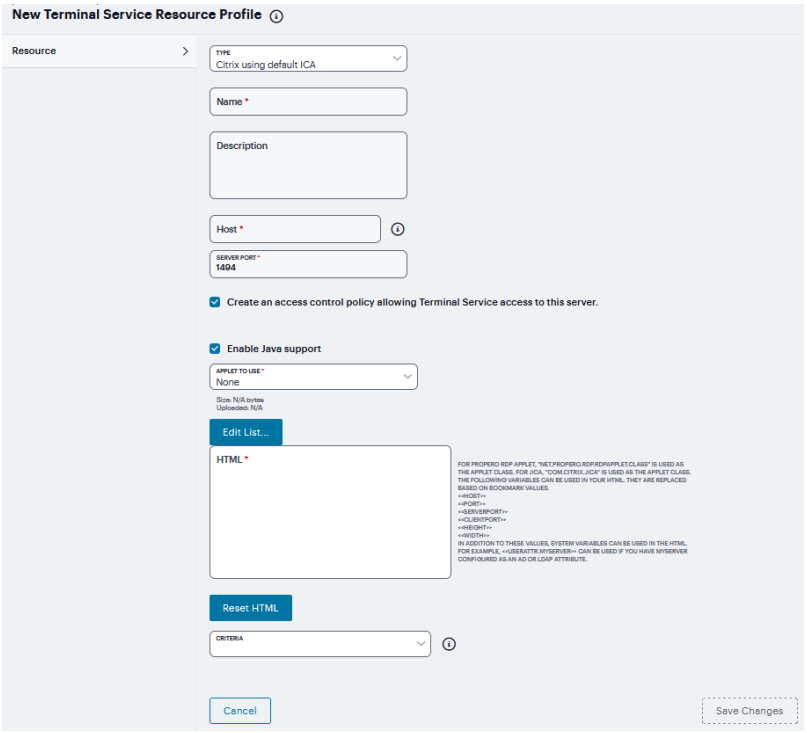


FIGURE 15.48 : Citrix using default ICA

6. Select the Java applet that you want to associate with the resource profile from the **Applet to use** list. Or, if the applet that you want to use is not currently available in the list, click **Edit list**.

FIGURE 15.49 : Java Applet

7. Click '**+**' to add an applet to this list.
8. Enter **Name** to identify the applet.
9. Click the text field to browse to the applet that you want to upload.
10. Select the **Uncompress archive file** check box if the file that you selected is an archive that contains the applet. Click **OK**.
11. Enter HTML with variables to replace the bookmark.
12. Select the **Criteria** from the drop down. If the Windows client launches, then this Java applet will not be used.
13. Click **Save Changes**.

Note: When you select an applet in the Java Applets dialog box, you are loading third-party software onto the Ivanti product. By clicking OK, you are agreeing to the following terms on behalf of yourself (as purchaser of the equipment) or the organization that purchased the Ivanti product, as applicable.

---

5. If **Citrix using custom ICA file** is selected from the **Type** list.
    1. Specify the ICA file that contains the session parameters that you want use in the Custom ICA File box. Note that you may download and customize the following ICA files from the system.
        - ICA file that comes with the system-To customize this file, click the Open link, save the file to your local machine, customize the file as required, and upload it back to the system using the Browse option. If you customize this file, you must replace the following parameters in the default.ica file: <CITRIX_CLIENT_NAME>, <APPDATA> and <TARGET_SERVER>.
        - ICA file that you have already associated with the resource profile-To customize this file, click the Current ICA File link, save the file to your local machine, and customize the file as required. Once you make changes, you must upload the revised version using the Browse option.
    2. Enter a unique **Name** and optionally a **Description** for the resource profile. (This name becomes the default session bookmark's name.)
    3. Select the Autopolicy: Terminal Services Access Control check box.
    4. Click '**+**' and Specify the Metaframe servers to which you want to enable access in the **Resource** field.
    5. Choose **Allow** to enable access to the specified resource or **Deny** to block access to the specified resource from the **Action** list. Click **Save Changes**.
    6. Specify the server and port to which this resource profile should connect in the Host field. When entering the server, you may enter a hostname or IP address.

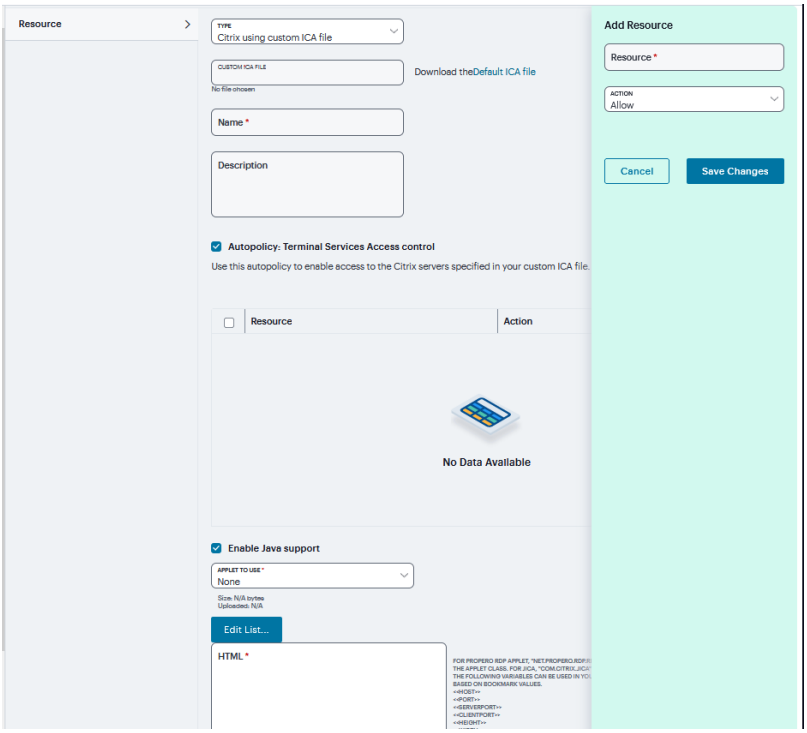


FIGURE 15.50 : Citrix using custom ICA file

7. If you want to enable intermediation using a Java client, select **Enable Java support** and then specify which Java client the system should use.
8. Select the Java applet that you want to associate with the resource profile from the **Applet to use** list. Or, if the applet that you want to use is not currently available in the list, click **Edit list**.

FIGURE 15.51 : Java Applet

9. Click '**+**' to add an applet to this list.
10. Enter **Name** to identify the applet.
11. Click the text field to browse to the applet that you want to upload.
12. Select the **Uncompress archive file** check box if the file that you selected is an archive that contains the applet. Click **OK**.
13. Enter **HTML code** with variables to replace the bookmark.
14. Select the **Criteria** from the drop down. If the Windows client launches, then this Java applet will not be used.
15. Click **Save Changes**.

6. If **Citrix Listed Applications** is selected from the Type list:

1. Enter a unique **Name** and optionally a **Description** for the resource profile. (This name becomes the default session bookmark's name.)
2. Enter the IP address and port of the Citrix MetaFrame server where the XML service is running.
   - You do not need to enter the port number if you are using the default value. The default port is 80 (if SSL is selected, the default port is 443).
   - You can enter more than one server. If the connection fails on one server, the next server in the list is used.
3. Click the **Use SSL for connecting to Citrix XML Service** check box to send the password through SSL instead of cleartext.

   Although cleartext is supported, we recommend you always use SSL to avoid any security issues.
4. Enter the **Username**, **Password**, and **Domain** name for connecting to the Citrix Metaframe server where the XML service is running.
   - You can enter variable credentials such as <USERNAME> and <PASSWORD>. If you use variable credentials, the Subset of selected Applications option is disabled in the Bookmarks window.
   - When the user accesses the application list, their credentials are submitted to the Citrix XML service, substituting the session context variables <USERNAME> and <PASSWORD>. Only the user's specific applications (as determined by the Citrix administrator) are returned.
5. Select the Autopolicy: Terminal Services Access Control check box.
6. Click '**+**' and Specify the Metaframe servers to which you want to enable access in the **Resource** field.
7. Choose **Allow** to enable access to the specified resource or **Deny** to block access to the specified resource from the **Action** list. Click **Save Changes**.
8. Specify the server and port to which this resource profile should connect in the Host field. When entering the server, you may enter a hostname or IP address.

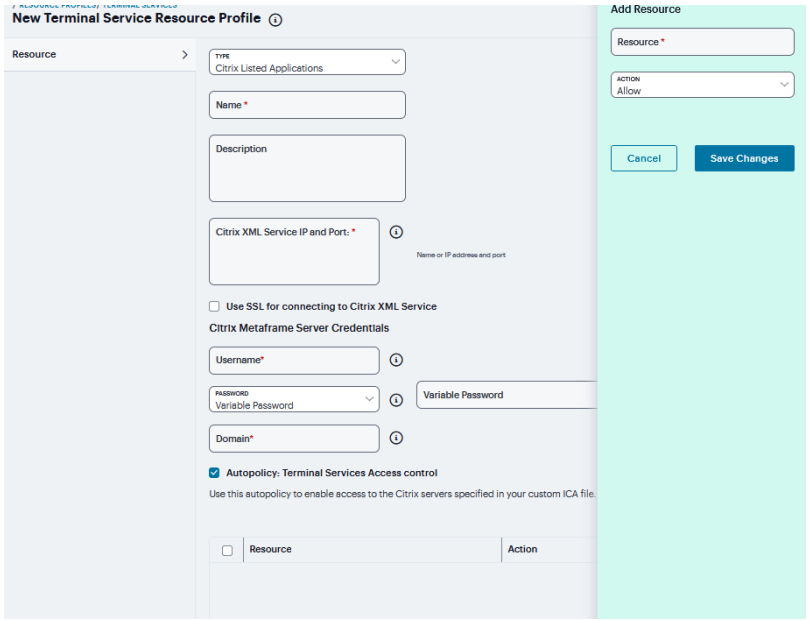


FIGURE 15.52 : Citrix Listed Applications

9. If you want to enable intermediation using a Java client, select **Enable Java support** and then specify which Java client the system should use.
10. Select the Java applet that you want to associate with the resource profile from the **Applet to use** list. Or, if the applet that you want to use is not currently available in the list, click **Edit list**.

FIGURE 15.53 : Java Applet

11. Click '**+**' to add an applet to this list.
12. Enter **Name** to identify the applet
13. Click the text field to browse to the applet that you want to upload.
14. Select the **Uncompress archive file** check box if the file that you selected is an archive that contains the applet. Click **OK**.
15. Enter **HTML code** with variables to replace the bookmark.
16. Select the **Criteria** from the drop down. If the Windows client launches, then this Java applet will not be used.

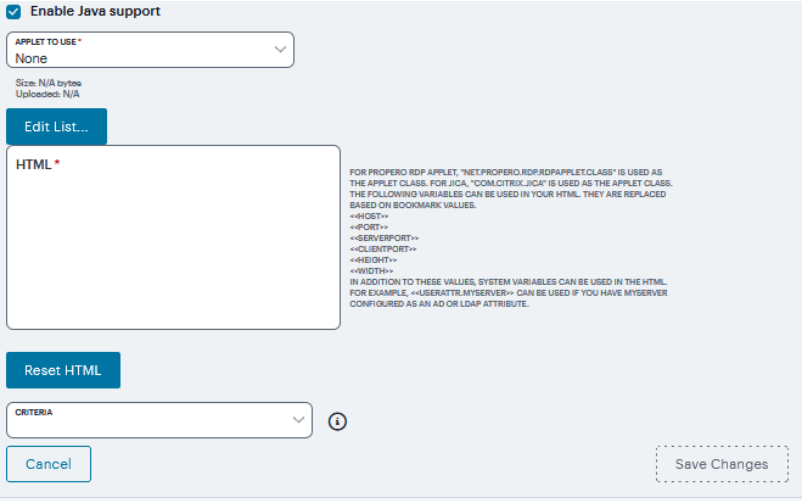


FIGURE 15.54 : Enable Java support

17. Click **Save Changes**.

Virtual Desktop

In addition to standard resource profiles and resource profile templates, you can configure virtual desktops as resource profiles. As with the other resource profiles, a virtual desktop profile contains all of the role assignments and end-user bookmarks required to provide access to an individual resource. Unlike other resource profile types, there is no resource policy to configure for virtual desktops due to the dynamic nature of virtual desktops. The IP address and port of the system is not known until the end user launches a session so dynamic ACLs are used. Icons in the Virtual Desktops section on the end user's home page represent desktops defined by the administrator. Clicking the icon launches the session using the Virtual Desktop Infrastructure (VDI) architecture.

The Citrix XenDesktop manages a pool of virtual desktops hosted on virtual machines and provides the connection management to those desktops. A list of XenDesktops is displayed to the end user as bookmarks. When a desktop is selected, the Citrix client is launched and the user can access that desktop.

VMware View Manager, formerly VMware VDI, lets you run virtual desktops in a data center that provide end users a single view of all their applications and data in a personalized environment regardless of the device or location they log in from.

To configure a Citrix XenDesktop or VMware View Manager profile:

1. Navigate to **Users > Resource Profiles > Virtual Desktops**.
2. Click '**+**' and Select **VMware View Manager** or **Citrix XenDesktop** from the Type drop-down list

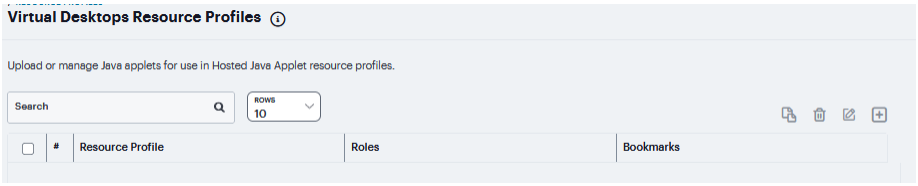


FIGURE 15.55 : VMware View Manager

3. Enter a **Name** and **Description** (optional) to identify this profile.
4. Enter the **Name** or **IP address** and port of the connection broker using the format ip:port.

   You can enter more than one IP address. Place each address on a separate line.
5. Select the **Use SSL for connecting to the Server** check box if **SSL** is required to connect to the server.
6. Enter the **Username** to connect to the connection broker or use the **<USERNAME>** session variable.
7. Enter the **Variable Password** or **Password**
   - To use a variable password to connect to the connection broker, select Variable Password and enter the variable in the form of <PASSWORD> or <PASSWORD@SEcAuthServer>.
   - Select Password to use a static password to connect to the connection broker and enter the user credential's password.
8. Enter the **Domain** where the connection broker is located.
9. Click **Save Changes**.

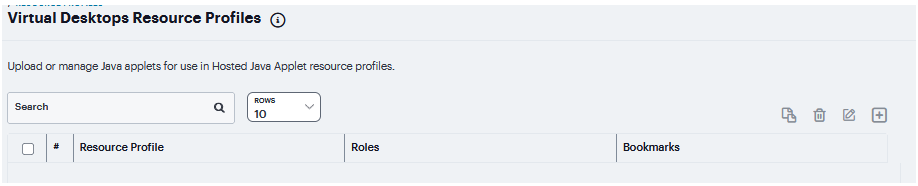


FIGURE 15.56 : Citrix XenDesktop

10. If you want to enable intermediation using a Java client, select **Enable Java support** and then specify which Java client the system should use (applicable only if Citrix XenDesktop is selected in type).
11. Select the Java applet that you want to associate with the resource profile from the **Applet to use** list. Or, if the applet that you want to use is not currently available in the list, click **Edit list**.

FIGURE 15.57 : Java Applet

HTML5 Access

A HTML5 Access resource profile is a profile that enables users to connect to Remote Desktops or to connect to internal server hosts in the clear using Telnet protocols or to communicate over an encrypted Secure Shell (SSH) session through a Web-based terminal session emulation.

The HTML5 license count was based on the number of active HTML5 sessions. The HTML5 licenses will be counted based on the number of active users. Each user will be allowed to access up to five user sessions.

To create a HTML5 Access resource profile:

1. Navigate to **Users > Resource Profiles > HTML5 Access**.
2. Click '**+**', Select the **Solution Type** as **Basic HTML5** or **Advanced HTML5**.

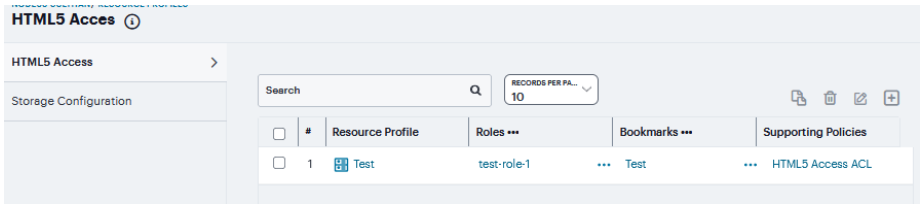


FIGURE 15.58 : HTML5 Access

3. From the Type list, specify the session type (**Windows RDP** or **SSH** or **Telnet**) for this resource profile. If you have selected Advanced HTML5 solution type, you can also specify **VNC** session type.
4. Enter a unique **Name** and optionally a **Description** for the resource profile.
5. In the **Host** field, enter the Hostname, IP or user attribute of the server to which this resource profile should connect.
6. In the **Server Port** field, enter the port on which the system should connect to the server. (By default, the system populates this field with port number 3389 if you select Windows RDP, port number 23 if you select Telnet, port number 22 if you select SSH and port number 5900 if you select VNC.)
7. Select the **Create an access control policy for HTML5 access** check box to enable access to the server specified in the Server Port box (enabled by default).
8. Click **Save Changes**.

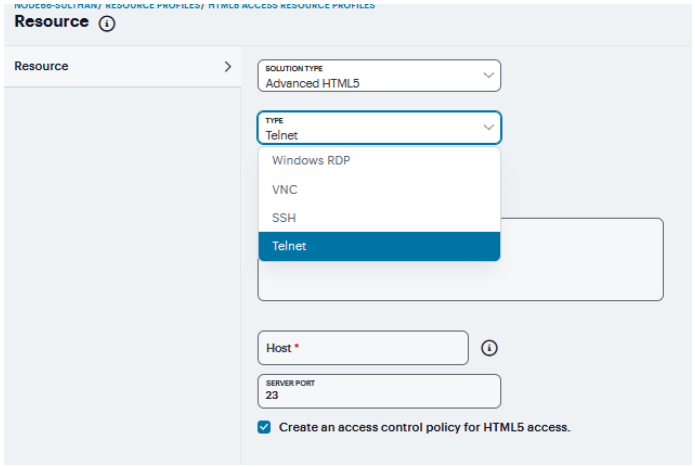


FIGURE 15.59 : HTML5 Access

To configure the external storage for session recordings:

1. Navigate to **Users > Resource Profiles > Storage Configuration**.
2. Select *Enable external storage*.
3. Enter the complete storage path to store the session recordings.
4. Enter the **Username** and **Password** required to access the location.
5. Click **Save Changes**.

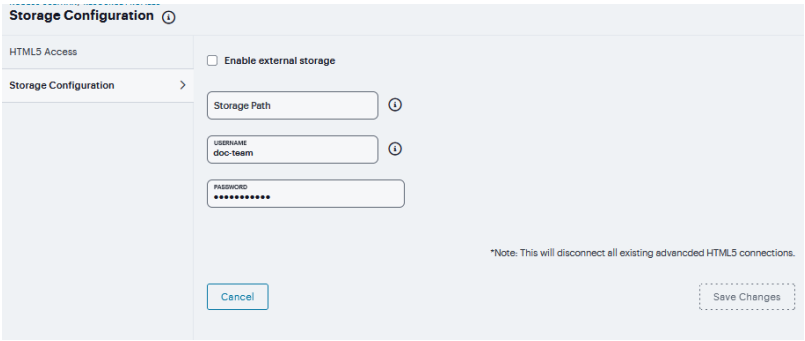


FIGURE 15.60 : Storage Configuration

SAM Resource Profiles

You can create two types of PSAM resource profiles:

- PSAM application resource profiles-These resource profiles configure PSAM to secure traffic to a client/server application. When you create a PSAM application resource profile, the PSAM client intercepts requests from the specified client applications to servers in your internal network.
- PSAM destination network resource profiles-These resource profiles configure PSAM to secure traffic to a server. When you create a PSAM destination network resource profile, the PSAM client intercepts requests from processes running on the client that are connecting to the specific internal hosts.

When creating PSAM resource profiles, note that the resource profiles do not contain bookmarks. To access the applications and servers that PSAM intermediates, users must first launch PSAM and then launch the specified application or server using standard methods (such as the Windows Start menu or a desktop icon).

When you enable JSAM or PSAM through Web rewriting autopolicies in the Users > Resource Profiles > Web Applications/Pages page of the admin console, the system automatically creates JSAM or PSAM autopolicies for you. You can only view these SAM policies through the appropriate Web resource profile-not through the SAM resource profile pages of the admin console.

Client Applications PSAM

To create a PSAM application resource profile:

1. Navigate to **Users > Resource Profiles > SAM > Client Applications**.
2. Click '**+**'. choose **PSAM** from the Type list
3. From the Application list, select one of the options.

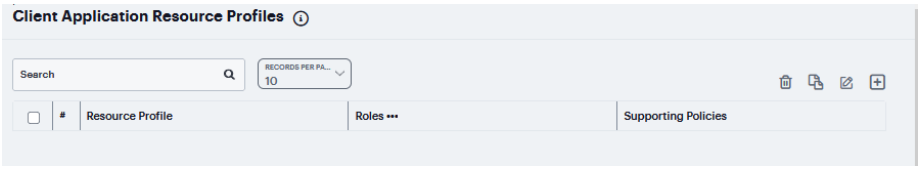


FIGURE 15.61 : Client Applications

- **Custom** - When you select this option, you must manually enter your custom application's executable file name (such as telnet.exe). Additionally, you may specify this file's path and MD5 hash of the executable file (although it is not required that you specify the exact path to the executable). If you enter an MD5 hash value, PSAM verifies that the checksum value of the executable matches this value. If the values do not match, PSAM notifies the user that the identity of the application could not be verified and does not forward connections from the application to the system.
- **Lotus Notes** - When you select this option, PSAM intermediates traffic from the Lotus Notes fat client application.
- **Microsoft Outlook** - When you select this option, PSAM intermediates traffic from the Microsoft Outlook application.
- **NetBIOS file browsing** - When you select this option, PSAM intercepts NetBIOS name lookups in the TDI drivers on port 137.
- **Citrix** - When you select this option, PSAM intermediates traffic from Citrix applications.

The system supports several mechanisms for intermediating traffic to the Lotus Notes, Microsoft Outlook, and Citrix applications.

- **Domain Authentication** - Select this option to allow integrated Windows applications, such as file sharing, Outlook, and so forth to authenticate to the domain controller when the client machine is part of a domain. Before using this option, you must:
  - Specify domain controllers that are reachable through the system in the PSAM Destination list so that LDAP and Kerberos traffic can be proxied and sent to the system.
  - Configure a PSAM Access Control Policy (ACL) to allow access to all domain controllers.

4. Enter a unique **Name** and optionally a **Description** for the resource profile.
5. Enter the **File Name** and **Path** and in case of **Windows Platform** enter **MD5 Hash**.
6. Under **Autopolicy: SAM Access Control** (this is applicable only for PSAM), click '**+**' specific **Resource** under the Base URL. Enter the full URL of the resource, select **Allow** or **Deny**, and click **Save Changes**.

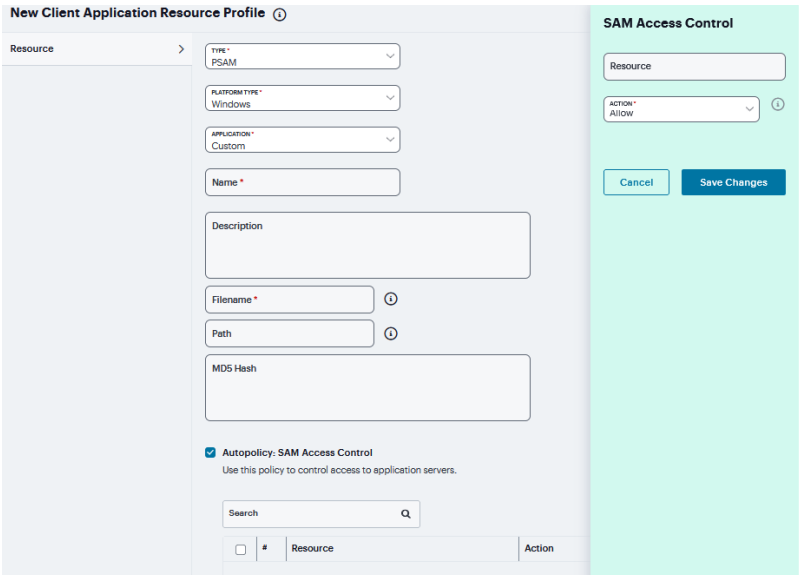


FIGURE 15.62 : Client Applications PSAM

Client Applications JSAM

JSAM resource profiles configure JSAM to secure traffic to a client/server application. When you create a JSAM application resource profile, the JSAM client tunnels network traffic generated by the specified client applications to servers in your internal network.

To create a JSAM applied

1. Navigate to **Users > Resource Profiles > SAM > Client Applications**.
2. Click '**+**'. choose **JSAM** from the Type list.
3. From the Application list, select one of the options.

- **Custom - Select this option to intermediate traffic to a custom application. Then:**

    1. Under JSAM Port Forwarding click '**+**'.
    2. In the **Server Name** field, enter the name or IP address of the remote server. If you are using automatic host mapping, enter the server as it is known to the application. If you enter an IP address, note that end users must connect to JSAM using that IP address in order to connect to the specified server.
    3. In the **Server Port** field, enter the port on which the remote server listens for client connections. For example, to forward Telnet traffic from a remote machine, specify port 23 for both the client port (on which JSAM listens) and the server port (on which the Telnet server listens).
        - To disable the registry change made by JSAM and restore the original copy of the etc/hosts file, users must uninstall the JSAM client using settings in the Preferences > Applications page of the end-user console. To re-enable the change, they need to reboot.
        - You can also use the restore system settings script. However, the restore system settings script cannot restore the hosts file successfully if you log in as a different user from the one that originally launched JSAM.
    4. In the **Client Loopback IP field**, provide a static loopback address. If you do not provide a static IP loopback address, the system assigns an IP loopback address dynamically.
    5. In the **Client Port** field, enter the port on which JSAM should listen for client application connections. Typically, the local port value is the same value as the server port; the local port value usually only differs for Linux or Macintosh non-root users who want to add applications for port forwarding that use ports under 1024.
    6. Click **Save Changes**.

4. Select the **Allow JSAM to dynamically select an available port if the specified client port is in use** check box if JSAM is listening for multiple hosts on the same port and you want JSAM to select an available port when the client port you specify is taken. The client application must allow you to specify the port number for the connection in order to use this option.
5. Select the **Create an access control policy allowing SAM access to these servers** check box to enable access to the list of servers specified in the Server column (enabled by default).

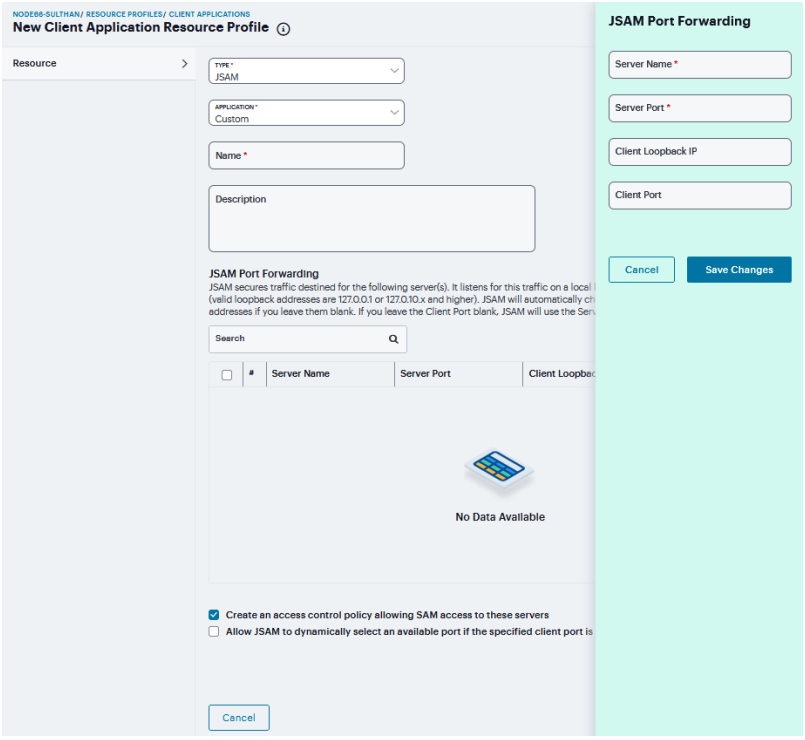


FIGURE 15.63 : Custom

- **Lotus Notes** - Select this option to intermediate traffic from the Lotus Notes fat client application. Then, in the Autopolicy: SAM Access Control section, create a policy that allows or denies users access to the Lotus Notes server:

    1. If it is not already enabled, select the **Autopolicy: SAM Access Control** check box.
    2. In the **Resource** field, specify the application server to which this policy applies. You can specify the server as a fully-qualified hostname or an IP/netmask pair. For example, if the fully-qualified hostname is notes1.yourcompany.com, add notes1.yourcompany.com and notes1 to the Resource field.
    3. From the **Action** list, select **Allow** to enable access to the specified server or **Deny** to block access to the specified server. Click **Save Changes**.

        You can only use JSAM to configure access to one Lotus Notes application per user role.

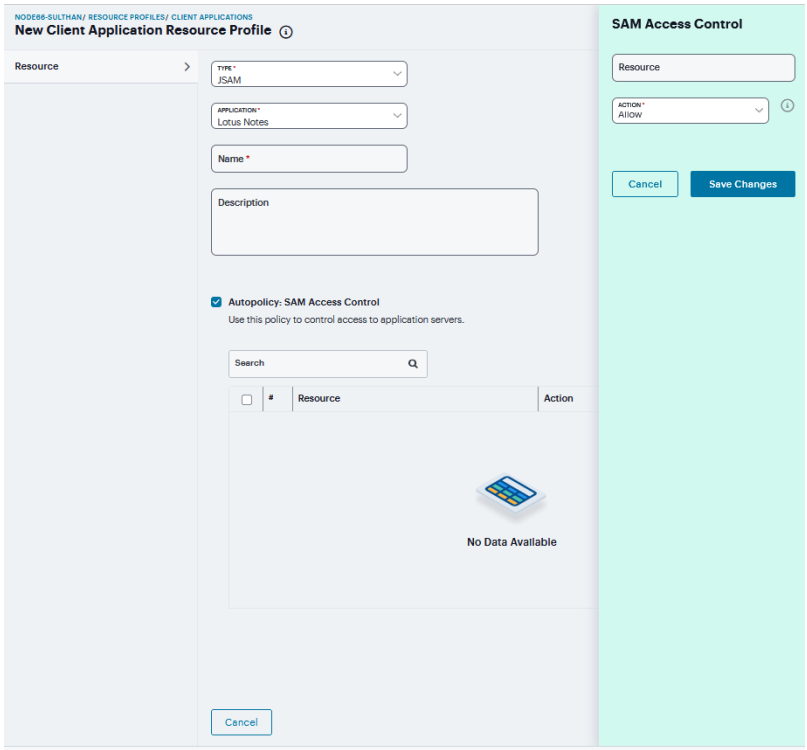


FIGURE 15.64 : Lotus Notes

- **Microsoft Outlook** - Select this option to intermediate traffic from the Microsoft Outlook application. Then:

    1. Enter a unique **Name** and optionally a **Description** for the resource profile.
    2. Enter the **Hostname** for each MS Exchange server in the Servers field. For example, if the fully-qualified hostname is exchange1.yourcompany.com, add exchange1.yourcompany.com to the Servers field.
        - You must enter the full name of the servers in this field since the system creates direct one-to-one mappings between the servers you enter here and IP addresses in the etc/hosts file. For more information about registry changes made by JSAM, see the Client-side Changes Guide on the Global Support Center.
        - The system does not support Outlook through SVW, since Outlook applications require HKLM registry key changes.
    3. Select the **Create an access control policy allowing SAM access to these server** check box to enable access to the server specified in the previous step (enabled by default).

Note: You can only use JSAM to configure access to one Microsoft Outlook application per user role.

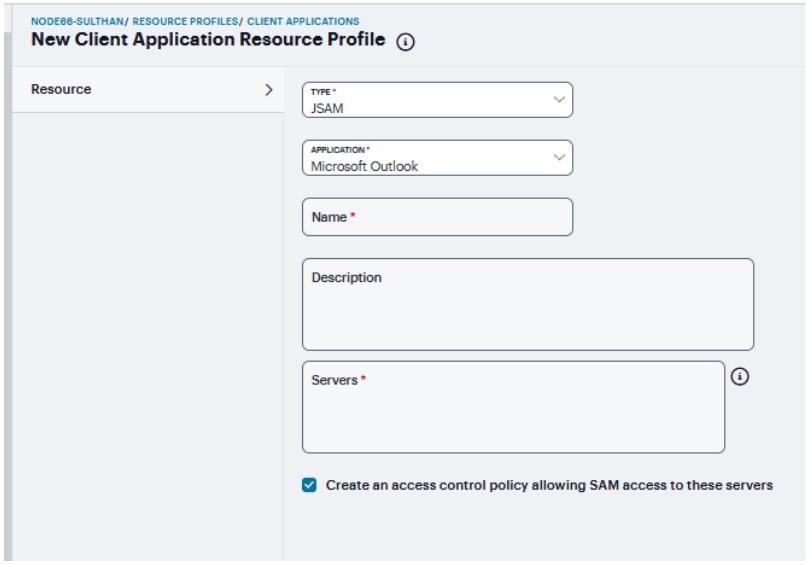


FIGURE 15.65 : Microsoft Outlook

- **NetBIOS file browsing** - Select this option to tunnel NetBIOS traffic through JSAM. Then:

  1. Enter a unique **Name** and optionally a **Description** for the resource profile.
  2. Enter the fully-qualified **Hostname** for your application servers in the Servers field.
     - You must enter the full name of the servers in this field since the system creates direct one-to-one mappings between the servers you enter here and IP addresses in the *etc/hosts* file. For more information about registry changes made by JSAM, see the Client-side Changes Guide on the Global Support Center.
     - If you want to enable drive mapping on a Windows client machine, use the standard NetBIOS file browsing option. When you do, JSAM automatically modifies the registry to disable port 445 on Windows machines, which forces Windows to use port 137, 138, or 139 for drive-mapping. Windows users need to reboot one time to enable the registry change to take effect.
  3. Select the **Create an access control policy allowing SAM access to these server** check box to enable access to the server specified in the previous step (enabled by default).

Note: You can only use JSAM to configure NetBIOS file browsing once per user role.

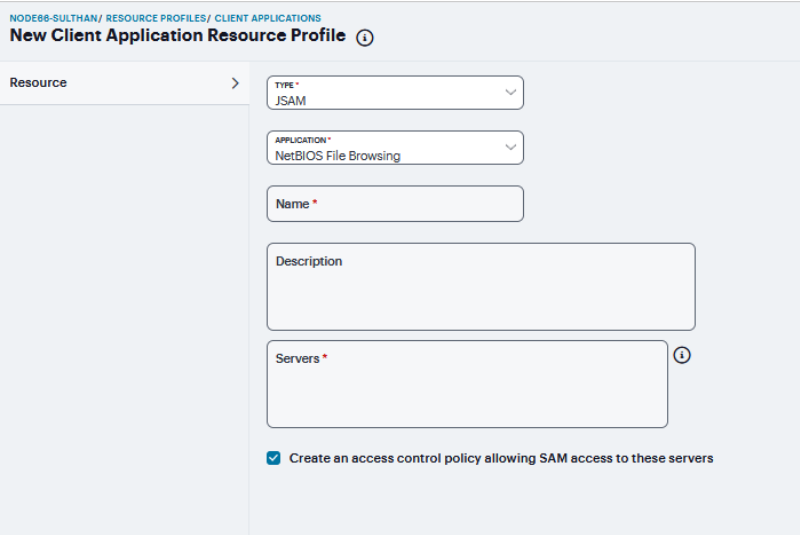


FIGURE 15.66 : NetBIOS file browsing

6. Click **Save Changes**.

PSAM Destinations

When you create a PSAM destination network resource profile, the PSAM client intercepts requests from processes running on the client to internal hosts. When destinations (using either IP address or hostnames) are configured on the system, all DNS and NetBIOS names are resolved through the system.

To create a PSAM destination network resource profile:

1. Navigate to **Users > Resource Profiles > SAM > PSAM Destinations**.
2. Click '**+**', enter a unique **Name** and optionally a **Description** for the resource profile.

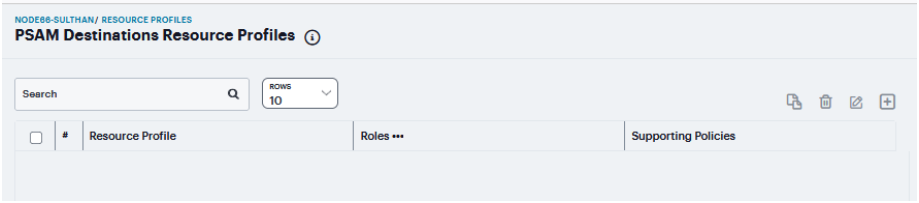


FIGURE 15.67 : PSAM Destinations

3. In the PSAM Destinations section, click '**+**', specify which servers you want to secure using PSAM. You can specify the servers as hostname or IP/netmask pairs. You may also include a port. and click **Save Changes**.
4. Select the **Create an access control policy allowing SAM access to this server** check box to enable access to the server specified in the previous step (enabled by default).

5. Click **Save Changes**.

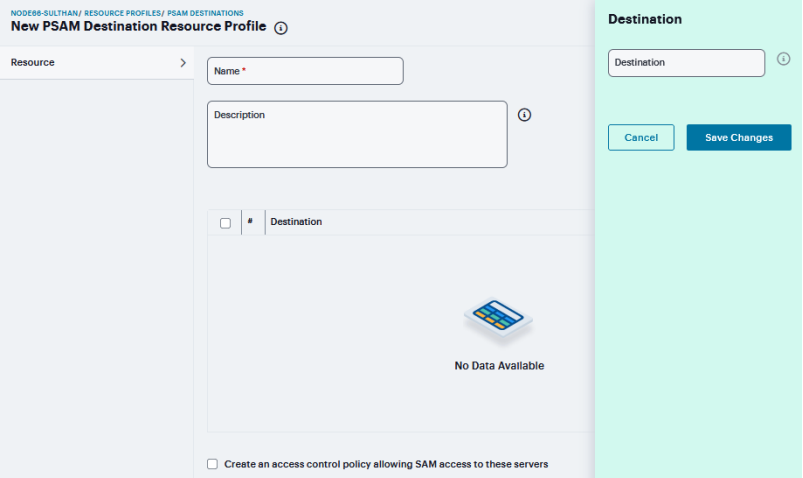


FIGURE 15.68 : PSAM Destinations section

Secure Mail

To use Secure Mail for iOS devices, you must enable it at the role level and then create a resource profile that specifies the Exchange server and encryption settings. You must also obtain and import an S/MIME certificate.

To define the Secure Mail resource profile:

1. Navigate to **Users > Resource Profiles > Mobile**.
2. Specify the information in the following table:

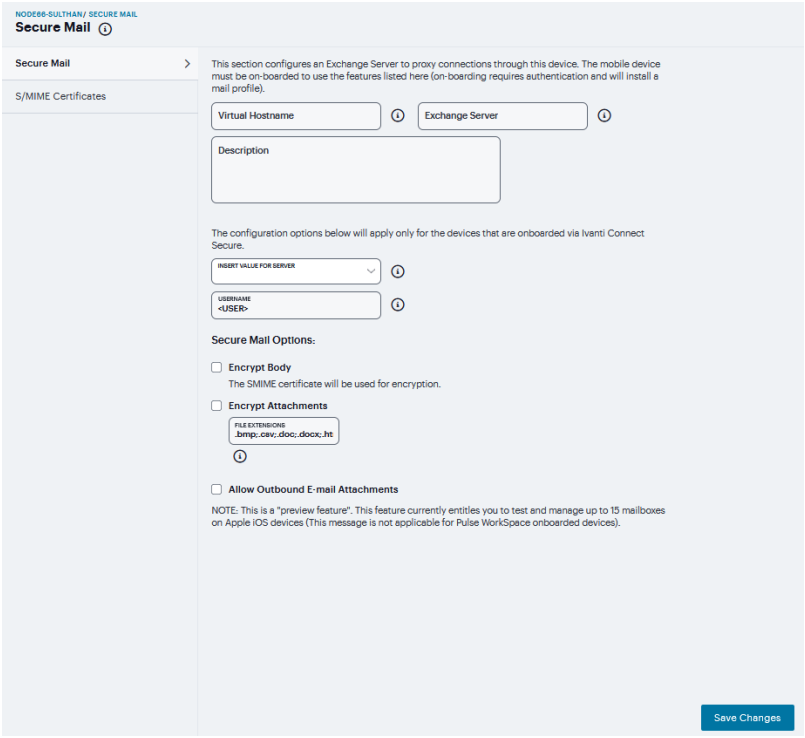


FIGURE 15.69 : Secure Mail

TABLE 15.1 : Secure Mail Settings

Setting	Guidelines
Virtual Hostname	Enter a hostname alias for the Exchange server, and update your DNS server to map the alias to the IP address of Ivanti Connect Secure. The name must be unique among all virtual hostnames. For example, if the virtual hostname is email.com, and the backend URL is https://mail.pulsesecure.net:8080, a client request to https://email.com/test1 via Ivanti Connect Secure is converted to https://mail.pulsesecure.net:8080/test1. The response to the converted request is sent to the client web browser.
Exchange Server	Enter the URL and port number of the Microsoft Exchange server, such as https://mail.pulsesecure.net:379. If the port number is omitted, it defaults to 80.
Description	Description of the Exchange server (optional).
Username	Select one of the following to specify the e-mail account format used by the Exchange server: • **None**: Inserts the <USER> variable for the user's login name for Ivanti Connect Secure (the default). • **Exchange 2007/2010/2013**: Inserts the <NTDOMAIN><USER> variables to include the user's domain before the login name. • **Office 365**: Inserts <USER>@domain.com, and you can enter the appropriate domain, such as <USER>@pulsesecure.net.
Secure Mail Options	Select one or more of the following encryption options: • **Encrypt Body**: Encrypts the body of the e-mail using an S/MIME certificate. The encrypted e-mail body can be viewed by any native e-mail client. Graphics embedded in the encrypted e-mail body are displayed twice on iOS devices. • **Encrypt Attachments**: Encrypts the e-mail attachments using a key generated by Ivanti Connect Secure. Encrypted attachments, which must be opened with Ivanti Mobile Client, are identified by a pulsesecure file extension, such

3. Click **Save Changes**.

S/MIME Certificate

If you enable Secure Mail, an S/MIME is required for each client device. You can generate an S/MIME certificate for each device or use a global certificate for all devices by requesting an S/MIME certificate from a Certificate Authority (CA) and importing the certificate and private key to Ivanti Connect Secure.

To generate or import an S/MIME certificate:

1. Navigate to **Users > Resource Profiles > Mobile > S/MIME Certificate**.

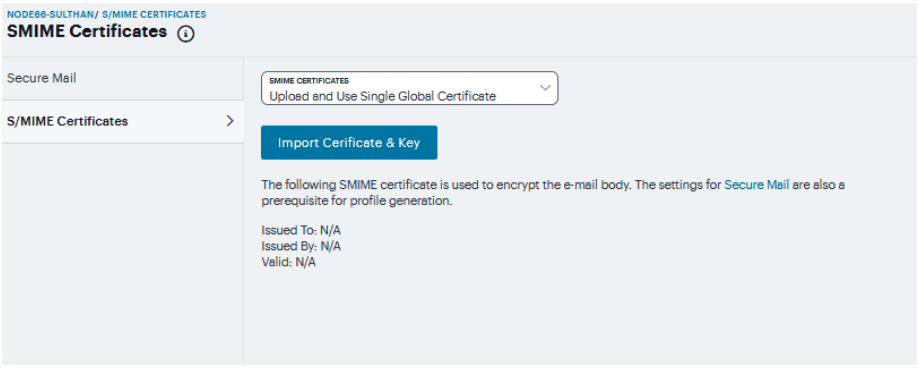


FIGURE 15.70 : S/MIME Certificate

2. Specify one of the following options:

TABLE 15.2 : S/MIME Certificate Settings

Setting	Guidelines
Generate per User Certificate	Select this option to use the SCEP server and a CSR template to generate a certificate for each client. Select a CSR template from the Use Certificate Template list. To create a CSR template, see Configuring Enterprise Onboarding.
Upload and Use Single Global Certificate	Select this option to use the same certificate for all client devices. Click **Import Certificate & Key**, click **file** field in one of the following forms to locate the **certificate file**, enter the **password key** if the file is encrypted, and then click **Import**. • **If certificate file includes private key**: When the certificate and key are contained in one file. • **If certificate and private key are separate files**: When the certificate and key are in separate files. • **Import via System Configuration file**: When the certificate and key are contained in a system configuration file that has been exported from Ivanti Connect Secure.

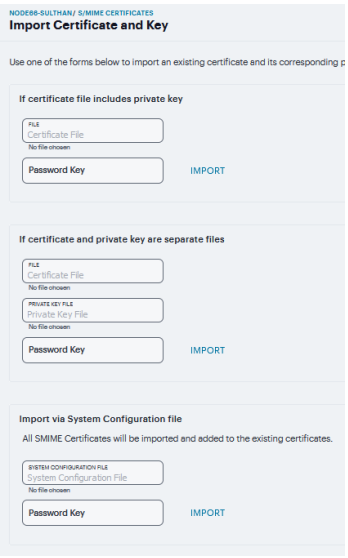


FIGURE 15.71 : S/MIME Certificate

Resource Policies

A resource policy is a system rule that specifies resources and actions for a particular access feature. A resource is either a server or file that can be accessed through the system, and an action is to "allow" or "deny" a resource or to perform or not perform a function. Each access feature has one or more types of policies, which determine the system's response to a user request or how to enable an access feature. You may also define detailed rules for a resource policy, which enable you to evaluate additional requirements for specific user requests.

You can create the following types of resource policies through the Resource Policies pages:

- **Web Resource Policies** - specify the Web resources to which users may or may not browse. They also contain additional specifications such as header caching requirements, servers to which java applets can connect, code-signing certificates that the system should use to sign java applets, resources that the system should and should not rewrite, applications for which the system performs minimal intermediation, and single sign-on options.
- **File Resource Policies** - specify the Windows, UNIX, and NFS file resources to which users may or may not browse. hey also contain additional specifications such as file resources for which users need to provide additional credentials.
- **Secure Application Manager Resource Policies** - allow or deny access to applications configured to use JSAM or PSAM to make socket connections.
- **Terminal Services Policies** - allow or deny access to the specified Windows servers or Citrix Metaframe servers.
- **VPN Tunneling Resource Policies** - allow or deny access to the specified servers and specified IP address pools.
- **HTML5 Access Resource Policies** - allow or deny clientless to terminal servers using RDP/SSH/Telnet protocols.

Note: You can also create resource policies as part of the resource profile configuration process. In this case, the resource policies are called "advanced policies."

Resource policies are an integral part of the access management framework, and therefore are available on all Ivanti Connect Secure products. However, you can access only resource policy types that correspond to your licensed features.

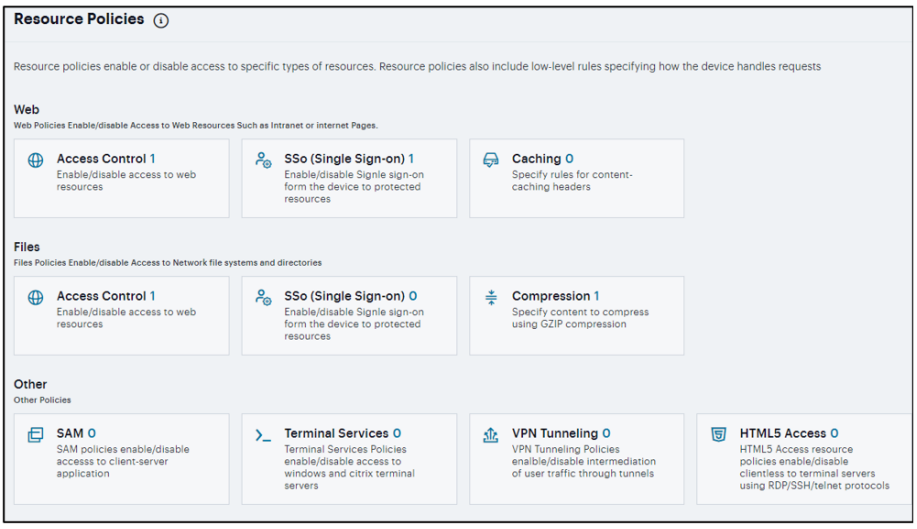


FIGURE 15.72 : Resource Policies

Ivanti Secure Access Client Connections

An Ivanti Secure Access component set includes specific software components that provide Ivanti Secure Access Client connectivity and services.

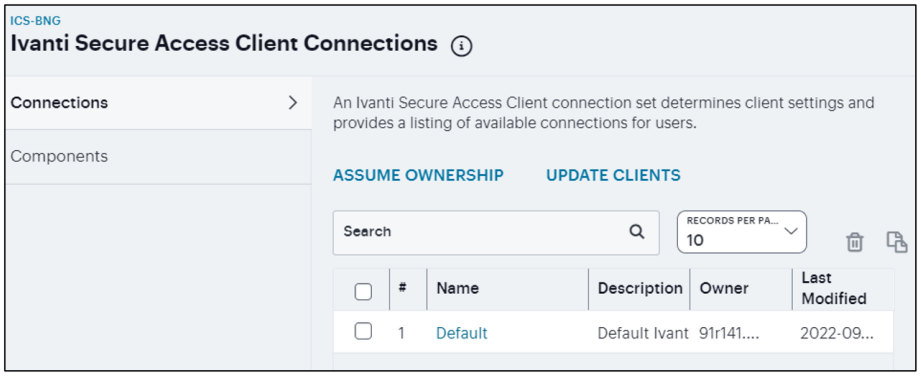


FIGURE 15.73 : Ivanti Secure Access Client Connections

Ivanti Secure Access Client Connection Set Options

The following items apply to all connections in a connection set.

- Allow saving logon information: Controls whether the Save Settings check box is available in login dialog boxes in Ivanti Secure Access Client. If you clear this check box, Ivanti Secure Access Client always requires users to provide credentials. If you select this check box, users have the option of saving their credentials.
- Ivanti Secure Access Client can retain learned user settings: These settings are retained securely on the endpoint, evolving as the user connects through

different Ivanti servers. Ivanti Secure Access Client can save the following settings:

  - Certificate acceptance
  - Certificate selection
  - Realm
  - Username and password
  - Proxy username and password
  - Secondary username and password
  - Role

- VPN only access: When Ivanti Secure Access Client connects to Ivanti Connect Secure having lock down mode enabled, it will enable lock-down mode and block network if VPN is not in connected state.

  When VPN only access option is enabled, the Enable captive portal detection and Enable embedded browser for captive portal will be automatically checked and cannot be edited.

- Display splash screen: Clear this check box to hide the Ivanti Secure Access Client splash screen that normally appears when Ivanti Secure Access Client starts.

- Dynamic certificate trust: Determines whether users can opt to trust unknown certificates. If you select this check box, a user can ignore warnings about invalid certificates and connect to the target Ivanti server.

- Dynamic connections: Allows connections within this connection set to be automatically updated or added to Ivanti Secure Access Client when the user connects to Ivanti Connect Secure through the user Web portal, and then starts Ivanti Secure Access Client through the Web portal interface. Dynamic connections are created as manual rather than automatic connections, which means that they are run only when the user initiates the connection or the user browses to a Ivanti server and launches Ivanti Secure Access Client from the server's Web interface.

  If dynamic connections are disabled, and the user logs in through the Web portal of a Ivanti server that is not already included in Ivanti Secure Access Client's connection set, then starting Ivanti Secure Access Client from the Web portal does not add a new Ivanti Secure Access Client connection for that Ivanti server. If you choose to disable dynamic connections, you can still allow users to manually create connections by enabling Allow User Connections.

- Enable captive portal detection: To detect the presence of a captive portal hotspot enable this option. It can be applied only to Ivanti Connect Secure and Ivanti Policy Secure (L3) connections.

- Enable embedded browser for captive portal: When enabled, Ivanti Secure Access Client uses an embedded web browser that the end user can use to traverse captive portal pages and to gain network connectivity for establishing a VPN connection. This applies only when captive portal detection is enabled.

- Enable embedded browser for authentication: When enabled, Ivanti Secure Access Client uses an embedded browser for web authentication, rather than external browser.
- FIPS mode enabled: Enable FIPS mode communications for all Ivanti Secure Access Client connections in the connection set. The Federal Information Processing Standard (FIPS) defines secure communications for the U.S. government. When a Ivanti Secure Access Client connection is operating in FIPS mode, FIPS On appears in the lower corner of the Ivanti Secure Access Client interface. If your Ivanti Connect Secure hardware does not support FIPS mode operations, FIPS mode configuration options are not present in the admin console interface. FIPS mode operations are supported on PSA-V Series Ivanti Gateways and some SA series appliances. The device must be running Ivanti Policy Secure R5.0 or later or Ivanti Connect Secure R8.0 or later.
- Prevent caching smart card PIN: Enabling this field will allow system administrators to prevent smart card PIN values from being cached. This feature is applicable only to Windows.
- Wireless suppression: Disables wireless access when a wired connection is available. If the wired connection is removed, Ivanti Secure Access Client enables the wireless connections with the following properties:
  - Connect even if the network is not broadcasting.
  - Authenticate as computer when computer information is available.
  - Connect when this network is in range.

Creating a Client Connection Set for Ivanti Connect Secure

To create a Ivanti Secure Access Client connection set:

1. Select **Users > Ivanti Secure Access Client > Connections**.
2. Click '+' to create a new connection set.
3. Enter a name and, optionally, a description for this connection set.

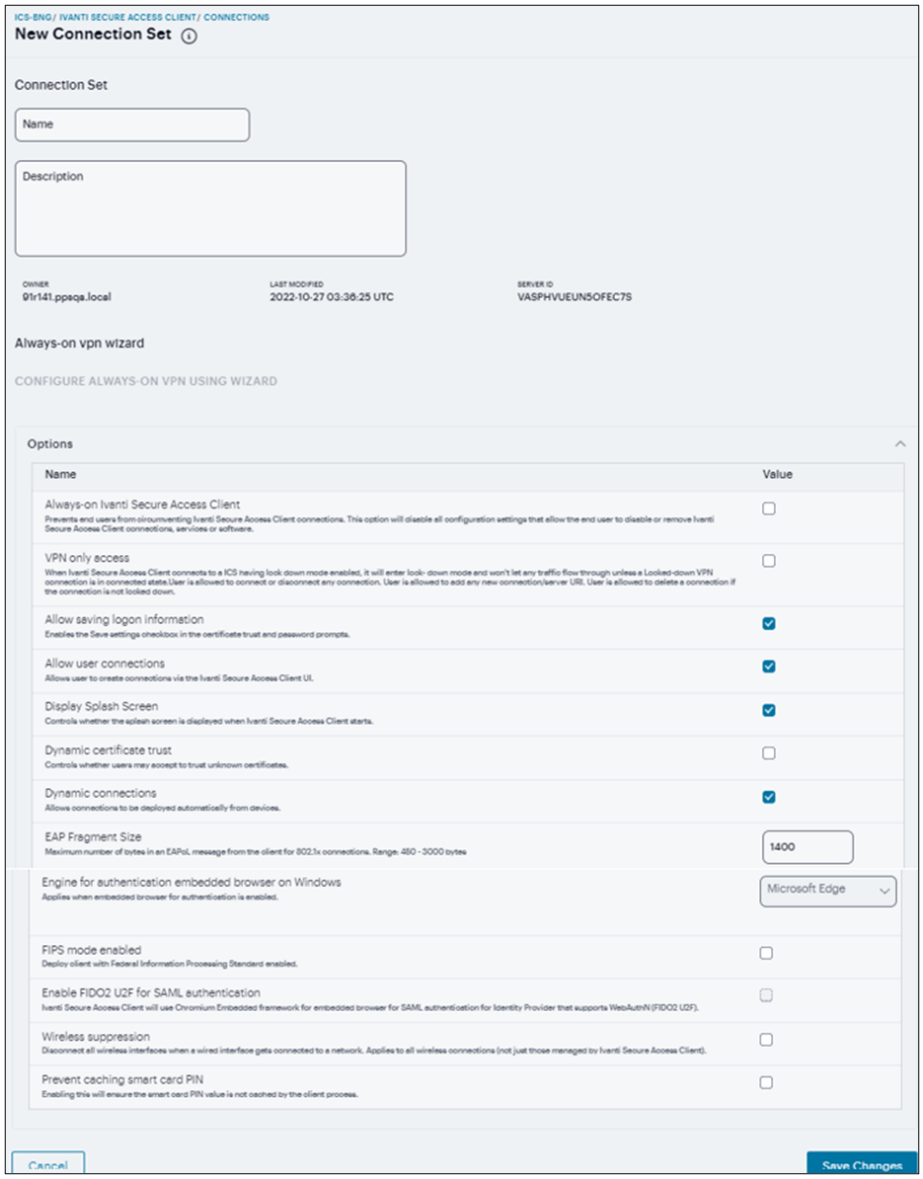


FIGURE 15.74 : Connection Set

4. Under Options, select or clear the following check boxes:

   - **Allow saving logon information**: Controls whether the Save Settings check box is available in login credential dialog boxes in Ivanti Secure Access Client. If you clear this check box, Ivanti Secure Access Client always requires users to provide credentials. If you select this check box, users have the option of saving their credentials.
   - **Allow user connections**: Controls whether connections can be added by the user through the Ivanti Secure Access Client interface.
   - **Display splash screen**: Clear this check box to hide the Ivanti Secure Access Client splash screen that normally appears when Ivanti Secure Access Client starts.
   - **Dynamic certificate trust**: Determines whether users can opt to trust unknown certificates. If you select this check box, a user can ignore

warnings about invalid certificates and connect to the target Ivanti server.

- **Dynamic connections**: Allows new connections to be added automatically to Ivanti Secure Access Client when the user logs into a Ivanti server through the server's Web portal, and then starts Ivanti Secure Access Client though the Web portal interface.
- **FIPS mode enabled**: Enable FIPS mode communications for all Ivanti Secure Access Client connections in the connection set. The Federal Information Processing Standard (FIPS) defines secure communications for the U.S. government. When a Ivanti Secure Access Client connection is operating in FIPS mode, FIPS On appears in the lower corner of the Ivanti Secure Access Client interface.
- **Wireless suppression**: Disables wireless access when a wired connection is available. Wireless suppression occurs only when the wired connection is connected and authorized.

5. Under Connections, click '+' to define a new connection.
6. Enter a name and, optionally, a description for this connection.
7. Select a type for the connection and then specify the connection. Type can be any of the following:
   - **Policy Secure (802.1X)**: Select this type if the connection establishes connectivity to an 802.1X wired or wireless device.
   - **Connect Secure or Policy Secure (L3)**: Select this type to define a connection for Ivanti Connect Secure or Ivanti Policy Secure.
8. The connection configuration options that appear depend on the connection type you select.

   After you have created the client connection set:
   - create a client component set and select this connection set.
   - open this saved connection set and create sub connection set for it.

Creating a Client Component Set for Ivanti Connect Secure

To create a Ivanti Secure Access Secure Client component set:

1. Select **Users > Ivanti Secure Access Client > Components**.
2. Click '+' to create a new component set.

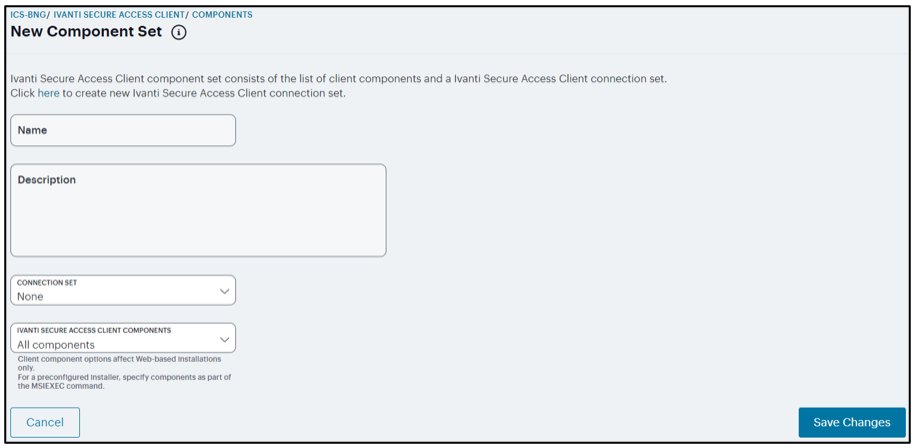


FIGURE 15.75 : Component Set

3. If you have not yet created a client connection set, select **Users > Ivanti Secure Access Client > Connections** and create a new connection set. Or you can use the default client configuration, which permits dynamic connections, and allows Ivanti Secure Access Client to automatically connect to Ivanti Policy Secure or Ivanti Connect Secure.
4. Specify a name for the client component set.
5. (Optional) Enter a description for this client component set.
6. Select a connection set that you have created, or use the default connection set.
7. For Ivanti Secure Access Client components, select one of the following options:
   - All components: Supports all Ivanti Secure Access Client connection types.
   - No components: Updates existing Ivanti Secure Access Client configurations, for example, to add a new connection. Do not use this setting for a new installation.
8. Click **Save Changes**.
9. After you create a component set, distribute Ivanti Secure Access Client to users through a role. When users access the role, the installer automatically downloads to the endpoint. The installer components and connections are applied to the endpoint client.
   - If client connections associated with the component set for a role are changed even though the list of components has not, the existing configuration on the endpoint is replaced immediately if the endpoint is currently connected, or the next time the endpoint connects.
   - If a user is assigned to multiple roles and the roles include different component sets, the first role in an endpoint's list of roles is the one that determines which client (component set) is deployed.

Manage Ivanti Secure Access Client Versions

This feature is supported for Ivanti Secure Access Client on macOS and Windows, and supported for iOS Mobile Client and Android Mobile Client also.

This feature allows admin to configure a minimum client version. If the client has version lower than the configured minimum version, then the ICS server will reject the client connection.

If the client is older than the configured minimum client version, then ICS gateway will reject the connection. User can upgrade it later through browser or SCCM server.

To enable this feature on Ivanti Connect Secure:

1. From the admin console, select **Users > Ivanti > Components**.
2. Select the Enable minimum client version enforcement check box (see). The following options appear:
    - Ivanti Secure Access Desktop Clients
    - Android Mobile Clients
    - iOS Mobile Clients

Enterprise Onboarding

Enterprise onboarding allows users to securely access enterprise network resources with almost any device. WiFi, VPN and certificate profiles can be defined for enterprise resources and downloaded to a device during onboarding, depending on the device type.

The profiles can be defined on a single Ivanti Connect Secure server dedicated to onboarding or they can be defined on each server. Alternatively, the profiles can be defined on a third-party MDM server, in which case users will see a link and instructions on the onboarding page to continue onboarding using the external MDM server.

Onboarding is initiated from the browser. The supported profiles depend on the device type and whether the Ivanti Secure Access Client is installed. Device Onboarding Profile supports:

- Android 4.0 or later: Supports all profiles, but the Ivanti Secure Access Client must be installed during onboarding.
- iOS 6.0 or later: Supports all profiles (Safari browser).
- Windows 7.0, 8.0, and 8.1: Supports WiFi and certificate profiles (IE, Firefox, or Chrome browser). The Ivanti Secure Access Client onboarding application must be installed during onboarding. Windows 8 RT and Windows 8 Phone are not supported.
- MAC OS X: Supports WiFi and certificate profiles (Safari browser).

Enterprise onboarding is enabled in the user role, and each profile can be applied to all user roles or specific roles. The SCEP server and CSR templates allow certificates to be generated dynamically for device and server authentication.

Defining the SCEP Server

The Simple Certificate Enrollment Protocol (SCEP) server configuration and CSR templates allows each client device to dynamically obtain certificates for authentication.

To define the SCEP server:

1. Log into the nSA as a Tenant Admin.
2. From the ICS menu, click the **Gateway > Gateway List** and then select any standalone ICS Gateway.
3. Navigate to **Users > Enterprise Onboarding**.

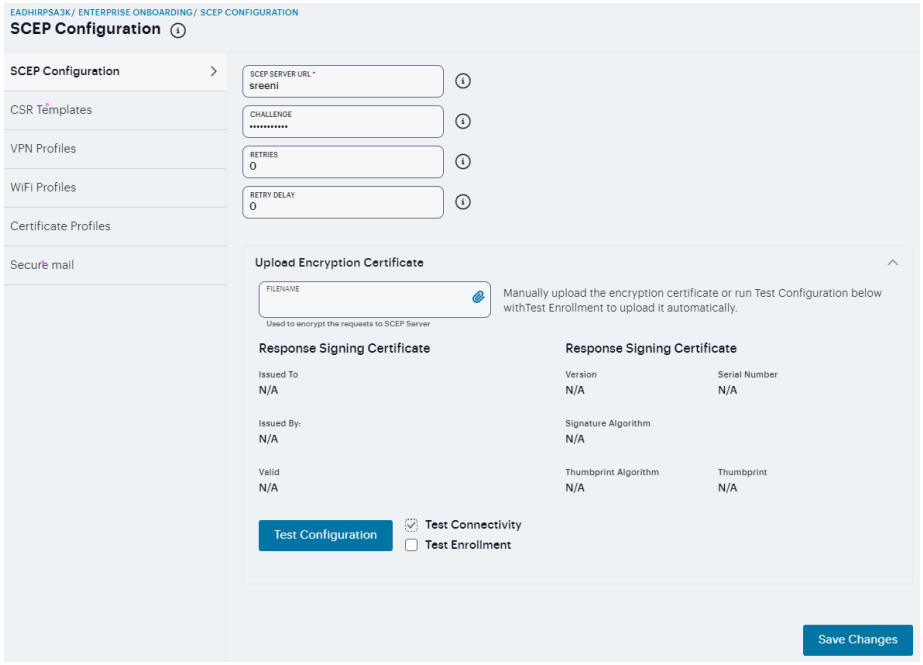


FIGURE 15.76 : SCEP Server

4. Enter the URL for the SCEP server.
5. Specify the password required by the SCEP server.
6. Specify the number of attempts to access the server when the first attempt fails.
7. Specify the number of seconds between retry attempts.
8. Click Browse to upload the certificate used to encrypt SCEP requests. To upload the certificate automatically, select the Test Enrollment check box, select a CSR template, and click **Test Configuration**.

9. Click **Save Changes**.

Defining CSR Templates

If the SCEP server is configured, the Certificate Signing Request (CSR) templates can be used in the VPN, WiFi, and certificate profiles to allow each onboarded device to dynamically obtain certificates for authentication on all mobile devices. Up to 10 templates can be defined.

To define CSR templates:

1. Navigate to **Users > Enterprise Onboarding** and select **CSR Templates**.

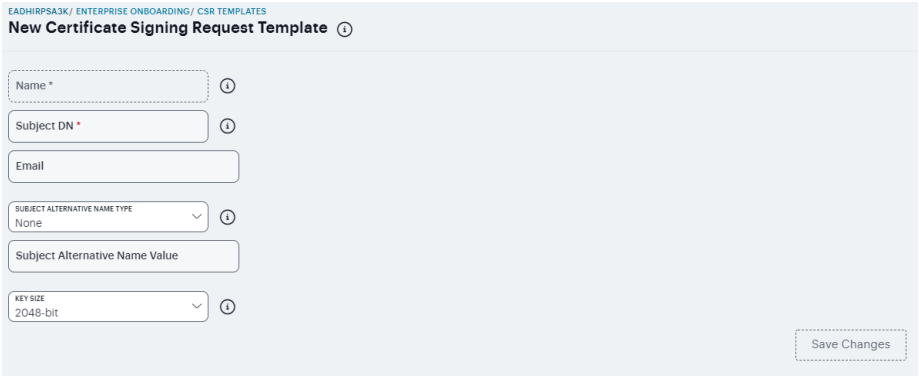


FIGURE 15.77 : CSR templates

2. Click '+' to add a new template.
3. Enter a unique template name.
4. Specify the subject distinguished name. For example: CN=<USERNAME>,OU=Engineering=Ivanti
5. (Optional) Specify an email address with the <USER> variable, such as <USER>@ivanti.com.
6. Select an alternative name type if the CA requires an alternative subject name.
7. Specify one or more values for the selected alternative name type. Multiple values must be separated by a comma or space.
8. Select the key size used by the SCEP server.
9. Click **Save Changes**.

Defining VPN Profiles

VPN profiles provide Android and iOS devices with secure access to enterprise networks. One or more VPN profiles can be assigned to specific user roles or to all roles. Up to 10 profiles can be defined.

To define VPN profiles:

1. Navigate to **Users > Enterprise Onboarding** and select **VPN Profiles**.

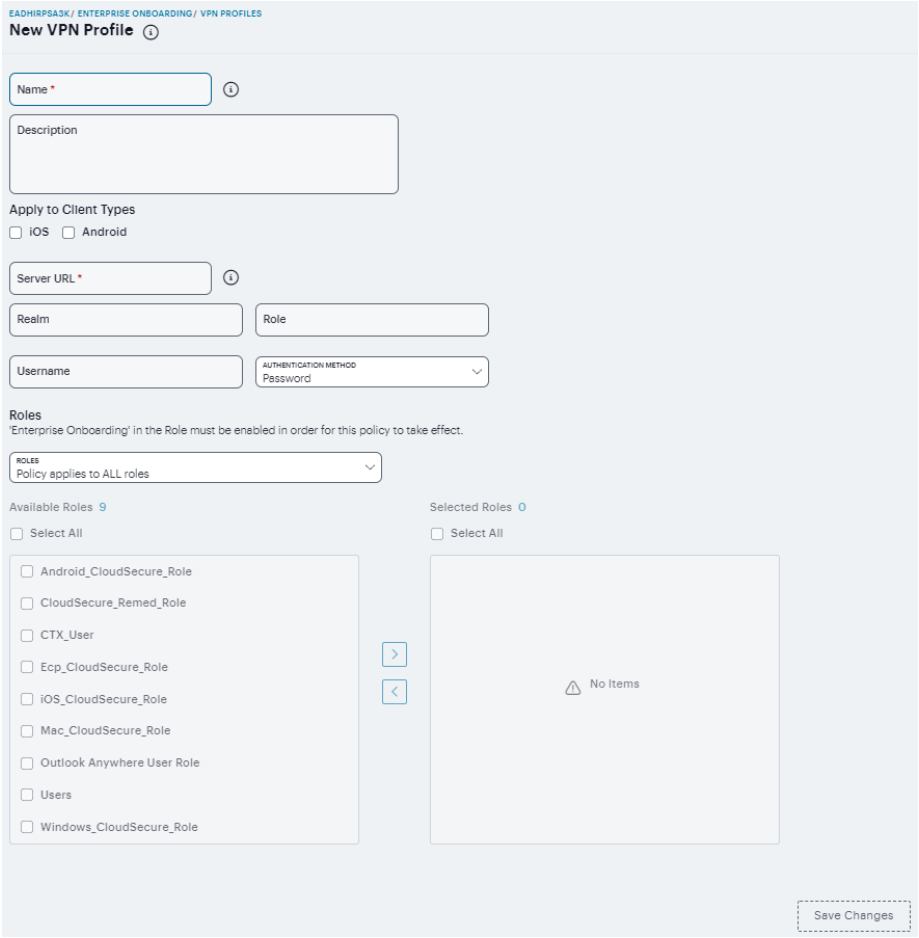


FIGURE 15.78 : VPN Profiles

2. Click '+' to add a new VPN profile.
3. Enter a unique name for the VPN profile.
4. (Optional) Enter a description of the VPN profile.
5. Select the device types the profile applies to (Android and iOS only).
6. Specify the URL of the VPN server.
7. Specify the realm name. The realm is required only if the sign-in URL has the User picks from a list of authentication realms option enabled.
8. Specify the user role. The user role is required if the role mapping rules for the user realm specify multiple roles and the User must select from among

assigned roles option is enabled.

9. Specify the <USER> variable for the user name.
10. Select Password or Certificate for the user authentication method.
11. Select one of the following options:
    - Policy applies to ALL roles - To apply this profile to all users.
    - Policy applies to SELECTED roles - To apply this profile only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
    - Policy applies to all roles OTHER THAN those selected below - To apply this profile to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
12. Click **Save Changes**.

Defining WiFi Profiles

WiFi profiles provide Android, iOS, MAC OS X, and Windows devices with secure access to wireless networks. One or more WiFi profiles can be assigned to specific user roles or to all roles. Up to 10 profiles can be defined.

To define WiFi profiles:

1. Navigate to **Users > Enterprise Onboarding** and select **WiFi Profiles**.

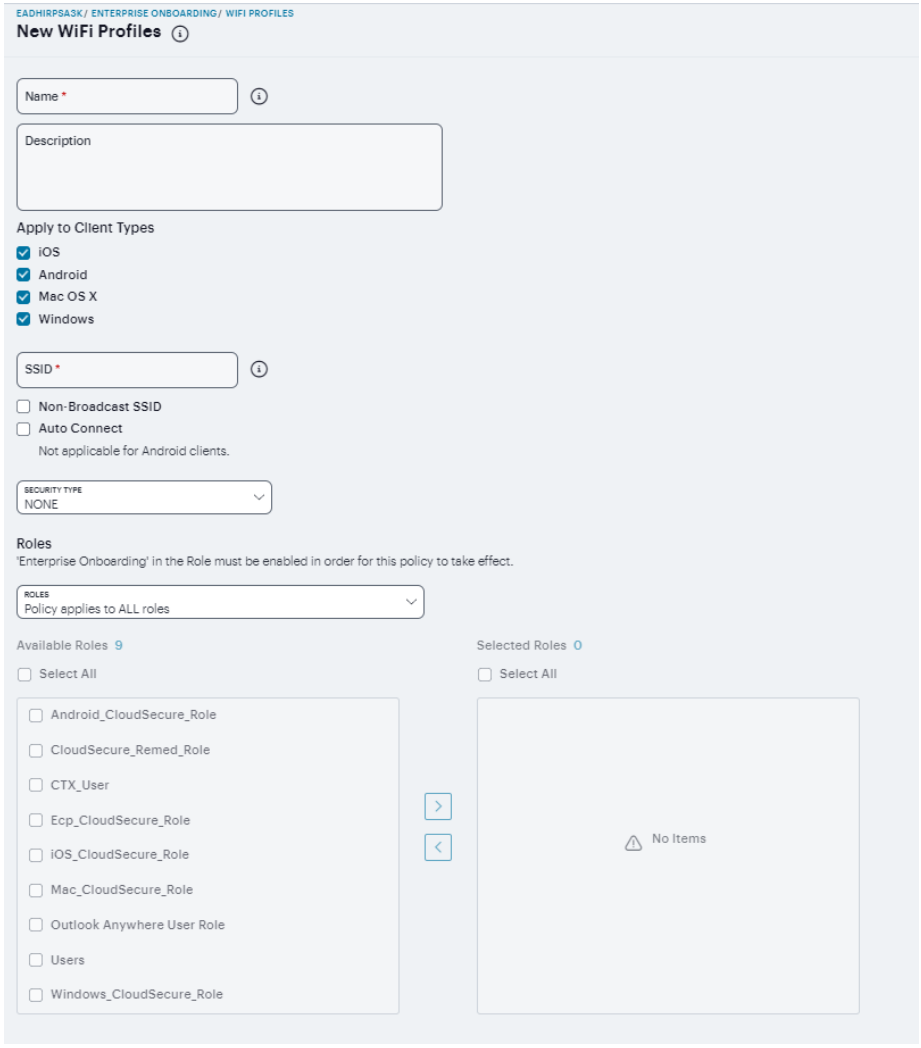


FIGURE 15.79 : Wi-Fi Profiles

2. Click '+' to add a new WiFi profile.
3. Enter a unique name for the WiFi profile.
4. (Optional) Enter a description of the profile.
5. Select the device types the profile applies to (Android, iOS, MAC OS X, and Windows).
6. Specify the server set ID of the wireless network.
7. Select the **Non-Broadcast SSID** check box if the wireless network does not broadcast its identity.
8. Select the **Auto Connect** check box to connect the client automatically when the network is detected (not supported by Android clients).
9. Select the type of authentication used by the network, and specify the password or enterprise settings, as required.
10. For the WPA Enterprise and WPA2 Enterprise security types, select the supported EAP protocols and specify the associated authentication settings.

11. The PEAP protocol is supported by all clients. Specify inner authentication method, username and password, outer identity, Trusted Server name, Trusted CA certificate.
12. The EAP-TLS protocol is supported by all clients. Specify User name, CSR template, IP address or FQDN name, Trusted CA certificate.
13. The TTLS protocol is supported by all clients. Specify inner authentication method, username and password, Trusted Server name, Trusted CA certificate.
14. Select a role from Policy applies to ALL roles, Policy applies to SELECTED roles, Policy applies to all roles OTHER THAN those selected below.
15. Click **Save Changes**.

Defining Certificate Profiles

Certificate profiles specify the device certificates sent to each client device during onboarding. Up to 10 profiles can be defined.

To define certificate profiles:

1. Navigate to **Users > Enterprise Onboarding** and select **Certificate Profiles**.

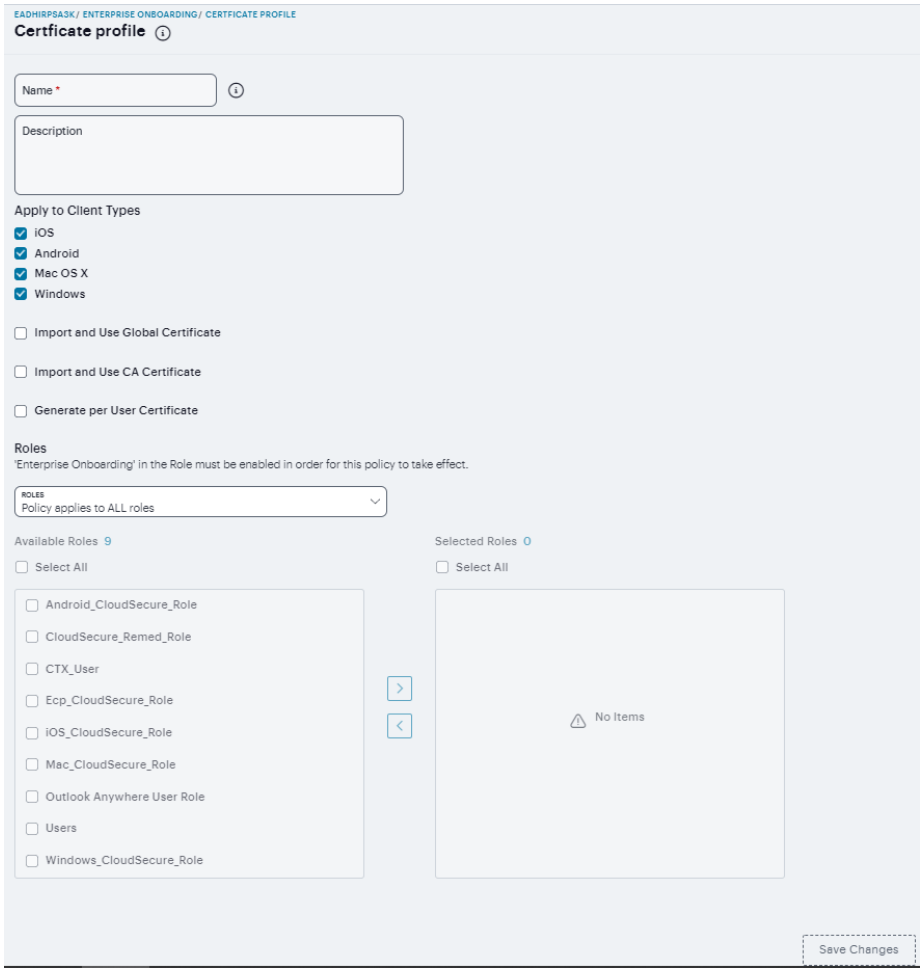


FIGURE 15.80 : Certificate Profiles

2. Click '+' to add a new certificate profile.
3. Select the device types the profile applies to (Android, iOS, MAC OS X, and Windows).
4. Select the **Import and Use Global Certificate** option to use the Ivanti Connect Secure global certificate to authenticate the client device. Click **Import Certificate & Key**, click **Browse** to locate the certificate file, and then click **Import**.
5. Select the **Import and Use CA Certificate** option to import any CA certificate (public Root CA, private Root CA, public intermediate CA, or private intermediate CA). These CA's can be used in WiFi profiles and must be downloaded to the client devices. Click Import and Use CA Certificate, click **Browse** to locate the certificate, and then click **Import CA Certificate**.
6. Select the **Generate per User Certificate** option to use the SCEP server and a CSR template to generate a certificate for each client. Select a CSR template from the Use Certificate Template list.
7. Select a role from Policy applies to ALL roles, Policy applies to SELECTED roles, Policy applies to all roles OTHER THAN those selected below.
8. Click **Save Changes**.

Defining Secure Mail

To define secure mail:

1. Navigate to **Users > Enterprise Onboarding** and select **Secure Mail**.

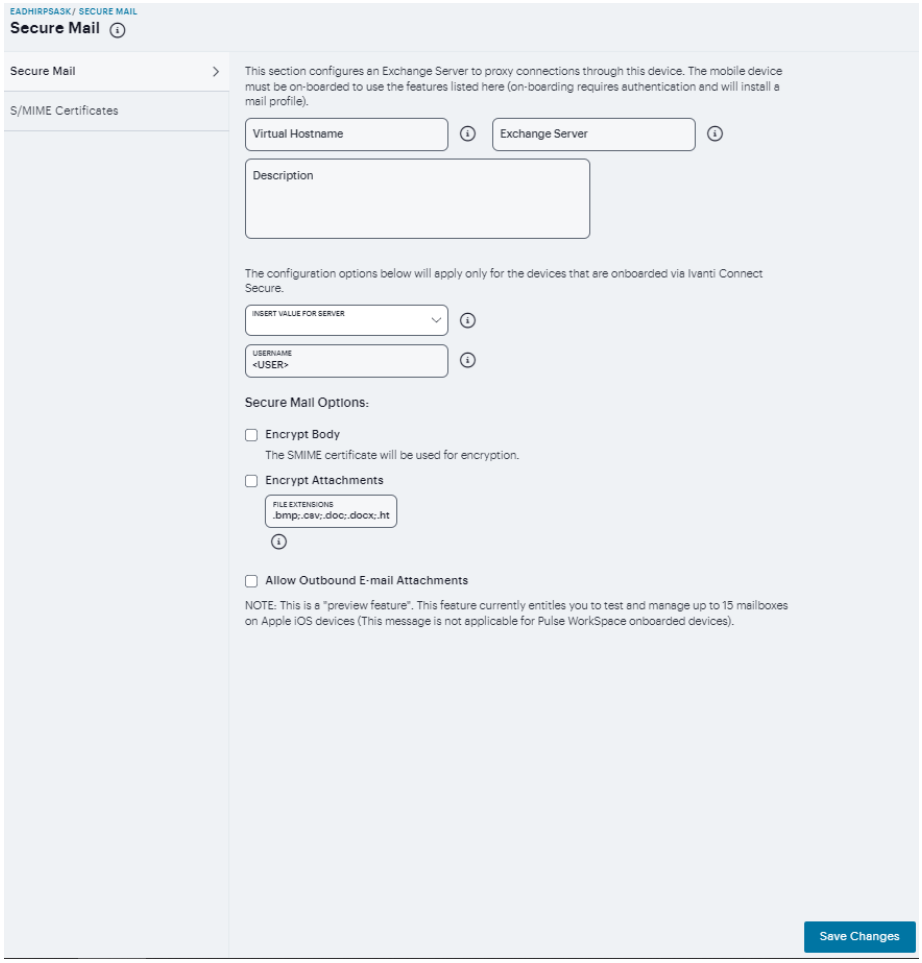


FIGURE 15.81 : Secure Mail

For the configuration details, see *Secure Mail* (page 414).

ICS Gateway Administration

Introduction

After you have logged into the nSA for the first time, you can create **authentication methods** and apply them to the **authentication policies** you define in your nSA deployment. You then apply an authentication policy, together with **admin rules**, to a **admin group**. A admin group forms part of a *Secure Access Policy*.

To view admin authentication methods currently defined on the nSA, see *Viewing Admin Authentication Methods* (page 436). To view user authentication policies, see *Viewing Admin Authentication Policies* (page 437).

This chapter includes workflows for configuring admin authentication according to each supported authentication type. nSA supports the following types:

- **Local authentication**: An authentication system that is internal to the nSA. You must create all users manually on the nSA, and update any required authentication policies. see *Workflow: Creating a Local Authentication Policy* (page 444).
- **Azure AD SAML authentication**: An existing remote SAML authentication system based on an Azure AD server. See *Workflow: Creating a SAML Authentication Policy With Azure AD and SAML(Custom)* (page 449).

- **SMAL Custom**: An customized remote SAML authentication system based on an on-premises ICS server. See *Workflow: Creating a SAML Authentication Policy With Azure AD and SAML(Custom)* (page 449).

After you have created the required authentication method and updated your admin authentication policies, you create admin rules and admin groups, see *Creating Admin Rules and Admin Groups* (page 438).

Optionally, you can associate each admin group with an *admin role*, see *Associating Admin Groups with Admin Roles* (page 442).

Viewing Admin Authentication Methods

To view the admin authentication methods defined on the nSA, click the **Administration** icon in the nSA menu, then select **Admin Management > Admin Authentication**.

The *Admin Authentication* page appears, showing all admin authentication methods:

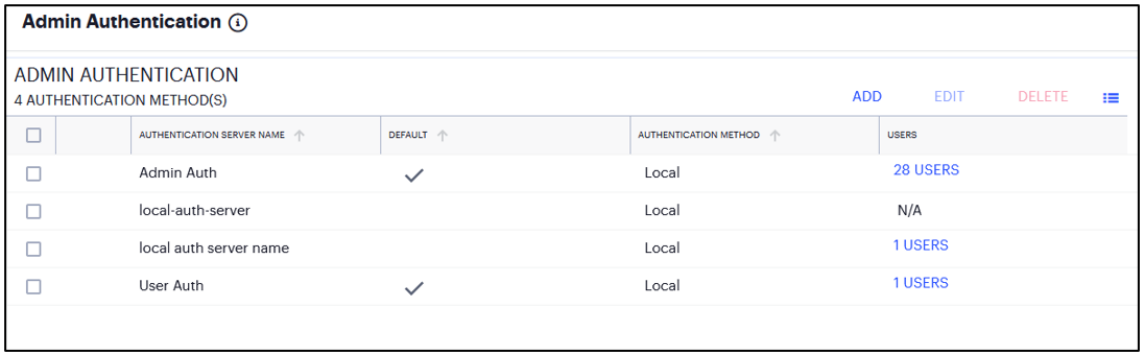


FIGURE 16.1 : Admin Authentication Methods

From this page, you can:

- Add a new authentication method by clicking **Add**.
- Edit an existing authentication method by selecting its check box and clicking **Edit**. Make any required updates and save the changes.
- Delete an unused authentication method by selecting its check box and clicking **Delete**. You must confirm the deletion.
- View the configured attributes for a SAML authentication method, where that method is configured for use with an authentication policy. To do this, click the arrow indicator to the left of the method name, where shown.

Viewing Admin Authentication Policies

To view the user authentication policies defined on the nSA, click the **Administration** icon in the nSA menu, then select **Admin Management > Admin Policies**.

The *Admin Policies* page appears, showing all user authentication policies.

FIGURE 16.2 : Admin Authentication Policies

nSA provides default/built-in authentication policies, suitable for the primary use-cases of administrative sign-in, user enrollment, and user sign-in:

- *Admin SignIn*. This policy is used whenever admin users log in. That is, for connection requests to the **/login/admin/* URL. It is referenced by the *ALLADMINUSERS* user rule, which associates it with the *ADMINISTRATORS* user rule group.

This policies is fixed and cannot be deleted. However, you can edit to reference a specific authentication method.

Furthermore, you can create additional custom authentication policies to enable bespoke authentication for specific groups of users or parts of your organization. Each policy should contain a unique access URL to which your users connect, and each should then be configured to link to an authentication method applicable for that purpose.

To learn more about how admin authentication policies are used in a nSA service.

From this page, you can:

- (For SAML authentication) Download policy metadata files that are required for external SAML enrollment or sign-in apps. To do this, select the check box for the required policy and click **Download**. Save the file to your local workstation.
- View the configured attributes for a SAML-authenticated policy, where that policy is configured with a valid SAML authentication method. To do this, click the arrow indicator to the left of the policy name, where shown.
- Add an authentication policy by clicking **Add**.
- Edit an existing authentication policy by selecting its check box and clicking **Edit**. Make any required updates and save the changes.
- Delete an unused authentication policy by selecting its check box and clicking **Delete**. You must confirm the deletion.

Creating Admin Rules and Admin Groups

After your authentication method is established and associated with an authentication policy, you can set up any required *admin rules* and *admin groups*. A admin rule identifies one or more admin users based on a test against a selected attribute present in a admin credential or profile, checked against either a local authentication record or from a SAML authentication service. For information about creating admin rules, see *Creating Admin Rules* (page 438).

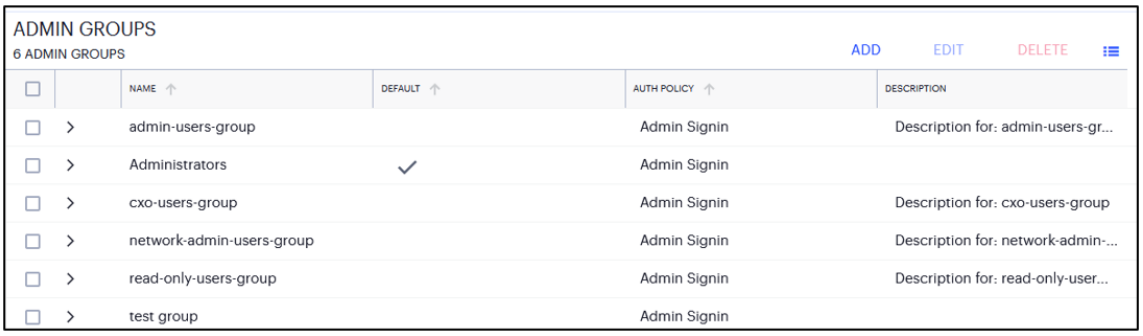


FIGURE 16.3 : Performing authentication through a Admin Group

You associate one or more user rules with an *authentication policy* to form a *user group* (see *Creating Admin Groups* (page 441)). Users requesting authorization for a service controlled by a Secure Access Policy must pass all the rules contained in the admin Group attached to the policy.

A admin group is required when defining a *secure access policy*. The admin group identifies the users and the authentication policy to which a secure access policy applies.

Optionally, you can associate each user group with an admin role, see *Associating Admin Groups with Admin Roles* (page 442).

Creating Admin Rules

Through admin rules, an admin can construct a test to provide authorization to only those users of a particular name, role, group, or some other stored attribute. In the rule configuration, you select the admin attribute on which you want a test to be performed.

nSA includes the following default admin rule:

- *ALLADMINUSERS*. This matches all admin users, and is referenced by the default *ADMINISTRATORS* admin group, which associates it with the built-in *Admin Signin* authentication policy.

Note: To read more about default admin groups, see *Creating Admin Groups* (page 441). To read more about built-in authentication policies, see *Viewing Admin Authentication Policies* (page 437).

This preset configuration of rules, groups, and policies is suitable for typical use cases involving whole-organization authorization needs. In other words, where you require only a single admin user authorization path that matches all users. For scenarios where you require more specific admin user authorization checks, you can create additional rules to match specific types of users.

When you create a rule, you select the admin attribute with which you want this rule to test. nSA provides the following rule attribute types:

- **username**: For local authentication methods, choose this attribute type to match against locally-defined user names.
- **SAML (Azure AD)**: For SAML authentication methods, choose this attribute type to match against user names or groups provided by the SAML service.
- **Custom**: For SAML authentication methods, choose this attribute type to match against a custom SAML attribute expression.

To create a admin rule:

1. From the nSA menu, click the **Administration** icon, then select **Admin Management > Admin Rules**.

   The *Admin Rules* page appears. This page lists all admin rules.

2. Click **Add**.

   The **Add Admin Rule** form appears.

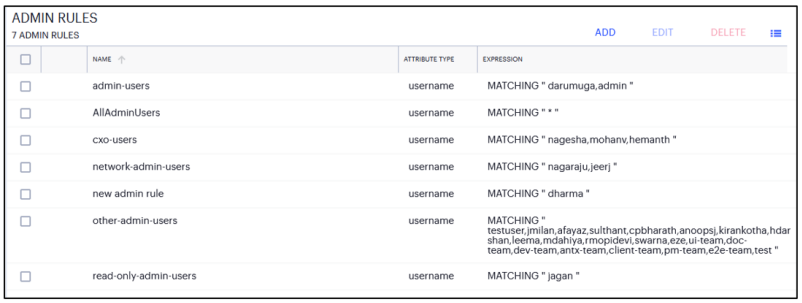


FIGURE 16.4 : Add Admin Rules

3. Enter a **Rule Name**.
4. Click **Select Attribute Type** and select one of the available options:
   - *Username*: Matches user names in a local authentication method. When you select this option, you must then:
     - Select an **Expression** type, either *Matching* or *Not Matching*.
     - For the **Admin** value, enter a match expression for the selected **Expression** type. For the value:
       * A comma-separated list of items is supported where required.
       * Wildcard matches are supported.
       * Special characters are supported.

* Single and double quotes are not supported.

Note: Ivanti recommends that a basic asterisk wildcard is not used when you intend to associate admin roles with user groups. Instead, a more-specific wildcard that only includes admin users is required in this case to prevent all users having total access rights.

- *SAML (Azure AD)*: Matches user names or groups in a SAML authentication method. When you select this option, you must then:
  - Select a **SAML Attribute Type**, either *Username* or *Group*.
  - For **Attribute Value**, enter a match expression for the selected **SAML Attribute Type** as a SAML expression.
- *Custom*. Matches against a custom SAML attribute expression. When you select this option, use the **Type or Create an Expression** property to enter an attribute expression. Supported formats include:
  - For simple user attribute key-value matching, use the syntax `userAttr.<attr-key> [=|!=] <attr-value>`. For example:

```
- userAttr.memberOf = "CN=sales,DC=example,DC=com"
- userAttr.mail = "user1@example.com"
- userAttr.realm = "Users"
- userAttr.department != "example_department"
```

  - To match against attributes that can have multiple values associated with a single attribute key, use the syntax `samlMultiValAttr.<attr-key> [=|!=] (<list>)`. For example:

```
- samlMultiValAttr.memberOf = ("CN=Employee,CN=Users,
↪DC=example_demo,DC=com")
- samlMultiValAttr.memberOf = ("CN=Users,DC=example_demo,
↪DC=com")
```

  - Use brackets and AND/OR operators to construct logical compound expressions:

```
- userAttr.groups = ("Group1" or "Group2")
- userAttr.realm = ("ztaqa") and samlMultiValAttr.memberOf
↪= ("CN=sales,DC=uisdp,DC=com")
- userAttr.realm = ("ztaqa") or samlMultiValAttr.memberOf
↪= ("CN=sales,DC=uisdp,DC=com")
- userAttr.realm != ("ztaqa") and samlMultiValAttr.
↪memberOf = ("CN=sales,DC=uisdp,DC=com")
```

5. Click **Create**.

   The new admin rule is added to the list of admin rules.
6. Repeat steps 3-6 for each required user rule.
7. (Optional) Edit an existing admin rule by selecting its check box and clicking **Edit**. Make any required updates and save the changes.

8. (Optional) Delete an unused admin rule by selecting its check box and clicking **Delete**. You must confirm the deletion.

After you have created all required admin rules, you can create admin groups, see *Creating Admin Groups* (page 441).

Creating Admin Groups

After you have created admin rules (see *Creating Admin Rules* (page 438)), you associate one or more admin rules with an authentication policy to form a Admin group.

Note: Admin groups are one of the four dimensions of a Secure Access Policy.

---

nSA includes the following default user group:

- *ADMINISTRATORS*. This admin group associates the default *ALLADMINUSERS* admin rule with the built-in *Admin Signin* authentication policy.

Note: To read more about built-in authentication policies, see *Viewing Admin Authentication Policies* (page 437).

This preset configuration of rules, groups, and policies is suitable for typical use cases involving whole-organization authorization needs. In other words, where you require only a single admin user authorization path that matches all users. For scenarios where you require more specific admin user authorization checks, you can create additional admin groups to make different associations of admin rules and custom authentication policies.

To create a admin group:

1. From the nSA menu, click the **Administration** icon, then select **Admin Management > Admin Groups**.

   The *Admin Groups* page appears. This page lists all admin rule groups.

2. Click **Add**.

   A form appears to enable you to create the admin group.

FIGURE 16.5 : Add Admin Groups

3. Enter a **Admin Group Name**.

4. Click **Select an Authentication Policy** and select the required authentication policy.
5. Add a **Description** for the admin group.
6. Select each of the listed **Admin Rules** that are required in the user group.
7. Click **Create**.

   The new admin group appears in the **admin Groups** list.
8. Repeat steps 2-7 to create all required user groups.
9. (Optional) To edit a listed admin group, click its **Edit** control and make any required updates.
10. (Optional) To delete an *unused* admin group, click its **Delete** control and confirm the deletion.

After you have created admin groups, you can optionally assign the admin group to an admin role, see *Associating Admin Groups with Admin Roles* (page 442).

Associating Admin Groups with Admin Roles

An admin role defines the elements of the admin interface that an associated admin user group can access.

The current admin can only access an individual admin interface page/workflow if their admin group is associated with an admin role that permits it. The tasks they can perform within that displayed element depends on the permissions set within the admin role.

Note: When you are using admin roles, Ivanti recommends that any admin rules for administrators does not use a basic asterisk wildcard, see *Creating Admin Rules* (page 438). Instead, a more-specific wildcard that only includes admin users is required in this case to prevent all users having total access rights.

Note: Admin roles are not created by the tenant admin using the nSA user interface. Rather, they are set up by the Ivanti DevOps team.

For example, the DevOps team might define the following admin roles:

- The *.Administrators* admin role has access to all user interface elements (full read, create, update, delete rights).
- The *.Read-Only Administrators* admin role has access to all user interface elements except workflows (read only).
- The *.Network Administrators* admin role has access to Gateways and Insights (read only).
- The *.CxOs* admin role has access to Insights only (read only).

Note: For more information about your assigned admin roles, please contact Ivanti DevOps.

The Admin can view admin roles in the **Administration > Admin Roles** page, and associate each role with a single user group.

To associate a user group with an admin role:

1. Log into the nSA as a Tenant Admin.
2. From the nSA menu, click the **Administration** icon, then select **Admin Roles**.

   A list of Admin Roles appears. For example:

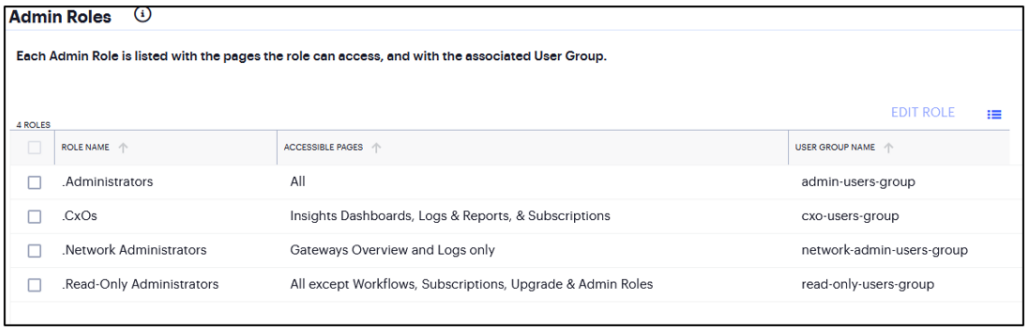


FIGURE 16.6 : Admin Roles

3. Click the *Edit* icon for the admin role you want to update.

   A dialog appears. For example:

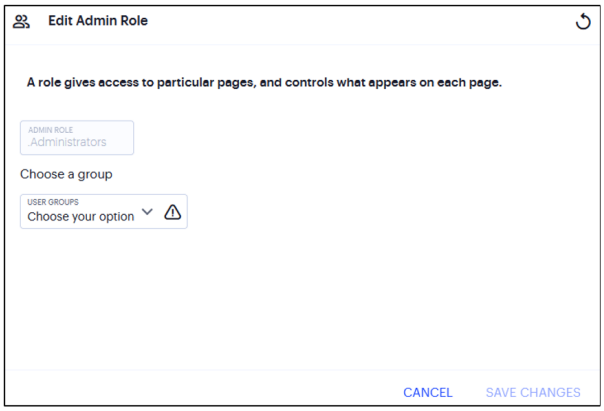


FIGURE 16.7 : Edit Admin Roles

4. Under **Choose group**, select the user group that you want the admin group to be associated with.
5. Click **Save Changes**.
6. (Optional) Repeat steps 3 to 5 for each admin role.

Workflow: Creating a Local Authentication Policy

This process involves creating a local authentication *method* and defining within it all user credentials necessary to identify and authenticate your end-users. Before you begin, make sure you have all user details (name and password) ready.

Note: nSA includes built-in default authentication policies, each of which references a built-in local authentication method.

To configure a *new* local authentication method:

1. Log into the nSA as a Tenant Admin
2. From the nSA menu, click the **Administration** icon, then select **Admin Management > Admin Authentication**.

   The **Admin Authentication** page appears. This page lists all existing admin authentication methods. For example:

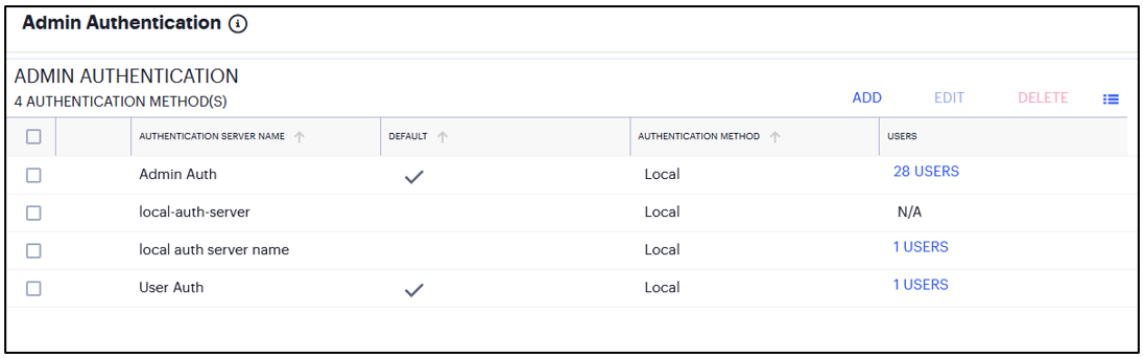


FIGURE 16.8 : Admin Authentication Methods

3. Click **Add**.

   A form appears that enables you to define the authentication method.

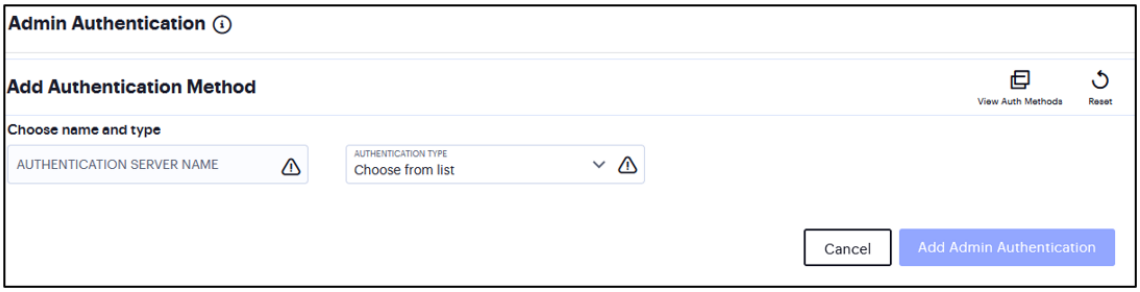


FIGURE 16.9 : Adding a new local user authentication method

Note: At any point during this process, you can reset the form data by clicking **Reset**. You can also view existing authentication methods in a pop-up

dialog by clicking **View Auth Methods**.

4. Under **Choose name and type**:
   - Enter an **Authentication Server Name**.
   - Select the **Authorization Type** of *Local*.

   The form expands to show additional local authentication settings:

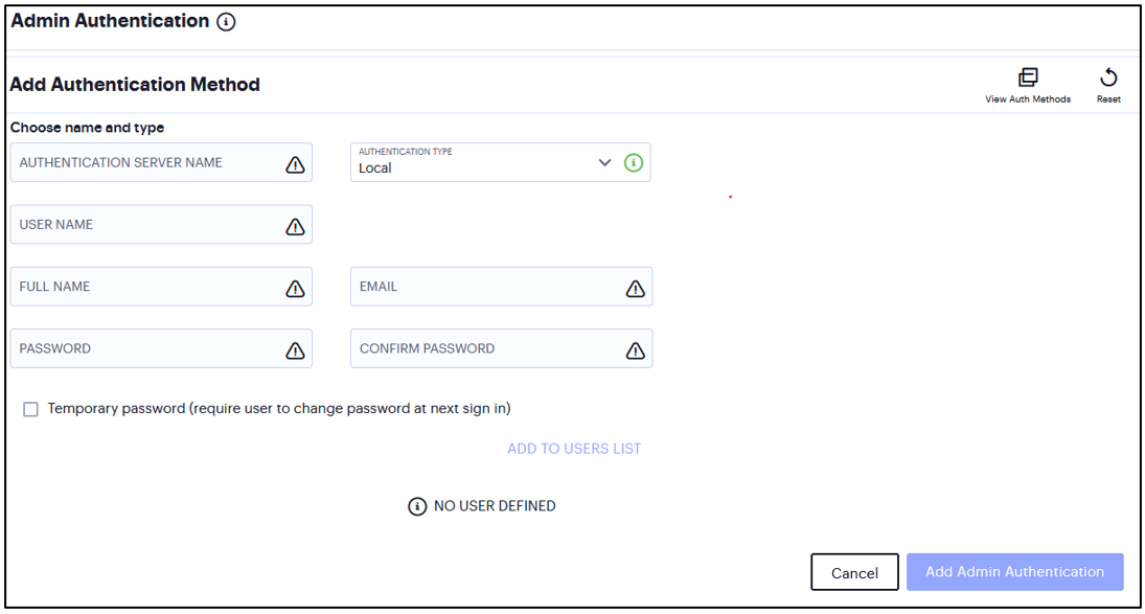


FIGURE 16.10 : Adding local users to a new authentication method

5. Enter the following settings:
   - Enter **User Name**, **Full Name**, and **Email** for the user.
   - Enter **Password** and **Confirm Password** for the user.
   - (Optional) Select the **Temporary Password** check box if you want the user to change their password when they first log in.
   - Click **Add To Users List**.

   The user is added to the list of users.
6. Repeat the previous step for each required user.
7. Click **Add Admin Authentication**.

   The new local user authentication method is added to the list of methods and the process is complete.
8. (Optional) To edit a listed authentication method, select its check box and click **Edit**. Make any required updates and confirm.
9. (Optional) To delete one (or more) *unused* authentication methods, select the check box for each, and click **Delete**. You must confirm the deletion.

After you have created your local authentication method, create or update your authentication policy with the new authentication method. In most cases, you need a minimum of one policy:

- admin sign-in

Note: nSA allows for the definition of custom policies to facilitate separate authentication endpoints for specific groups of users. To learn more, see *Viewing Admin Authentication Policies* (page 437).

Repeat the following steps for each policy, starting with enrollment:

1. From the nSA menu, click the **Administration** icon, then select **Admin Management > Admin Policies**.

   The **Admin Policies** page appears. This page lists all existing user authentication policies.

FIGURE 16.11 : Admin Authentication Policies

   To learn more about the policies on this page, see *Viewing Admin Authentication Policies* (page 437).

   From this page, either create a new custom policy or edit an existing policy.

2. To add a new custom policy, click **Add**.

   The **Add Authentication Policy** form appears.

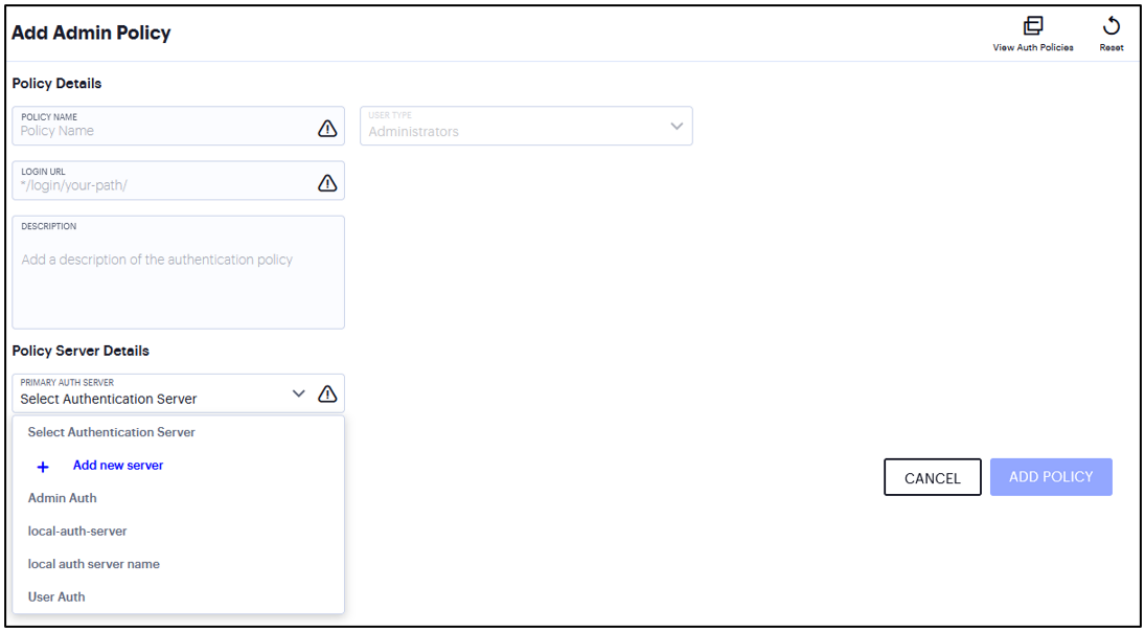


FIGURE 16.12 : Add Admin Authentication

Note: At any point during this process, you can reset the form data by clicking **Reset**. You can also view existing authentication policies in a pop-up dialog by clicking **View Auth Policies**.

3. Enter a **Policy Name**.
4. Enter a **Login URL** using the format */login/<path>/*.

   The URL must start with "*/login/*" and cannot contain any special characters. <path> should be set to a unique value reflecting the endpoint URL you want to define for this authentication policy (appended with a backslash):

   - In the case of admin sign-in policies, this is the URL endpoint (appended to the tenant FQDN) to which new users are invited to connect to enroll or sign-in a device with the nSA. Example value: "*/login/admin/*".
5. (Optional) Enter a description for the authentication policy.
6. Select a **User Type** based on the intended authentication activity for this policy. Choose from:

   - **Administrators**: Select this option to define the authentication endpoint for administrator-level sign-in. This endpoint is used for administrator login to the nSA only.
7. Under **Policy Server Details**, click **Primary Auth Server**, and select the required authentication method for the policy from the drop-down list:

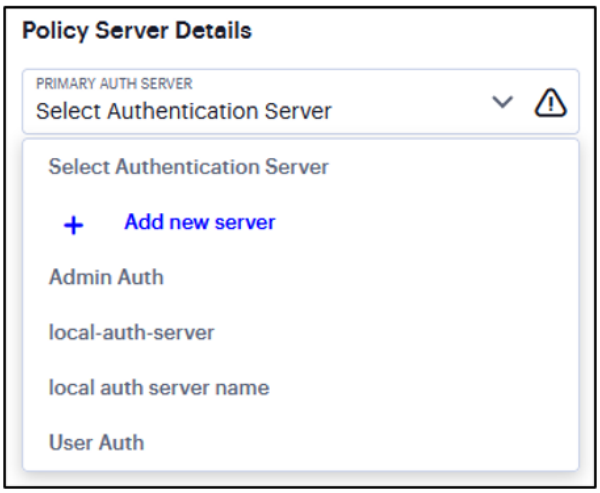


FIGURE 16.13 : Selecting an authentication method for this policy

Alternatively, select *Add New Server* and create a new authentication method as per the steps described earlier in this section.

8. Click **Add Policy** to create the new policy.

   The new policy is added to the list of authentication policies.

If you instead elect to update an existing custom or built-in policy:

1. Select the checkbox adjacent to the relevant policy and click **Edit**.

   The **Edit authentication policy** form appears.

   Note: For built-in authentication policies, all properties except **Primary Auth Server** are read-only.

   ---

2. Set the **Primary Auth Server** to be the new local user authentication method (indicated):

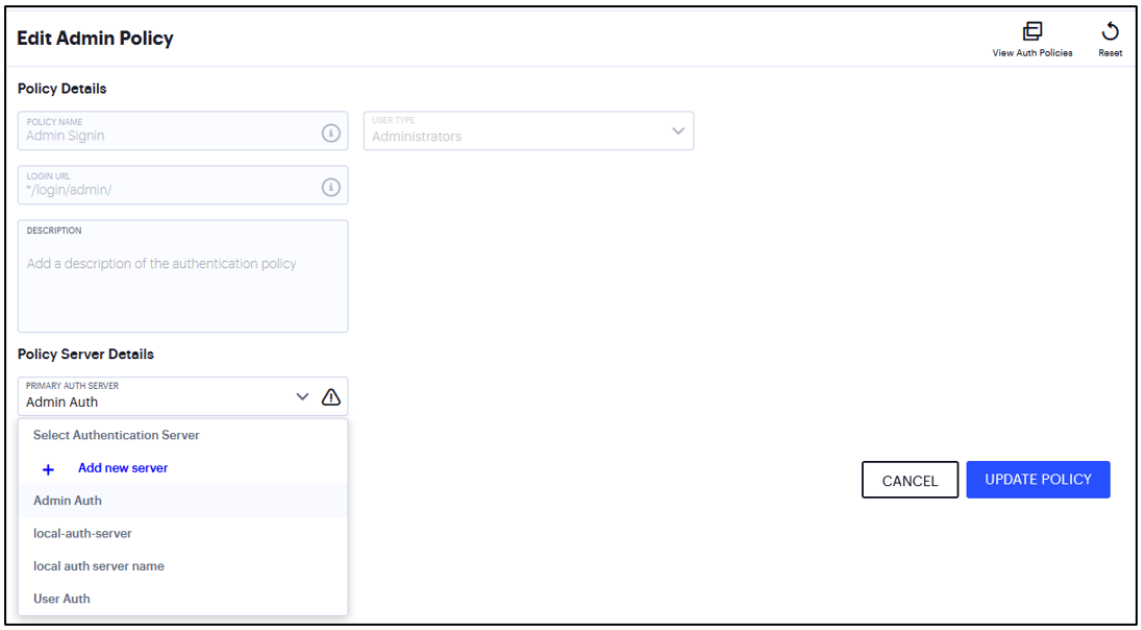


FIGURE 16.14 : Editing the primary auth server

3. Click **Update Policy**.

   The list of authentication policies updates.

4. Repeat until all required authentication policies are updated.

To ensure that your admin can access the authentication mechanism defined in the policies you configure through this process, make sure your *Secure Access Policies* are configured with a **Admin Group** in which these authentication policies are defined.

Workflow: Creating a SAML Authentication Policy With Azure AD and SAML(Custom)

Note: You can use the same work flow for creating SAML (Custom) as well.

nSA supports the use of a cloud-based Active Directory (AD) SAML service to provide authentication for your users.

If you choose to use AD as a SAML Identity Provider (IdP), you do not create any users locally on the nSA. All users will already be present in your remote SAML service.

Configuring nSA to use SAML authentication requires you to create separate SAML apps on the Azure AD platform for the following primary activities:

- Admin sign-in

The nSA includes built-in default authentication policies for each of these purposes, and also includes the ability to create your own custom policies for separate authentication of specific admin groups. You create an authentication method referencing one of the Azure AD SAML apps described above and then assign the method to an authentication policy of the same type (either the built-in policy, or one you create). Begin with enrollment, and then repeat the process for user sign-in.

1. Log into the nSA as a Tenant Admin.
2. From the nSA menu, click the **Administration** icon, then select **Admin Management > Admin Authentication**.

   The *Admin Authentication* page appears. This page lists all existing user authentication methods:

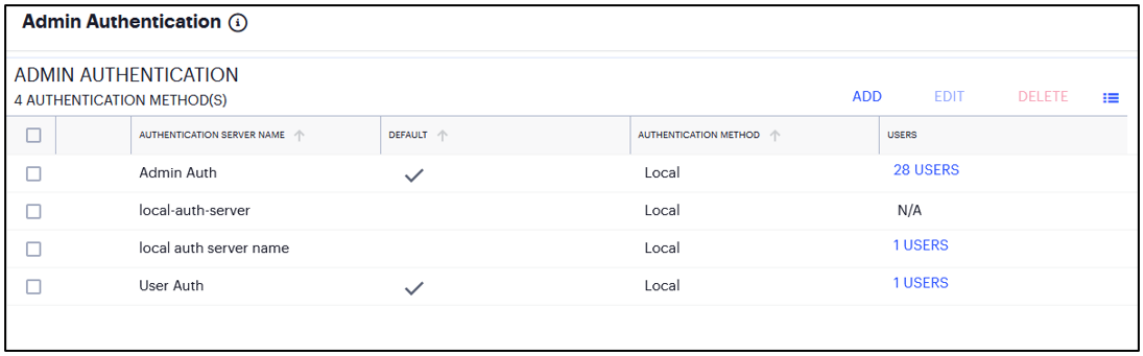


FIGURE 16.15 : Admin Authentication Methods

3. Click **Add**.

   A form appears that enables you to define the authentication method:

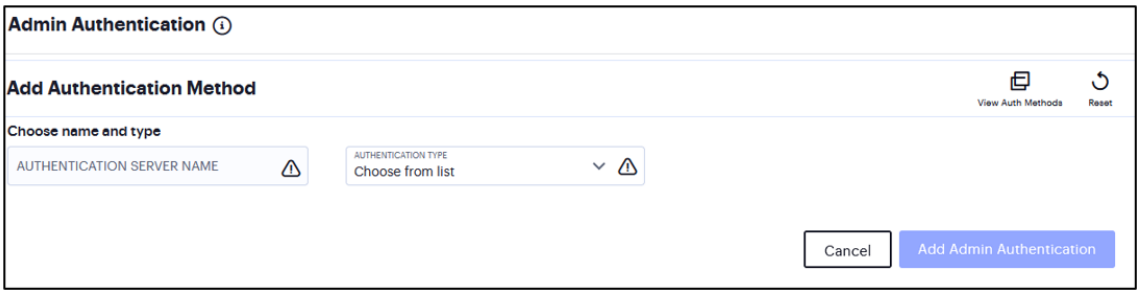


FIGURE 16.16 : Adding a admin authentication method

Note: At any point during this process, you can reset the form data by clicking **Reset**. You can also view existing authentication methods in a pop-up dialog by clicking **View Auth Methods**.

4. Under **Choose name and type**:
   - Enter an **Authentication Server Name**. For example: *Enrollment* or *SignIn*.

- Select the **Authorization Type** of *SAML (Azure AD)*.

The form expands to show additional settings:

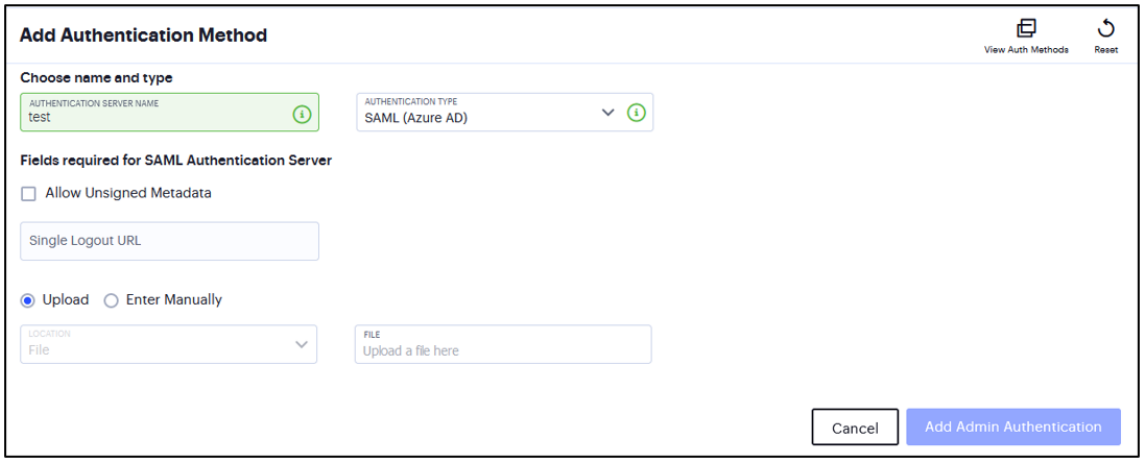


FIGURE 16.17 : Configuring SAML (Azure AD) authentication settings

5. (Optional) Enter a **Single Logout URL**. For more information.
6. To provide your SAML IdP settings, select one of the following:
   - Select **Upload** to upload a digitally-signed (or unsigned) federation metadata XML definition file downloaded for this SAML activity from Azure AD. That is, for either user enrollment or user sign-in.

     Note: By default, the ICS expects a signed metadata definition file. To allow an unsigned metadata file, select **Allow Unsigned Metadata**.

     Then, upload your metadata file by clicking **Upload a file here**.
   - Select **Enter Manually** to manually enter the required IdP SAML settings. Use this option in scenarios where a SAML federation metadata file is not available or incomplete.

     Then, enter the following details:

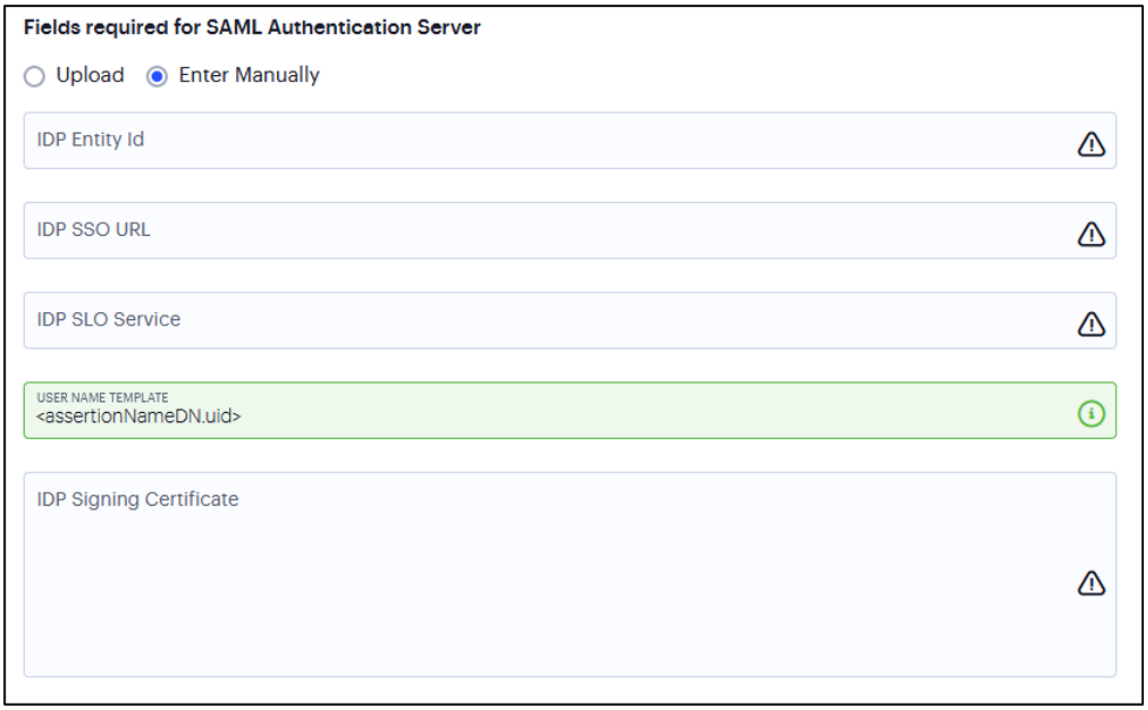


FIGURE 16.18 : Configuring SAML (Azure AD) IdP settings manually

The following minimum settings are required for your SAML authentication service to function correctly. Each setting relates to a value configured in the SAML application on your IdP. Contact your IdP administrator to obtain the relevant details:

- **IDP Entity ID**: The entity ID is sent as the Issuer value in the SAML assertion generated by the IdP. Enter the Issuer value in assertions generated by the SAML identity provider.
- **IDP SSO URL**: A URL provisioned by the SAML IdP to support service-provider-initiated Single Sign-On. Use the format `https://<FQDN>`.
- **IDP Slo Service**: (Optional) A URL to specify the Single Log-Out/sign out endpoint if you want to force re-authentication for increased security. Use the format `https://<FQDN>`. For more information.
- **User Name Template**: Specify how the system is to derive the username from the SAML assertion. The default value can be used, or replaced with an alternative specifier. For example: `<assertionNameDN.uid>`, the NameID value where ICS is the IdP, the UID from X509SubjectName, `<userAttr.attr>`, attr from AttributeStatement attributes.
- **IDP Signing Certificate**: The signing certificate to be used with the SAML app on the IdP. Type or paste in the contents of your Base-64 encoded public key.

Note: If, at a later date, you need to modify the metadata definition file, edit

the authentication method through the *User Authentication* page and repeat this step. However, note that federation metadata files from Azure AD are digitally-signed and so cannot be manually edited prior to upload back into nSA. This process supports replacing a definition file *only* with another digitally-signed and validated definition file.

7. Confirm that your settings are correct, then select **Add Admin Authentication** to create the authentication method.

   The new SAML user authentication method is added to the list of methods displayed in the **Admin Authentication** page, and the process completes.

After you have created your SAML authentication method, create or update your authentication policies with the new authentication method:

1. From the nSA menu, click the **Administration** icon, then select **Admin Management > Admin Policies**.

   The **Admin Policies** page appears. This page lists all existing user authentication policies.

FIGURE 16.19 : Admin Authentication Policies

   To learn more about the policies on this page, see *Viewing Admin Authentication Policies* (page 437).

   From this page, either create a new custom policy or edit an existing policy.

2. To add a new custom policy, click **Add**.

   The **Add Authentication Policy** form appears.

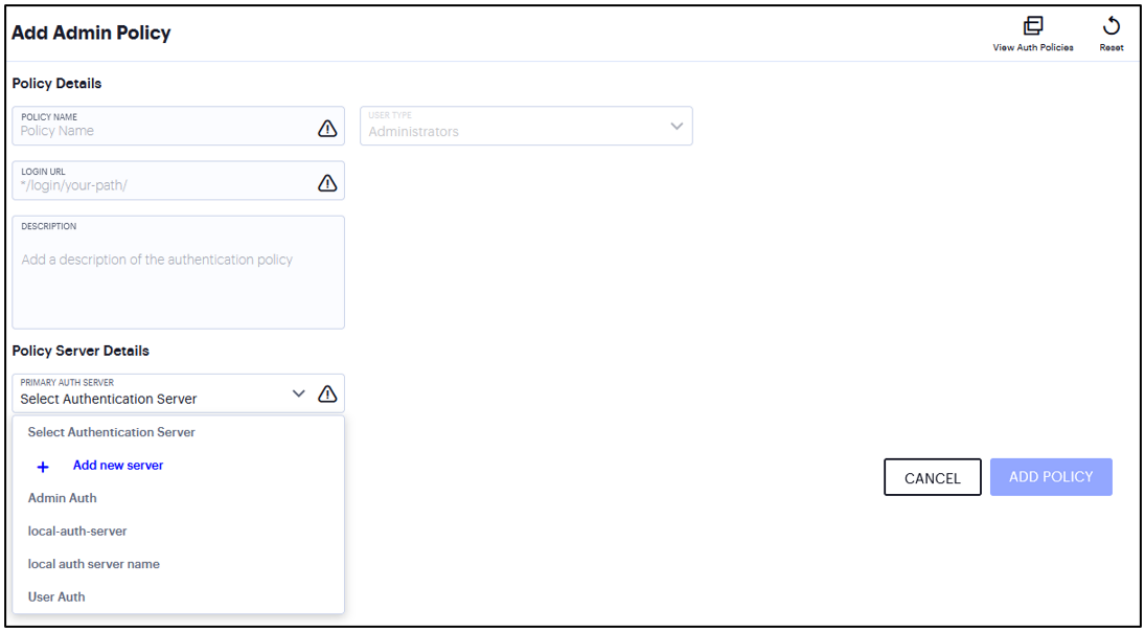


FIGURE 16.20 : Add Admin Authentication

Note: At any point during this process, you can reset the form data by clicking **Reset**. You can also view existing authentication policies in a pop-up dialog by clicking **View Auth Policies**.

3. Enter a **Policy Name**.
4. Enter a **Login URL** using the format */login/<path>/*.

   The URL must start with "*/login/*" and cannot contain any special characters. <path> should be set to a unique value reflecting the endpoint URL you want to define for this authentication policy (appended with a backslash):

   - In the case of admin sign-in policies, this is the URL endpoint (appended to the tenant FQDN) to which new users are invited to connect to enroll or sign-in a device with the nSA. Example value: "*/login/adminlogin/*".

Note: In some enrollment circumstances, such as when using a device pre-installed with an older version of Ivanti Secure Access Client, you connect directly to the enrollment policy endpoint to enroll the device. For more details, see *Viewing Admin Authentication Policies* (page 437).

5. (Optional) Enter a description for the authentication policy.
6. Select a **User Type** based on the intended authentication activity for this policy. Choose from:

   - **Administrators**: Select this option to define the authentication endpoint for administrator-level sign-in. This endpoint is used for administrator login to the nSA only.

7. Under **Policy Server Details**, click **Primary Auth Server**, and select the required authentication method for the policy from the drop-down list:

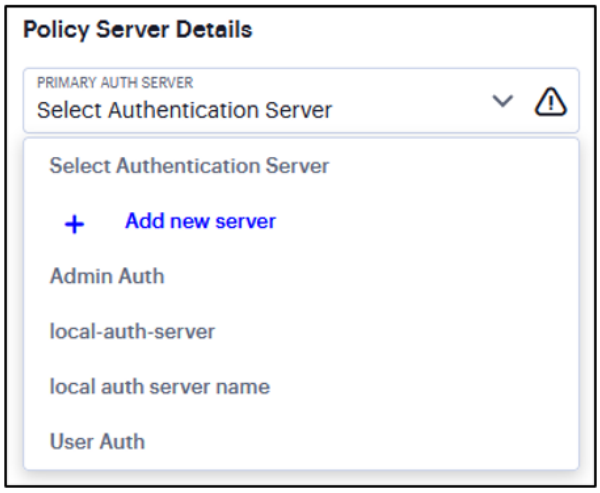


FIGURE 16.21 : Selecting an authentication method for this policy

   Alternatively, select *Add New Server* and create a new authentication method as per the steps described earlier in this section.

8. Click **Add Policy** to create the new policy.

   The new policy is added to the list of authentication policies.

If you instead select to update an existing custom or built-in policy:

1. Select the checkbox adjacent to the relevant policy and click **Edit**.

   The **Edit authentication policy** form appears.

   Note: For built-in authentication policies, all properties except **Primary Auth Server** are read-only.

   ---

2. Set the **Primary Auth Server** to be the new SAML user authentication method (indicated):

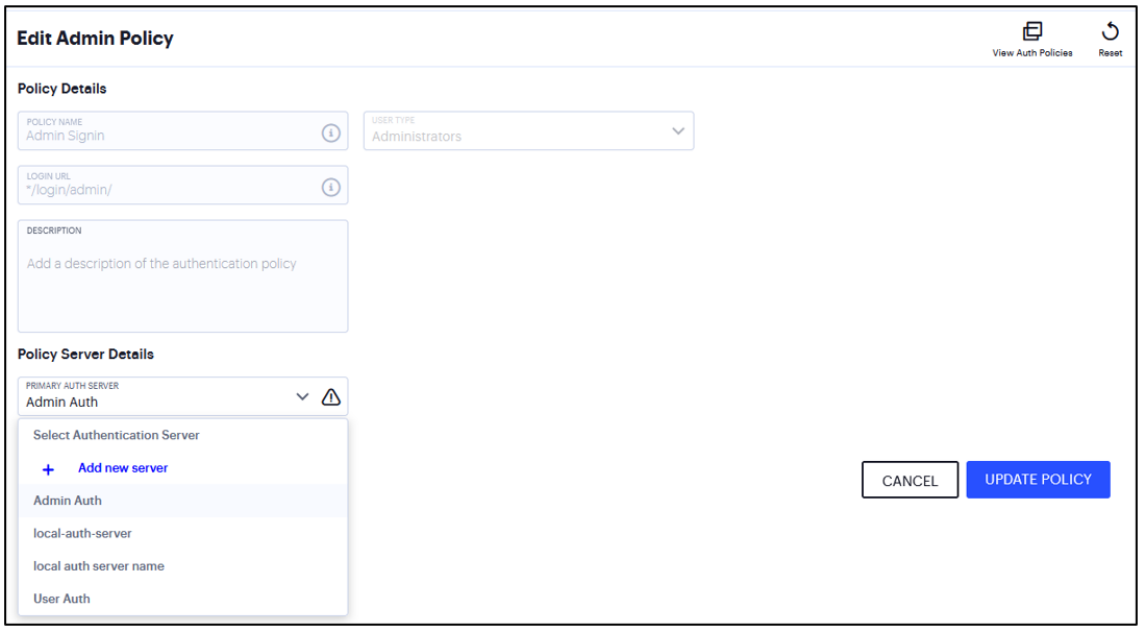


FIGURE 16.22 : Editing the Primary Authentication Server

3. Click **Update Policy**.

   The list of authentication policies updates.

4. Repeat until all required authentication policies are updated.

At this point, the nSA uses the uploaded Federation Metadata to contact the SAML service. After this process completes, a **Download** function becomes available for each relevant policy. This metadata file is required to configure trusted communication with the remote SAML service.

1. Refresh your browser until the **Download** action is visible for the relevant policies.
2. Select the check box for the policy metadata you want to download and clear all other check boxes.
3. Click **Download** and save the metadata file.

Note: As mentioned previously, make sure you repeat this procedure for each required SAML app on your Azure AD platform. That is, you require separate XML metadata files for the enrollment authentication policy and the login authentication policy.

After the **Admin Authentication** workflow is complete, you can configure the Azure AD platform with the XML configuration of the nSA.

Finally, to ensure that your users can access the authentication mechanism defined in the policies you configure through this process, make sure your *Secure Access Policies* are configured with a **Admin Group** in which these authentication policies are defined. To learn more.

nSA Licensing/Subscription

Licenses/subscriptions are added to your nSA by Ivanti.

The **Subscriptions** page displays the licenses/subscriptions that are active on your nSA. To access this page, click **Administration > Subscriptions**.

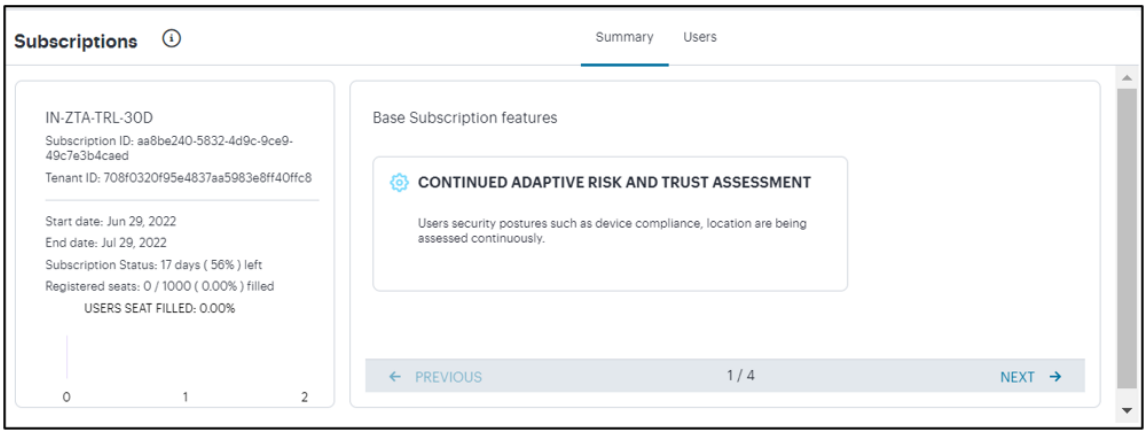


FIGURE 17.1 : Subscriptions Summary Page

The **Summary** tab displays for each subscription/license:

- License/Subscription high-level details, including dates and usage metrics.
- One or more descriptions of the features in the license/subscription. Where there are multiple features, use **Previous** / **Next** to navigate.

When any defined limit on the license/subscription is met, a message appears:

- At 75% utilization of seats, an information message appears at the bottom of the screen. You can optionally click **Close**.
- At 90% utilization of seats, a modal message appears at login. Click **Dismiss** to clear the message.
- When 25% of the duration of the license/subscription remains, a modal message appears at login. Click **Dismiss** to clear the message.

The **Users** page lists users and their devices registered on nSA.

Summary information for the nSA licenses/subscriptions is displayed at the top of the page:

- Total number of seats.
- Total number of issued named user license seats. Each of these is listed in the table below the summary.
- The percentage of seats consumed.

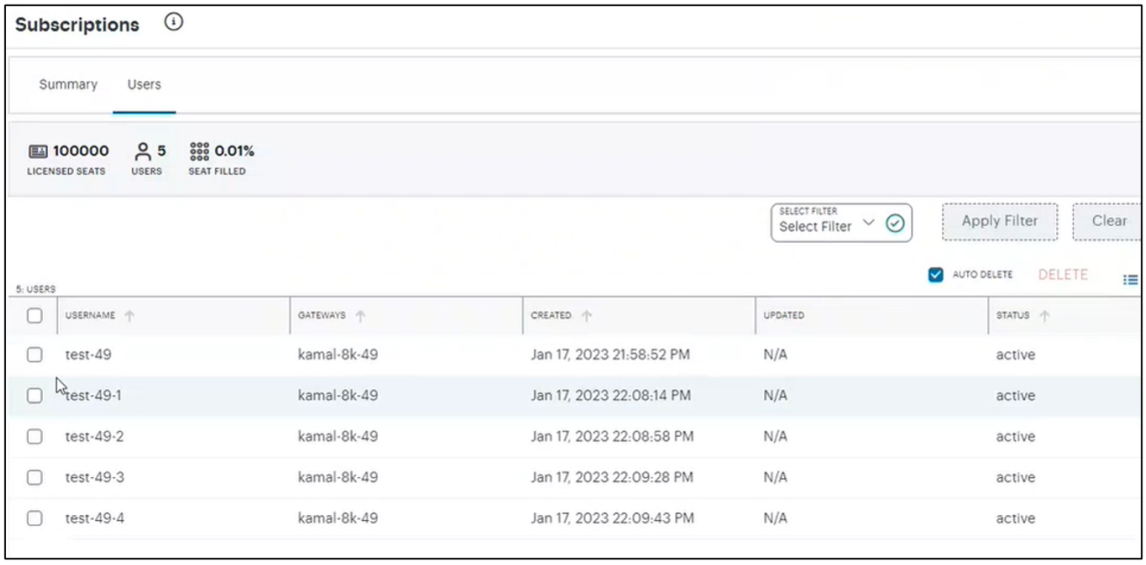


FIGURE 17.2 : Subscriptions Users Page

For each named user, the following information is displayed:

- The name of the user.
- The gateways enrolled for that user.
- Updated time shows an N/A for ICS gateways.
- The status of the named user license seat of that user.

You may need to remove users when there is any changes in the organization. To delete one or more named users, select the corresponding check boxes and click **Delete**.

You may want to automatically remove the license of users who have not logged-in in the last 30 days. To delete those users automatically, select the **Auto Delete** check box.

The counts in the Users page, and information in the Summary page get updated accordingly.

Using the Troubleshooting Tools

Introduction

The Troubleshooting page enables you to investigate issues that might be affecting your Gateway or preventing it from operating normally.

This page is intended to enable Ivanti Technical Support teams to help resolve problems with your Gateway infrastructure. Due to the potential for system performance to be impacted through the use of these features, Ivanti recommends you only use this page when advised to do so.

The following tools are available through the Gateways > Troubleshooting page:

- **Debug logs** - Work with Ivanti Technical Support teams to diagnose system issues.
- **Network troubleshooting commands** - Use standard network commands, such as ping, traceroute, NSlookup, and other commands to diagnose networking issues.
- **System snapshots** - Work with Ivanti Technical Support teams to reproduce and diagnose system issues.
- **tcpdump** - Sniff packet headers to diagnose networking issues.

To access Troubleshooting page:

1. Log in to the Ivanti Neurons for Secure Access portal as a Tenant Admin. See *Logging in to Ivanti Neurons for Secure Access* (page 5).
2. Use the Gateway Switcher and select **Ivanti Connect Secure**.

3. From the Ivanti Connect Secure menu, click the **Gateways** icon, then select **Gateways > Gateways List**.

   The All Gateways page is displayed showing a list of standalone ICS Gateways and cluster nodes.

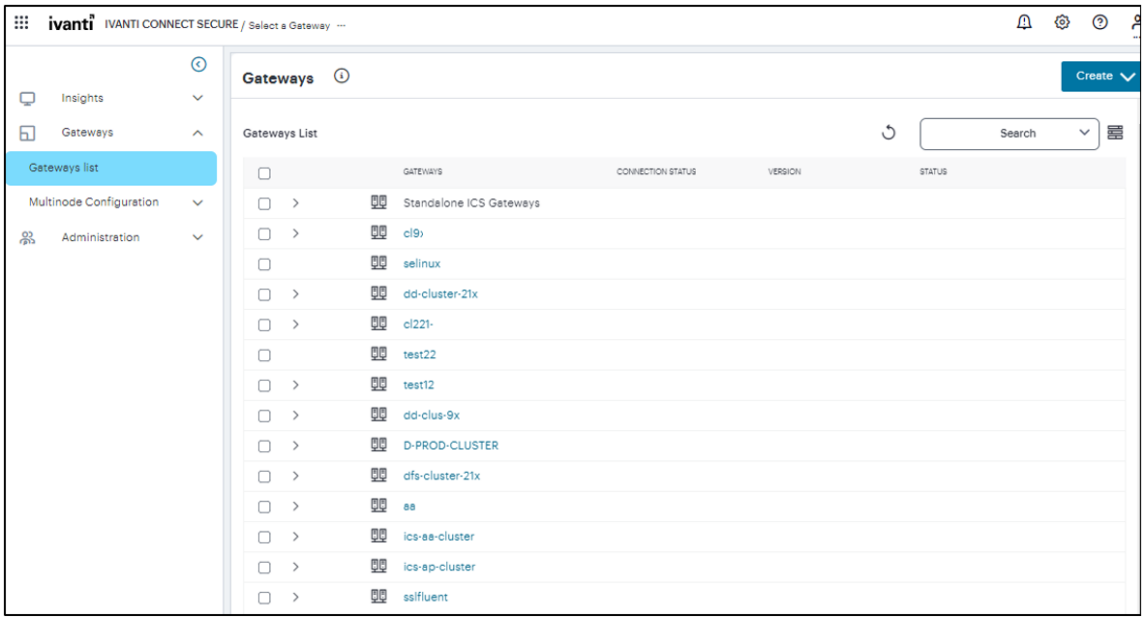


FIGURE 18.1 : Gateways list

4. In the All Gateways page, double-click the required Gateway from the list.
5. From the Ivanti Connect Secure menu, click the **Gateways** icon, then select **Gateways > Troubleshooting**.

   The Troubleshooting Overview page appears.

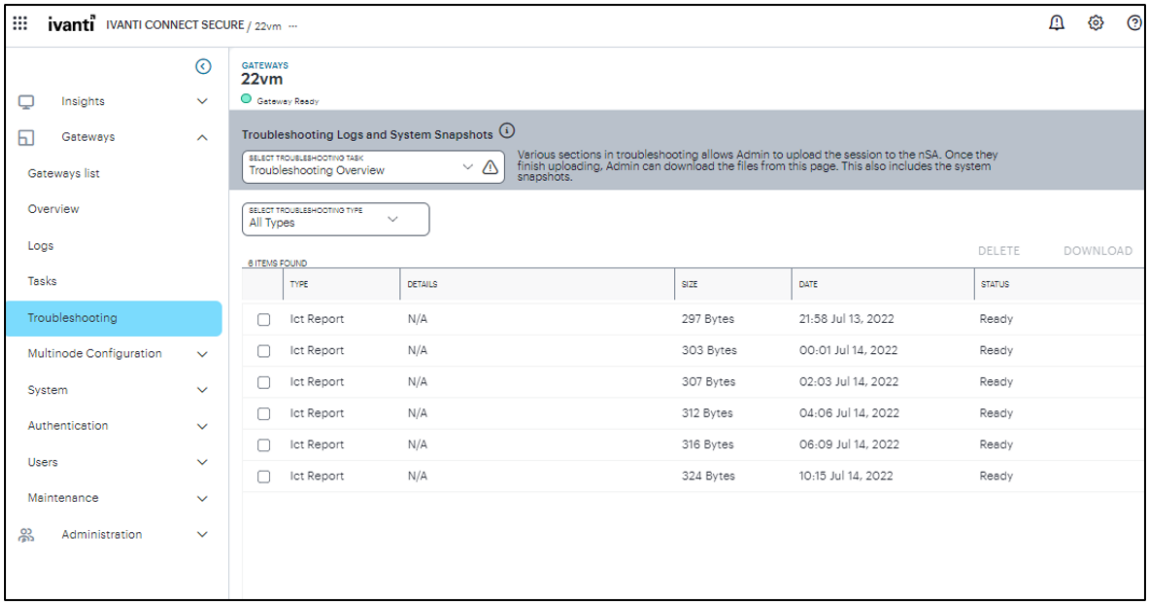


FIGURE 18.2 : Troubleshooting Overview page

Using the Debug Log

The Ivanti Technical Support teams might direct you to create a debug log to assist them in helping you debug an issue with the system.

To use debug logging:

1. From the **Troubleshooting Logs and System Snapshots** drop-down menu, select **Debug Log**.

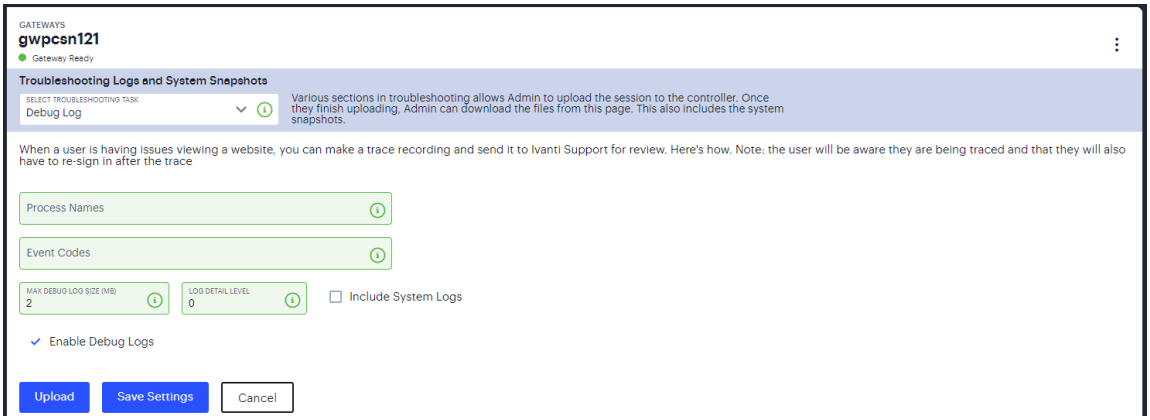


FIGURE 18.3 : Debug Log Configuration page

2. Specify the **Process Name**.
3. Specify the **Event Code**.
4. Specify a **Maximum debug log file size**. The default is 2 MB. The maximum is 250 MB.
5. Specify the debug **Log detail level**.
6. Select *Include System Logs** option to include system logs in the debug log file. Recommended.
7. Select **Enable Debug Logs**.
8. Click **Save Settings**. The system begins generating debug log entries.
9. Click **Upload**.

   A confirmation message is displayed. You can then download the file from the Troubleshooting Overview page and analyze the logs.

Using Network Troubleshooting Commands

You can run common network troubleshooting commands such as arp, ping, ping6, traceroute, traceroute6, NSlookup, and AvgRTTs from the admin console. You can use these connectivity tools to see the network path from the system to a specified server. If a client can ping or traceroute to the access system, and the access system can ping the target server, any remote users should be able to access the server through the access system.

To run network troubleshooting commands:

1. From the **Troubleshooting Logs and System Snapshots** drop-down menu, select **Commands**.

FIGURE 18.4 : Network Troubleshooting Commands page

2. Select a network troubleshooting command from the options:
    - Ping/Ping6
    - Traceroute/Traceroute6
    - NSLookup
    - ARP
    - AvgRTTs
    - Portprobe
    - Cluster Roundtrip
3. When prompted:
    - Specify the IP address or hostname for the target server.
    - Select the interface from which to send the command.
4. Click **Start** to run the command and write the output to the screen.

Using System Snapshots

A snapshot of the system state captures details that can help Ivanti Technical Support teams diagnose system performance problems. The system stores up to ten snapshots, which are packaged into an encrypted “dump” file that you can download and then e-mail to Ivanti Technical Support teams.

To create and manage system snapshots:

1. From the **Troubleshooting Logs and System Snapshots** drop-down menu, select **System Snapshots**.

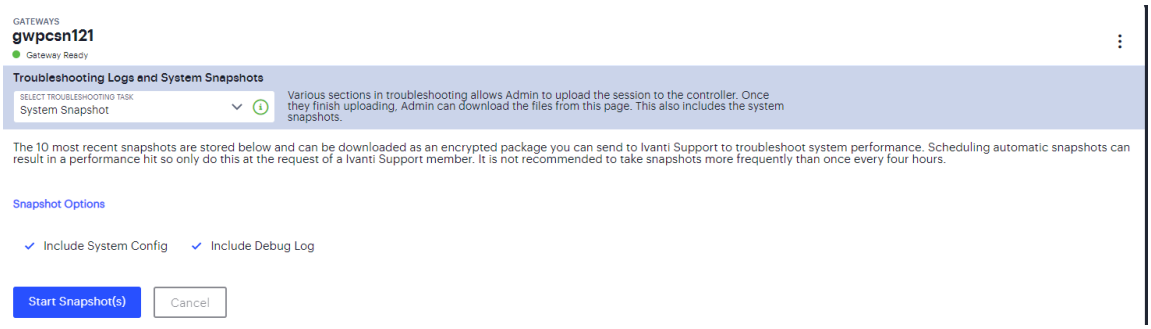


FIGURE 18.5 : System Snapshots Configuration page

2. Select **Include system config** to include the system configuration file in the snapshot.
3. Select **Include debug log** to include debug logs (if any).
4. Click **Start Snapshot(s)**.

   A confirmation message is displayed. You can then download the file from the Troubleshooting Overview page and analyze the logs.

Using the TCP Dump Utility

To use TCP Dump utility:

1. From the **Troubleshooting Logs and System Snapshots** drop-down menu, select **TCP Dump**.
2. Configure the following:
   - Select the ports on which to sniff (Internal, External, Management).
   - Specify a Filter expression.
   - Select a promiscuous mode option.

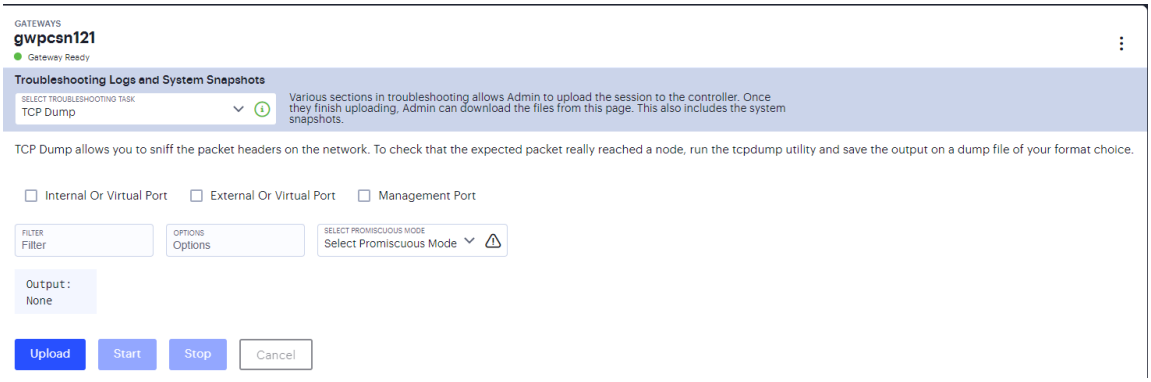


FIGURE 18.6 : TCP Dump Configuration page

3. Click **Start** to start the TCP Dump process.
4. Click **Stop** to write the TCP Dump output to the screen.
5. Click **Upload**.

   A confirmation message is displayed. You can then download the file from the Troubleshooting Overview page and analyze the logs.