BeyondTrust

BeyondInsight for Unix & Linux 23.1 User Guide

TC:9/1/2023

Table of Contents

BeyondInsight for Unix & Linux User Guide **5**
BeyondTrust Product Name Conventions 5
Overview 5
Run BIUL **7**
Set Up the Console Using the First Run Wizard 7
View the BIUL Home page 8
View the BIUL Dashboard **11**
Hosts Inventory with BIUL **12**
Discover Host Methods 12
BIUL Hosts Inventory Grid 16
Use Privilege Escalation for BIUL Credentials 20
Profile Servers in BIUL 21
Manage AD Bridge Hosts 23
Manage PMUL Hosts 28
Manage Solr 31
Deploy Keyfiles 32
Delete Hosts 33
View Host Details 34
Manage Client Registration Profiles 37
Use SSH Keys **39**
Deploy an SSH Key 39
Download a Public Key 39
Rotate a Public Key 39
Disable a Key 40
Manage SSH Fingerprints **41**
Manage Credentials in BIUL **42**
Use Credential Rules **44**
One-Click Actions 44
Add a Network Credential Rule 44
Add a Host Credential Rule 44
Delete a Credential Rule 45

View Credential Rules on a Host 45
Manage the Registry Name Service 46
Manage Registry Name Service Groups 46
Manage Policy Service Groups 47
Manage FIM Service Groups 48
Manage Privilege Management for Networks Service Groups 49
Manage Log Server Service Groups 50
Manage Log Archive Service Groups 51
Configure Settings and Manage Software 52
Manage BIUL Settings 53
Add a Directory Service Connection 56
Manage BIUL Console Access 57
Configure Role-Based Access 61
Integrate Password Safe with BIUL 63
Configure the PMUL Integration 66
Manage Software 67
Manage SIEM Connections 70
Add SMTP Server Connection 73
Manage Certificates 74
Manage PMUL Policies 76
View Server Details 76
Manage a Policy 77
Manage PMUL Role-Based Policies 80
Role-Based Policy Roles 81
Role-Based Policy Users and User Groups 87
Role-Based Policy Command Groups 90
Role-Based Policy Host Groups 91
Role-Based Policy Schedule Groups 92
Role-Based Policy Backup and Restore 94
Manage Privilege Management for Networks Policies 95
Manage Sudo Policies 99
Manage File Integrity Monitoring Policies 101
File Integrity Monitoring Reports 104

File Integrity Monitoring Clients 105
Manage PMUL Script-Based Policies 107
View PMUL Settings 109
AD Bridge Local Policy Editor 111
Audit Activity Using BIUL 112
Perform a Unified Search 112
View PMUL Events 113
View Console Audit Activities 114
Replay Sessions in BIUL 115
View Entitlement Reports 117
Manage PMUL Licenses 118
View PMUL Licensing 118
View Tasks and Task Details in BIUL 120
Notifications 122
View Notification Details 122
About BIUL 124
Links 124
Legal 124
About BeyondTrust 124
Troubleshoot Common Issues with BIUL 125
Troubleshoot Password Safe Issues 126

BeyondInsight for Unix & Linux User Guide

This guide shows system administrators and security administrators how to configure and use BeyondInsight for Unix & Linux (BIUL). It provides an overview of how BIUL works and instructions for its configuration and use.

BeyondTrust Product Name Conventions

This guide uses the following naming conventions for BeyondTrust products:

BeyondInsight for Unix & Linux (formerly PowerBroker Servers Management Console)	BIUL
Privilege Management for Unix and Linux (formerly PowerBroker for Unix and Linux)	PMUL
Active Directory Bridge	AD Bridge or ADB
Solr **(deprecated as of 23.1 release)** (formerly PowerBroker Solr)	Solr
File Integrity Monitoring	FIM
Advanced Control and Audit	ACA
Role-Based Policy	RBP

Overview

BIUL is a web-based tool that you can use to:

- Manage software for AD Bridge and PMUL.
- Remotely assess the suitability of a remote host's state by running a profile. After a profile is complete, installs, uninstalls, domain joins, and other actions can be performed on remote hosts.
- Manage PMUL licenses on policy servers.
- Manage PMUL script, File Integrity Monitoring (FIM), and role-based policies.
- Manage Sudo host groups and FIM policy host assignment.
- View, replay, and audit PMUL logs.

Core Features

These features are found in the menu, under tiles, and on the main pages for menu items.

Feature	Description
Dashboard	Provides visual insight into host and software metrics.
Host Discovery	The first stage of adding any remote hosts to be managed by the console. Hosts available by SSH are added.

Feature	Description
Hosts Inventory	The central page of the console. On the **Hosts > Hosts Inventory** page, you can profile targets, install, and uninstall AD Bridge, PMUL, and Solr. Additionally, you can remove hosts, upgrade software, join hosts to domains, manage SSH fingerprints, and assign log servers to be indexed by Solr.
Credentials	Manage user credentials for remote assets (typically SSH credentials).
SSH Fingerprints	Manage SSH fingerprints for remote hosts.
Registry Name Service	Manage PMUL Registry Name Service systems.
Policy Management	Manage Privilege Management for Networks, FIM, and role-based and script-based policies on PMUL policy servers.
Audit	View, replay, and audit PMUL events and I/O logs. I/O logs can be replayed as they occur. Users can add comments on the logs. Query and view PMUL and AD Bridge events that have been exported to an external SIEM.
License Management	View and manage license information for PMUL.
Tasks	View details about results and status of any remote actions performed by the console.
Settings	Configuration settings available to the end user, including integration settings for products like Password Safe.
Notifications	Users with the software administrator role can view notifications that are triggered when given conditions arise within BIUL. The notification details provide options for remediation of the condition.

Solr

Note: *As of version 23.1, Solr is deprecated. BeyondInsight for Unix & Linux no longer supports installing Solr, but features that use an existing Solr installation will continue to work.*

Run BIUL

Log in to the console using a supported browser: https://localhost:4443. If this is your first time logging into the console, the First-run wizard starts.

IMPORTANT!

If the wizard starts and this is not the first time the console has been run, do not go through the wizard again. All data in the system will be lost. Contact BeyondTrust Technical Support, at https://www.beyondtrust.com/support.

Set Up the Console Using the First Run Wizard

If this is the first time you are logging on to the console, complete the wizard and configure the system settings.

Configure BIUL

The following sections match the layout of the First-run wizard in BeyondInsight for Unix & Linux (BIUL). Please follow along for assistance with BIUL's initial configuration and setup.

1. **Welcome:** Read the available information carefully to ensure a smooth configuration process.

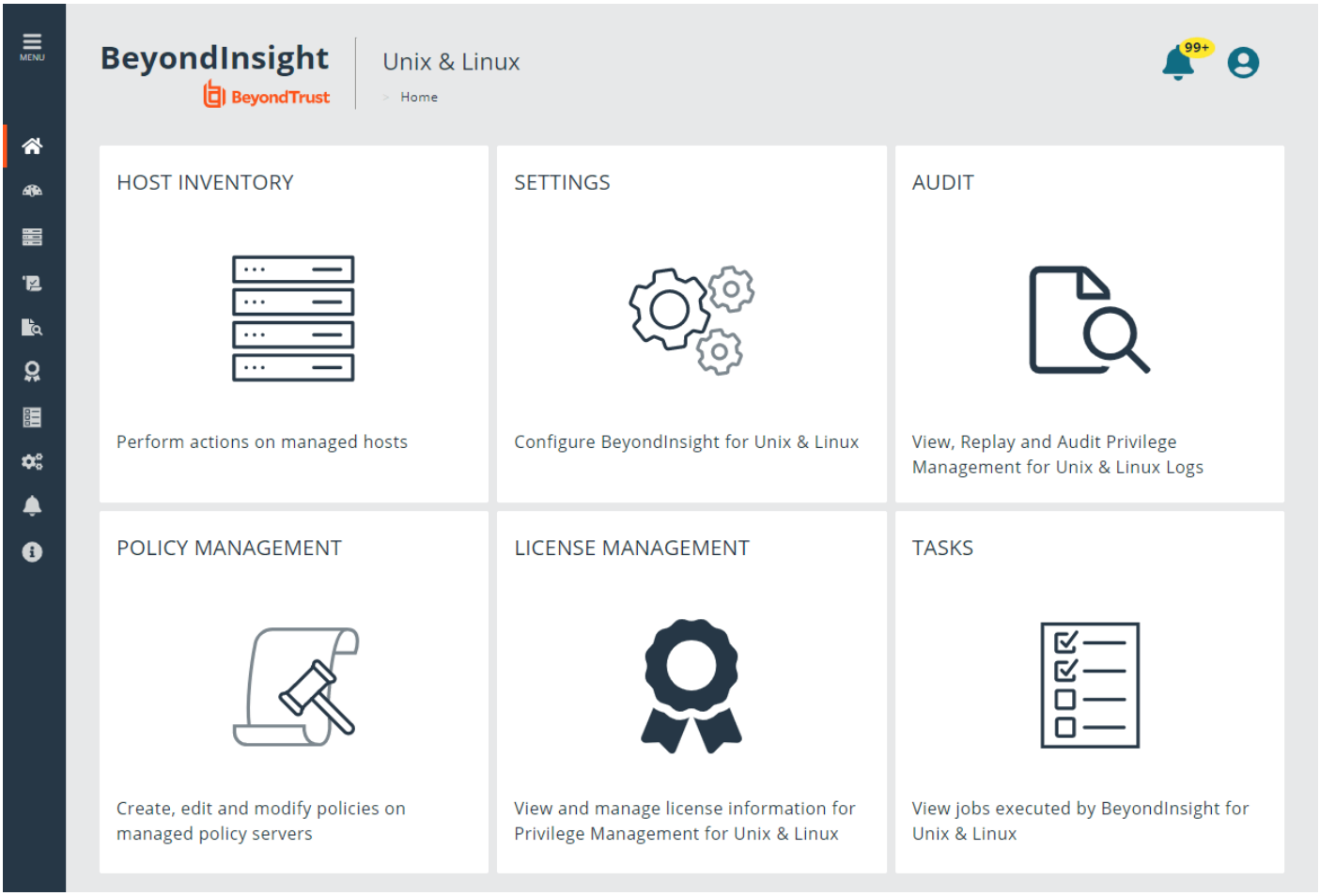
***Note:** Proceeding will reset the database to its initial state. This is an unrecoverable action.*

2. **Users:**
    - Create the administrative accounts that will be used to log into the console. On this step, you can add multiple accounts.
    - After entering each new account, click **Save** to confirm the account details and to populate a list of accounts under **Configured Host Users**.
    - To delete an account, click the **Delete** icon next to the account's name.
    - When you've added the desired number of accounts, click **Next Step**.
3. **Credentials:** Create credentials for remote hosts. The credentials are used to connect to the remote hosts.
4. **Summary:** Review the settings and save. You are now able to log in to the console using the administrator account you created in the wizard.

For more information on BIUL configuration, see Configure BeyondInsight for Unix & Linux, at https://www.beyondtrust.com/docs/privilege-management/console/beyondinsight-unix-linux/install/configure.htm.

View the BIUL Home page

The **Home** page allows administrators to view the main BIUL options, for quick access.



The options include:

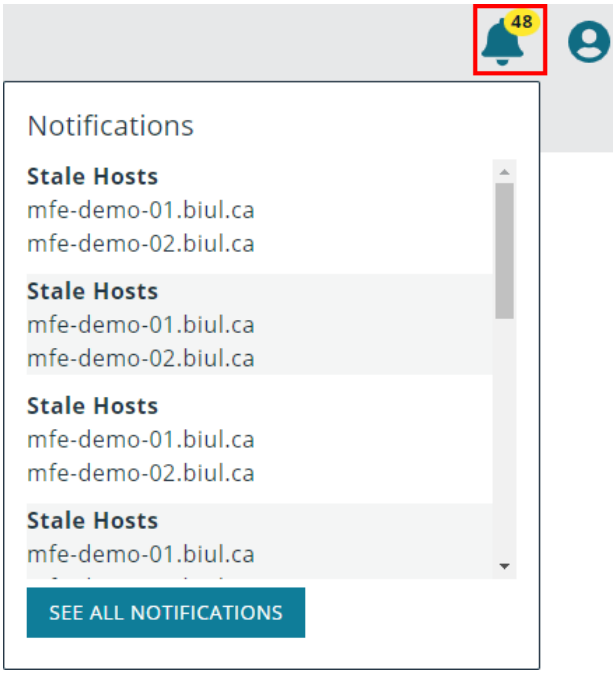
- **Host Inventory:** Discover, add, and manage hosts for BIUL.
- **Settings:** Configure settings for BIUL.
- **Audit:** View, replay, and audit Privilege Management for Unix and Linux (PMUL) logs.
- **Policy Management:** Create, edit, and modify policies on managed policy servers.
- **License Management:** View and manage license information for PMUL.
- **Tasks:** View jobs executed by BIUL.

To access an option, click the tile associated with it.

Notifications Panel

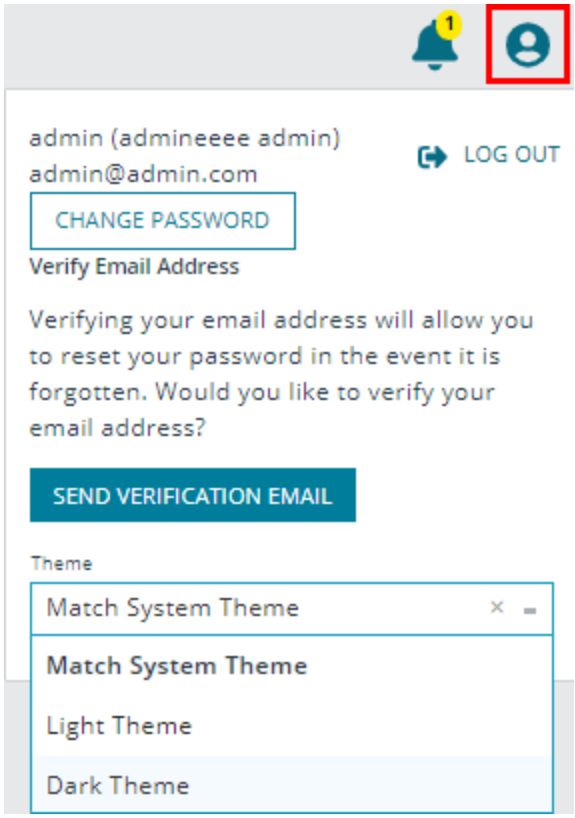
At the top right of the BIUL interface, click the **Notifications** icon to get a list of host notifications. To go to the **Notifications** page, click **See All Notifications**.

For more information, see "Notifications" on page 122.



User Account Profile and Log Out

In the top-right corner, click the **User Account Profile** icon to view your current account profile information, including your full logged-in user name, email address, change password option, and theme options.



> **Note:** *The **User Account Profile** icon is accessible from any page in the BIUL interface.*

Change Password

To change your BIUL access password, click **Change Password**, complete the fields, and then click **Change Password**.

Verify Email Address

Verifying your email address allows you to reset your password in the event that you forget it.

> **IMPORTANT!**
>
> *SMTP settings must be configured for the email functionality (send verification email, forgot password) to be available. To configure SMTP settings, see "Add SMTP Server Connection" on page 73.*

To verify your email:

1. Click **Send Verification Email**.
2. You will receive an email with a link.
3. Click the link, and you must then log back in to the application to verify your identity and validate the connection.

Your user email is now marked as *verified* in the BIUL database. This also activates and displays the **Forgot Password?** option on your log in screen.

Themes

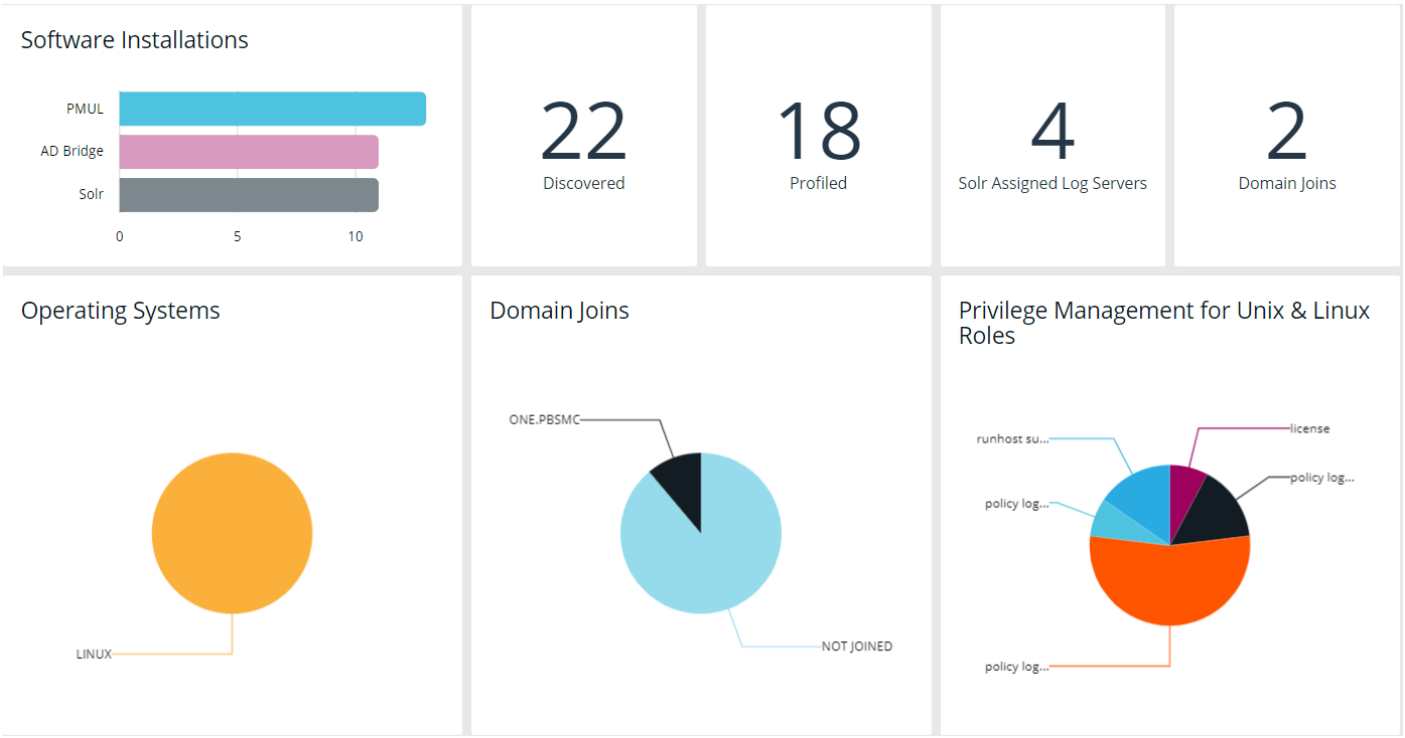
You can select themes for your BIUL environment. From the dropdown list, select **Match System Theme**, **Light**, or **Dark** theme (try it!).

Log Out

To log out of BIUL, click **Log Out**.

View the BIUL Dashboard

The dashboard provides an easy-to-read visual summary of the console data metrics.



Summary Metrics

The top section of the dashboard displays the following details:

- **Software Installations:** Lists the products and the number of hosts where the product is installed.
- **Discovered:** The number of discovered and available hosts.
- **Profiled:** The number of successfully profiled hosts.
- **Solr Assigned Log Servers:** The number of log servers using Solr indexing.
- **Domain Joins:** The number of hosts joined to a domain.

Charts

The following statistics are provided:

- **Operating Systems:** Displays the most common operating systems discovered on the network.
- **Domain Joins:** Displays the most common domains joined by discovered hosts.
- **Privilege Management for Unix and Linux Roles:** Displays the most common PMUL roles discovered on hosts.

Hosts Inventory with BIUL

On the **Hosts Inventory** page, you can find hosts that are accessible using SSH. Discovered assets are stored as hosts and can also be managed on the **Hosts Inventory** page.

This stage does not require a credential. It performs a port scan to test for an SSH connection.

Hosts are discovered in parallel batches to avoid saturating the network connection. The default size is **20**. This can be configured by changing the pool settings option.

> *For more information, please see Configure BIUL at https://www.beyondtrust.com/docs/privilege-management/console/beyondinsight-unix-linux/install/configure.htm.*

Discover Host Methods

Hosts are discovered through the following methods:

- Scan for Hosts
- Import Hosts
- Scan the Registry Name Service

To access any of these methods, on the **Host Inventory** page, **click** the **Add Hosts** dropdown menu.

> ***Note:** While using any of these methods, the grid refreshes automatically every 5 seconds.*

Scan for Hosts

IP addresses can be added using one of the following formats:

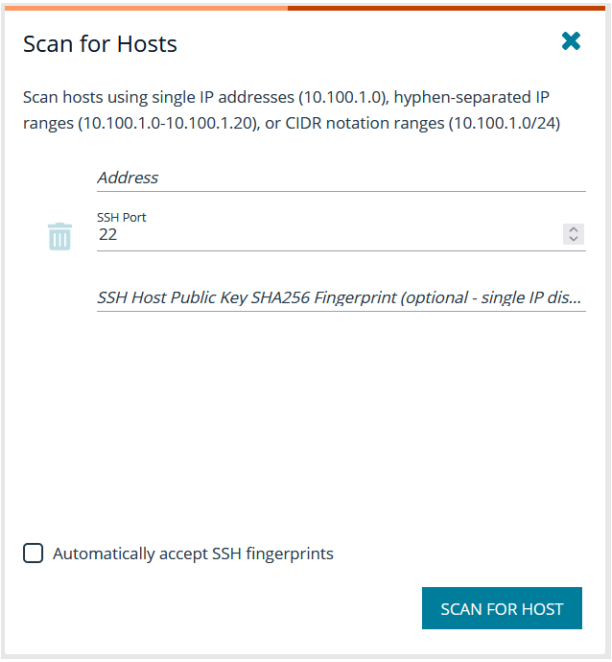
- **Single IP:** To discover a single host, type the IP address. For example, 10.1.100.15.
- **IP Range:** Discover any hosts in a range. For example, 10.1.100.15–10.1.100.20.
- **CIDR Notation:** Discover hosts in a CIDR block. For example, 10.100.1.10/24.

To manually discover hosts:

1. Enter the IP addresses using one of the accepted formats.
2. Enter an SSH port. The value should map to the SSH port for the host provided. If no SSH port is provided, the default port is **22**. Each discovery scan uses a single port regardless of the number of machines.

> ***Note:*** *To update the SSH port for the host, navigate to* ***Host Details****. The value can then be configured under* ***General*** *>* ***Connection Details****.*

3. When discovering a single host, you can enter an SSH fingerprint using SHA-256 format. If the value matches the received fingerprint, the host is automatically accepted. This is optional and only applies when performing single IP discovery.
4. Check the **Automatically accept SSH fingerprints** box to accept all SSH fingerprints for discovered hosts. If the host already exists in the system, the SSH fingerprint is ignored.
5. Click **Scan for Host**.



> ***Tip:*** *Search for non-sequential IP addresses at the same time by entering each IP address before clicking* ***Scan for Host****.*

Import Hosts

To import hosts, create a CSV file with a host address, port, and SSH fingerprint (optional) per line. Do not use headers in the file.

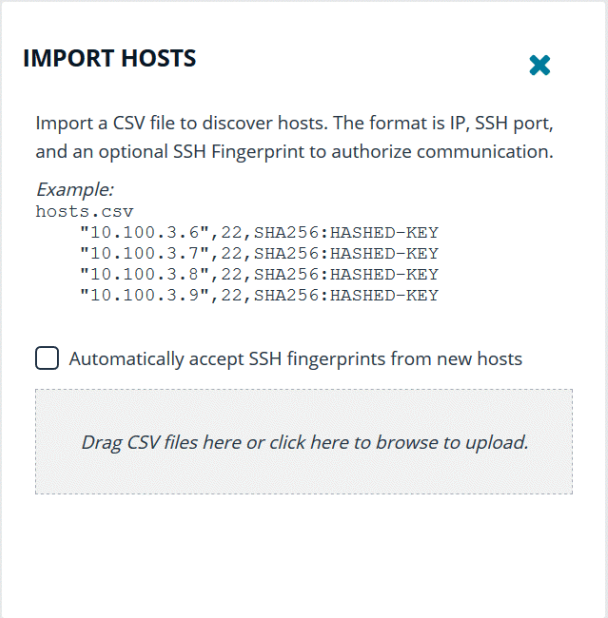
The contents of a valid file may look like the following:

```
"10.100.3.6",22,SHA256:HASHED-KEY
"10.100.3.7",22,SHA256:HASHED-KEY
"10.100.3.8",22,SHA256:HASHED-KEY
"10.100.3.9",22,SHA256:HASHED-KEY
```

> ***Note:*** *The CSV file can contain fingerprints in the SHA-256 format. If the fingerprint matches, the SSH fingerprint is accepted.*

To import a CSV file:

1. On the **Host Inventory** page, click the targeted area to upload a CSV file in the **Import Hosts** pane. Alternatively, drag the file into the targeted area.
2. Check the **Automatically accept SSH fingerprints from new hosts** box to automatically accept discovered fingerprints.
3. Locate the CSV file, and then click **Open**.

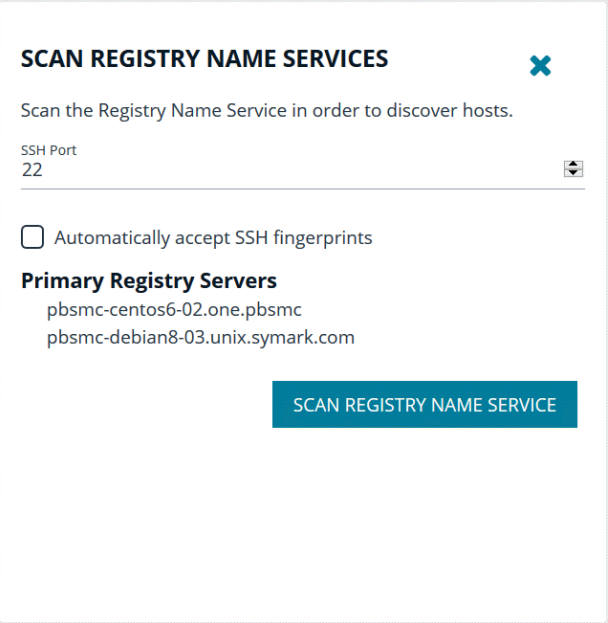


Scan the Registry Name Service

The Registry Name Service can be scanned in order to discover hosts. This scans the servers listed in **Primary Registry Servers** for all of the hosts in the network, adding previously unknown hosts to the console as appropriate.

To scan the Registry Name Service:

1. In the **Registry Name Service** section, enter an **SSH Port**. The value should map to the SSH port for the host provided. If no SSH port is provided, the default port is **22**. Each discovery scan uses a single port regardless of the number of machines.
2. Check the **Automatically accept SSH fingerprints** box to accept all SSH fingerprints for discovered hosts. If the host already exists in the system, the SSH fingerprint is ignored.
3. Click **Scan Registry Name Service**.

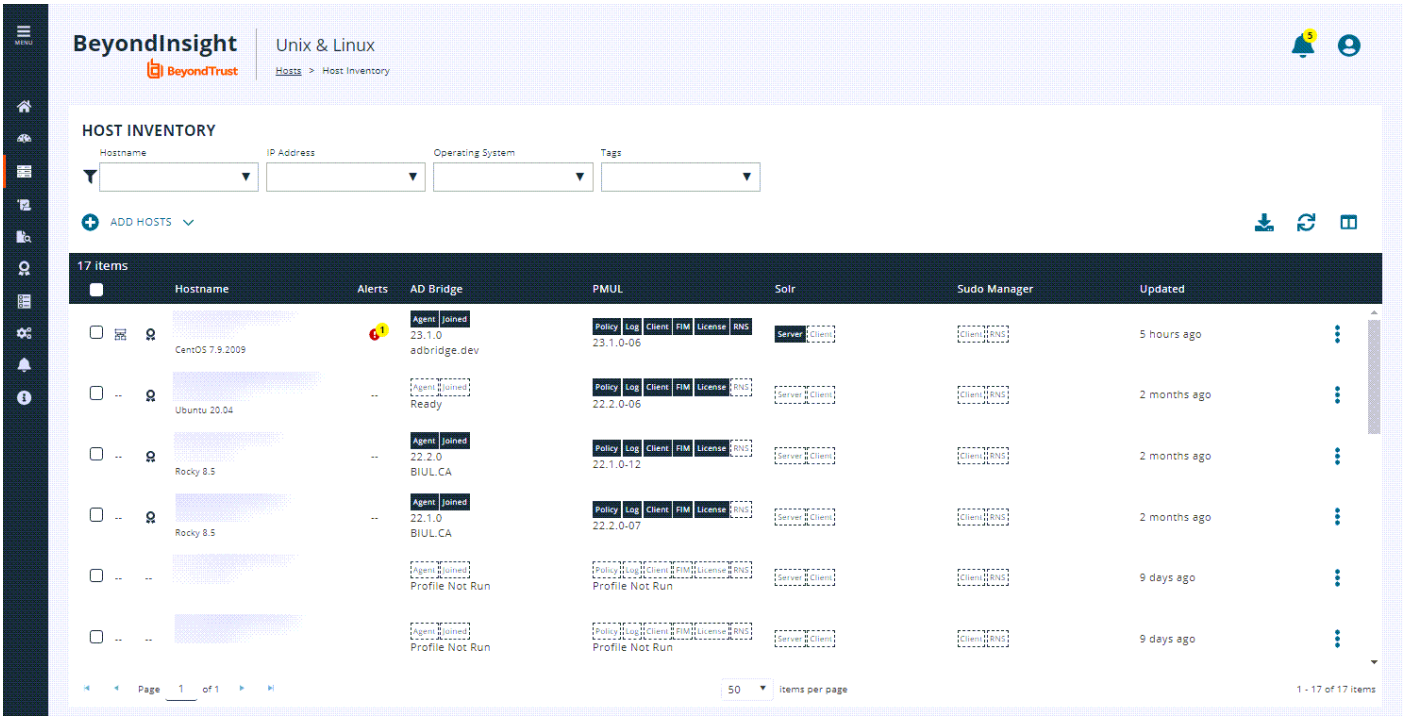


*For more information on the Scan Registry Name Service action, please see the **Tasks > Task Details** page. Any new hosts found will appear on the **Hosts > Hosts Inventory** page.*

BIUL Hosts Inventory Grid

On the **Hosts > Hosts Inventory** page, you can manage hosts and software deployments. A smart form assists in generating actions to run on one or many hosts, and you are notified when actions are complete. Hosts can be filtered by **Hostname**, **IP Address**, **Operating System**, and **Tags**.

Most actions require credentials be provided so the console can authenticate with the selected host. Credentials are managed on the **Credentials** page.



For more information, please see the following:

- *"View Tasks and Task Details in BIUL" on page 120*
- *"Manage Credentials in BIUL" on page 42*

Use the Hosts Inventory Grid

The **Hosts Inventory** page displays all the assets found during a discovery.

Click on the **Hostname** and **Updated** headers to sort and refresh the grid. When performing an action, you can quickly select all of the hosts in a grid by checking the box in the header row. To view more details about a host, select a host, and then at the far right, click the ellipsis menu icon and select **View Host Details**.

For more information on adding hosts, please see "Hosts Inventory with BIUL" on page 12.

Choose Host Inventory Columns to Display

You can choose which columns to display in the grid.

To select which columns to display, at the top-right of the grid, click the **Choose Columns to Display** icon and select one or more columns to display.

The columns appear from left to right in the grid, in the order that you select them.

Download the Results Data

You can download the results data as a JSON or CSV file. To download a results file, click the **Download** icon, and then select **JSON File** or **CSV File**. The file downloads to your **Download** folder.

Primary Server Columns

The following indicators are possible:

PMUL License Primary		Indicates Primary License servers.
Registry Name Service Primary		Indicates Primary Registry Name Service servers.

Hostname Column

The DNS name of the host. This column also contains the host IP address, operating system, and version.

Alerts Column

The following indicators are possible:

Error		Indicates a critical issue with the host.
Warning		Indicates a problem with the host.

Install Status Columns

The following columns provide information on installed components. The available columns are:

AD Bridge

If AD Bridge is installed, the **AD Bridge** column displays the software version number, agent, and joined status.

- **Agent:** Indicates if the agent is installed.
- **Joined:** Indicates the domain joined status, which will either display it is not joined or the domain the host is joined to.

PMUL

If PMUL is installed, the **PMUL** column displays the version number and an icon for each feature and role the host has enabled.

- **Policy:** Policy server
- **Log:** Log server
- **Client:** Submit or run host
- **FIM:** FIM policy applied to the server
- **License:** License server
- **RNS:** Registry Name Service server

Solr

- **Server:** Solr Server
- **Client:** Client (indexed machine)

> ***Note:*** *As of version 23.1, Solr is deprecated. BeyondInsight for Unix & Linux no longer supports installing Solr, but features that use an existing Solr installation will continue to work.*

Sudo Manager

- **Client:** Client (index machine)

Updated Column

The last time data related to the host changed.

Manage a Host

On the **Hosts > Hosts Inventory** page, access host actions for a server from the vertical ellipsis menu. Select **Peform Host Actions** from the menu to start the **Host Actions** wizard. Host actions include:

- Profile
- Install software for AD Bridge, and PMUL
- Join domain
- Deploy keyfile

Additionally, from the menu for each server, you can:

- View host details
- Delete hosts

When using the **Host Actions** wizard, only 25 hosts are displayed at a time. Select **Check All** to apply settings to all discovered hosts.

Apply Updates to Servers Using Bulk Actions

Alternatively, you can apply actions to more than one server at a time. On the **Hosts > Hosts Inventory** page, you can select more than one host and select the **Actions** menu.

Use Privilege Escalation for BIUL Credentials

Most actions require a credential be supplied in BeyondInsight for Unix & Linux (BIUL). This is the account BIUL authenticates as on selected servers. However, this account might not have sufficient privileges to execute the required commands. The console allows users to choose a **Delegation Tool** to escalate user privileges. Selecting **sudo su** requires the user to choose a second credential to delegate to.

Profile Servers in BIUL

Run a profile on a host to gather preinstall check information. This check ensures that a host is prepared for software installs. Profiling requires a credential that is a valid SSH user for a selected host. This credential does not require superuser privileges, but the credential must have write permission on the host's remote working directory.

> ***Note:*** *By default, the remote working directory is* ***/tmp****. You can configure a remote working directory. For more information, please see* *"Configure Settings and Manage Software" on page 52**.*

> ***Note:*** *To access the hosts, a valid SSH credential with administrative rights on the host is required.*

You can run a profile *immediately*, or run it as a *scheduled task*.

Profile a Host Immediately

Run a profile *immediately*, and the **Tasks** page appears, with the **Task Summary** panel open, displaying the results.

1. Go to the **Hosts > Host Inventory** page.
2. Select a host, and then at the far right, click the ellipsis menu icon and select **Perform Host Actions**.
3. Select **Profile**, and then click **Next Step**.
4. On the **Credential Selection** page, select a logon credential to access the remote system. If you cannot log on as root, then select one of the following to run the action with escalated privileges: **pbrun**, **sudo**, or **sudo su**. This might require choosing a second credential.
5. Select **Run Now**, and then click **Next Step**.
6. Review the **Summary** page, and then click **Finish**.
7. Review the **Task** page and verify the completed status of attempted actions under **Task Summary**.
8. To view more information about **Task Status**, click **Task Details**.

Profile a Host as a Scheduled Task

Set up a profile to run as a *scheduled task*. After the task has run per your schedule, you can open the **Tasks** page and locate and click the task to see the results in the **Task Summary** panel.

1. Go to the **Hosts > Host Inventory** page.
2. Select a host, and then at the far right, click the ellipsis menu icon and select **Perform Host Actions**.
3. Select **Profile**, and then click **Next Step**.
4. On the **Credential Selection** page, select a logon credential to access the remote system. If you cannot log on as root, then select one of the following to run the action with escalated privileges: **pbrun**, **sudo**, or **sudo su**. This might require choosing a second credential.
5. Select **Schedule**, and the **Calendar** tool appears.
6. Select the *month*, *week*, and *day* for the task. The full day hours are displayed. To display just the business hours, at the bottom left of the hours, click the **Show business hours** button. Click it again for full day hours.
7. Double-click the *top* or *bottom* of the hour you want to select, and the **Event** scheduling dialog box appears.
8. Verify/set the **Start** date and time, and then select the **Timezone**.

9. (Optional). Set the number of **Retries**.
10. If you want the task to be repeated, select the frequency to repeat.
11. Click **Save**.
12. Click **Next Step**.
13. Review the **Summary** page, and then click **Finish**.
14. The **Tasks** page appears. Verify that the information in the **Scheduled Summary** panel is accurate.
15. (Optional). You can *update*, *pause*, or *delete* the schedule by using the buttons at the bottom of the panel.

Profile a Host using a Credential Rule

To avoid requiring password authentication when you run a host profile, configure a *credential rule*. Use default credentials to run a profile on one or many hosts.

1. Go to the **Hosts > Hosts Inventory** page.
2. Select the hosts you want to profile:
    - **Single host**: Select the host, and then at the far right, click the ellipsis menu icon and select **Profile Host with Default Credentials**.
    - **Multiple hosts**: To select the hosts to profile, check the boxes on the left of the hostnames. From the **Actions** menu, select **Profile Host with Default Credentials**.

For more information on setting up default credentials, please see "Use Credential Rules" on page 44.

Manage AD Bridge Hosts

> ***Note:*** *To access the hosts, a valid SSH credential with administrative rights on the host is required.*

Install and Upgrade AD Bridge

To install or upgrade AD Bridge hosts:

1. Go to the **Hosts > Host Inventory** page.
2. Select a host, and then at the far right, click the ellipsis menu icon and select **Perform Host Actions**.
3. On the **Primary Action** page, select **Active Directory Bridge**.
4. On the **Secondary Action** page, select one from the following:
    - **Install:** Install AD Bridge software.
    - **Upgrade:** Upgrade AD Bridge software to the version loaded in the console. If you select **Upgrade**, you can skip to step 6.
5. If you select **Install**, you can configure the Active Directory information on the **Action Requirements** page. By default, the **Use Domain Browser** toggle is turned on. To manually enter the information, click the toggle to turn it off.
    - **Perform optional Domain join:** Select to join the Active Directory host to the domain. The join action occurs after the AD Bridge software installation completes. The toggle is turned on by default. Click the toggle if you do not want to join the host to the domain at this time.
    - **Forest:** Select the forest from the list. The forest listed here is the directory service connection already configured from the **Settings > Directory Services** menu.
    - **Domain:** Select a domain from the list.
    - **OU:** Click **Browse** to search for the OU.
    - **AD Credential:** Select the credential you want to use to access Active Directory. This credential is added when you create the directory services connection.
    - **Additional Arguments:** Add domain-join cli arguments.
6. On the **Credential Selection** page, select a logon credential to access the remote system. If you cannot log on as root, then select one of the following to run the action with escalated privileges: **pbrun**, **sudo**, or **sudo su**. This might require choosing a second credential.
7. Review the **Summary** page, and then click **Finish**.
8. Review the **Task** page and verify the completed status of attempted actions under **Task Summary**.
9. To view more information about **Task Status**, click **Task Details**.

Join the Host to an Active Directory Domain

To join selected AD Bridge hosts to a domain:

1. Go to the **Hosts > Host Inventory** page.
2. Select a host, and then at the far right, click the ellipsis menu icon and select **Perform Host Actions**.
3. On the **Primary Action** page, select **Active Directory Bridge**.

4. On the **Secondary Action** page, select **Domain join**.
5. On the **Action Requirements** page, select the Active Directory information. By default, the **Use Domain Browser** toggle is turned on. To manually enter the information, click the toggle to turn it off.
    - **Forest:** Select the forest from the list. The forest listed here is the directory service connection already configured from the **Settings > Directory Services** menu.
    - **Domain:** Select a domain from the list.
    - **OU:** Click **Browse** to search for the OU.
    - **AD Credential:** Select the credential you want to use to access Active Directory. This credential is added when you create the directory services connection.
    - **Additional Arguments:** Add **domain-join cli** arguments.
6. On the **Credential Selection** page, select a logon credential to access the remote system. If you cannot log on as root, then select one of the following to run the action with escalated privileges: **pbrun**, **sudo**, or **sudo su**. This might require choosing a second credential.
7. Review the **Summary** page, and then click **Finish**.
8. Review the **Task** page and verify the completed status of attempted actions under **Task Summary**.
9. To view more information about **Task Status**, click **Task Details**.

For more information, please see Domain Join Tool Commands, at https://www.beyondtrust.com/docs/ad-bridge/getting-started/linux-admin/domain-join-tool.htm.

Remove the Host from an Active Directory Domain

You can remove an Active Directory host from a domain.

To remove a joined domain:

1. Go to the **Hosts > Host Inventory** page.
2. Select a host, and then at the far right, click the ellipsis menu icon and select **Perform Host Actions**.
3. On the **Primary Action** page, select **Active Directory Bridge**.
4. On the **Secondary Action** page, select **Domain Leave**.
5. On the **Action Requirements** page, check the box **Delete Computer account in Active Directory**, and then select an Active Directory credential from the list.
6. On the **Credential Selection** page, select a logon credential to access the remote system. If you cannot log on as root, then select one of the following to run the action with escalated privileges: **pbrun**, **sudo**, or **sudo su**. This might require choosing a second credential.
7. Review the **Summary** page, and then click **Finish**.

Join the Host to an Azure Tenant Application

To join selected AD Bridge hosts to a Azure application, an application must have already been appropriately configured in Azure.

To join selected AD Bridge hosts to an Azure application:

1. Go to the **Hosts > Host Inventory** page.
2. Select a host, and then at the far right, click the ellipsis menu icon and select **Perform Host Actions**.

3. On the **Primary Action** page, select **Active Directory Bridge**.
4. On the **Secondary Action** page, select **Tenant Join**.
5. On the **Action Requirements** page, enter the Azure application information. As noted above, an Azure application must already have been configured.
    - **Tenant ID:** The tenant ID from the Azure application configuration.
    - **Application ID:** The application ID from the Azure application configuration.
    - **Secret:** An application secret value from Azure. This value must have been created in the Azure application (see link below).
    - **License Key:** An AD Bridge license key to license the endpoint at the same time as joining the Azure tenant.
6. On the **Credential Selection** page, select a logon credential to access the remote system. If you cannot log on as root, then select one of the following to run the action with escalated privileges: **pbrun**, **sudo**, or **sudo su**. This might require choosing a second credential.
7. Select **Run Now**.
8. Review the **Summary** page, and then click **Finish**.
9. Review the **Task** page and verify the completed status of attempted actions under **Task Summary**.
10. To view more information about **Task Status**, click **Task Details**.

Note: *To reduce the data entry required at Step 5 above, it is possible to create a Join template under* ***Settings > Software > AD Bridge > (ellipsis menu at right) > Manage Join Templates****. Here you can save the tenant ID, application ID, and license key as a template, and then, at step 5 above, select that template to populate those fields when joining a specific host to the tenant. Note that you will still need to provide an application secret. For more information, see "AD Bridge Join Templates" on page 69.*

For more information on joining an Azure Tenant, see Join an Azure AD Tenant, at https://www.beyondtrust.com/docs/ad-bridge/getting-started/installation/join-an-azure-ad-tenant.htm.

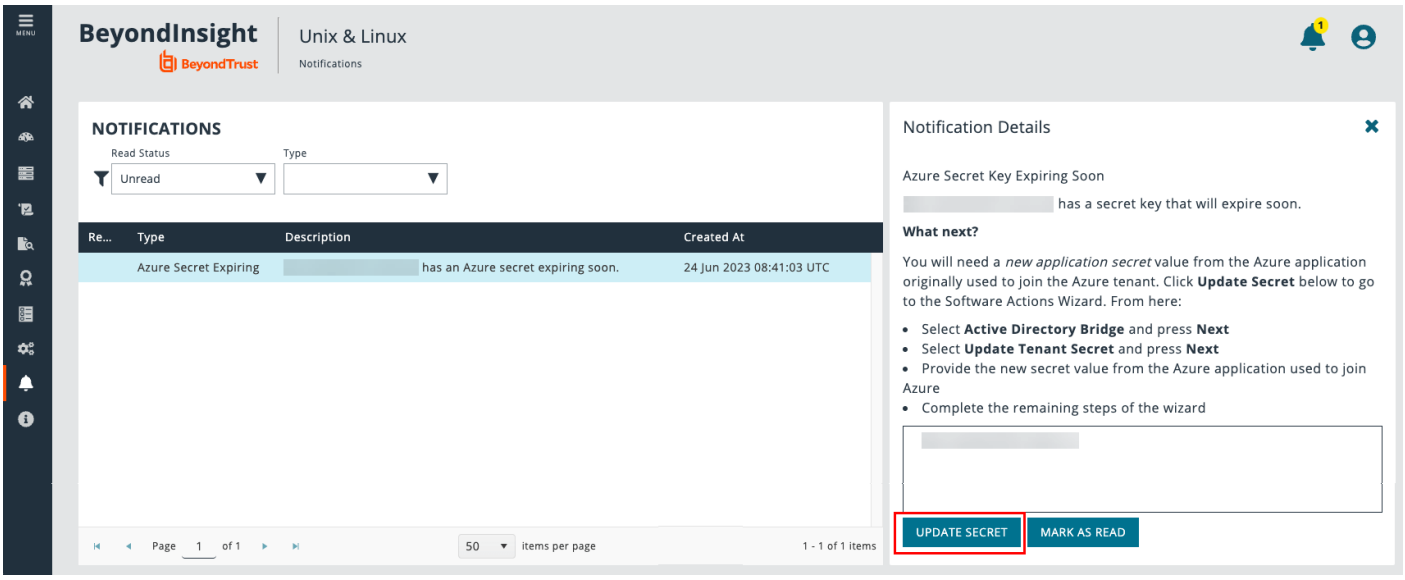
Remove the Host from an Azure Tenant Application

To remove a host from an Azure application:

1. Go to the **Hosts > Host Inventory** page.
2. Select a host, and then at the far right, click the ellipsis menu icon and select **Perform Host Actions**.
3. On the **Primary Action** page, select **Active Directory Bridge**.
4. On the **Secondary Action** page, select **Tenant Leave**.
5. On the **Credential Selection** page, select a logon credential to access the remote system. If you cannot log on as root, then select one of the following to run the action with escalated privileges: **pbrun**, **sudo**, or **sudo su**. This might require choosing a second credential.
6. Select **Run Now**.
7. Review the **Summary** page, and then click **Finish**.

Update the Azure Application Secret for a Host

The Azure application secret has a configurable expiration date. When BeyondInsight for Unix & Linux identifies that a host is using an Azure application secret that will expire soon, a notification is generated. The notification details provides you with some guidance to update the application secret.



To update the application secret used by a host to connect to an Azure application, a secret must have already been configured in Azure.

> ***Tip:*** *If you view an Azure Secret Key Expiring Soon notification, you can update the secret from the* ***Notification Details*** *panel by clicking the* ***Update Secret*** *button. Alternately, follow the procedure that appears next to perform the update.*

To update the application secret:

1. Go to the **Hosts > Host Inventory** page.
2. Select a host, and then at the far right, click the ellipsis menu icon and select **Perform Host Actions**.
3. On the **Primary Action** page, select **Active Directory Bridge**.
4. On the **Secondary Action** page, select **Tenant Secret**.
5. On the **Action Requirements** page, enter the new Azure application secret value. As noted above, an Azure application must already have been configured.
6. On the **Credential Selection** page, select a logon credential to access the remote system. If you cannot log on as root, then select one of the following to run the action with escalated privileges: **pbrun**, **sudo**, or **sudo su**. This might require choosing a second credential.
7. Select **Run Now**.
8. Review the **Summary** page, and then click **Finish**.
9. Review the **Task** page and verify the completed status of attempted actions under **Task Summary**.
10. To view more information about **Task Status**, click **Task Details**.

> *For more information on joining an Azure Tenant, see Join an Azure AD Tenant, at https://www.beyondtrust.com/docs/ad-bridge/getting-started/installation/join-an-azure-ad-tenant.htm.*

Uninstall AD Bridge

When you uninstall AD Bridge, you can also choose to leave the domain and delete the Active Directory account.

1. Go to the **Hosts > Host Inventory** page.
2. Select a host, and then at the far right, click the ellipsis menu icon and select **Perform Host Actions**.
3. On the **Primary Action** page, select **Active Directory Bridge**.
4. Select **Uninstall**.
5. On the **Action Requirements** page, select one of the following:
    - **Uninstall:** Uninstall AD Bridge software from the host.
    - **Leave and Uninstall:** Remove the host from the domain and uninstall AD Bridge software.
    - **Leave Domain, Delete Account, and Uninstall:** Remove the host from the domain, delete the Active Directory account in Active Directory, and remove the AD Bridge software.
    - **AD Credential:** The credential to use to access Active Directory. The setting is required when you select **Leave Domain, Delete Account, and Uninstall**. This credential is added when you create the directory services connection.
6. On the **Credential Selection** page, select a logon credential to access the remote system. If you cannot log on as root, then select one of the following to run the action with escalated privileges: **pbrun**, **sudo**, or **sudo su**. This might require choosing a second credential.
7. Review the **Summary** page, and then click **Finish**.

Manage PMUL Hosts

Note: *To access the hosts, a valid SSH credential with administrative rights on the host is required.*

To manage Privilege Management for Unix and Linux (PMUL) hosts:

1. Go to the **Hosts > Host Inventory** page.
2. Select a host, and then at the far right, click the ellipsis menu icon and select **Perform Host Actions**.
3. Choose the action to perform, and then follow the procedures in this section.

Software is installed with default configuration values, unless **RNS Primary and All Components** is selected. If not detected during installation, the installer generates network and REST encryption keys. All future PMUL installations will use these keys. The keys can be managed on the **Settings** page.

Install the PMUL Policy Server

To install the PMUL Policy Server:

1. Go to the **Hosts > Host Inventory** page.
2. Select a host, and then at the far right, click the ellipsis menu icon and select **Perform Host Actions**.
3. Select **Privilege Management for Unix and Linux**, and then select **Next Step**.
4. Select **Install**, and then click **Next Step**.
5. On the **Action Requirements** page, select an installation template. The features enabled in the template affect the options available. The following list displays default templates.
    - **All Components:** All PMUL components will be installed except for RNS server.
    - **License Server Only:** Only the PMUL license server will be installed.
    - **Policy and Log Server Only:** All server components of PMUL will be installed except for RNS server.
    - **Submit and Run Host Only:** The client components of PMUL will be installed.
    - **Primary Registry Server and All Components:** All PMUL components will be installed including RNS server.
6. After selecting a template, you can choose to use client registration. Note that some features selected in installation templates may require or disallow using client registration. To use client registration select a **Client Registration Server**, and then select a **Client Registration Profile**.
7. If you choose not to use client registration, you can manually select multiple policy, log, and license servers if your Installation template allows it. If you are installing a new primary policy, log, or license server click the toggle switch to indicate that this host will become a new primary policy, log, or license server.
8. On the **Credential Selection** page, select a logon credential to access the remote system. If you cannot log on as root, then select one of the following to run the action with escalated privileges: **pbrun**, **sudo**, or **sudo su**. This might require choosing a second credential.
9. Review the **Summary** page, and then click **Finish**.
10. Review the **Task** page and verify the completed status of attempted actions under **Task Summary**.
11. To view more information about **Task Status**, click **Task Details**.

For more information please see the following:

- *On installation templates, "Privilege Management for Unix and Linux Installation Templates" on page 68*
- *On client registration profiles, "Manage Client Registration Profiles" on page 37*
- *On policy caching, "Set up Policy Caching" on page 36*

Upgrade the PMUL Policy Server

To upgrade the Policy Server to the version loaded in the console:

1. Go to the **Hosts > Host Inventory** page.
2. Select a host, and then at the far right, click the ellipsis menu icon and select **Perform Host Actions**.
3. Select **Privilege Management for Unix and Linux**, and then click **Next Step**.
4. Select **Upgrade**, and then click **Next Step**.
5. On the **Credential Selection** page, select a logon credential to access the remote system. If you cannot log on as root, then select one of the following to run the action with escalated privileges: **pbrun**, **sudo**, or **sudo su**. This might require choosing a second credential.
6. Review the **Summary** page, and then click **Finish**.
7. Review the **Task** page and verify the completed status of attempted actions under **Task Summary**.
8. To view more information about **Task Status**, click **Task Details**.

Uninstall the PMUL Policy Server

To remove the Policy Server:

1. Go to the **Hosts > Host Inventory** page.
2. Select a host, and then at the far right, click the ellipsis menu icon and select **Perform Host Actions**.
3. Select **Privilege Management for Unix and Linux**, and then click **Next Step**.
4. Select **Uninstall**, and then click **Next Step**.
5. On the **Credential Selection** page, select a logon credential to access the remote system. If you cannot log on as root, then select one of the following to run the action with escalated privileges: **pbrun**, **sudo**, or **sudo su**. This might require choosing a second credential.
6. Review the **Summary** page, and then click **Finish**.
7. Review the **Task** page and verify the completed status of attempted actions under **Task Summary**.
8. To view more information about **Task Status**, click **Task Details**.

Configure SIEM for Use With a Privilege Management for Unix and Linux Server

Note: *To configure a SIEM connection, it must first be set up under* ***Settings > SIEM Connections****. For more information, please see "Manage SIEM Connections" on page 70.*

To configure SIEM for use with a PMUL server:

1. Go to the **Hosts > Host Inventory** page.
2. Select a host, and then at the far right, click the ellipsis menu icon and select **Perform Host Actions**.
3. Select **Privilege Management for Unix and Linux**, and then click **Next Step**.
4. Select **Configure a SIEM for use with one or more Privilege Management for Unix & Linux servers**, and then click **Next Step**.
5. On the **Action Requirements** page, select a SIEM connection from the dropdown.
6. On the **Credential Selection** page, select a logon credential to access the remote system. If you cannot log on as root, then select one of the following to run the action with escalated privileges: **pbrun**, **sudo**, or **sudo su**. This might require choosing a second credential.
7. Review the **Summary** page, and then click **Finish**.
8. Review the **Task** page and verify the completed status of attempted actions under **Task Summary**.
9. To view more information about **Task Status**, click **Task Details**.

Manage Solr

Note: *As of version 23.1, Solr is deprecated. BeyondInsight for Unix & Linux no longer supports installing Solr, but features that use an existing Solr installation will continue to work.*

Deploy Keyfiles

The **Deploy PMUL Network and REST encryption key files** action uses the network and encryption keys configured on the **Settings > Integration** page.

To deploy keyfiles:

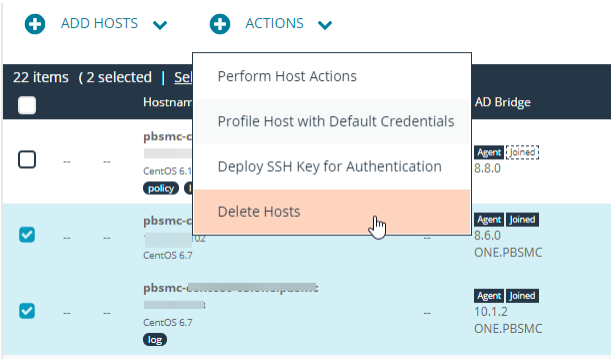
1. Go to the **Hosts > Host Inventory** page.
2. Select a host, and then at the far right, click the ellipsis menu icon and select **Perform Host Actions**.
3. Select **Privilege Management for Unix and Linux**, and then select **Next Step**.
4. Select **Deploy PMUL Network and REST encryption key files**, and then click **Next Step**.
5. On the **Credential Selection** page, select a logon credential to access the remote system. If you cannot log on as root, then select one of the following to run the action with escalated privileges: **pbrun**, **sudo**, or **sudo su**. This might require choosing a second credential.
6. Review the **Summary** page, and then click **Finish**.
7. Review the **Task** page and verify the completed status of attempted actions under **Task Summary**.
8. To view more information about **Task Status**, click **Task Details**.

Delete Hosts

The **Delete Host** action removes the selected host from the console database. No action is taken on the host nor on any credentials the console may have stored for it.

To delete a host:

1. Go to the **Hosts > Hosts Inventory** page.
2. Select the host you want to delete:
    - **Single host**: Select the host, and then at the far right, click the ellipsis menu icon and select **Delete Hosts**.
    - **Multiple hosts**: For all hosts you want to delete, check the boxes on the left of the hostnames. From the **Actions** menu, select **Delete Hosts**.
3. To confirm, click **Delete**.



View Host Details

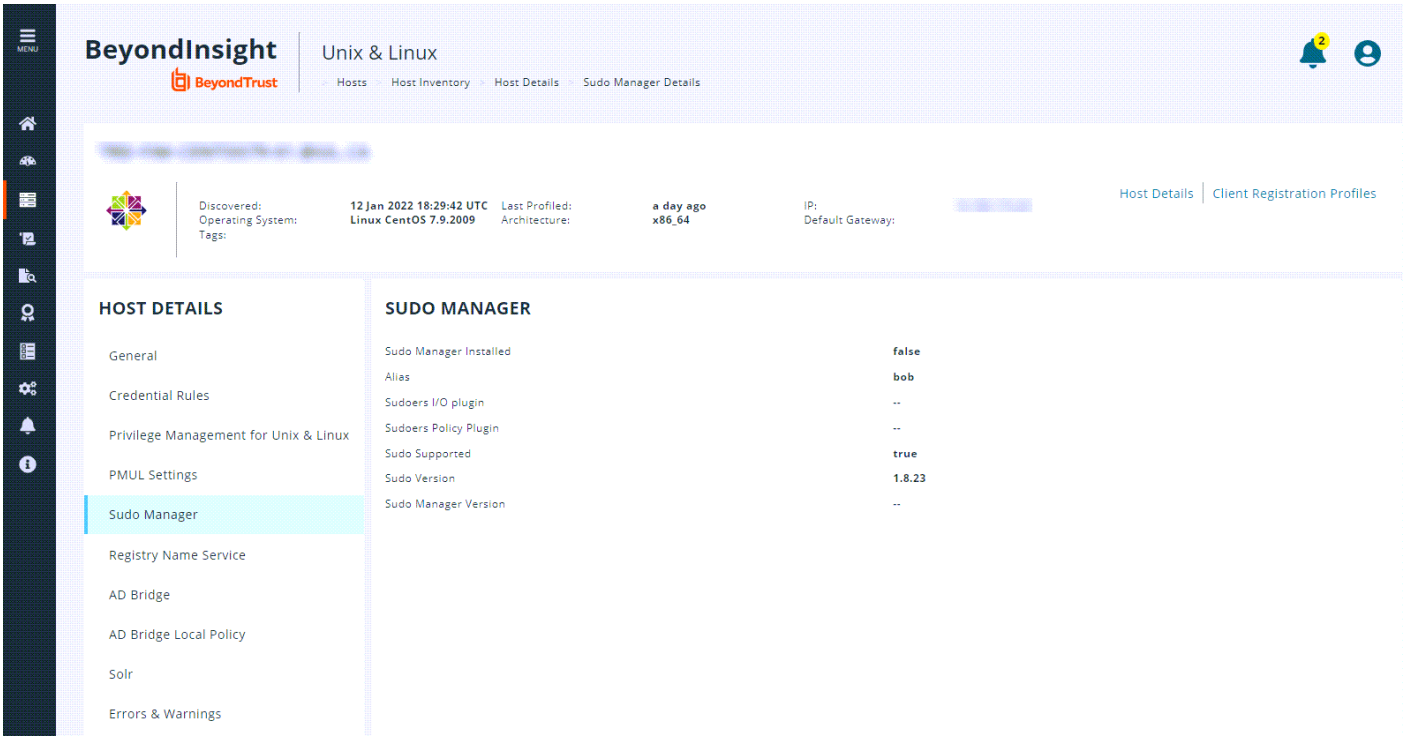
You can view more information about host servers including errors and warnings for particular products deployed.

On the **Host Details** panel, you can manage the following settings:

- Configure the Privilege Management for Unix and Linux (PMUL) **Rest API Time Correction**, which is the acceptable time offset between BeyondInsight for Unix & Linux (BIUL) and the PMUL host in seconds.

To view more information about a host:

1. On the **Hosts > Host Inventory** page, select a server, and then at the far right, click the ellipsis menu icon and then select **View Host Details**. At the top, general host details are displayed, including:
    - **Discovered**
    - **Last Profiled**
    - **IP**
    - **Operating System**
    - **Architecture**
    - **Default Gateway**
    - **Tags**
2. Select an entry in the **Host Details** panel to view details about the host collected by BIUL. Details on errors and warnings are included here, if any.



REST API Connectivity

BIUL automatically configures a REST connection to PMUL Policy Servers.

Note the following when using the REST API:

- REST API connections can only be made to a Policy Server with PMUL v 9.4 or later.
- REST connectivity does not open any firewall ports. This must be done by the user.
- By default, PMUL uses self-signed certificates. BIUL does not verify a certificate authority.

To assist in sourcing errors and troubleshooting connections, a task displays on the **Tasks** page. Additional troubleshooting information may be available on the **Host Details** page.

Tag a Discovered Host

Tags are user-defined values that can be assigned to hosts to aid in filtering the discovered hosts in the **Hosts Inventory** grid. Tags are freely entered and as such allow the user to navigate to and manage hosts quickly.

Example: *You can create a tag for all hosts in a group such as* ***Log Servers****. Assign that tag to the log servers in your environment. Tags can then be used for filtering throughout the application. To find the log servers in the* ***Hosts Inventory*** *grid, simply filter by the* ***Log Servers*** *tag.*

Create a New Tag

To create a new tag for a discovered host:

1. Go to **Hosts > Hosts Inventory** page.
2. Select a host, and then at the far right, click the ellipsis menu icon and select **View Host Details**.
3. Under **General Details**, type the desired tag name in the **Add tags** field, and press **Enter**.

Assign Tags to Hosts

To assign an existing tag to a discovered host:

1. Go to **Hosts > Hosts Inventory** page.
2. Select a host, and then at the far right, click the ellipsis menu icon and select **View Host Details**.
3. Under **General Details**, click the **Add tags** field and enter the tag name or scroll until you find the desired tag.
4. Select the tag to apply it to the host.

Filter Hosts by Tags

To filter discovered hosts by a specific tag:

1. Go to **Hosts > Hosts Inventory** page.
2. Click the **Tags** dropdown menu at the top of the **Host Inventory** grid.
3. Enter the tag name in the **Search Term** field and click **Update** to filter the results.

Delete an Existing Tag

To delete an existing tag on a discovered host:

1. Go to **Hosts > Hosts Inventory** page.
2. Select a host, and then at the far right, click the ellipsis menu icon and select **View Host Details**.
3. Under **General Details**, click the **Add tags** field, and scroll till you find the desired tag.
4. Click the **X** that appears beside the tag name to delete it from the list.

Set up Policy Caching

A cached policy can be used when the client is offline and cannot connect to the policy server. Setting up policy caching is optional.

The following must be in place to activate policy caching:

- The policy server must allow caching of policy by clients. Set this option during the policy server installation or set **allowcaching** in the **pb.settings** file after installation.
- The client must enable caching of policy from the server. Set this option during the installation of the client.

Policy caching can be configured during policy server or client installations, if the installation template used:

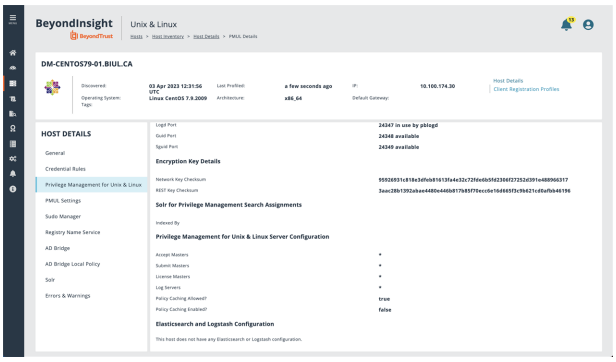
- Includes installation of a policy server. Set the **Allow Caching** option.
- Includes installation of a submit host and run host, and the installation uses client registration. Set the **Enable caching** option.

Policy caching is not supported on license server installs.

Since one applies to policy servers and one applies to policy clients, a PMUL host would not typically have both **Allow Caching** and **Enable caching** set.

To view the status of policy caching:

1. Go to **Hosts > Hosts Inventory** page.
2. Select a host, and then at the far right, click the ellipsis menu icon and select **View Host Details**.
3. Under **Privilege Management for Unix and Linux**, scroll to the **Configuration** section, and verify the values for **Policy Caching Allowed?** and **Policy Caching enabled?**



Manage Client Registration Profiles

Client Registration Profiles (CRP) simplify PMUL deployments by allowing the user to configure some environmental settings during an installation. For example, a profile might be used to copy encryption keys from machine to machine to enable communication, to copy a settings file, or to immediately join RNS groups. Without using CRP, administrators must manually provision files, keys, etc. on every host. CRP provides a centralized, customizable definition of what an installation looks like and handles that provisioning. A Client Registration Profile editor is available for policy and RNS servers on the **Client Registration** page.

> ***Note:*** *Client Registration Profiles can optionally be used with any PMUL install, but must be used with RNS.*

To manage Client Registration Profiles go to **Hosts > Hosts Inventory > View Host Details > Client Registration Profiles**. A new Client Registration Profile can be created by selecting **Add New Registration Profile**, entering a **Profile name**, and clicking **Create**.

Update a Profile

Existing Client Registration Profiles can be edited by selecting an entry from the **Client Registration Profiles** list. As necessary, configure the following options and select **Save** to save your changes or **Reset** to undo all changes.

Settings File

Provide the path to a **pb.settings** file to copy to clients. Set destination to save the file to an alternative location.

The following options are available:

- **Setting File Source**
- **Setting File Destination**

File Deployment Operations

Provide paths to files to copy from server to client. Set **Destination** to save files to an alternative location.

The following options are available:

- **Filename**
- **Destination**

Settings Controlled File Deployment Operations

Copy files pointed to by **pb.settings** keys to copy said files from server to client. Set destination to save files to an alternative location.

The following options are available:

- **Setting name**
- **To**

Certificate Deployment Operations

Copy certificates from the server to the client. If only **Destination** is set, a certificate will be saved to the provided path. If **Setting Name** is provided, a certificate will be saved to the value of that setting. If **Setting Name** and **Key** are provided, a certificate pair is saved to the value of those settings.

The following options are available:

- **Setting name**
- **Key setting name**
- **Destination**

Role Registration

Assign Registry Name Services groups and roles within. Select a **Category** and **Group Name** and **Role** options for the category will become available.

The following options are available:

- **Category**
- **Group name**
- **Role**

Post-Install Scripts

Provide paths to scripts to be executed on the client after installation. Configure the paths to scripts in the **Filename** field.

Use SSH Keys

SSH keys can be used for authentication rather than user names and passwords. At startup, BeyondInsight for Unix & Linux (BIUL) creates a new keypair if there isn't one in the system.

BIUL maintains one active key at a time.

Deploy an SSH Key

You can deploy a key to one or more servers by using the **Actions** menu.

> ***Note:*** *Credentials imported from Password Safe cannot use the BIUL SSH key for authentication.*

To deploy SSH keys:

1. Go to the **Hosts > Host Inventory** page.
2. Select one or more hosts:
    - **Single host**: Select the host, and then at the far right, click the ellipsis menu icon and select **Deploy SSH Key For Authentication**.
    - **Multiple hosts**: For all hosts you want to deploy an SSH key to, check the boxes on the left of the hostnames. From the **Actions** menu, select **Deploy SSH Key For Authentication**.
3. Select a credential from the list.
4. Click **Deploy SSH Keys**. The current active SSH key is added to the user's authorized keys (**~/.ssh/authorized_keys file**) on the selected hosts.

Download a Public Key

You can download the public key to use external to BIUL, for instance, by adding the key to a virtual machine template.

1. Go to the **Hosts > SSH Keys** page.
2. Click **Manage SSH Keys**, and then select **Download Public Key**.

Rotate a Public Key

You can rotate the SSH key and push to known hosts already using a key.

1. Go to the **Hosts > SSH Keys** page.
2. Click **Manage SSH Keys**, and then select **Rotate SSH Key**.
3. Select one of the following:
    - **Deploy To Latest:** Push the new key to hosts that are known by BIUL to be using the most recent active key.
    - **Deploy To All:** Push this key to all hosts that BIUL has pushed keys to before.
4. Click **Rotate SSH Key**.

Disable a Key

You can disable the SSH key.

1. Go to the **Hosts > SSH Keys** page.
2. Select one or more keys in the list.
3. From the **Actions** menu, select **Disable Keys**.
4. To confirm the action, click **Disable**.

Manage SSH Fingerprints

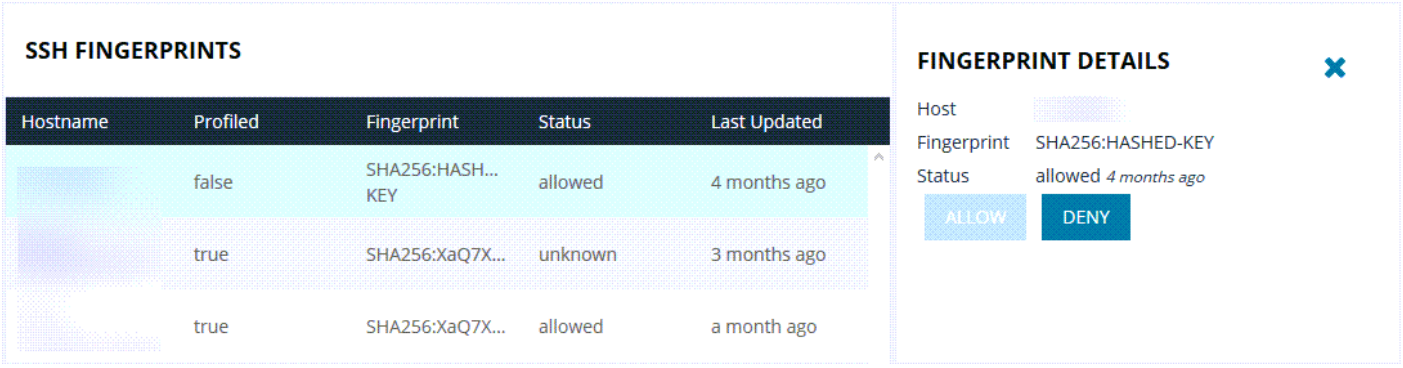
You can *accept* or *reject* SSH fingerprints. When BeyondInsight for Unix & Linux (BIUL) connects to a host, fingerprints are retrieved. Communication is not established with the host until a fingerprint is accepted.

A fingerprint can be in one of the following states:

- **Unknown:** The fingerprint must be reviewed.
- **Allowed:** The fingerprint passed review.
- **Denied:** The fingerprint was rejected, and the host is not trusted.

To manage SSH fingerprints:

1. From the menu, select **Hosts > SSH Fingerprints**.
2. Click a fingerprint to open **Fingerprint Details**.
3. Click **Allow** to trust the fingerprint or **Deny** to reject it.



Manage Credentials in BIUL

On the **Hosts > Host Credentials** page, you can manage remote host access credentials. A credential is locally persisted account information (local or domain account) that can be used to authenticate a remote session on a given host, usually in the form of Secure Shell (SSH) credentials. Console credentials and remote credentials are not synchronized. Changes to credentials in the console are not propagated to hosts. When an action runs, an error is displayed on the **Tasks** page when console credentials and credentials on the host do not match.

Types of credentials:

- **Host credentials:** Credentials that can access a host. Username and password are saved locally, typically SSH credentials.
- **Password Safe credentials:** You cannot change the Password Safe credentials on the **Credentials** page. Passwords are not saved in the console.

For more information on Password Safe credentials, please see "Import Password Safe Managed Accounts" on page 63.

Add Credentials

On the **Credentials** page:

1. Click **Manage Credentials > Create Credential**.
2. Enter the following required information:
    - **Username**
    - **Description**
    - **Password**
    - **Confirm Password**
3. Click **Save**.

Update Credentials

On the **Credentials** page:

1. In the **Credentials** list, select the credential to be updated. Use the filter options to shorten the list of credentials to select from. The **Update Credential** section is displayed.
2. Update any of the following information:
    - **Description**
    - **Password**
    - **Confirm Password**
3. Click **Save**.

Delete Credentials

On the **Credentials** page:

1. In the **Credentials** list, select the credential to be removed. Use the filter options to shorten the list of credentials to select from. The **Update Credential** section is displayed.
2. Select **Delete Credential** and confirm by clicking **OK**.

Use Credential Rules

Use credential rules to apply default credentials to hosts either directly or using a range of IP addresses. When a credential rule is applied to a host, administrators no longer need to enter a *user name / password* credential; instead, the system evaluates the rules and selects a credential to use with the host.

There are two types of rules: *host* and *network*.

Multiple rules can apply to a single host. In terms of rule precedence, a host specific rule (bound by host ID) is used in preference to all others rules that might be applied to that host.

For either host or network rules, a privilege escalation method can be saved with the authentication credential. Actions that require elevated privilege take advantage of this saved method. Applying delegation to a host is optional.

Credentials must already be created on the **Credentials** page so they are available to select when creating a rule.

For more information, please see "Manage Credentials in BIUL" on page 42.

One-Click Actions

Using default credentials enables *one-click* actions; you can select an action on a host without entering a user name and password. Running a host profile is an example of an action that can be selected without providing the host credential.

For more information, please see "Profile a Host using a Credential Rule" on page 22.

Add a Network Credential Rule

A network credential rule applies to an IP range added using CIDR notation.

1. Go to the **Hosts** page, and then select **Credential Rules**.
2. Click the **Network Rules** tab.
3. Click **Add New Credential Rule.**
4. Enter the IP address range following the CIDR notation format. For example, 10.100.1.0/24.
5. Select a logon credential from the list.
6. Select a delegation strategy and corresponding credential.
7. Click **Create Credential Rule**.

Add a Host Credential Rule

A host credential rule applies to specific hosts. Add the host name or IP address of the host. A credential rule is created for each host. A host using a default credential configured does not require a credential when running actions.

1. Go to the **Hosts** page, and then select **Credential Rules**.
2. Click the **Host Rules** tab.
3. Click **Create New Credential Rule**.
4. Search for hosts using either host name or IP address filters.

5. Select a login credential from the list.
6. Select a delegation strategy and corresponding credential.
7. Click **Create Credential Rule**.

Delete a Credential Rule

You can delete a credential rule when it is no longer required.

1. Go to the **Hosts** page, and then select **Credential Rules**.
2. Click the tab for the credential rule type.
3. Select the rule, and then click **Delete Credential Rule**.

> ***Note:*** *If you remove a credential from the* ***Host Credentials*** *page, then any credential rules using that credential are also deleted.*

View Credential Rules on a Host

You can view a list of all credential rules assigned to a host on the **Host Details** page. You can also create and change the host rule. Only one host rule is permitted for a host.

> *For more information, please see "View Host Details" on page 34.*

Manage the Registry Name Service

To manage service groups, the user must select the primary registry server on which the service groups reside, and then choose the service group to manage the hosts joined to that group and their roles within. Hosts can be filtered by **Hostname** and **IP Address**.

> *For more information on the registry name service (RNS), please see the Privilege Management for Unix and Linux Administration Guide at https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm.*

To manage service groups, navigate to **Hosts > Registry Name Service**. Membership can be managed on the **Service Group** page with options to add, promote, and remove hosts.

The following **Service Group Categories** are available:

- **Registry**
- **Policy**
- **File Integrity Monitoring**
- **Privilege Management for Networks**
- **Log**
- **Log Archive**

Manage Registry Name Service Groups

RNS groups allow clients to discover the services provided by RNS. To manage RNS groups, select **Registry** from the **Service Group Categories** list and choose a service group entry.

Add a Server

To add an available host to the service group:

1. On the **Service Group** page, click **Add Servers**.
2. In the **Add Servers** list, select **Add** to add a host to the service group.

Promote a Server

To promote a secondary RNS server in the service group, click **Promote**. The server's role is set as a **Primary** RNS server and the previous primary is set to the **Secondary** role.

Remove a Server

To remove a server from the service group, select **Remove** on a server entry and confirm by clicking **OK**.

> ***Note:** A primary server must be demoted to a secondary role before it can be removed, unless there are no other members (secondaries or clients) of the group.*

Manage Policy Service Groups

Policy service groups define the policy sources and clients for Privilege Management for Unix and Linux policy. To manage policy service groups, select **Policy** from the **Service Group Categories** list and choose a service group entry.

A new policy service group can be added by clicking **Add Service Group**, entering a **Service group name**, and clicking **Create**.

An existing policy service group can be deleted by clicking the trash bin icon and confirming by clicking **Delete**.

Add a Server

To add an available host to the service group:

1. On the **Service Group** page, click **Add Servers**.
2. In the **Add Servers** list, select **Add** to add a host to the service group.

Add a Client

To add an available host to the service group:

1. On the **Service Group** page, click **Add Clients**.
2. In the **Add Clients** list, select **Add** to add a host to the service group.

Promote a Server

To promote a secondary server in the service group, click **Promote**. The server's role will be set as a **Primary** server and the previous primary will be set to the **Secondary** role.

Remove a Server or Client

To remove a server or client from the service group, select **Remove** on a server or client entry and confirm by clicking **OK**.

Note: *A primary server must be demoted to a secondary role before it can be removed, unless there are no other members (secondaries or clients) of the group.*

Manage FIM Service Groups

File Integrity Monitoring (FIM) service groups define the policy sources and clients for FIM policy. To manage FIM service groups, select **File Integrity Monitoring** from the **Service Group Categories** list and choose a service group entry.

A new policy service group can be added by clicking **Add Service Group**, entering a **Service group name**, and clicking **Create**.

An existing policy service group can be deleted by clicking the trash bin icon and confirming by clicking **Delete**.

Add a Server

To add an available host to the service group:

1. On the **Service Group** page, click **Add Servers**.
2. In the **Add Servers** list, select **Add** to add a host to the service group.

Add a Client

To add an available host to the service group:

1. On the **Service Group** page, click **Add Clients**.
2. In the **Add Clients** list, select **Add** to add a host to the service group.

Promote a Server

To promote a secondary server in the service group, click **Promote**. The server's role will be set as a **Primary** server and the previous primary will be set to the **Secondary** role.

Remove a Server or Client

To remove a server or client from the service group, select **Remove** on a server or client entry and confirm by clicking **OK**.

> ***Note:*** *A primary server must be demoted to a secondary role before it can be removed, unless there are no other members (secondaries or clients) of the group.*

Manage Privilege Management for Networks Service Groups

Privilege Management for Networks (PMN) service groups define the policy sources and clients for PMN policy. To manage PMN, select **Privilege Management for Networks** from the **Service Group Categories** list and choose a service group entry.

A new policy service group can be added by clicking **Add Service Group**, entering a **Service group name**, and clicking **Create**.

An existing policy service group can be deleted by clicking the trash bin icon and confirming by clicking **Delete**.

Add a Server

To add an available host to the service group:

1. On the **Service Group** page, click **Add Servers**.
2. In the **Add Servers** list, select **Add** to add a host to the service group.

Add a Client

To add an available host to the service group:

1. On the **Service Group** page, click **Add Clients**.
2. In the **Add Clients** list, select **Add** to add a host to the service group.

Promote a Server

To promote a secondary server in the service group, click **Promote**. The server's role will be set as a **Primary** server and the previous primary will be set to the **Secondary** role.

Remove a Server or Client

To remove a server or client from the service group, select **Remove** on a server or client entry and confirm by clicking **OK**.

> ***Note:*** *A primary server must be demoted to a secondary role before it can be removed, unless there are no other members (secondaries or clients) of the group.*

Manage Log Server Service Groups

Log Server service groups define where audit and event logs are recorded. To manage Log Server service groups, select **Log** from the **Service Group Categories** list and choose a service group entry.

A new policy service group can be added by clicking **Add Service Group**, entering a **Service group name**, and clicking **Create**.

An existing policy service group can be deleted by clicking the trash bin icon and confirming by clicking **Delete**.

Add a Server

To add an available host to the service group:

1. On the **Service Group** page, click **Add Servers**.
2. In the **Add Servers** list, select **Add** to add a host to the service group.

Add a Client

To add an available host to the service group:

1. On the **Service Group** page, click **Add Clients**.
2. In the **Add Clients** list, select **Add** to add a host to the service group.

Promote a Server

To promote a secondary server in the service group, click **Promote**. The server's role will be set as a **Primary** server and the previous primary will be set to the **Secondary** role.

Remove a Server or Client

To remove a server or client from the service group, select **Remove** on a server or client entry and confirm by clicking **OK**.

> ***Note:*** *A primary server must be demoted to a secondary role before it can be removed, unless there are no other members (secondaries or clients) of the group.*

Manage Log Archive Service Groups

Log Archive service groups define where audit and event logs are archived. To manage Log Archive service groups, select **Log Archive** from the **Service Group Categories** list and choose a service group entry.

A new policy service group can be added by clicking **Add Service Group**, entering a **Service group name**, and clicking **Create**.

An existing policy service group can be deleted by clicking the trash bin icon and confirming by clicking **Delete**.

Add a Server

To add an available host to the service group:

1. On the **Service Group** page, click **Add Servers**.
2. In the **Add Servers** list, select **Add** to add a host to the service group.

Add a Client

To add an available host to the service group:

1. On the **Service Group** page, click **Add Clients**.
2. In the **Add Clients** list, select **Add** to add a host to the service group.

Promote a Server

To promote a secondary server in the service group, click **Promote**. The server's role will be set as a **Primary** server and the previous primary will be set to the **Secondary** role.

Remove a Server or Client

To remove a server or client from the service group, select **Remove** on a server or client entry and confirm by clicking **OK**.

Note: *A primary server must be demoted to a secondary role before it can be removed, unless there are no other members (secondaries or clients) of the group.*

Configure Settings and Manage Software

From the **Settings** page, you can configure the following:

- **Console Access:** Add new users and groups to BeyondInsight for Unix & Linux (BIUL).
- **Roles:** Manage the assignment of roles to users.
- **Software:** Manage BeyondTrust software versions.
- **System:** Manage BIUL settings.
- **Directory Services:** Manage directory services connections.
- **SIEM Connections:** Manage SIEM Elasticsearch and Logstash connections.
- **Integration:** Manage integration settings for external BeyondTrust integrations.
- **Certificates:** Manage certificates.

Manage BIUL Settings

Deployment Settings

To configure deployment settings:

1. Select the **Settings** menu.
2. Click **System**.
3. Set the **Remote Working Directory** for deployments. For example, **/tmp**.
4. Enable or disable **Verify SSH Fingerprints** to verify if a host is trusted by BIUL by default upon discovery.
5. Click **Save Settings**.

Authentication Timeout Settings

The following options are available to configure **Authentication Timeout Settings** for the BIUL console. The settings are specified in minutes.

1. Select the **Settings** menu.
2. Click **System**.
3. Set values for the following timeout settings:
    - **Total Session Length**
    - **Session Timeout Warning**
    - **Total Idle Length**
    - **Idle Timeout Warning**
4. Click **Save Settings**.

Application Settings

Configure application settings if you want to use the password reset feature available on the BIUL logon page.

> ***Note: Enforce Email Verification*** *is not available if there are no users with the* ***sysadmin*** *role or* ***accountadmin*** *role with a verified email, or if the currently logged on user has not verified their address. This is to prevent a lockout.*

1. Select the **Settings** menu.
2. Click **System**.
3. Enter the base URL for BIUL. For a standalone deployment with default port, the URL is https://<hostname>:4443/. On the BeyondTrust appliance, the URL is https://<hostname>/pbsmc/. The BIUL URL is required for password reset and email verification; the URL is used to format links in emails.
4. (Optional). Check the box to turn on **Enforce Email Verification**. When this setting is turned on, BIUL users must have verified email addresses to authenticate. When the email account is verified and authenticated, the password reset link on the logon page is available to the user.

5. (Optional). Check the box to **Disable System Provided Certificate Authority**. When BIUL is turned on we create a signing authority, and then sign our own certificates for use with things like *solr*.Use this option when you are using signed certificates, and specifically do not want to use our authority at all.
6. Click **Save Settings**.

User Lockout Settings

A user can try to log on five times (the default value) before the account is locked out. The default lockout period is 30 minutes. You can change the default settings

Lockout settings are on by default.

To change default lockout settings:

1. Select the **Settings** menu.
2. Click **System**.
3. Set the number of attempts the user can try to logon. The default is 5.
4. Set the authentication window for logon attempts. This is the length of time the user can try to logon. The default is 5 minutes.
5. Set the user lockout period. The default is 30 minutes.
6. Click **Save Settings**.

An administrator can unlock a user account on the **User Details** page in the Console Access. Select the user and click **Unlock User**.

For more information, please see "Unlock a User Account" on page 60.

Set up Password Reset

A **Reset Password** link is available on the BIUL logon page. A local user must verify their email address to use the password reset feature. Verifying the email address must be completed (regardless of whether the account verification is enabled).

***Note:** The password reset feature is not available to directory service users.*

To use the **Reset Password** link for local accounts, the following must be in place:

- SMTP settings must be configured for your mail server. If the SMTP server is not configured the **Send Verification Email** option is not available.
- Application settings must be configured.
- The email address for your BIUL account must be verified and authenticated. Only after the address is verified can it be used to reset a password.

A BIUL administrator can send a verification email.

To send an email verification:

1. Click the **Settings** menu, and then click **Console Access**.
2. Click the **Users** tab.
3. Click the edit icon for a local user account to display the **User Details** page.
4. Click **Send Verification Email**.

The user receiving the verification email must click the link and provide credentials to authenticate the account. After this authentication the email account is verified and can be used in a password reset.

Add a Directory Service Connection

BeyondInsight for Unix & Linux (BIUL) supports connections to the following directory service providers:

- Active Directory
- Red Hat Identity Management (IdM)/FreeIPA
- OpenLDAP

More than one directory service provider can be configured in the same deployment.

In some cases, the connection type might be set to **Unknown**. This can occur if the data existed previous to BIUL 9.4. The connection will work. However, we recommend selecting the appropriate connection type from the list.

To add a connection:

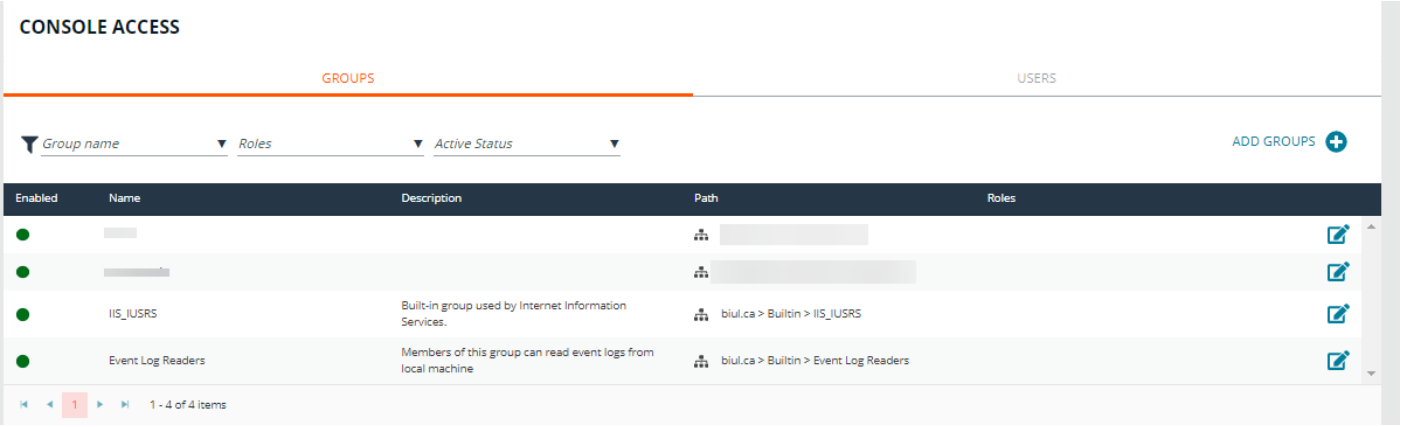
1. Select the **Settings** menu, and then click **Directory Services**.
2. Click **Add Connection**.
3. Select the connection type from the list.
4. Select the settings for the connection, including domain, user credentials, and port. Ensure the correct format is used for the user names.
    - **Active Directory**: Enter the user name in the user principal name (UPN) format (admin@domain) or in the sAMAccountName format (domain@admin).
    - **IdM and OpenLDAP**: Enter the user name in bind DN format (cn=admin,dc=domain,dc=tes).
5. (Optional). Click **Test Settings** to ensure the connection between BIUL and the directory service works.
6. Click **Save Directory Service Settings**.

Delete a Directory Connection

1. Select the **Settings** menu, and then click **Directory Services**.
2. Select a connection.
3. Click **Delete Connection**.
4. Click **Delete** to confirm.

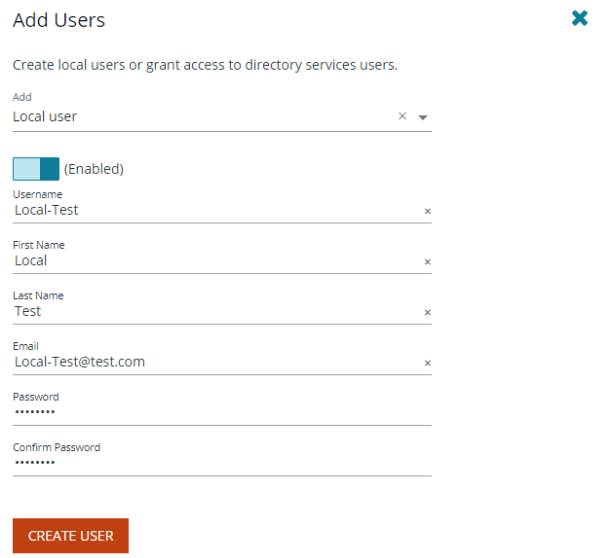
Manage BIUL Console Access

You can add and manage user accounts and groups in the console.



Add a Local User Account

1. Select the **Settings** menu.
2. Click the **Console Access** tile.
3. Click the **Users** tab, and then click **Add Users**.
4. Click **Add > Local User**.
5. Enter the following information:
    - **Enabled:** Enable or disable the user account.
    - **Username:** This will be used to authenticate the account in the console and must be unique in the system. Once the **Username** has been saved, it cannot be changed.
    - **First Name:** The user's first name.
    - **Last Name:** The user's last name.
    - **Email:** The user's email address.
    - **Password:** The user's password. Used to authenticate the account in the console. Must be at least 8 characters.
    - **Confirm Password:** Must match the **Password** value.
6. Click **Create User**.



Assign a Role to a User Account

1. Select the **Settings** menu.
2. Click the **Console Access** tile.
3. In the **Console Access** list, click the **Users** tab.
4. Click the edit icon for a local user account to display the **Edit User Details** page.

5. On the **User Details** panel, click **Roles**.
6. Select from the following roles:
    - **System Administrator**
    - **API User**
    - **Auditor**
    - **Account Administrator**
    - **Policy Administrator**
    - **Software Administrator**

> *For more information about role-based access, please see "Configure Role-Based Access" on page 61.*

Update a Local User Account

1. Select the **Settings** menu.
2. Click the **Console Access** tile.
3. In the **Console Access** list, click the **Users** tab.
4. Click the edit icon for a local user account to display the **Edit User Details** page.
5. On the **User Details** panel, click **Details** (by default, this option is displayed). The following configuration options are available:
    - **Enable User:** Enable or disable the user account.
    - **First Name:** The user's first name.
    - **Last Name:** The user's last name.
    - **Email:** The user's email address.
6. Click **Save User**.

Update Password for a Local User Account

1. Select the **Settings** menu.
2. Click the **Console Access** tile.
3. In the **Console Access** list, click the **Users** tab.
4. Click the edit icon for a local user account to display the **Edit User Details** page.
5. On the **User Details** panel, click **Authentication**.
6. Change the password, and then click **Update Password**.

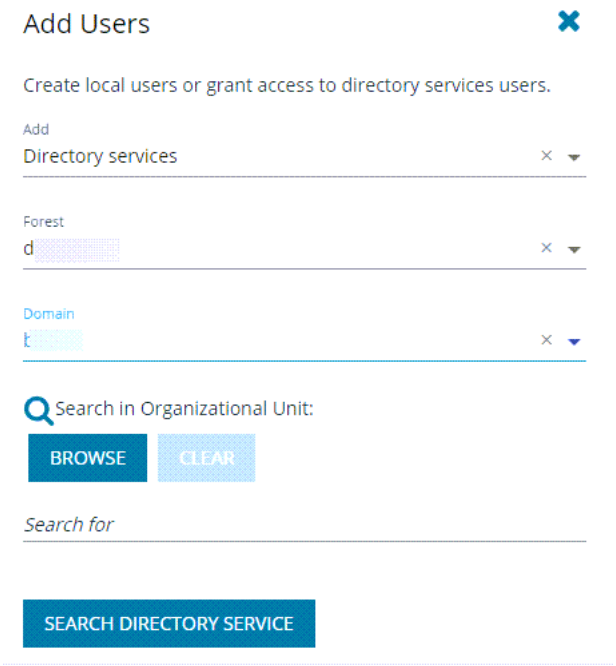
Delete a Local User Account

1. Select the **Settings** menu.
2. Click the **Console Access** tile.
3. In the **Console Access** list, click the **Users** tab.

4. Click the edit icon for a local user account to display the **Edit User Details** page.
5. Click the trashcan icon, and then click **OK** to confirm the deletion.

Add a Directory Services User

1. Select the **Settings** menu.
2. Click the **Console Access** tile.
3. In the **Console Access** list, click the **Users** tab.
4. Click **Add Users**.
5. From the **Add** list, select **Directory services**.
6. Select the Directory services **Forest** and **Domain**.
7. To search in an organizational unit (OU), click **Browse** and select an OU.
8. In the **Search for** box, enter the search criteria for the Directory services object. To help narrow the search, from the list at the right, you can select a **Query Type**.
9. Click **Search Directory Service**. Search results are displayed.
10. Select the user or group from the search results and it is added to the **Console Access** list.



Note: *The user is enabled or disabled depending on the Directory services configuration. The object configuration must be updated using Directory services.*

Add a Directory Services Group

You can only add a group already created in Directory services. The group is enabled or disabled depending on the Directory services configuration. The object configuration must be updated using Directory services.

1. Select the **Settings** menu.
2. Click the **Console Access** tile.
3. In the **Console Access** list, click the **Groups** tab.
4. Click **Add Groups**.
5. Select the Directory services **Forest** and **Domain**.
6. To search in an organizational unit (OU), click **Browse** and select an OU.
7. In **Search for**, enter the search criteria for the Directory Services object. To help narrow the search, from the list at the right, you can select a **Query Type**.
8. Click **Search Directory service**. Search results are displayed.
9. Select the group from the search results and it is added to the **Console Access** list.

Assign a Role to a Group

1. Select the **Settings** menu.
2. Click the **Console Access** tile.
3. In the **Console Access** list, click the **Groups** tab.
4. Click the edit icon for a group to display the **Group Details** page.
5. Select the **Roles** tab.
6. Select from the following roles:
    - **System Administrator**
    - **API User**
    - **Auditor**
    - **Account Administrator**
    - **Policy Administrator**
    - **Software Administrator**

For more information about role-based access, please see "Configure Role-Based Access" on page 61.

Delete a Directory Services User or Group

1. Select the **Settings** menu.
2. Click the **Console Access** tile.
3. In the **Console Access** list, click the **Users** or **Groups** tab.
4. Click the edit icon for a local user account or group to display the **Edit User/Group Details** page.
5. Click the trashcan icon, and then click **OK** to confirm the deletion.

Unlock a User Account

1. Select the **Settings** menu.
2. Click the **Console Access** tile.
3. In the **Console Access** list, click the **Users** tab.
4. Find the user account in the list, and then click the edit icon.
5. Click **Unlock User**.

Configure Role-Based Access

Access control provides a role-based system to authenticate users in BeyondInsight for Unix & Linux(BIUL). Users are assigned roles based on the level of access they need to do their BIUL job functions.

Areas in the console require certain permissions. If a user is not assigned those permissions, then they cannot access those features in the console. For example, the **policyadmin** role is required for an authenticated user to interact with policy.

Roles can be assigned to either a user account or a group.

> ***Note:*** *The account created during the first run wizard is assigned the* ***sysadmin*** *role. This role has full privileges in the system.*

The following roles are available:

- **sysadmin:** All roles; can do everything
- **policyadmin:** Full access to policy management
- **softwareadmin:** Full access to software management (deploy software, remove, etc.)
- **auditor:** Full access to log features
- **accountadmin:** Full access to controlling console access
- **apiuser:** Full access to using the public REST API

Full access to the entitlement gives the user or group the following permission attributes: **create**, **view**, **update**, and **delete**.

You can assign roles in two ways:

- On the **Settings > Console Access > Users** page. Provision roles on the details page for users and groups.
- On the **Settings > Roles > Users** page. See the following sections for details.

> *For more information on provisioning roles for users, please see "Assign a Role to a User Account" on page 57.*

Assign a Role to User Accounts

1. Click **Settings > Roles**.
2. Select a role from the list.
3. Click the **Users** tab.
4. Click the **Users without this role** button to see users that do not currently have this role.
5. Check the boxes for users you want to add.
6. Click **Add Selected Users**.

Assign a Role to Groups

1. Select **Settings > Roles**.
2. Select a role from the list.
3. Click the **Groups** tab.

4. Click the **Groups without this role** button to see groups that do not currently have this role.
5. Check the boxes for groups you want to add.
6. Click **Add Selected Groups**.

Integrate Password Safe with BIUL

Use Password Safe to Manage Credentials

You can use Password Safe to manage credentials. Then, when you run actions on your hosts, passwords are retrieved at runtime from Password Safe rather than storing the passwords locally.

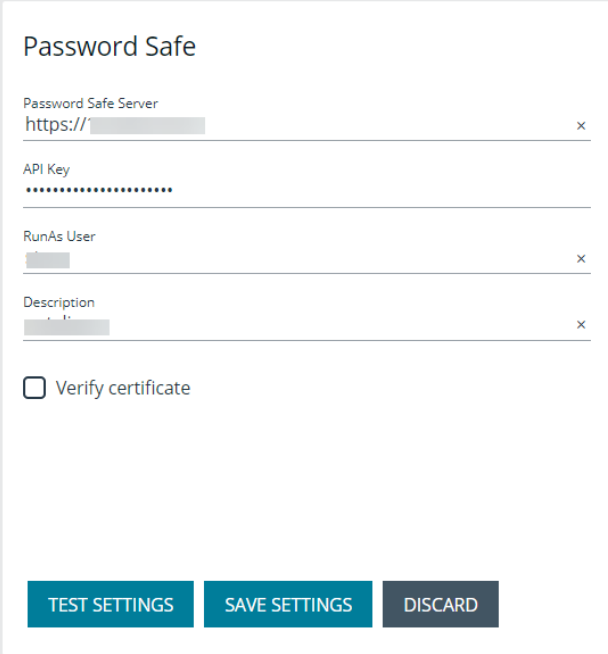
This section provides Password Safe configuration information within the console.

> *For more information on configuring Password Safe, please see BeyondTrust Password Safe Guides at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/index.htm.*

Configure Password Safe

Configure the settings for the Password Safe server. To configure the Password Safe integration:

1. In the console, select the **Settings** menu.
2. Click **Integration**.
3. Enter the following information:
    - **Password Safe Server:** The location of the Password Safe server. Do not add a trailing slash. For example, https://pbps_server.
    - **API Key:** The API key generated in BeyondInsight.
    - **RunAs User:** The BeyondInsight account under which the requests will be made. This Password Safe user must be in a **User Group** with API access and with an access policy that has auto-approve enabled for access.
    - **Description:** A text entry to provide any additional details (optional).
    - **Verify certificate:** Disabling this option bypasses certificate validation.
4. (Optional). To ensure the connection works, click **Test Settings**.
5. Click **Save Settings**.



Import Password Safe Managed Accounts

A Password Safe managed account must be imported as a BeyondInsight for Unix & Linux (BIUL) credential.

> ***Note:** Password Safe account details such as **username** and **password** cannot be changed in BIUL. These details are read-only values. The password is managed by Password Safe and retrieved dynamically.*

To import a managed account:

1. In the console, go to **Hosts > Host Credentials**.
2. Click **Manage Credentials** and select **Import from Password Safe**.
3. Select the managed accounts from the list of results the console can access and click **Import Selected**. You can filter the managed accounts by **Username** and **Description**. Imported accounts are displayed on the **Credentials** page.

Note: *A status 200 might be displayed if the selected managed account already exists as a console credential.*

The following example is intended to provide a high-level configuration and is provided only as an overview.

Example: *In this example, the goal is to use an account called **biul_user** on a host at 10.100.10.10 to perform a **Profile Servers** action. BeyondInsight/Password Safe is running at https://my_pbps.*

1. *Enable **biul_user** in the Password Safe API.*
   - *In BeyondInsight, add the 10.100.10.10 asset if required, and then choose the **Add/ Edit Password Safe** option for 10.100.10.10 in the **Assets** grid.*
   - *On the **Local Accounts** tab, select **Add**, and then provide the details for **biul_user**. Ensure the **Enable for API Access** option is selected.*
2. *Get an API Key and whitelist **BeyondInsight for Unix & Linux:***
   - *In BeyondInsight, go to **Configure > Password Safe > Application API Registration**.*
   - *Create a new registration.*
   - *Add the BIUL IP address to the source addresses list.*
   - *Disable the certificate required option.*
   - *An API key is generated when the registration is saved. This key is used in console.*
3. *Configure an Access Policy in BeyondInsight:*
   - *Go to **Configure > Password Safe > Access Policies**.*
   - *Create a policy.*
   - *In the **Access** section, ensure **Approvers** is set to auto-approve.*
4. *Configure an API User Group in BeyondInsight:*
   - *Go to **Configure > Accounts**.*
   - *Create a group. Ensure **Enable API Application** is selected and the registered application is selected.*
   - *In **Smart Rules**, select the **Roles** option for the **All Managed Accounts** rule.*
   - *Choose **Requestor** under **Password Safe**.*
   - *Select the access policy created earlier as the access policy.*
5. *Create an API User in BeyondInsight:*
   - *Go to **Configure > Accounts**, and add an account. Ensure it belongs to the group created earlier.*
6. *Configure Password Safe in BIUL:*
   - *Go to **Settings > Integration**.*
   - *Enter the details for the Password Safe server. The **API Key** was obtained in step 2 and the **RunAs User** is the account created in step 5. The URL would be https://my_pbps.*

7. *Add **biul_user** to BIUL:*
    - *Go to **Hosts > Credentials**.*
    - *Click **Add Credential** and select **Import from Password Safe**.*
    - *In the list, select **biul_user**.*
    - *Click **Import Selected**. The imported account is displayed on the **Credentials** page.*
8. *Use the **biul_user** in the console:*
    - *From the **Hosts > Host Inventory** page, choose **Perform an Action > Profile Servers**, select a host, and select **Perform Host Actions** from the menu.*
    - *Select **Privilege Management for Unix and Linux**, and then select **Profile**.*
    - *On the Credential Management page, select the **biul_user**.*
    - *Go through the remaining pages on the Perform Host Actions wizard.*

Configure the PMUL Integration

Upload key files to confirm the files on the host are synchronized with the keys used by the console.

> ***Note:*** *If no key files are present, the console creates them during the next installation of Privilege Management for Unix and Linux (PMUL) for versions 9.4.5 and later.*

To configure PMUL:

1. In the console, select the **Settings** menu, then click **Integration**.
2. If you do not want to verify certificates, turn on **Bypass SSL certificate validation**.
3. Choose whether to enable or disable **Role entitlement reporting by default**.
4. Choose whether to enable or disable **Prevent role entitlement reporting override**. When the toggle is enabled, all new role based policies will default to entitlement reporting enabled, or vice versa if set to **false**. The setting can be locked so the default value is both set and unchangeable per policy. This is for new policies only; disabling entitlement reporting will not change the values for existing policies.
5. Upload network or REST key files to the console.

Manage Software

View Software Managed by BeyondInsight for Unix & Linux

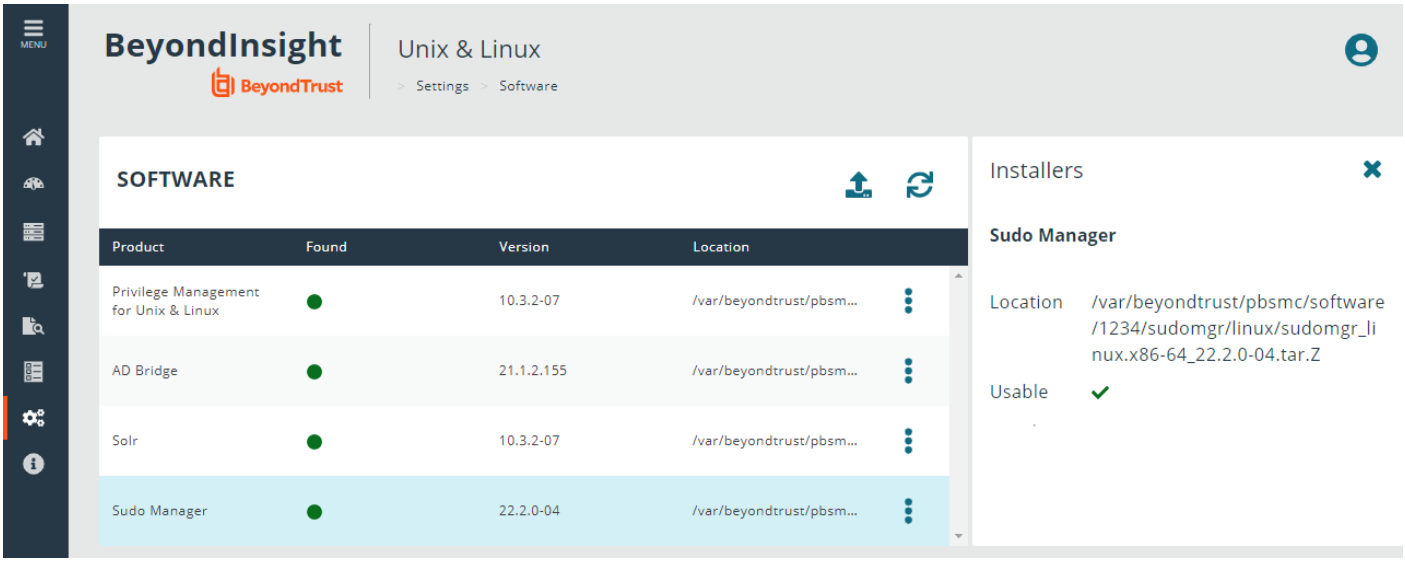
The **Settings > Software** page lists the software managed by BeyondInsight for Unix & Linux (BIUL). Basic information includes:

- Product name
- Visual indication the software is present (green dot) or not (gray dot)
- Version currently installed
- Location of the software

To update the list, click the **Refresh** icon.

View Software Details

On the **Settings > Software** page, you can get more detailed information for each software product listed. To view details on specific software, at the far right of the software listing, click the vertical ellipsis menu icon, and then select **View Details**. The **Installers** side panel appears at the right of the software product table. The panel list is scrollable.



To view details for a different product, click the **vertical ellipsis** on that product's row. The **Installers** side panel displays the new product information.

To close the panel, at the top-right of the panel, click the **X** button.

Upload Software Packages

You can upload Privilege Management for Unix and Linux (PMUL) and AD Bridge software packages on the Software page.

> *For more information, please see Upload Software, at https://www.beyondtrust.com/docs/privilege-management/console/beyondinsight-unix-linux/install/install-windows.htm#upload-software.*

Privilege Management for Unix and Linux Installation Templates

Use installation templates to apply different components to a PMUL server.

Some templates are preset and read-only:

- All components
- License Server only
- Policy and Log Server
- Submit and Run Host Only
- Primary Registry Server and All Components

Apply an installation template when running the Host Actions wizard for a PMUL install.

> *For more information, please see "Install the PMUL Policy Server" on page 28.*

Create an PMUL Installation Template

You can create a custom PMUL installation template. For example, you might want a template to only install the log server feature. Create a template called **Log Server** and select only **Install Log Server**.

> ***Tip:** You can select an existing template and click **Clone** to start with a base configuration for a new template.*

To create an installation template:

1. Go to the **Settings > Software** page.
2. At the far right of the Privilege Management for Unix and Linux row, click the vertical ellipsis menu icon, and then select **Manage Installation Templates**.
3. Click **Add New Template**.
4. Enter a **Name** for the template, and then click **Create**.
5. Select the template options. The template settings are automatically saved.

Clone a PMUL Installation Template

You might want to clone a PMUL installation template in order to make a backup of an existing one, or use it as a template to create a new one.

To clone an installation template:

1. On the **Installation Templates** panel, select a template, and then click **Clone**.
2. Enter a **Name** for the template, and then click **Create**.
3. Select the template options. The template settings are automatically saved.

Delete a PMUL Installation Template

To delete an installation template:

1. On the **Installation Templates** panel, select a template.
2. Click **Delete**, and then click **OK** to confirm.

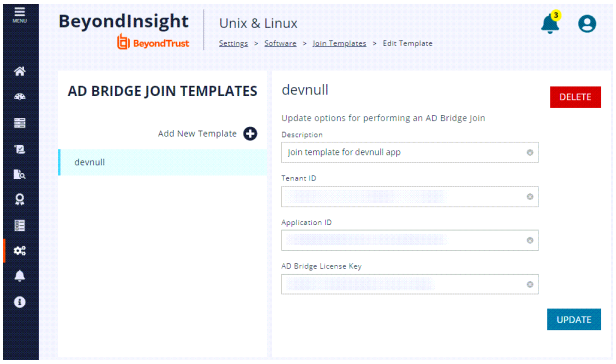
AD Bridge Join Templates

To reduce data entry when joining the host to an Azure tenant application, use AD Bridge (ADB) join templates. When joining a specific host to the tenant, select the template to populate the tenant ID, application, and license key fields automatically.

To create an ADB join template:

1. Select **Settings > Software**.
2. At the far right of theAD Bridge row, click the vertical ellipsis menu icon, and then select **Manage Join Templates**.
3. Click **Add New Template**.
4. Enter a **Name** and **Description** for the template.
5. Enter the **Tenant ID**, **Application ID**, and **AD Bridge License Key**.
6. Click **Create**. The template is added to the list on the left.

When using the template, you must still provide an application secret.



> *For more information, see "Join the Host to an Azure Tenant Application" on page 24.*

Update an AD Bridge Join Template

To update an existing ADB join template:

1. On the **AD Bridge Join Templates** panel, select the template to update.
2. Update the information for the template.
3. Click **Update**.

Delete an AD Bridge Join Template

To delete an existing ADB join template:

1. On the **AD Bridge Join Templates** panel, select the template to delete.
2. Click **Delete**, and then click **OK** to confirm.

Manage SIEM Connections

You can set up SIEM connections to integrate with Privilege Management for Unix and Linux (PMUL) and AD Bridge events. The available connection types are **Elasticsearch** and **Logstash**.

IMPORTANT!

*You can have only **one** Elasticsearch type connection.*

For information on configuring a SIEM connection for use with a PMUL server, please see "Configure SIEM for Use With a Privilege Management for Unix and Linux Server" on page 29.

Add a SIEM Connection

1. On the sidebar menu, click **Settings > SIEM Connections**.
2. In the **SIEM Connections** left panel, click **Add Connection**.
3. On the **Create New SIEM Connection** page, select the SIEM connection type.
4. In the **SIEM Connection Details** section, enter a **name** and **URL** for the connection.
5. Optionally, check the box to verify the **certificate** for the connection. You can use this option in the case of unknown signer, for example, if a self-signed certificate is in use.

For an **Elasticsearch** connection type:

1. In the **Elasticsearch Connection Details** section, select a credential type from the list: **Username and Password** or **API Key**.
2. Depending on the credential type you select, enter the following:
   - **Username** and **Password**
   - **API ID** and **API Key**
   - **Cloud ID**
3. You can leave the **Optional Search Index Patterns Overrides** section fields as is, because there are default pattern values. Optionally, enter the following:
   - PMUL Index Patterns
   - PMUL Session Replay Index Patterns
   - AD Bridge Index Patterns
4. Proceed to the *"To complete the process for either connection type"* section (after the Logstash section, next).

***Note:** You can define the location of an Elasticsearch instance using two methods within BIUL:*
- ***Directly specifying the URL of the Elasticsearch instance.** This method specifies the location of Elasticsearch but contains no information about the location of Kibana.*
- ***Providing a CloudID identifying the Elasticsearch instance.** This method encodes the locations of both Elasticsearch and Kibana. Only connections using CloudID can identify the location to deploy the Kibana dashboard.*

For a **Logstash** connection type:

1. Click the **Information** icon (next to **Logstash Connection Details**) to see sample configuration examples, and additional pipelines information
2. In the **Logstash Connection Details** section, enter a **Username** and **Password**.

To complete the process for either connection type:

1. In the **BeyondInsight for Unix & Linux Logging** section, select the logging option(s), to send BIUL **Console Audit Data**, **System Logs**, or **Task Logs** to the SIEM. When enabled, data that is regularly stored in the local log file or BIUL database is additionally forwarded to the elastic connection. This data is in the elastic common schema format. The data is then available via a grid in the **Audit > Unified Search > BeyondInsight for Unix & Linux** section.
2. Optionally, to test your updated settings and connection, click **Test Settings**, and check for the success message.
3. Click **Save SIEM Connection**.

Edit a SIEM Connection

You can change the settings for an existing SIEM connection.

1. On the sidebar menu, click **Settings > SIEM Connections**.
2. In the **SIEM Connections** list, select a connection.
3. On the **Edit SIEM Connection** page, make your modifications, and then click **Save SIEM Connection**.
4. Optionally, to test your updated settings and connection, click **Test Settings**.

Deploy a Kibana Dashboard

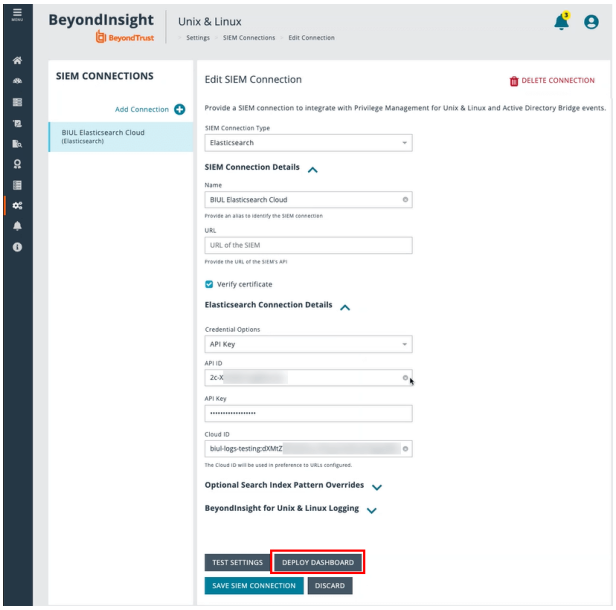
Connections using CloudID can identify the location to deploy the Kibana dashboard.

To deploy a Kibana dashboard, you must:

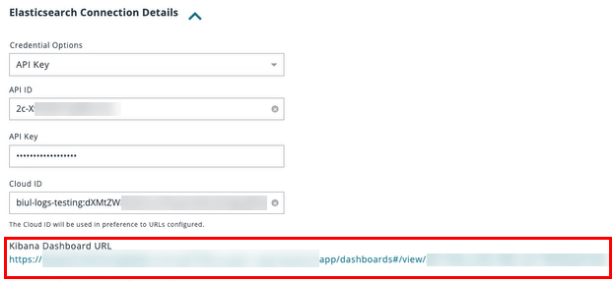
- Configure Elasticsearch in BIUL.
- Associate a Kibana instance with the Elasticsearch instance.
- Connect to your Elasticsearch instance using a CloudID.

To deploy a Kibana dashboard using BIUL:

1. On the sidebar menu, click **Settings > SIEM Connections**.
2. In the **SIEM Connections** list, select your Elasticsearch connection.
3. On the **Edit SIEM Connection** page, click to open the **Elasticsearch Connection Details**.
4. Click **Deploy Dashboard**.

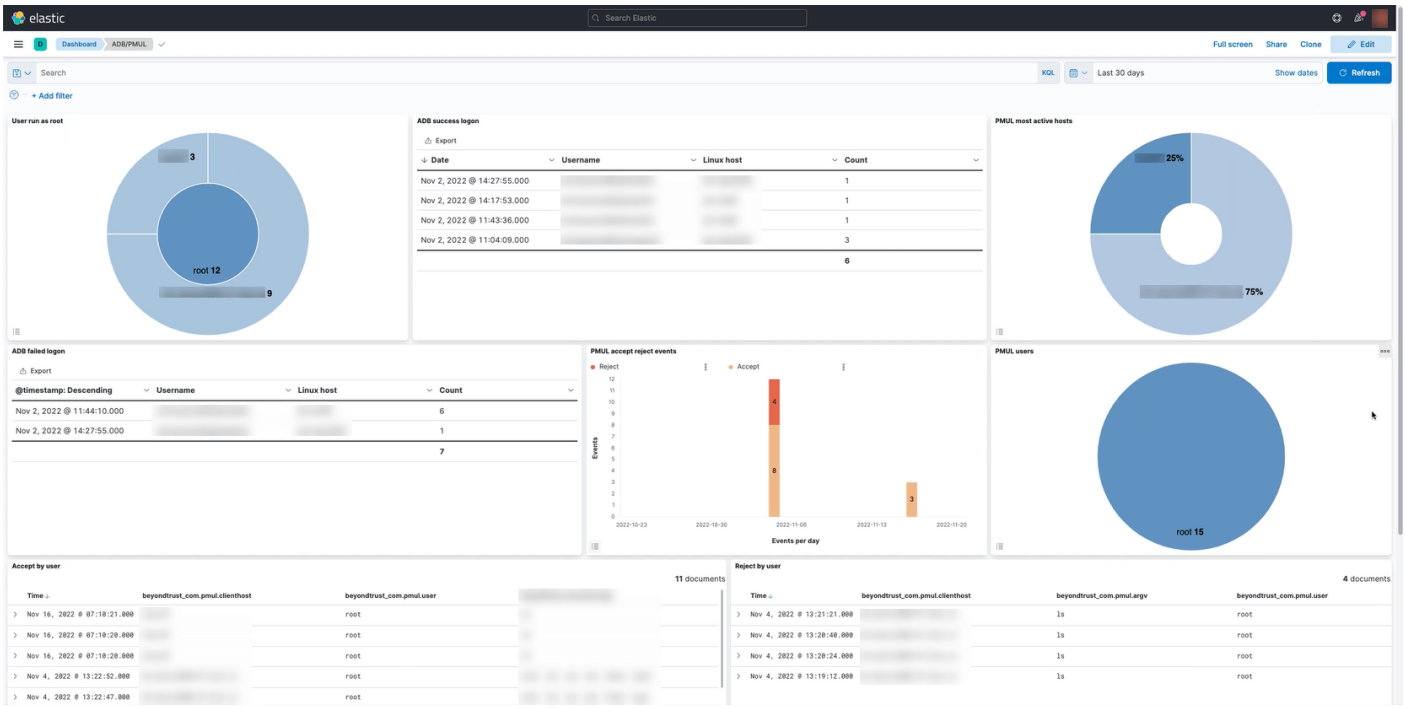


5. The **Kibana Dashboard URL** appears.



6. Click the link to access the Kibana dashboard.

> ***Note:*** *This is a prebuilt Kibana dashboard layout defined by BeyondTrust. The dashboard provides a few visualizations relevant to BeyondTrust products, including AD Bridge authentication events and PMUL policy events.*



Delete a SIEM Connection

To delete an existing SIEM connection:

1. On the sidebar menu, click **Settings > SIEM Connections**.
2. In the **SIEM Connections** list, select a connection.
3. On the **Edit SIEM Connection** page, at the far right, click **Delete Connection**.
4. To confirm the deletion, click **Delete**.

Add SMTP Server Connection

To provide local BeyondInsight for Unix & Linux (BIUL) users access to the **Reset Password** link on the BIUL logon page, add SMTP server details. Using the password reset feature requires a verified email address.

IMPORTANT!

The configured SMTP server must support encrypted sessions. The protocols to be supported by the SMTP Server are STARTTLS and TLS.

1. Select the **Settings** menu.
2. Click the **Integration** tile.
3. Enter the information for the mail server, including: server address, port, and user credentials.
4. (Optional). Click **Test Settings** to ensure there is a connection to the mail server.
5. Click **Save Settings**.

For more information on setting up a local account to use password reset, please see "Configure Settings and Manage Software" on page 52.

Manage Certificates

On the **Manage Certificates** page, you can:

- Add certificate authorities (CA) to the BeyondInsight for Unix & Linux (BIUL) trusted certificate pool
- Upload server and client certificates for remote connections
- Generate certificate signing requests

The CA and TLS certificates generated by BIUL are created during the application's lifecycle, using the system supplied cryptographically secure PRNG for entropy.

The CA is unique per installation.

IMPORTANT!

*The SSL certificate for the BIUL cannot be updated or deleted from the **Manage Certificates** page. For information on the SSL certificate configuration, see the BIUL Installation Guide, at https://www.beyondtrust.com/docs/privilege-management/console/beyondinsight-unix-linux/install/configure.htm.*

Add a Certificate Authority

An uploaded CA is added to the BIUL trusted certificate pool.

When BIUL connects to a remote service, a trusted CA in the BIUL database is added to the trusted certificate pool for that connection.

To add a CA:

1. Go to **Settings > Certificates**.
2. Click **Add Certificate > Upload a Certificate Authority**.
3. Click the upload arrow and navigate to the .PEM file location.
4. Click **Upload File**.

A CA can be removed when no longer required.

An uploaded CA is added to Solr during deployment or adoption actions for the Solr instance.

***Note:** As of version 23.1, Solr is deprecated. BeyondInsight for Unix & Linux no longer supports installing Solr, but features that use an existing Solr installation will continue to work.*

For more information, please see "Manage Solr" on page 31.

Upload Certificates

When deploying a Solr instance or assigning a log server, BIUL searches the host for a certificate with the same name (wildcards supported). If found, that certificate is used for the host. Otherwise, BIUL generates a certificate using the BIUL CA.

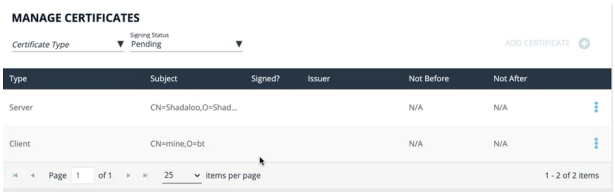
1. Go to **Settings > Certificates**.
2. Click **Add Certificate > Upload Existing Certificate**.
3. Select the host to copy the certificate to.
4. Select a certificate type.
5. Click the upload arrow and navigate to the certificate file location.
6. Click **Upload Files**.

Create a Certificate Signing Request

You can create a request to sign a certificate by a CA. After the certificate is signed, you can upload to the host.

To request a signed certifcate:

1. Go to **Settings > Certificates**.
2. Click **Add Certificate > Create Certificate Signing Requests**.
3. Fill out the form with details, including host, common name, organization, and organization email.
4. Select a certificate type: client or server.
5. Select a SAN type: DNS Name, IP address, or email address.
6. Click **Create**.
7. After the request is created, you can view the **Pending** status for the request.



8. At the far right of the certificate row, click the vertical ellipsis menu icon and select **Certificate Details**.
9. Click **Download as PEM**. After the certificate is signed, upload the certificate to complete the request.

Certificate Expiry

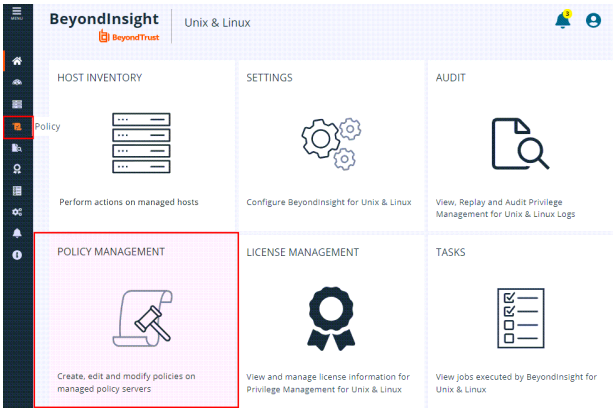
A warning icon indicates a certificate is expiring soon or is already expired.

Manage PMUL Policies

The **Policy** section allows you to manage creating, updating, and deleting Privilege Management for Unix and Linux(PMUL) policy types:

- Role-based policy
- Script-based policy
- File Integrity Monitoring (FIM) policy
- Privilege Management for Networks policy
- Sudo policy

To access the **Policy** page, from the **Home** page, click either the **Policy Management** tile or the **Policy** icon on the main menu on the left.



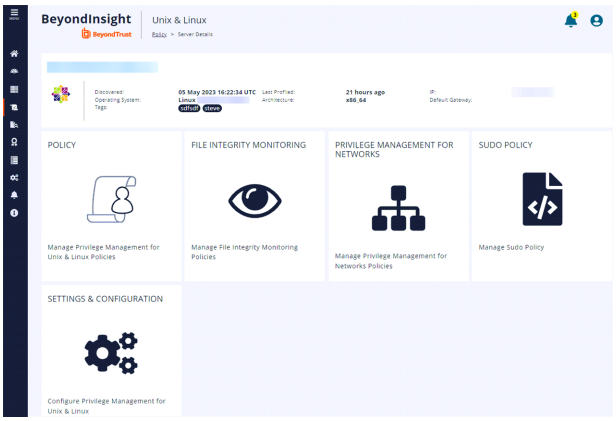
View Server Details

To locate a server and view the server details, you can filter hosts by **Hostname**, **IP Address**, and **Tags**. The policy server list is made of known policy servers with working REST connections. If a server is listed in gray, the server has an unsupported version of PMUL installed and must be upgraded to enable policy management.

To view server details:

1. Go to the **Policy** page.
2. In the **Hostname** list, select a server entry, and then at the far right, click the vertical ellipsis menu icon and select **Server Details**.

The server details are listed at the top, and you can click any of the tiles below to access a policy type to manage.



Manage a Policy

To manage policies, you must select the policy server on which the policy resides, and then choose the type of policy you wish to manage.

To select a policy server and policy to manage:

1. Go to the **Policy** page.
2. In the **Hostname** list, select a server entry, and then at the far right, click the vertical ellipsis menu icon and select which type of policy you want to manage.
3. You can also access the different policy types by clicking the tiles on the **Server Details** page.

Note: *If the host is configured as a client in the Registry Name Service, you must edit policy on the primary registry server.*

For more information on PMUL policies, please see the following:

- *Privilege Management for Unix and Linux Administration Guide, at https://www.beyondtrust.com/docs/privilege-management/unix-linux/admin/index.htm.*
- *Privilege Management for Unix and Linux Policy Language Guide, at https://www.beyondtrust.com/docs/privilege-management/unix-linux/policy-language/index.htm.*

Role-Based vs. Script-Based Policies

A PMUL policy server is either in *role-based* or *script-based* policy mode. A server in *role-based* mode only uses role-based policy and ignores all script policies. A server in *script-based* policy mode only uses script policies.

When accessing the **Policy** management page for a selected host, the landing page indicates the policy mode the host is using: *role-based* or *script-based*. To change the policy mode from one to the other, click the **Settings & Configuration** tile, and go to **Privilege Management for Unix and Linux Policy Settings**.

Manage Policy Server Mode

To manage a script policy on a server which is in role-based mode, you can switch the server mode. You can also switch from script-based policy mode to role-based mode.

Note: *Switching modes disables the previously configured mode and policies are no longer available to requesting clients. Policies are not removed when switching modes. This option can be changed at any time.*

To manage Policy Server mode:

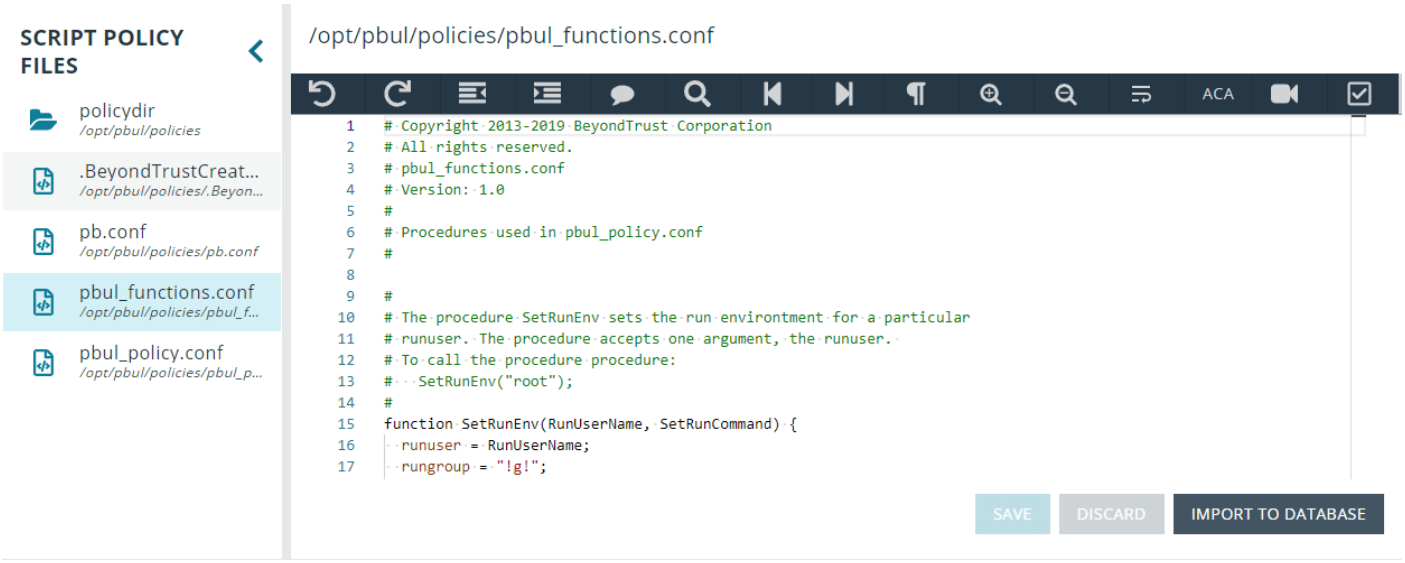
1. Go to the **Policy** page.
2. In the **Hostname** list, select a server entry, and then at the far right, click the vertical ellipsis menu icon and select **Configuration**.
3. Click the **Privilege Management for Unix & Linux Configuration** tab.
4. In the **Policy Mode** section, click **Enable Script Based Policy** or **Enable Role Based Policy** to enable the preferred policy mode.

BeyondInsight for Unix & Linux Code Editor

BeyondInsight for Unix & Linux (BIUL) provides an editor component with a number of features to assist with writing code.

- Syntax highlighting
- Line numbering
- Font size control
- Formatting
- Find and replace tools
- Soft wrapping
- Diff tool

Different toolbar options may be available based on the type of script in the editor. Most of the features are available in the toolbar, and keyboard shortcuts can also be used. The editor is used in the **Policy Management** section where applicable.



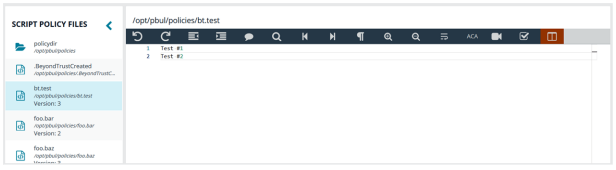
> ***Note:*** *Sudo does not support ACA or IOlog playback. The options are not visible in the toolbar when editing a Sudo policy.*

Using the Diff Tool

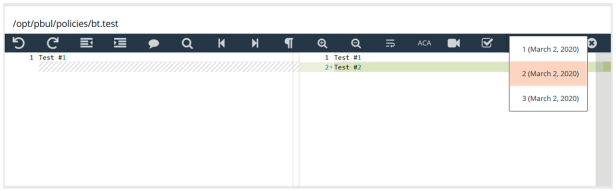
Use the diff tool to compare different versions of a policy. The policy must have change management turned on and versions of the policy must exist in the database.

To use the diff tool:

1. Select the policy, and then click the **Versions** toolbar button.



2. Select a version to compare. The differences are calculated and highlighted. Change the content in the current policy, if needed.



3. Click **Close Diff Editor**.

Version Control

Some policy types support version control. Each time a policy is changed, its version is incremented. The policy with the highest version is the one that is applied.

For policies that support version control, a **Versions** menu item is available to allow the user to choose a specific version to edit.

> ***Note:*** *Saving a policy makes it the most recent version, which makes it the active policy. Take this into consideration when saving older versions of the files.*

Change Management

BIUL allows users to enable Change Management in the console.

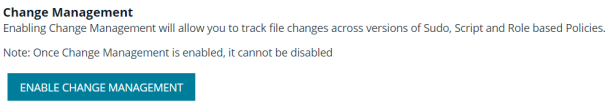
If Change Management is not enabled on the selected server, the option to enable change management is available in the console.

IMPORTANT!

Once Change Management is enabled, it cannot be disabled.

To enable Change Management:

1. Go to the **Policy** page.
2. In the **Hostname** list, select a server entry, and then at the far right, click the vertical ellipsis menu icon and select **Configuration**.
3. Click the **Privilege Management for Unix & Linux Configuration** tab.
4. Click the **Enable Change Management** button.

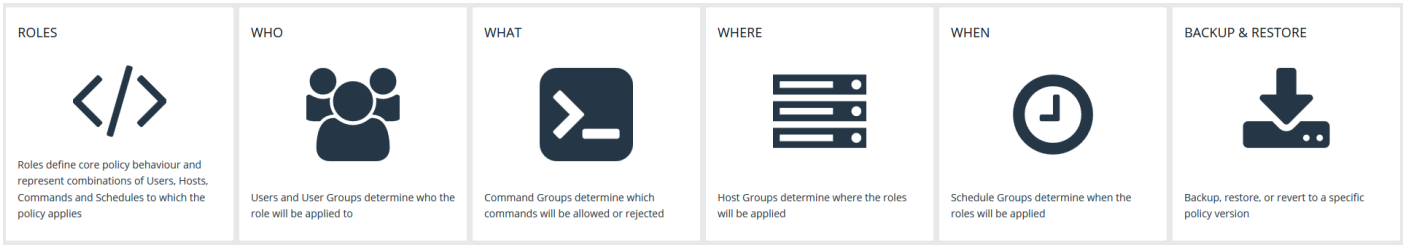


Manage PMUL Role-Based Policies

Note: *Role-based policy management is disabled on hosts configured to use script-based policy. For more information, please see* *"Role-Based vs. Script-Based Policies" on page 77*.

A Privilege Management for Unix and Linux (PMUL) role-based policy defines which users can use commands and when they can perform these actions on hosts. These role entities are then associated to a role. A **User**, **Host**, **Command**, and **Schedule** entity can be used in multiple roles, allowing the user to create a single definition and share it. The role-based policy editor is divided into sections allowing for the management of roles and each of the role entities.

Choose the PMUL role-based policy option and an appropriate policy server from the selection lists to load the **Role Based Policy** menu.



Note: *Fields may be disabled during policy configuration when the options are not available for the installed version of PMUL.*

Entitlement Reporting

PMUL hosts running 10.1 and later in **Role Based Policy Mode** can take advantage of Entitlement reporting to discover who is able to do what, where, and when.

Entitlement reporting can be enabled per policy or to all role-based policies.

A default value for reporting can be configured in **Settings**; if enabled, all new role-based policies defaults to entitlement reporting enabled, or vice versa if set to **false**. Additionally, this setting can be locked so the default value is both set and unchangeable per policy. This is for new policies only; disabling entitlement reporting does not change the values for existing policies.

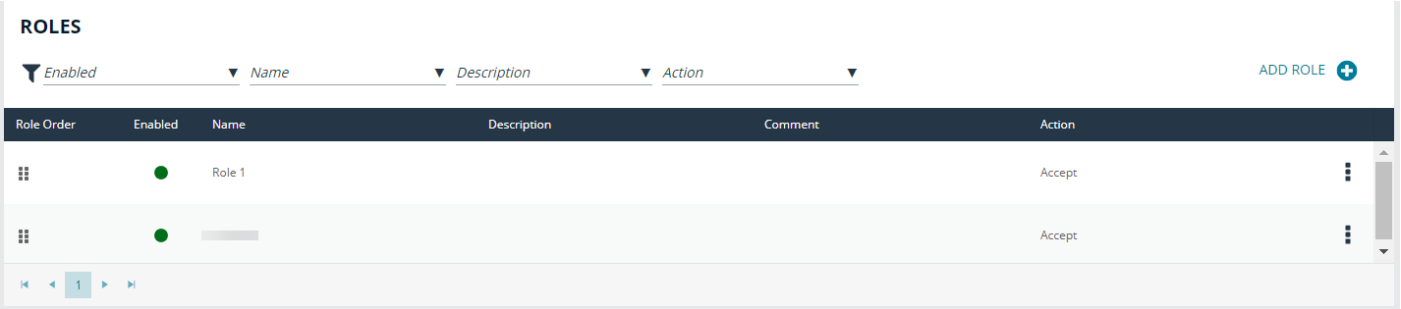
For more information, please see the following:

- *"Configure the PMUL Integration" on page 66*.
- *"View Entitlement Reports" on page 117*.

Role-Based Policy Roles

A list of available roles shows the existing entities. This list is searchable and can be filtered by **Enabled**, **Disabled**, or all options. Selecting the **Add Role** option creates a role.

- To edit an existing role, select an entry from the **Roles** list and click **Edit**.
- To delete an existing role, select an entry from the **Roles** list and click **Delete**.

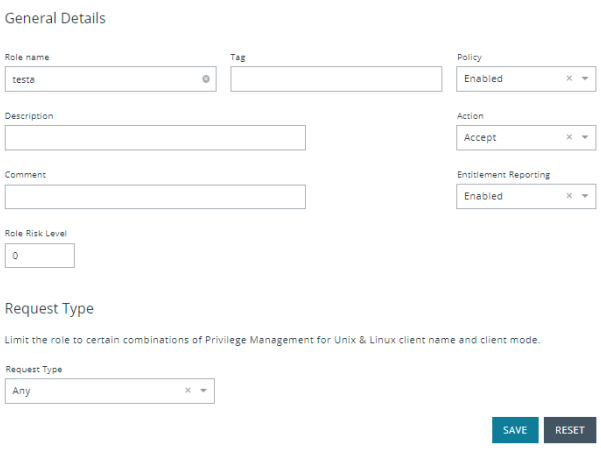


Role Ordering

The order in which role-based policies are applied can be set by ordering the roles in the list of available roles. Click and drag a role entry up or down in the **Roles** list to establish the priority order. Changes to role order is saved automatically.

General Details

The following options are available:



- **Role name:** This should be unique on the policy server.
- **Tag:** Add a tag to the role. Once added, tags function as a filter and can be used to sort through policy roles.
- **Description:** A brief description to identify the role.
- **Comment:** The admin can add a comment here. These are only visible to the admin.
- **Role Risk Level:** The perceived risk level of the policy.
- **Request Type:** Allows the administrator to specify which request types this policy will apply to. For example, a policy might apply to commands issued only by **pbrun** invocations. Use the dropdown to select the appropriate request type, or select **Any**. The default value is to allow any request type.
- **Policy Enabled:** Whether or not the role is active (default **Enabled**).
- **Action:** Whether this should trigger an accept or reject action (default **Accept**).
- **Entitlement Reporting:** Whether or not Entitlement Reporting is enabled (default **Disabled**).

Note: *If Change Management is enabled, an additional* ***Change requested by [loggedInUserName]*** *field is visible and requires you to enter a reason for the change. For more information, see* *"Change Management" on page 79*.

Click **Save**.

Assignments

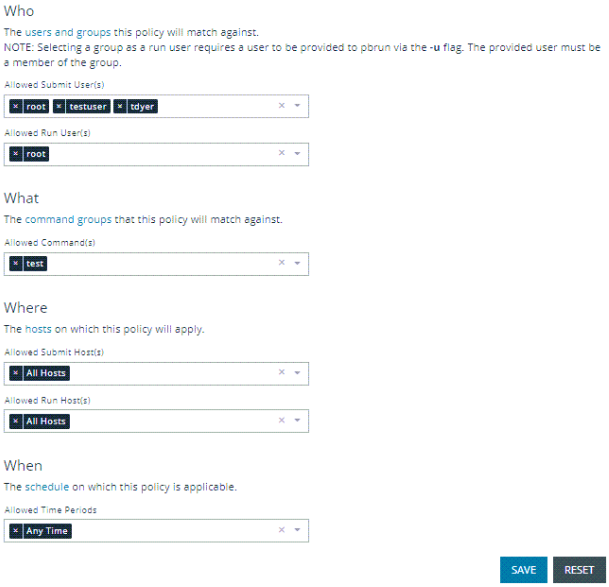
Assign allowed users, hosts, commands, and schedule to a role. Each role can have zero to many relationships with each entity type. This is managed using the lists matching the appropriate entity. The following configuration sections are available:

- **Who:** Defines which users the policy applies to. This item is divided into two user types:
  - **Submit Users**
  - **Run Users**

  These lists contain the user entities.

  Select **Use Default Group and Working Directory** to automatically populate the run users in a script block on the **Script Policy** page. Changing the block properties is not recommended.
- **What:** Defines which commands the policy applies to. This list contains the command entities.
- **Where:** Defines which hosts the policy applies to. This item is divided into two host types:
  - **Submit Hosts**
  - **Run Hosts**

  These lists contain the host entities.



- **When:** Defines which schedule the policy applies to. This list contains the schedule entities.

> ***Note:*** *If Change Management is enabled, an additional* ***Change requested by [loggedInUserName]*** *field is visible and requires you to enter a reason for the change. For more information, see* *"Change Management" on page 79**.*

Click **Save**.

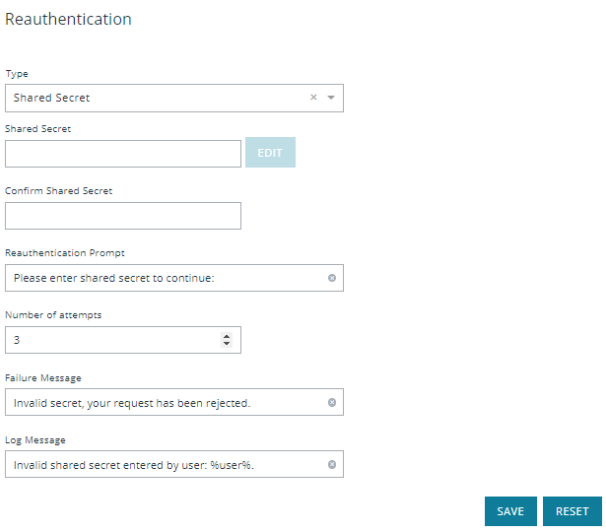
Reauthentication

If configured, this feature requires users to reauthenticate themselves when this policy is invoked. Only one reauthentication method can be configured per policy. Most reauthentication options allow for customization of messages and prompts to be displayed to the user as well as logs. Reauthentication can be enabled in a number of configurations:

- **None:** Reauthentication is not required.
- **Shared Secret:** Create a shared secret value. The user must provide it to reauthenticate.
- **Privilege Access Management (PAM):** A number of PAM modules can be selected, or a custom one can be provided. Additionally, most options allow the user to configure where the authentication will occur.

To configure the **Shared Secret** option:

1. From the **Type** dropdown, select **Shared Secret**.
2. Enter the **Shared Secret** and confirm it.
3. Enter a **Reauthentication Prompt** message, or use the default.
4. Enter the **Number of attempts** (retries) before reauthentication locks up.
5. Enter the **Failure Message** the user sees if reauthentication fails, or use the default.
6. Enter the **Log Message** that is recorded in the log when reauthentication fails, or use the default.

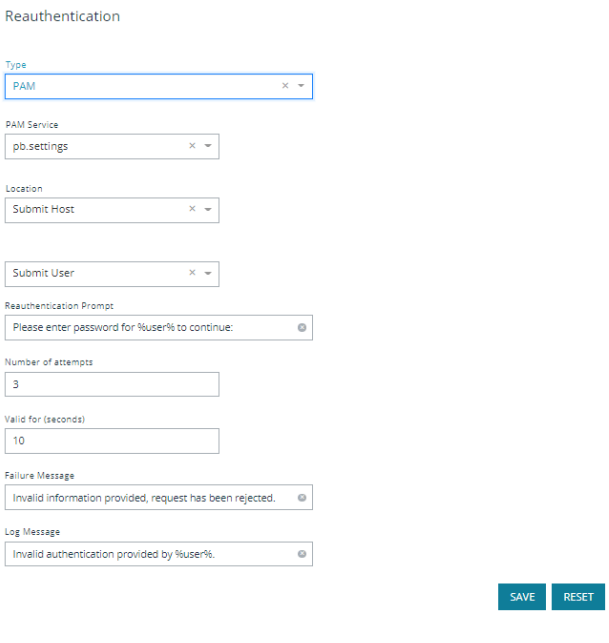


> ***Note:*** *If Change Management is enabled, an additional* ***Change requested by [loggedInUserName]*** *field is visible and requires you to enter a reason for the change. For more information, see* *"Change Management" on page 79*.

7. Click **Save**.

To configure the **PAM** option:

1. From the **Type** dropdown, select **PAM**.
2. Select the **PAM Service** to use for authentication.
3. Select the **Location** to use, where the authentication happens. If you select the **Run Host** option, you only need to complete steps 4 and 5, and then click **Save**.
4. Select the **User Type**, whether you are providing authentication for the user requesting the elevation, the user running the command, or some other user. If you select **Custom**, enter a custom user name.
5. Enter a **Reauthentication Prompt** message, or use the default.
6. Enter the **Number of attempts** (retries) before reauthentication locks up. That depends entirely on the policies imposed by the authentication services that PMUL accesses through PAM.
7. Enter the **Valid** time length, in seconds, or use the default. This is how long the reauthentication is cached for, before a login is required again.
8. Enter the **Failure Message** the user sees if reauthentication fails, or use the default.
9. Enter the **Log Message** that is recorded in the log when reauthentication fails, or use the default.



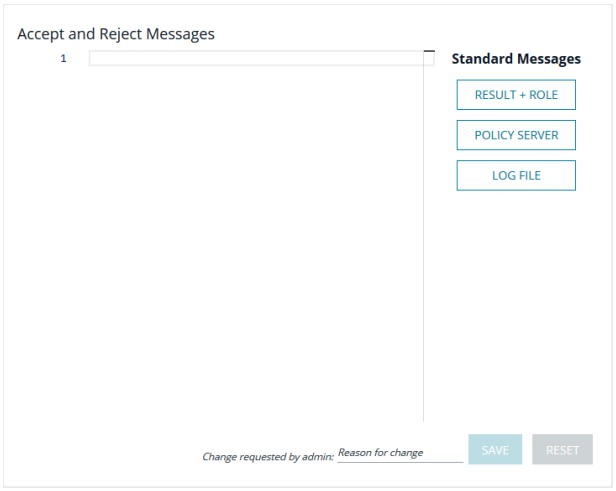
10. In the **Change requested by [loggedInUserName]** field, enter a reason for the assignment or change.

> ***Note:*** *If Change Management is enabled, an additional* ***Change requested by [loggedInUserName]*** *field is visible and requires you to enter a reason for the change. For more information, see* *"Change Management" on page 79*.

11. Click **Save**.

Messages

Enables the administrator to output a message to the user when this policy is processed. This field can interpolate variables to provide a custom, context specific message using the PMUL template syntax of **%<variable>%**. A few options are available using buttons to quickly insert the most popular options. Values can also be entered freely.

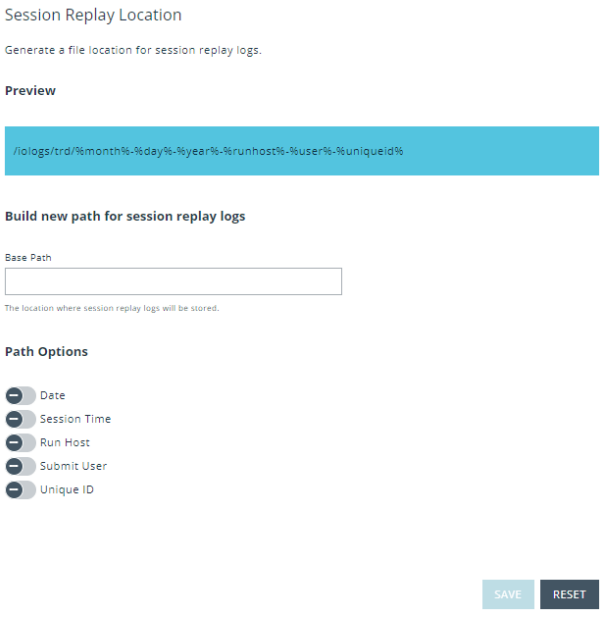


> ***Note:*** *If Change Management is enabled, an additional* ***Change requested by [loggedInUserName]*** *field is visible and requires you to enter a reason for the change. For more information, see* *"Change Management" on page 79*.

Click **Save**.

Session Replay

Generate a file location for session replay logs and configure **Path Options**.The **Session Replay Location** field allows for the use of variables in the file name. BIUL provides a template builder to assist with creating the path; select the build option, provide a path to save the file, and select the desired variable options. Values can also be entered freely.

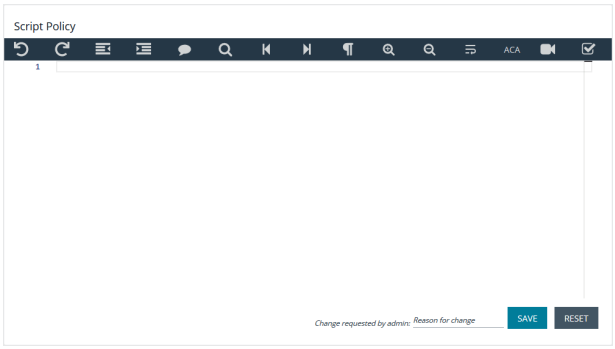


> ***Note:*** *If Change Management is enabled, an additional* ***Change requested by [loggedInUserName]*** *field is visible and requires you to enter a reason for the change. For more information, see* *"Change Management" on page 79*.

Click **Save**.

Script Policy

A configuration area to include a custom script. Script policy can be entered into the code editor to set the script content.

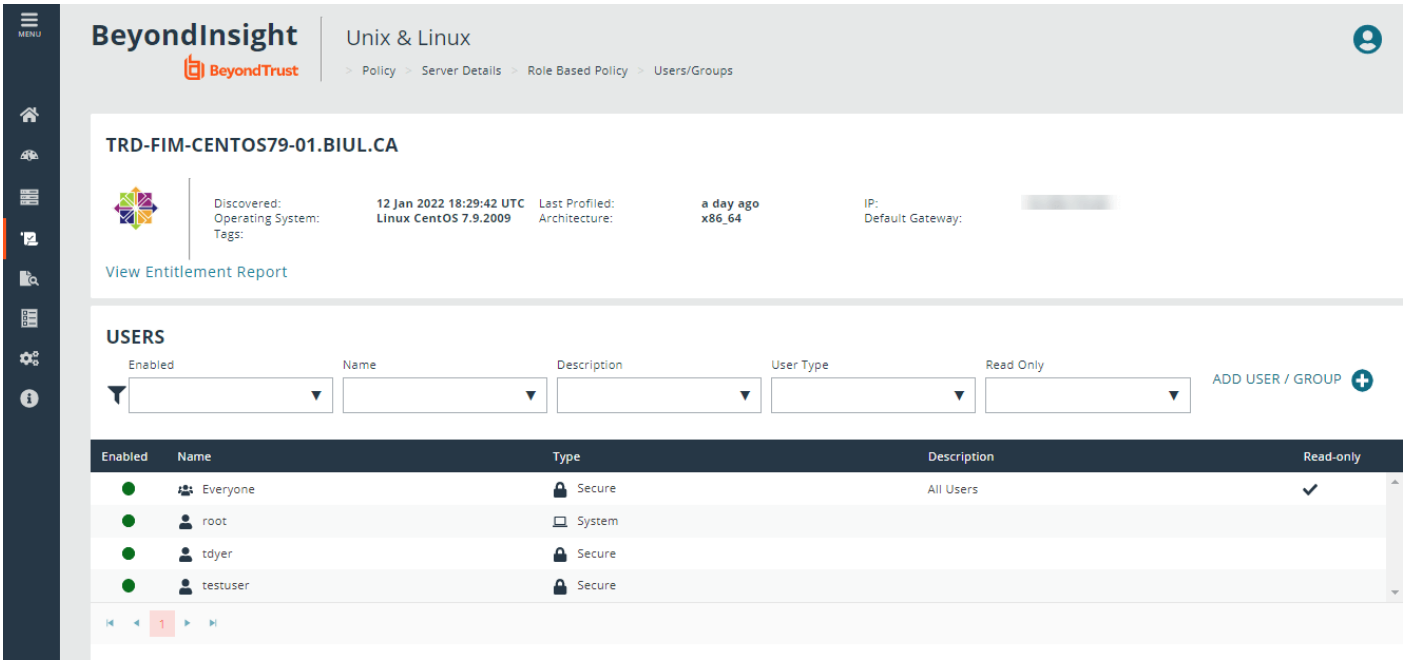


> ***Note:*** *If Change Management is enabled, an additional* ***Change requested by [loggedInUserName]*** *field is visible and requires you to enter a reason for the change. For more information, see* *"Change Management" on page 79**.*

Click **Save**.

Role-Based Policy Users and User Groups

Users and user groups determine *who* the role will be applied to.



> ***Note:*** *Role-based policy management is disabled on hosts configured to use script-based policy. For more information, please see* *"Role-Based vs. Script-Based Policies" on page 77**.*

User and User Group Types

There are three types of users and user groups:

- **Secure:** A user or group not associated with any system. The name and credential are added to the policy.
- **System:** The users and groups are retrieved from the selected host. System roles are only available with Privilege Management for Unix and Linux versions 9.4.4 or later.
- **Directory Service:** The users and groups are retrieved from Directory Service. Create a connection to Directory Service on the **Settings > Integration** page.

> ***Note:*** *If a wildcard character (*) is in the username, the user is treated as a group.*

Add a Secure User

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry, and then at the far right, click the ellipsis menu icon and select **Server Details**.
3. Click **Policy**.

4. Click **Who**.
5. Click **Add User / Group** and select **Secure User**.
6. Enter **Username**, **Description**, and choose to enable or disable the entry.
7. Click **Save Changes**.

Add a Secure Group

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry, and then at the far right, click the ellipsis menu icon and select **Server Details**.
3. Click **Policy**.
4. Click **Who**.
5. Click **Add User / Group** and select **Secure Group**.
6. Enter **Group name**, **Description**, and choose to make the group active or inactive.
7. In the **Group members** section, enter existing secure users in the **Username** field to add them to the group.
8. Click **Save Changes**.

Delete a Secure User or Group

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry, and then at the far right, click the ellipsis menu icon and select **Server Details**.
3. Click **Policy**.
4. Click **Who**.
5. Select a secure user or group entry from the **Users** list.
6. On the **Users and Groups** pane, click **Delete User** or **Delete Group** to delete the entry.

Add a System User or Group

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry, and then at the far right, click the ellipsis menu icon and select **Server Details**.
3. Click **Policy**.
4. Click **Who**.
5. Click **Add User / Group** and select **System User** or **System Group**. A list of available entries is displayed on the **Users and Groups** pane.
6. On the **Users and Groups** pane, check the box to import users or user groups. The imported users or user groups are displayed in the **Users** list.

Remove a System User or Group

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry, and then at the far right, click the ellipsis menu icon and select **Server Details**.
3. Click **Policy**.

4. Click **Who**.
5. Select a system user or group entry from the **Users** list.
6. On the **Users and Groups** pane, click **Remove User** or **Remove User Group** to remove the entry.

Add a Directory Service User or Group

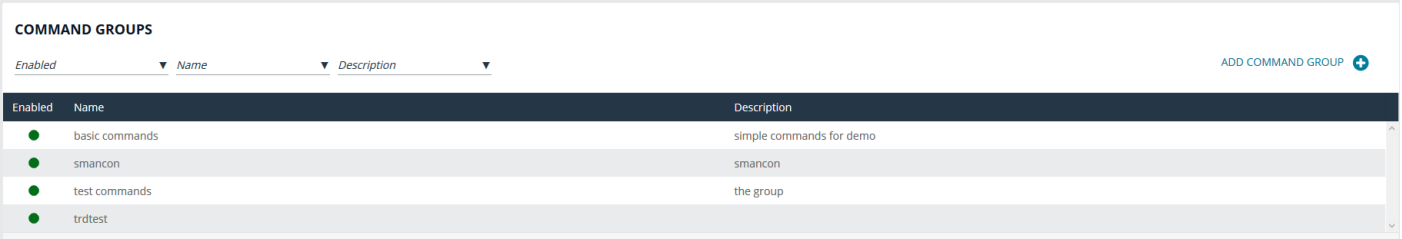
1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry, and then at the far right, click the ellipsis menu icon and select **Server Details**.
3. Click **Policy**.
4. Click **Who**.
5. Click **Add User / Group** and select **Directory Service Users and Groups**.
6. On the **Users and Groups** pane, select the **Search Type** to **Find Users** or **Find Groups**.
7. Enter the **Forest** and **Domain**.
8. Click **Browse** to filter by organizational unit (OU) and enter criteria in the **Search for** field.
9. Click **Search Directory Service**.
10. Check the box to import Directory Service users or user groups. The imported users or user groups are displayed in the **Users** list.

Remove a Directory Service User or Group

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry, and then at the far right, click the ellipsis menu icon and select **Server Details**.
3. Click **Policy**.
4. Click **Who**.
5. Select a Directory Service user or group entry from the **Users** list.
6. On the **Users and Groups** pane, click **Remove User** or **Remove Group** to remove the entry.

Role-Based Policy Command Groups

Command Groups determine *which commands* will be allowed or rejected.



> ***Note:*** *Role-based policy management is disabled on hosts configured to use script-based policy. For more information, please see "Role-Based vs. Script-Based Policies" on page 77.*

Add a Command Group

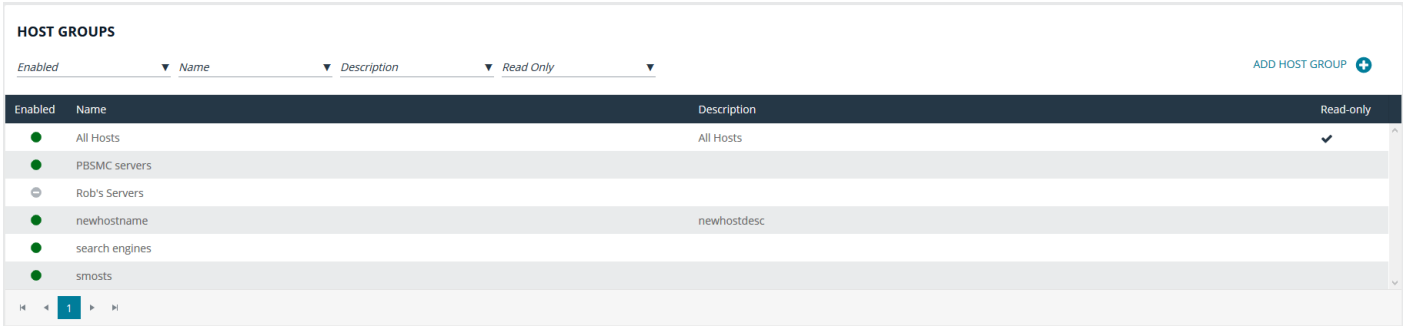
1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry, and then at the far right, click the ellipsis menu icon and select **Server Details**.
3. Click **Policy**.
4. Click **What**.
5. Click **Add Command Group**.
6. Enter **Command Group Name**, **Command Group Description**, and choose whether the Command Group is enabled or disabled.
7. Enter **Commands**. When adding a command to the list, you must enter **Command**, which is the command a Privilege Management for Unix and Linux user types. Optionally, you can enter **Executed**, which is executed in place of the **Command**.
8. Click **Save**.

Delete a Command Group

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry, and then at the far right, click the ellipsis menu icon and select **Server Details**.
3. Click **Policy**.
4. Click **What**.
5. Select an existing entry from the **Command Groups** list.
6. Click **Delete**.

Role-Based Policy Host Groups

Host Groups determine *where* the roles are applied.



> ***Note:*** *Role-based policy management is disabled on hosts configured to use script-based policy. For more information, please see "Role-Based vs. Script-Based Policies" on page 77.*

Add a Host Group

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry, and then at the far right, click the ellipsis menu icon and select **Server Details**.
3. Click **Policy**.
4. Click **Where**.
5. Click **Add Host Group**.
6. Enter **Host Group Name**, **Host Group Description**, and choose whether the Host Group is enabled or disabled.
7. Enter **Matching Hosts**.
8. Click **Save**.

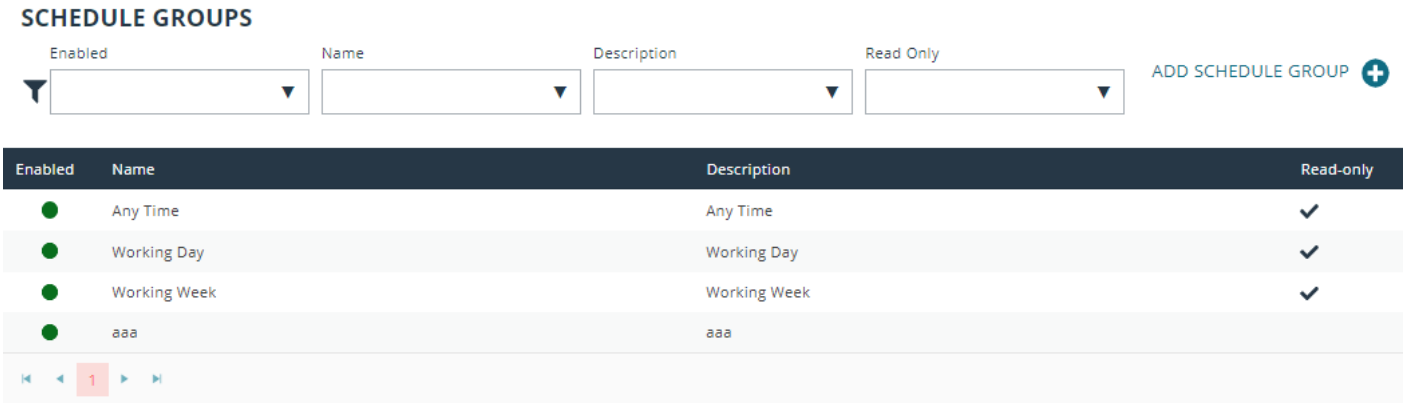
Delete a Host Group

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry, and then at the far right, click the ellipsis menu icon and select **Server Details**.
3. Click **Policy**.
4. Click **Where**.
5. Select an existing entry from the **Host Groups** list.
6. Click **Delete**.

Role-Based Policy Schedule Groups

Schedule Groups determine *when* roles are applied. When adding a schedule, there are two types of dates you can create in your schedule:

- **Fixed Schedule:** Choose a specific date range. If the end date is not specified, the range defaults to continuous. If the start date is not specified, the default starts immediately.
- **Recurring Schedule:** Choose active blocks of time per day. Choose a range of 15 minute blocks per each day for a full calendar week.



Note: *Role-based policy management is disabled on hosts configured to use script-based policy. For more information, please see "Role-Based vs. Script-Based Policies" on page 77.*

Add a Schedule Group

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry, and then at the far right, click the ellipsis menu icon and select **Server Details**.
3. Click **Policy**.
4. Click **When**.
5. Click **Add Schedule Group**.
6. Enter **Schedule Group Name**, **Schedule Group Description**, and choose whether the Schedule Group is enabled or disabled.
7. Configure schedules using **Recurring Schedule** and **Fixed Schedule** options.
8. Click **Save**.

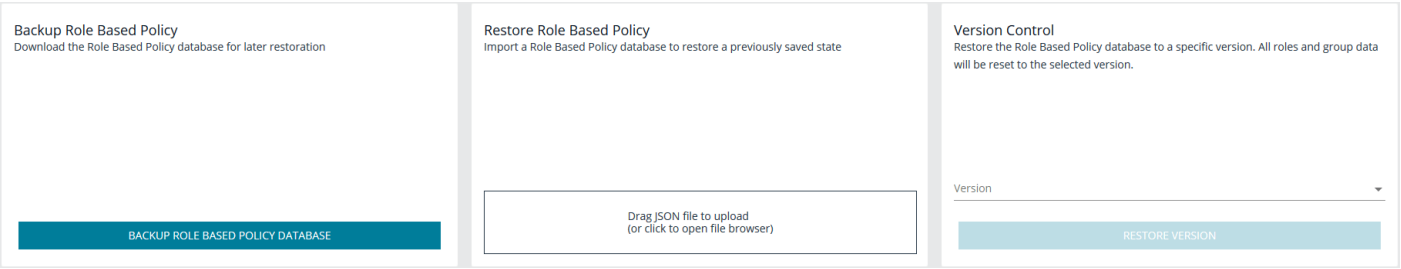
Delete a Schedule Group

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry, and then at the far right, click the ellipsis menu icon and select **Server Details**.
3. Click **Policy**.
4. Click **When**.
5. Select an existing entry from the **Schedule Groups** list.
6. Click **Delete**.

Role-Based Policy Backup and Restore

Role-based policy data can be managed in this section. Use the **Backup Role Based Policy** option to download a copy of the policy database on the selected policy server. Use the **Restore Role Based Policy** action to upload and set the current policy to the provided backup. **Version Control** can be used to restore the database to a particular version by selecting the desired version from the **Version** list and clicking **Restore Version**.

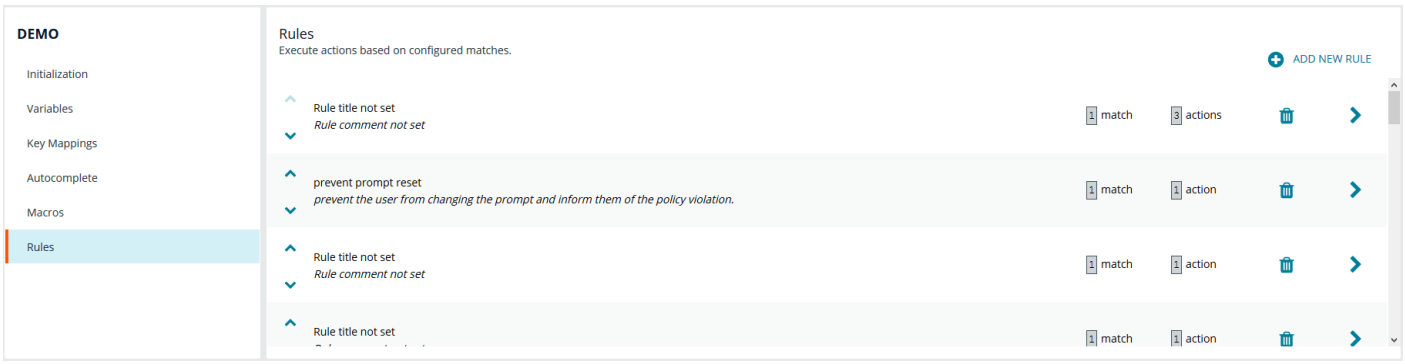
> ***Note:*** *Role-based policy management is disabled on hosts configured to use script-based policy. For more information, please see* *"Role-Based vs. Script-Based Policies" on page 77*.



Manage Privilege Management for Networks Policies

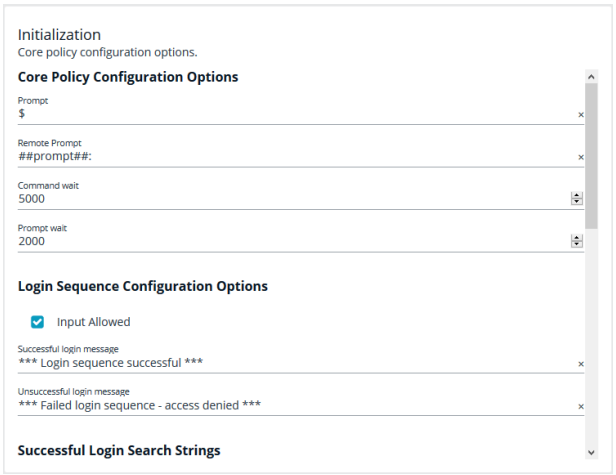
Privilege Management for Networks policy is managed from the **Policy Management > Server Details > Privilege Management for Networks** section. From here, you can add, delete, or clone a policy, as well as configure the settings for Privilege Management for Networks.

Privilege Management for Networks management is divided into sub-sections, which allow you to edit settings according to your specific parameters.



Initialization

Configure core policy options, including sections for login sequence and policy-wide defaults.



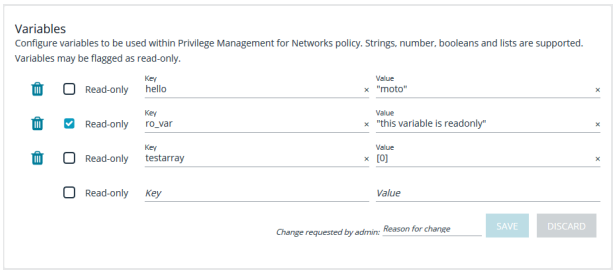
The following configuration options are available:

- **Core Policy Configuration Options:** Enter a name for the policy, a symbol for the prompt you want to display, and a remote prompt. The remote prompt is what the system waits to see before letting the user type. Enter the time (in seconds) for the command and prompt wait.
- **Login Sequence Configuration Options:** Select whether input is allowed or not, and then type in a message to display when the login sequence is successful or unsuccessful.
- **Successful Login Search Strings:** This is what the device outputs when a login is successful. For example, the search string output can be set to *last login*. In this scenario, when you log in to your machine, the last login message is displayed to indicate you have successfully authenticated.

- **Password Matching Search Strings:** These are values to look for, should the user be prompted to enter a password. The policy will read the output from the remote system, such as a router, and if the output matches one of these configured values, this means the system is asking for authentication.
- **Prerun Commands:** These are run before the policy is executed. For example, if the policy sets the value of prompt to **Prompt**, then you know you are ready for input when you receive the prompt message.

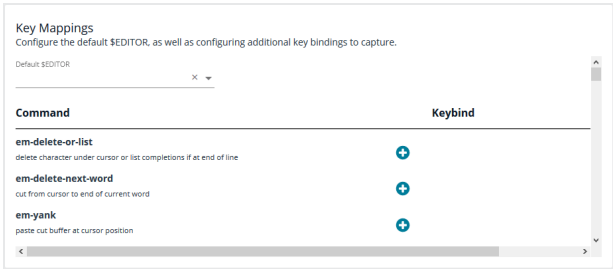
Variables

Variables must be defined within a policy. This section is used to configure variables, set defaults, and mark variables as read-only. Strings, numbers, booleans, and lists are supported. Variables may be flagged as read-only. When finished, click **Save**.



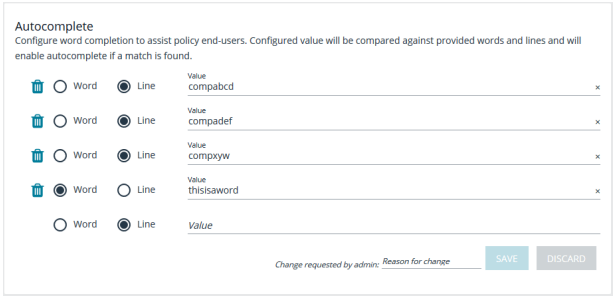
Key Mappings

This section enables configuration of keyboard input. To set a key mapping, use the **Default $Editor** dropdown to choose the policy's default editor type (**vi** or **emacs**), and then click the **+** option next to the keyboard action. A message displays, indicating the system is waiting for input. While BIUL is listening for keystrokes, input the key or key combination you want to set. Key bindings can be cleared by selecting the **X** next to the binding. When finished, click **Save**.



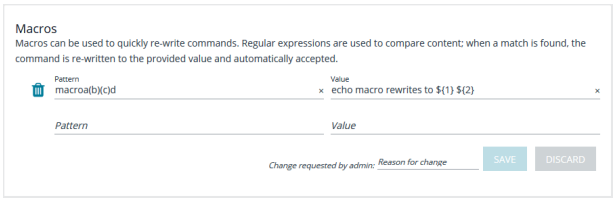
Autocomplete

In this section, you can configure word completion to assist policy end users. The configured value is compared against provided words and lines and enables autocomplete if a match is found. The user can then use the autocomplete key (**Tab**) to accept the matching value. When finished, click **Save**.



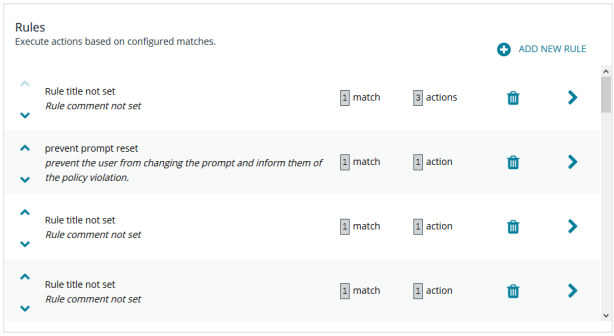
Macros

Macros can be used to quickly rewrite commands. Regular expressions are used to compare content. When a match is found, the command is re-written to the provided value and is automatically accepted. When finished, click **Save**.



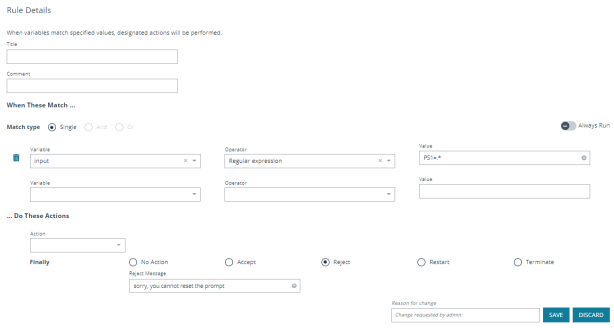
Rules

The core of Privilege Management for Networks is handled in this section. The **Rules** summary page allows you to create a new **Rule** or reorder them.



To add a new item, click **Add New Rule**. This brings up the **Rule Details** page. This is the same page that displays when you click on the chevron icon to edit an existing rule.

Within the editor one or more matches can be created where a match is a check of some sort. For example, variable equality or a regular expression result. More than one match can be joined together using either a logical *and* or logical *or*. If a match is found, the associated actions that are invoked can be configured using editor. Matches can have zero to many actions.



Add a Policy

To add a policy:

1. On the **Privilege Management for Networks** page, click **Create New Policy**.
2. Enter the **Policy name**.
3. In the **Change requested by [loggedInUserName]** field, enter a reason for the assignment or change.
4. Click **Create**.

Delete a Policy

On the **Privilege Management for Networks** page, click the trash bin icon on the policy you want to remove. Click **OK** to confirm.

Clone a Policy

You may want to clone a policy in order to make a backup, or use it as a template to create a new one. On the **Privilege Management for Networks** page, click the clone icon on an existing policy, enter a unique **Policy name**, and click **Clone**.

> ***Note:*** *Each policy requires a unique name. In order to clone a policy, you must give it a new name; otherwise, the* ***Clone*** *button does not activate.*

Configure Privilege Management for Networks

To configure Privilege Management for Networks, the path to a valid Password Safe runfile script and certificate must be provided, as well as a list of Password Safe servers that can provide credentials.

To configure Privilege Management for Networks:

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry, and then at the far right, click the vertical ellipsis menu icon and select **Server Details**.
3. On the **Server Details** page, select **Settings & Configuration > Privilege Management for Networks Configuration**.
4. Configure the following options:
    - **Password Safe Runfile**
    - **Certificate path**
    - **Password Safe Servers**
5. In the **Change requested by [loggedInUserName]** field, enter a reason for the assignment or change.
6. Click **Save**.

Manage Sudo Policies

Clients using Sudo Manager generate *events*, which are captured in the standard stream as PMUL events. These are therefore visible in the PMUL events grid, or, if enabled, the Elasticsearch instance that PMUL events are forwarded to.

Sudo policies are managed via direct REST calls to a selected policy server. The policy manager lists all known policies and enables creation, update, and deletion. BIUL integrates with the Sudo Manager change management system so that previous versions of a policy are available.

BIUL provides support for Sudo Manager for software deployment, policy management, alias management and assignment, and event auditing. You can assign multiple hosts to use a shared Sudo policy in the form of *Aliases*.

Create a Sudo Policy

To create a Sudo policy:

1. On the **Menu**, click **Policy**.
2. Using the filtering options (or from the list), select a server.
3. At the right of the server hostname row, click the vertical ellipsis menu icon, and then select **Sudo Policy**.
4. Click **Policy**.
5. On the **Sudo Policies** page, at the right, click **Create New Sudo Policy**.
6. On the **Create New Sudo Policy** panel, enter a **Hostname/Alias** and a **Filepath**.
7. Click **Create**.

Edit a Sudo Policy

To edit a Sudo policy:

1. On the **Menu**, click **Policy**.
2. Using the filtering options (or from the list), select a server.
3. At the right of the server hostname row, click the vertical ellipsis menu icon, and then select **Sudo Policy**.
4. Click **Policy**.
5. On the **Sudo Policies** page, from the dropdown list, select a **Sudo Alias**. The Sudo policies list appears.
6. In the list, click the policy **Name**. The policy code editor opens.
7. Edit the policy script, and then click **Save**.

For more information about using the code editor, see "BeyondInsight for Unix & Linux Code Editor" on page 78.

Delete a Sudo Policy

To delete a Sudo policy:

1. On the **Menu**, click **Policy**.
2. Using the filtering options (or from the list), select a server.
3. At the right of the server hostname row, click the vertical ellipsis menu icon, and then select **Sudo Policy**.

4. Click **Policy**.
5. On the **Sudo Policies** page, from the dropdown list, select a **Sudo Alias**. The Sudo policies list appears.
6. At the right of the Sudo policy that you want to delete, click the **Delete** icon.

Assign, Reassign, or Remove a Sudo Policy Aliases

Aliases are named when you create a Sudo policy and enter a **Hostname/Alias**. When at least one exists, you can assign it to one or more servers.

To manage the Sudo policy aliases:

1. On the **Menu**, click **Policy**.
2. Using the filtering options (or from the list), select a server.
3. At the right of the server hostname row, click the vertical ellipsis menu icon, and then select **Sudo Policy**.
4. Click **Alias**.
5. On the **Sudo Alias** page, use the filtering options and select one or more servers.
6. At the far right, click the **Actions** menu item, and then click **Sudo Policy Assignment**. The **Alias Assignment** panel opens.
7. From the dropdown list, select a **Sudo Alias** and click **Apply**.

To assign a *different* alias to a server with an existing one, follow the same procedure as above, and at the final step, select a different alias and click **Apply**.

To *remove* an Alias from a server with an existing one, follow the procedure above, and at the final step, click **Remove Assignment**.

Manage File Integrity Monitoring Policies

Create file integrity policy definitions to monitor for file changes. A policy definition includes a target that identifies the type of object that you want to monitor. Some of the target types include directory, device, symbolic link, script, and executable.

You can assign attributes to the target type. An attribute is an action you want to monitor and includes the following examples:

- File moves
- File ownership changes
- Date and time changes

A policy definition can contain more than one target.

Create a FIM Policy

To create a FIM policy:

1. On the **Home** page, click **Policy Management**.
2. Using the filtering options (or from the list), select a **server**.
3. At the right of the server hostname row, click the vertical ellipsis menu icon, and then select **FIM**.
4. Click **Policies**.
5. At the right, click **Create New FIM Policy**.
6. In the **Create New Policy** panel, and enter a name for the policy.
7. In the **Change requested by [loggedInUserName]** field, enter a reason for the change.
8. Click **Create**.

To create a FIM rule for the policy:

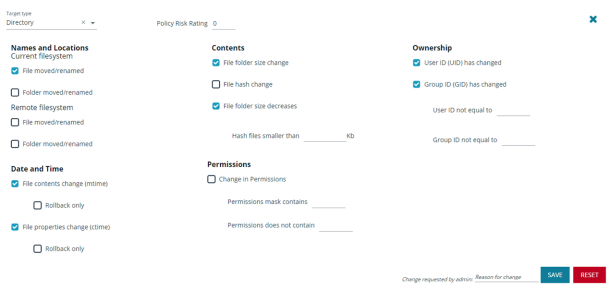
1. In the list, click the **Policy name** you have just created.
2. On the **Policy Details** page, at the right, click **Add New FIM Rule**.
3. In the **Create new FIM rule** panel, enter a **Rule name**.
4. In the **Change requested by [loggedInUserName]** field, enter a reason for the change.
5. Click **Create**.

> ***Note:*** *To delete a FIM Rule, click the appropriate FIM policy to navigate to* ***Policy Details > Rules****. Click the trash bin icon to delete the FIM Rule for the policy.*

To add a FIM target:

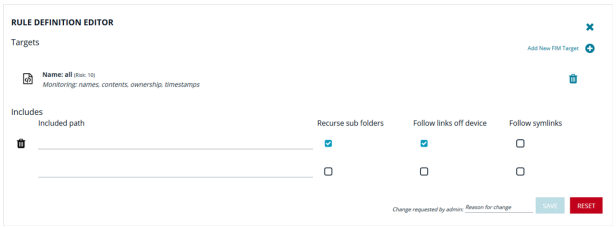
1. On the **Policy Details** page, click on the rule name you have just created.
2. On the **Rule Definition Editor** page, click **Add New FIM Target** to add a target to the definition.

3. Select a **Target type**, and then set attributes you want to monitor.

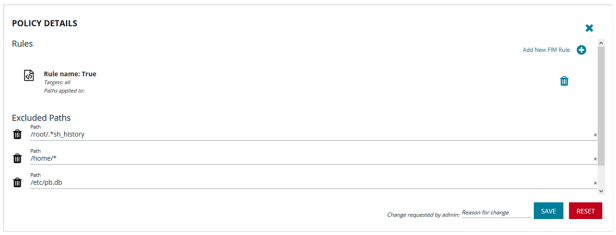


4. You can assign a policy risk rating. The accepted values are between **1** to **10**. A risk rating weighs the severity of the monitored actions configured for the targets.
5. In the **Change requested by [loggedInUserName]** field, enter a reason for the change.
6. Click **Save**.
7. On the **Policy Details** page, click on the rule you just created.
8. On the **Rule Definition Editor** page, enter **Included path** entries. Optionally, check the boxes:
    - **Recurse sub folders**
    - **Follow symlinks**
    - **Follow links off device**

    The policy applies to all files in the path.



9. In the **Change requested by [loggedInUserName]** field, enter a reason for the change.
10. Click **Save**.
11. In the **Exclude Paths** section, enter paths that you do not want to monitor.
12. In the **Change requested by [loggedInUserName]** field, enter a reason for the change.
13. Click **Save**.



Clone a FIM Policy

You may want to clone a policy in order to make a backup, or use it as a template to create a new one. On the **File Integrity Monitoring** page, select the clone icon on an existing policy, enter a unique **Policy name**, and click **Clone**.

> ***Note:*** *Each policy requires a unique name. In order to clone a policy, you must give it a new name; otherwise, the* ***Clone*** *button does not activate.*

Delete a FIM Policy

To delete a FIM policy:

1. Go to the **Policy Management** page.
2. Using the filtering options (or from the list), select a **server**.
3. At the right of the server hostname row, click the vertical ellipsis menu icon, and then select **FIM**.
4. Click **Policies**.
5. In the **FIM Policies** list, click the trash bin icon at the right of the policy you want to remove, and then click **Delete** to confirm.

File Integrity Monitoring Reports

File Integrity Monitoring (FIM) reports are available within the BeyondInsight for Unix & Linux (BIUL) console, in addition to being available from a command line. FIM reports are stored on policy servers and are available under the **Policy** section of the console.

To access FIM reports:

1. On the **Home** page, click **Policy Management**.
2. Using the filtering options (or from the list), select a **server**.
3. At the right of the server hostname row, click the vertical ellipsis menu icon, and then select **FIM**.
4. On the **FIM** page, click **Reports**.
5. On the **FIM Reports** page, do either of the following:
    - Use the filtering options to find a specific report
    - Find it directly in the list.
6. To view the details of the report, at the far right of the report summary line, click the **right-facing arrow** icon.
7. To view more specific information, on the **FIM Report Details** page, use the filtering options to narrow down your information search.
8. To view the file's **Policy Violation Details**, double-click on a file information row, and consult the details panel on the right.
9. When done with the details of that file, you can click another information row in the table and view its details, or click the **X** at the top-right of the panel to close it.

To go to a different report for the *same* server, on the breadcrumbs line at the top of the page, click **FIM Reporting**.

To view **FIM Reports** for a *different* server, on the left menu, click **Policy** and start again.

File Integrity Monitoring Clients

The **File Integrity Monitoring Clients** page lists all known endpoints that use a selected policy server. This information is obtained via the Profile action in the **Hosts Inventory** section, by reading each endpoints **pb.settings** file. This section allows the administrator to perform the actions detailed in this topic.

For more information on the Profile action, please see the following:

- *Profile Hosts, in the BIUL RNS Deployment Guide, at https://www.beyondtrust.com/docs/privilege-management/console/beyondinsight-unix-linux/rns-deployment/profile-hosts.htm.*
- *"Profile Servers in BIUL" on page 21*

Policy Assignment

By selecting *one or more* endpoints in the list, endpoints can be configured to use specific File Integrity Monitoring (FIM) policies, which themselves are managed in the **Policies** section. A list of available policies are then displayed. An endpoint can be assigned only one FIM policy at a time; changing the assigned policy removes any previous assignment.

To assign or change the currently assigned FIM policy:

1. On the **Home** page, click **Policy Management**.
2. Using the filtering options (or from the list), select a **server**.
3. At the right of the server hostname row, click the vertical ellipsis menu icon, and then select **FIM**.
4. On the **FIM** page, click **Clients**.
5. On the **FIM Clients** page, do either of the following:
    - Use the filtering options to find a specific client.
    - Find it directly in the list.
6. To select a FIM client, at the left of its hostname, check the box.

***Note:** If you want to make the same assignment or change in assignment for multiple clients, you can. To do so, select multiple clients at this step. Once you click **Apply** at step 10, the change applies to all clients selected.*

7. At the far right, click the **Actions** menu, and then select **FIM Policy Assignment**.
8. On the **Policy Assignment** panel, at the right of the **Policy name** field, click the dropdown arrow, and then select a policy to assign or reassign.
9. In the **Change requested by [loggedInUserName]** field, enter a reason for the assignment or change.

***Note:** The step above is only available if you have enabled **Change Management** on the FIM Policy server.*

10. Click **Apply**.
11. To close the **Policy Assignment** panel, click the **X** at the top-right of the panel.

FIM Reports Execution

By selecting *one or more* endpoints in the list, endpoints can execute the assigned FIM report. The time it takes to complete the task varies based on a number of factors, including hardware, complexity, and scope of the FIM policy. **FIM Report Execution** requires credentials to authenticate into the endpoint to execute the task.

> ***Tip:*** *You can also use default credentials that you set up under* ***Hosts > Credential Rules****. For more information, please see* *"Use Credential Rules" on page 44**.*

An option to update the base file state from which further reports would compare against, is available (the **Update the report database** option at Step 8, which can be toggled **ON** or **OFF**).

To run FIM reports:

1. On the **Home** page, click **Policy Management**.
2. Using the filtering options (or from the list), select a **server**.
3. At the right of the server hostname row, click the vertical ellipsis menu icon, and then select **FIM**.
4. On the **FIM** page, click **Clients**.
5. On the **FIM Clients** page, do either of the following:
    - Use the filtering options to find a specific client.
    - Find it directly in the list.
6. To select a FIM client, at the left of its hostname, check the box.

> ***Note:*** *If you want to run a FIM report for multiple clients using the same credentials, you can. To do so, select multiple clients at this step. Once you click* ***Apply*** *at step 13, the reports are run for all clients selected.*

7. At the far right, click the **Actions** menu, and then select **FIM Reports Execution**.
8. On the **Run FIM Reports** panel, if you want to update the report database, click the **Update the report database** toggle to **ON**. Turning it on changes the baseline to the results of the report that you are about to run. As a result, any future report will be reported in terms of a *deviation* or *difference* from this one.

> ***Note:*** *Steps 9-11 are optional fields, if you have defined Credential Rules for the hosts selected. Steps 10 and 11 are also optional, based on the* ***permissions of the user*** *selected at Step 9, and the* ***strategy*** *selected at Step 10.*

9. At the right of the **Login Credential** field, click the dropdown arrow and select a credential.
10. At the right of the **Delegation Strategy** field, click the dropdown arrow and select a strategy.
11. Depending on the option you select, you might need to enter a delegated credential. If so, at the far right of the **Delegated Credential** field, click the dropdown arrow and select a delegated credential.
12. In the **Change requested by [loggedInUserName]** field, enter a reason for the change.
13. Click **Apply**.
14. To close the **Policy Assignment** panel, click the **X** at the top-right of the panel.

> ***Note:*** *You can view the current status of the task in the* ***Tasks*** *section.*

Manage PMUL Script-Based Policies

> ***Note:*** *Script-based policy management will be disabled on hosts configured to use role-based policy. For more information, please see* *"Role-Based vs. Script-Based Policies" on page 77*.

To manage script-based policies:

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry, and then at the far right, click the vertical ellipsis menu icon and select **PMUL Policy**.
3. Select an existing script file to open it in the editor. Alternatively, click **Create New Script** and provide a **Filename** to create a script-based policy.

4. After you edit the script, select the **Validate** button from the toolbar. This will verify script syntax is correct. If an error is found, a notification displays in red stating the file syntax is invalid.

> ***Note:*** *When **Validate** is selected, only the syntax is verified. This does not verify the policy definition or included policies.*

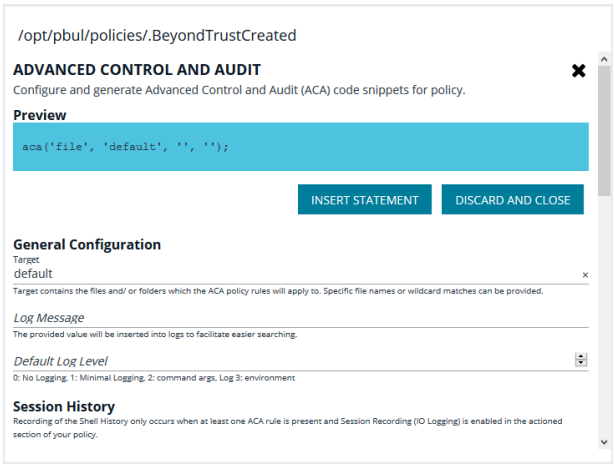
> ***Note:*** *Script-based policies can reside in either the file system under the folder defined as the **policydir** in Privilege Management for Unix and Linux settings or as objects in the change management database. Files that are in the database support version control. Files that are not in the database can be added by choosing the **Import to Database** option under the **Script Editor**.*

The Script Policy editor uses the code editor to assist the user managing the policy. **Discard** will revert the document to its original state. **Save** will write the file changes to either the file system or the database.

Advanced Control and Audit

The Advanced Control and Audit (ACA) editor allows users to configure an ACA statement. It is available on the code editor toolbar.

1. Select the **ACA** button in the script editor. This will open the ACA editor.
2. Define the following:
   - **Target:** The target contains the files and folders the ACA policy rules will apply to.
   - **Log Message:** The provided value will be inserted into logs to facilitate easier searching.
   - **Default Log Level:** Assign a number for the log level to use as a default.
   - **Session History:** If either **Audit command History** or **Continue On Error** are enabled, **Enable Session History** is added to the ACA statement.



- **File System Operations:** Check the box for the file system operation you want to audit. Selecting an operation allows you to set whether the operation is allowed or blocked. Additionally, a log level can be configured for an operation. System operations that are not assigned a log level are automatically assigned the default log level.

Note: *File operations that are not selected are not audited.*

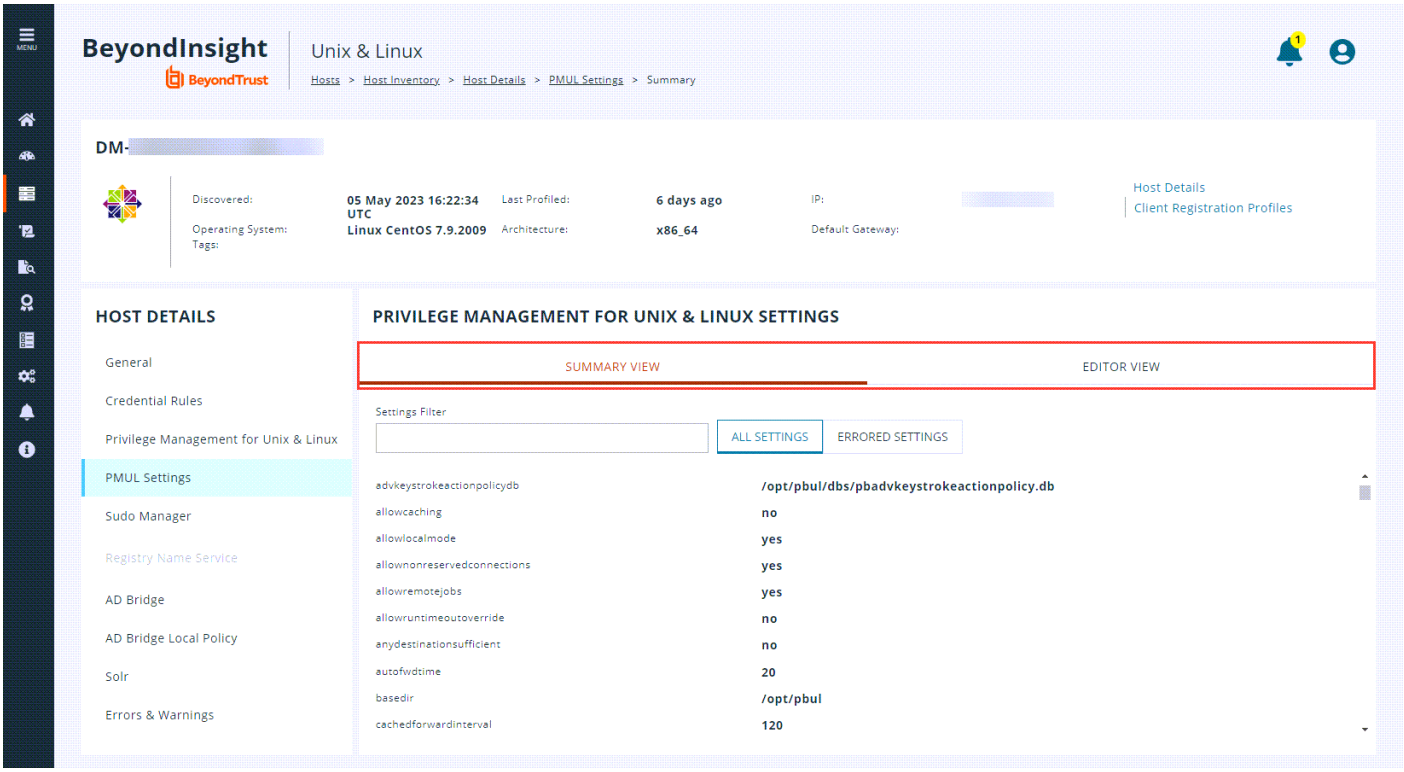
After configuring your ACA policy, click the **Insert Statement** button under the ACA policy preview to add the statement to the policy.

For more information on ACA, please see the Privilege Management for Unix and Linux Policy Language Guide, at https://www.beyondtrust.com/docs/privilege-management/unix-linux/policy-language/index.htm.

View PMUL Settings

1. Go to the **Hosts > Host Inventory** page, select a server entry, and then at the far right, click the ellipsis menu icon and select **View Host Details**.
2. On the **Host Details** panel, select **PMUL Settings**. The **Privilege Management for Unix and Linux Settings** pane is displayed.

The **PMUL Settings** details include **Summary View** (default) and **Editor View** options.



In both views, use the **Settings Filter** and options to quickly access the setting you are looking for. The default uses the **All Settings** option. Use the **Errored Settings** option to show only those settings whose values are not valid, and need to be resolved.

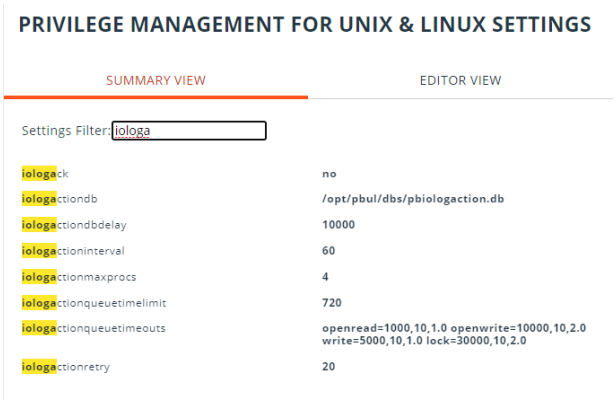
IMPORTANT!

Starting with the BIUL 23.1 release, you can correct and save the invalid (errored) values in the editor, as long as you correct all of them. If you are using a previous version, you need to edit the settings file directly on the PMUL host.

Use the Summary View

The **Summary View** is the default view for the **PMUL Settings** page, displaying the current parameters for all settings. Use the **Settings Filter** to shorten the list of settings to view.

When you need to update settings, use the **Editor View**.

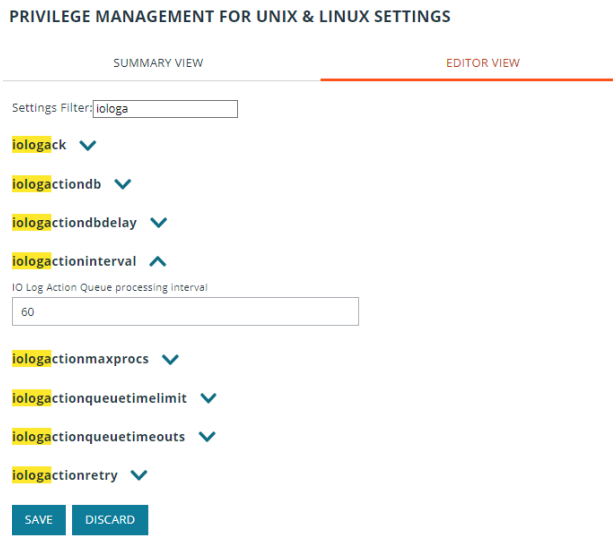


Use the Editor View

On the **Host Details > PMUL Settings** page, click the **Editor View** tab. Use the **Settings Filter** to shorten the list of settings to view.

To change the parameter for a setting:

1. To the right of the setting, click the down arrow to open the parameter field.
2. Enter the new parameter.
3. Click **Save**.



AD Bridge Local Policy Editor

The **AD Bridge Local Policy** section lists the settings and values and provides the ability to edit them.

> ***Note:*** *A credential is required to view the AD Bridge local policy settings. If a credential rule matching the host exists, that credential is used. If no credential rule exists, one can be created on the* ***AD Bridge Local Policy*** *page or by going to* ***Hosts > Credential Rules > Host Rules*** *and creating one.*

To edit the AD Bridge local policy settings for a host:

1. Go to the **Hosts > Host Inventory** page, select a server entry, and then at the far right, click the ellipsis menu icon and select **View Host Details**.
2. On the **Host Details** panel, select **AD Bridge Local Policy**. The **AD Bridge Local Policy** pane is displayed.

> ***Note:*** *This option is only available if the host has AD Bridge installed.*

3. Use the **Local Policies Filter** to filter settings by keyword. This filters both on the setting name and the setting description.
4. You can change and save multiple settings at once.
5. Click **Save**.

> ***Note:*** *Settings are loaded and saved over SSH, so there might be a delay to perform those operations.*

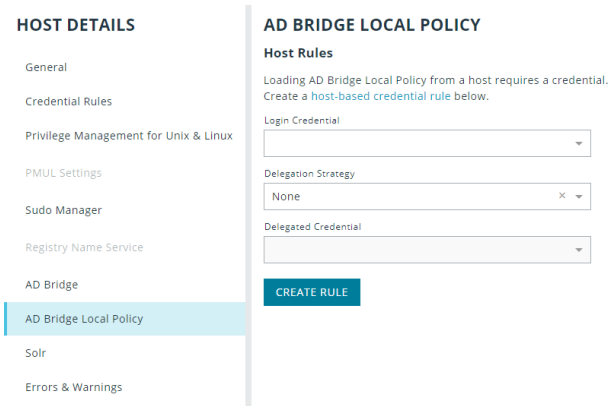
> *For more information on setting up a credential rule, see "Use Credential Rules" on page 44.*

Create a Credential Rule from the AD Bridge Local Policy Pane

When you access the **AD Bridge Local Policy** pane, if no credential rule exists for that host, you are presented with the **Host Rules** option, to immediately create a host-based credential rule.

To create a host-based credential rule:

1. Select the **Login Credential**.
2. (Optional). Select a **Delegation Strategy**.
3. If needed, select the **Delegated Credential**.
4. Click **Create Rule**.



Audit Activity Using BIUL

From the **Audit** page, you can access:

- **Unified Search:** Search for Privilege Management for Unix and Linux(PMUL), Active Directory Bridge (AD Bridge), and BeyondInsight for Unix & Linux (BIUL) events
- **PMUL Events:** View and download PMUL event logs
- **Console Audit:** View activity within the PMUL console
- **Session Replay:** View, replay, and audit PMUL session replays

Note:
- *As of PMUL version 10.3, event log information is retrieved from databases. Previous versions of PMUL support log files.*
- *A minimum version of PMUL 10.0 is required to view log contents. In earlier versions, the log must be downloaded to view.*

Perform a Unified Search

The unified search gathers log files from PMUL, Active Directory Bridge (AD Bridge), and BIUL. You can then search from a single line for PMUL, AD Bridge, and BIUL events, simultaneously.

IMPORTANT!

Currently, Elasticsearch is the only supported SIEM. This section will only be available if there is a configured and working connection to Elasticsearch.

To perform a search:

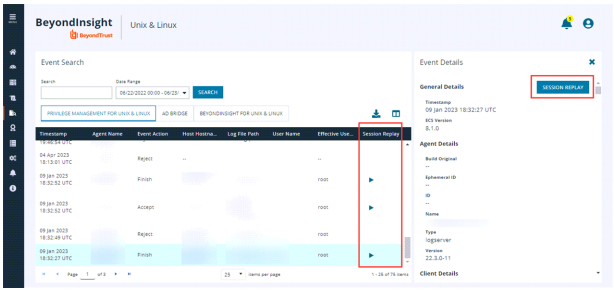
1. From the sidebar menu, select **Audit > Unified Search**.
2. Enter a search query to display the list of events. Search options include:
    - **Fuzzy / partials matches:** Default. Searching for *tree*, for example, returns results with *tree* and *pinetree*.
    - **Exact matches:** Use double quotes. Searching for "*sudo*", for example, and results only contain *sudo*.
    - **Logical AND:** Results must have both values, as in *sudo* AND *emacs*.
    - **Logical OR:** Results may contain either value, as in *sudo* OR *emacs*.
    - **Logical NOT:** Results will exclude value, as in *sudo* NOT *visudo*.
    - **Operator precedence:** Using brackets, as in *(sudo AND emacs)* or *(sudo AND vi)*.
    - **Date and time options:** Use these to set ranges, including some defaults, and the ability to set *begin* and *end* times.

Note: *When writing your query, you do not need to capitalize the logical operators (and, or, not).*

3. Click **Search**.

> ***Tip:*** *You can also just click* ***Search****, without entering any criteria. Unified search has default criteria that return all available events.*

4. To view the results, click the **Privilege Management for Unix and Linux**, **AD Bridge**, or **BeyondInsight for Unix & Linux** button. Click to toggle a selection *on* or *off*. The result *count* appears at the bottom right of the grid (as number of **items**). At the bottom of the grid, you can also find the *page count*, along with the page navigation icons.
5. For full event details, click on a row. The **Event Details** panel displays on the right.



> ***Tip:*** *When you choose which event search columns to display in the grid, select the* ***Session Replay*** *option (see below). This way, when looking at the events list, you see an icon in the column that indicates that a recorded session exists. When you open the* ***Event Details*** *panel, you see the* ***Session Replay*** *button.*

Replay Sessions from the Events Details Panel

Events that are associated with IO Logs provide links to the Session Replay player. To play the file, in the **Events Details** panel, click the **Session Replay** button. Optionally, you can enter a **Comment** and set the **Audit Status**, and then click **Save**.

> *For more information, see "Replay Sessions in BIUL" on page 115.*

Choose Event Search Columns to Display

You can choose which columns to display in the grid.

To select which columns to display, at the top-right of the grid, click the **Choose Columns to Display** icon and select one or more columns to display.

The columns appear from left to right in the grid, in the order that you select them.

Download the Results Data

You can download the results data as a JSON or CSV file. To download a results file:

1. After you perform a search, click the **Privilege Management for Unix and Linux**, **AD Bridge**, or **BeyondInsight for Unix & Linux** results button. Click to toggle a selection *on* or *off*.
2. At the right, click the **Download** icon, and then select **JSON File** or **CSV File**. The file downloads to your **Download** folder.

View PMUL Events

1. From the sidebar menu, select **Audit > PMUL Events**.
2. Find the host name in the list. Use the **Hostname**, **IP Address**, and **Tags** filters to refine the list of results displayed.

3. At the far right of the server entry row, click the arrow.
4. On the **Event Log** page, click the **Event Source** dropdown menu and select the log you want to view.
5. For full event details, click on a row. The **Event Details** panel is displayed on the right. Use the **Filter event keys** field to refine the list of results displayed.
6. To close the **Event Details** panel, click the **X** icon.

View Console Audit Activities

You can view user session information, such as user name, user ID, timestamp, user roles, and request URL.

1. From the sidebar menu, select **Audit > Console Audit**.
2. On the **Console Audit** page, use the filters to refine the list of user sessions displayed.
3. At the far right of the session row, click the arrow.
4. On the **Session Details** page, view more information, such as user name, user roles, HTTP method, and URL. Use the filters at the top of the columns to refine the list of results displayed.
5. For full event details, click on a row. The **Request Details** panel is displayed on the right.
6. To close the **Request Details** panel, click the **X** icon.

Replay Sessions in BIUL

Using session replay, you can view and replay I/O logs.

Enable Session Recording in Script Policy Mode

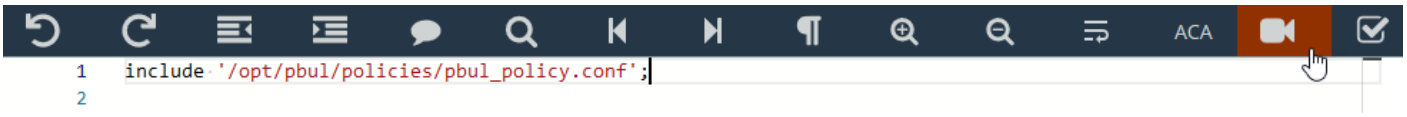
> ***Note:*** *As of version 23.1, Solr is deprecated. BeyondInsight for Unix & Linux no longer supports installing Solr, but features that use an existing Solr installation will continue to work.*

IMPORTANT!

To turn on session recording, Solr must have been installed using BeyondInsight for Unix & Linux and log servers must have been assigned to a Solr server. For more information, please see "Manage Solr" on page 31.

To turn on session recording in script-based policy mode:

1. From the sidebar menu, select **Policy**.
2. In the **Hostname** list, select a server entry, and then at the far right, click the ellipsis menu icon and select **PMUL Policy**.
3. Select a script policy file to edit. The file is displayed in an editor.
4. Click the **Session Replay Path** button from the toolbar.
5. Enter a **Base Path** for the log file.
6. (Optional). In the **Filename Options** area, use the variables to build a file path and name for the session to be written to. Select from the suggested variables to add unique properties to the path or file name.
7. (Optional). In the **Session Replay Options** area, use the variables to generate a command history list in the replay viewer. Select from the following: **Include Command History**, **Display Warnings**, and **Limit Size**. If you create an Advanced Control and Audit (ACA) statement, you can add command history to the statement.
8. Click the **Insert Location** option to add the logs to the script policy file.
9. Click **Save** in the editor to save the script policy file.



> *For more information about ACA statements, please see "Advanced Control and Audit" on page 107.*

Enable Session Recording in Role-Based Policy Mode

> ***Note:*** *As of version 23.1, Solr is deprecated. BeyondInsight for Unix & Linux no longer supports installing Solr, but features that use an existing Solr installation will continue to work.*

IMPORTANT!

To turn on session recording, Solr must have been installed using BeyondInsight for Unix & Linux and log servers must have been assigned to a Solr server. For more information, please see "Manage Solr" on page 31.

To turn on session recording in role-based policy mode:

1. From the sidebar menu, select **Policy**.
2. In the **Hostname** list, select a server entry, and then at the far right, click the vertical ellipsis menu icon and select **PMUL Policy**.
3. Click the **Roles** tile.
4. On the **Roles** page, select a role entry, then at the far right, click the vertical ellipsis menu icon and select **Edit Role**.
5. On the **Edit Role** page, select **Session Replay**.
6. Enter a **Base Path** for the log file.
7. (Optional). In the **Path Options** area, use the variables to build a file path and name for the session to be written to. Select from the suggested variables to add unique properties to the path or file name.
8. Click **Save**.

Play a Recorded Session

To play an I/O log session:

1. From the sidebar menu, select **Audit > Session Replay**.
2. Find the host name in the list. Use the **Hostname**, **IP Address**, and **Tags** filters to refine the list of results displayed.
3. At the far right of the server entry row, click the arrow.
4. On the **Sessions** page, logs indexed by BIUL are displayed. As necessary, use filters and **Search** to locate a log. Click on an entry to display activity and user feedback.
5. Select the **Playback** icon to start the log player.
6. On the **Session Replay** page, select one of the following modes:
    - **File:** File displays the contents of an I/O log immediately.
    - **Playback:** Replays the I/O log in real time as the events occurred, so an administrator can view what the user entered.
7. On the **Session Replay** page, you can play, pause, stop, set the speed of the session, zoom in and out, and use full screen.
8. If ACA policy is enabled and configured, a *command history* is displayed, allowing you to navigate to specific events in an I/O log. The command history indicates if the ACA status is allowed or rejected.
9. Optionally, enter a **Comment** and **Audit Status** on a log. For example, you can enter a comment or set a flag to provide warnings of a problem or to approve the content. Click **Save**.

View Entitlement Reports

PMUL hosts running version 10.1 and later in **Role-based policy mode** can take advantage of entitlement reports to discover who is able to do what, where, and when.

Turn on Entitlement reporting when you configure a role-based policy. Entitlement reporting can be enabled per policy or for all role-based policies.

To view Entitlement reports:

1. Go to the **Policy** page.
2. Find the host name in the list. Use the **Hostname**, **IP Address**, and **Tags** filters to refine the list of results displayed.
3. At the far right of the server entry row, click the **vertical ellipsis** menu, and then select **PMUL Policy**.
4. Click the **View Entitlement Report** tile.
5. To change the report details displayed, use the **Report Level**, **Run Host**, **Run User**, **Submit User**, **Submit Host**, and **Command** filters. Report levels provide varying levels of detail, with higher numbers providing more details.

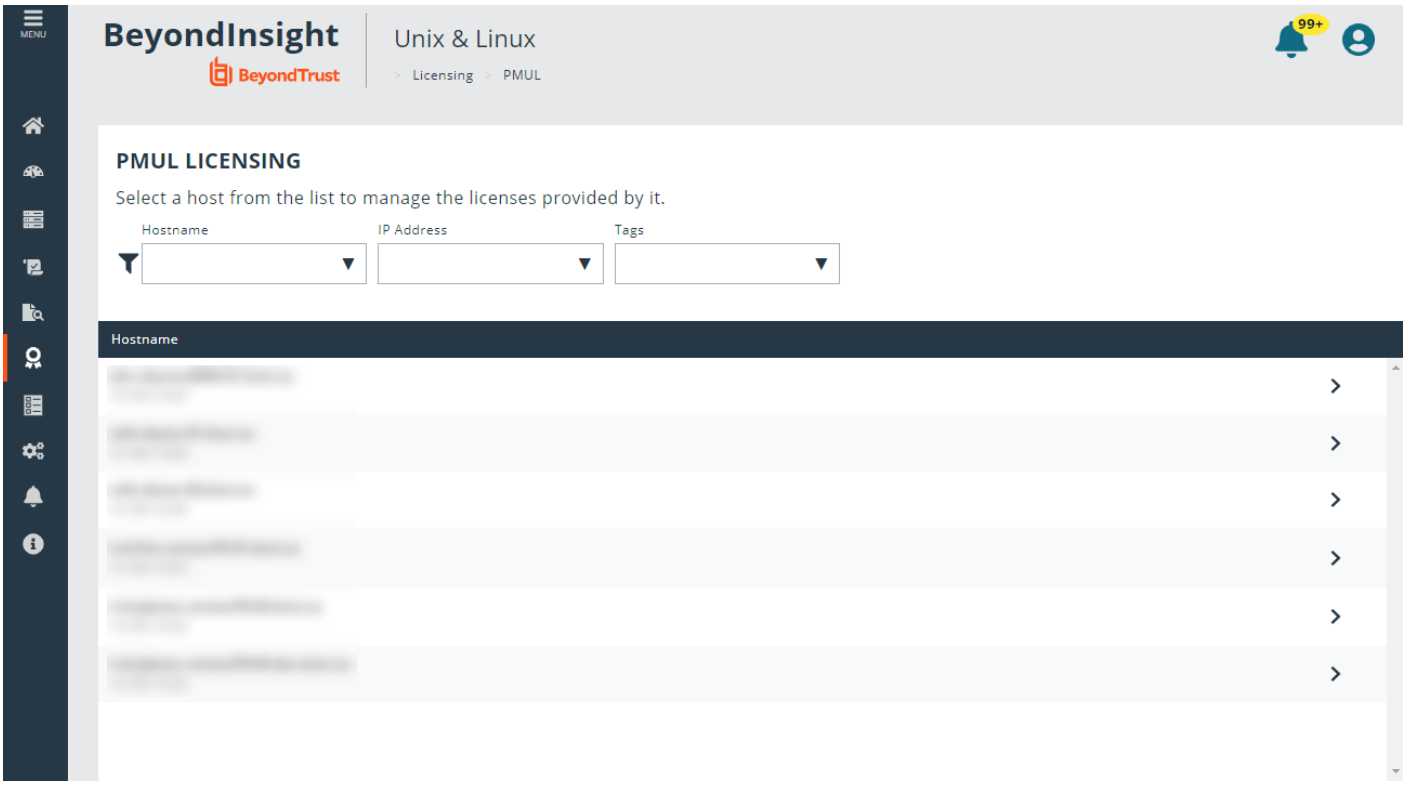
For more information, please see the following:

- *"Configure the PMUL Integration" on page 66*
- *"Manage PMUL Role-Based Policies" on page 80*

Manage PMUL Licenses

On the **PMUL Licensing** page, you can view and download information about PMUL licenses used by the various hosts. The licensing details include a **General Details** and a **Client Usage** view.

> *For Privilege Management for Unix and Linux versions 9.4.5 and earlier, the license is entered in a text box. In versions 10.0 and later, the user can upload a license file. For more information, see "Upload a JSON File" on page 119.*



The following reporting options are available from the **PMUL Licensing** page:

- A PDF file showing the summary details, in the **General Details** view.
- A CSV export file of the detailed license usage, in the **Client Usage** view.
- A JSON export file of the detailed license usage, in the **Client Usage** view.
- A PDF export file of the detailed license usage, in the **Client Usage** view.

View PMUL Licensing

1. From the sidebar menu, click **License Management**. You can also click the **License Management** tile on the **Home** page.
2. Find the license server in the list. Use the **Hostname**, **IP Address**, and **Tags** filters to refine the list of results displayed.
3. At the far right of the server entry row, click the arrow.

The **Licensing Details** page default view is the **General Details** for the server.

General Details

The **General Details** view displays a summary of PMUL license usage for the selected license server, broken down by the licensed PMUL components, but without specific details of the host names, IP addresses, etc. of the clients.

To download a PDF document of the general details for this server, at the far right of the page, click the **PDF** icon.

Upload a JSON File

You can upload a JSON file containing PMUL license information to send to the license server, to update the license with more clients or updated licensing dates. This updates the specifics of the data shown on the **License Management** page, for that licensing server.

Your uploading options are:

- Drag JSON files to the area at the bottom of the **Licensing Details > General Details** view.
- Click in the area at the bottom of the **Licensing Details > General Details** view to browse for JSON files to upload.

Client Usage Details

To view the details of each individual license client, the PMUL components for which they are licensed, and the relevant dates applicable to the license, click **Client Usage**. To reduce the list displayed, use the various filters provided.

Choose Licensing Details Columns to Display

You can choose which columns to display in the grid.

To select which columns to display, at the top-right of the grid, click the **Choose Columns to Display** icon and select one or more columns to display.

The columns appear from left to right in the grid, in the order that you select them.

To view the **Client Usage Details** for a specific client, click the entry in the table. The **Client Details** panel opens to the right of the entry.

To download various details files, do the following:

- For a CSV file of the detailed license usage, at the far right of the page, click the **Download** icon, and then select **CSV**.
- For a JSON file of the detailed license usage, at the far right of the page, click the **Download** icon, and then select **JSON**.
- For a PDF document of the general details for this server, at the far right of the page, click the **PDF** icon.

View Tasks and Task Details in BIUL

Host actions are organized and grouped on the **Tasks** page. Tasks can be filtered by the following options:

- **Task Type**
- **Date Range**
- **Username**
- **Pending Status**
- **Success Status**
- **Failure Status**

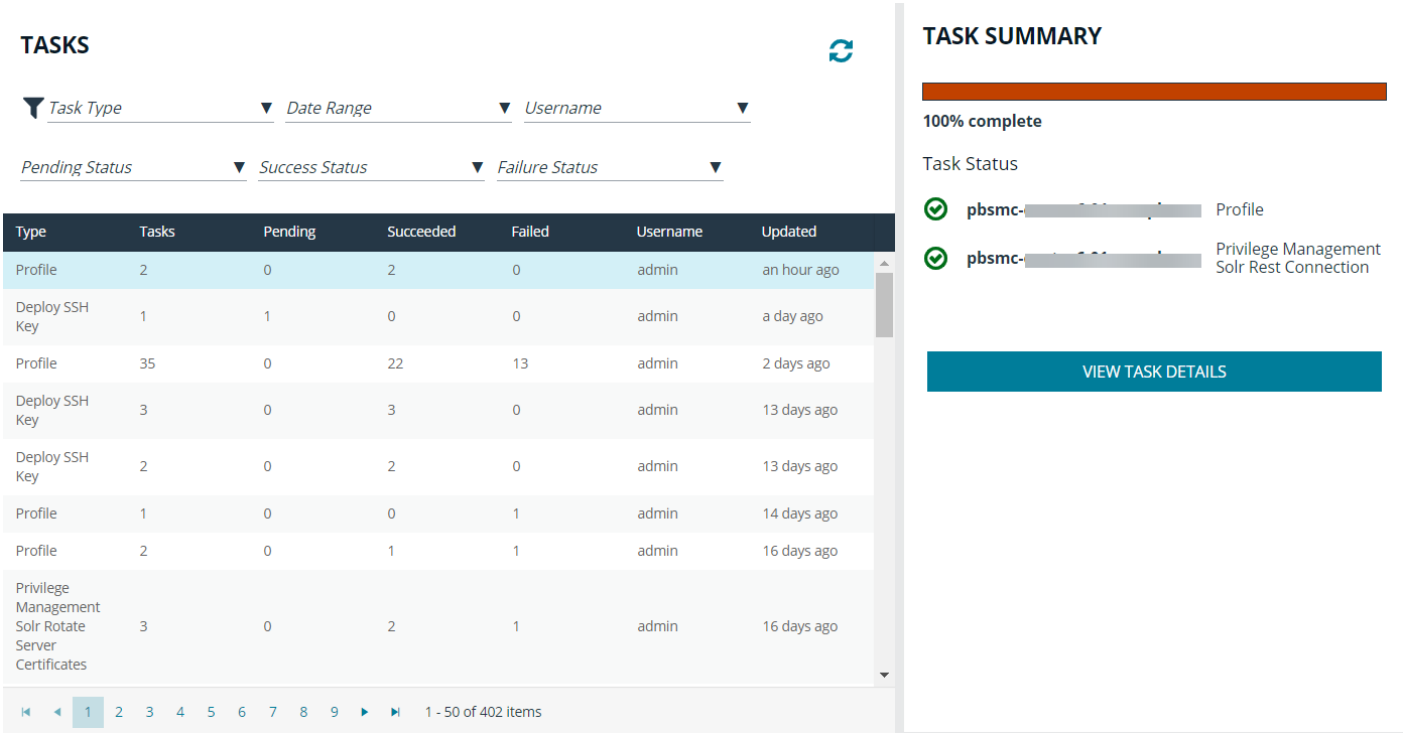
View Tasks

The task details grid includes the following:

- **Type:** The type of task that was run. Options include:
  - **Profile**
  - **Discovery**
  - **Install**
  - **Upgrade**
  - **Uninstall**
  - **Assign Log Server**
  - **Domain Join**
  - **Encryption Keyfiles Deployment**
- **Tasks:** The number of hosts the operation was performed on.
- **Pending:** The number of tasks that have yet to be run.
- **Succeeded:** The number of tasks completed successfully.
- **Failed:** The number of tasks completed unsuccessfully.
- **Username:** The user who executed the task.
- **Updated:** The last time the task entry was updated.

To view task details:

1. Go to the **Tasks** page.
2. Use the filtering options to reduce the list of tasks to choose from. For example, tasks can be listed by date range finding only those tasks that occurred in the selected time frame.
3. Select a task. A **Task Summary** is displayed.
4. From the **Task Summary**, click **View Task Details**.

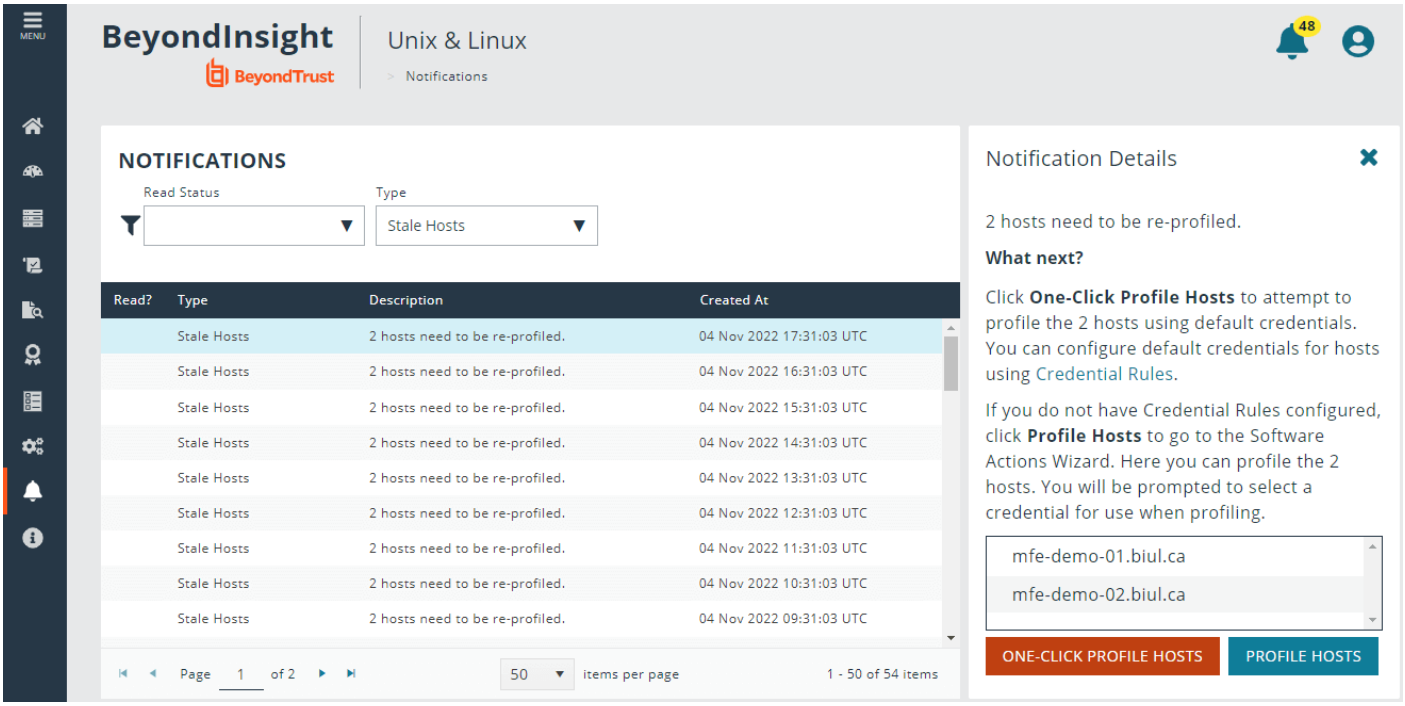


Task Details

The **Task Details** page provides detailed output of individual tasks. Information is presented in an easy to read manner to help with troubleshooting.

Notifications

On the **Notifications** page, users can view notifications when given conditions arise within BeyondInsight for Unix & Linux (BIUL). The notifications are specific to a logged-in user.



View Notification Details

To view notifications details:

1. On the sidebar menu, click **Notifications**.
2. On the **Notifications** page, if necessary, use the filtering options to reduce the list size.
    - **Read Status:** Read status can be **Read** or **Unread**.
    - **Type:** Currently, only **Stale Host** is available. When one or more hosts have not been profiled for more than a week, a notification is created for *software admin* or *sysadmin* users.

> ***Note:*** *The parameters defining stale hosts is not configurable. The period is defined as **7 days**.*

3. To view the **Notification Details**, click a notification row. The **Notification Details** panel provides options for remediation of the condition.
4. As described in the panel, to re-profile the hosts listed in the notification, click **One-Click Profile Hosts** or **Profile Hosts**.
    - The **One-Click Profile Hosts** option uses the existing BIUL *default credentials* feature.
    - The **Profile Hosts** option uses the existing **Software Actions** menu.

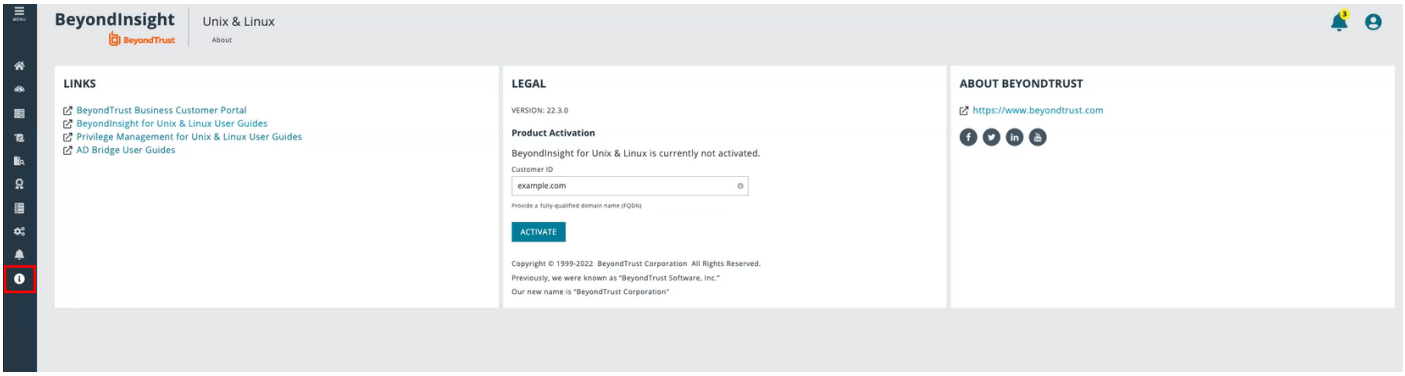
*For more information on **Software Actions**, see "Profile Servers in BIUL" on page 21.*

Access the Notifications Panel

At the top right of the BIUL interface, click the **Notifications** icon to get a list of host notifications. To go to the **Notifications** page, click **See All Notifications**.

About BIUL

The **About** page provides useful information and links to resources for your BeyondInsight for Unix & Linux (BIUL) product. To access the page, from the sidebar menu, click **About**.



Links

The **Links** panel provides links to the BeyondTrust Customer Portal, and BIUL/PMUL/AD Bridge documentation on our website.

Legal

The **Legal** panel offers a registration option for your product. To complete the process, provide a *fully-qualified domain name (FQDN)*, and then click **Activate**.

> ***Note:*** *This feature is optional, and you have full access to the BIUL functionality whether you register or not. We encourage you to complete this activation, as it provides us with confirmation that the product is being used. No critical or confidential information about your company is transmitted, aside from the product being activated.*

About BeyondTrust

The **About BeyondTrust** panel provides the many ways to communicate with us. Click any of the links to reach us.

Troubleshoot Common Issues with BIUL

Application Logs

Application logs are available. The location differs based on the operating system:

- For systemd machines, use **systemd run journalctl -u pbsmc**.
- For SysV or Upstart machines, the log is located in **/var/log/pbsmc.log**.
- For Windows machines, the log is located in **ProgramFiles (x86)\PBSMC\pbsmc.log**.

Common Error Messages

Hosts section displays credential error when selecting actions

If there are no credentials stored and an action is chosen requiring authentication, an error is displayed.

***Oops, No Products Found* displayed on Management page**

BeyondInsight for Unix & Linux cannot locate either the Privilege Management for Unix and Linux or BeyondInsight for Unix & Linux software to deploy.

> *For more information, please see Copy ISO Files to the Console Server at https://www.beyondtrust.com/docs/privilege-management/console/beyondinsight-unix-linux/install/install-windows.htm#copy-iso-files.*

Unable to install PMUL, and AD Bridge

> *For more information, please see the **Tasks** page.*

Discover does not locate a host

Verify the host is available, reachable from the network, and from an SSH-enabled port.

Unable to connect to PMUL using REST

> *For more information, please see the **Tasks** page. In most cases, the port is not available. Check the **REST** port on the **Host Details** page, and verify your firewall is accepting connections.*

Troubleshoot Password Safe Issues

Certificates

Password Safe is installed with a self-signed certificate. If this is not changed to a trusted issuer, the certificate should be added to the BeyondInsight for Unix & Linux systems certificate store to be trusted. The following provides high-level steps on importing certificates.

1. Copy the public certificate from the Password Safe server to the BeyondInsight for Unix & Linux server. This should be a .crt file.
2. Install the .crt file to the system key store. The process is different depending on the operating system.

macOS

1. Open **Keychain Access**, and drag the .crt file into the **System** node.
2. Double-click to open and expand the **Trust** leaf.
3. Select **Always Trust**.

Windows

1. Click **Start** and type **MMC**.
2. From the **File** menu, select **Add/Remove Snap-In > Certificates > Add**.
3. Select **Computer Account**, and click **Next**.
4. Select **Local Computer**.
5. After the snap-in is added, expand **Certificates** and right-click **Trusted Root Certification Authorities**.
6. Select **All Tasks > Import** and add the .crt file.

CentOS and Red Hat Linux

If not available, install ca-certificates

```
yum install ca-certificates
```

Enable dynamic configuration

```
update-ca-trust force-enable
```

Copy the .crt

```
cp <cert.crt> /etc/pki/ca-trust/source/anchors/
```

Update the trusted list

```
update-ca-trust extract
```

Debian and Ubuntu

Copy the .crt file

```
cp <cert.crt> /usr/local/share/ca-certificates
```

Update the cert list

```
sudo update-ca-certificates
```

Refresh the cert list

```
sudo update-ca-certificates --fresh
```

For more in-depth system information, please see the appropriate operating system documentation.