



BeyondTrust

BeyondInsight for Unix & Linux User Guide

Table of Contents

BeyondInsight for Unix & Linux User Guide	4
Overview of BeyondInsight for Unix & Linux	5
Install BeyondInsight for Unix & Linux	6
Prepare for the BeyondInsight for Unix & Linux Installation	6
Install BeyondInsight for Unix & Linux on Linux	7
Install BeyondInsight for Unix & Linux on Windows	8
Uninstall BeyondInsight for Unix & Linux	10
Configure BeyondInsight for Unix & Linux	11
Run BeyondInsight for Unix & Linux	12
View the BeyondInsight for Unix & Linux Home	13
View the BeyondInsight for Unix & Linux Dashboard	14
Discover Hosts with BeyondInsight for Unix & Linux	15
Use the BeyondInsight for Unix & Linux Hosts Inventory Grid	18
Use Privilege Escalation for BeyondInsight for Unix & Linux Credentials	21
Profile Servers in BeyondInsight for Unix & Linux	22
Manage AD Bridge Hosts	23
Manage Privilege Management for Unix and Linux Hosts	24
Manage Privilege Management for Unix and Linux Basic Hosts	26
Install and Manage Solr	28
Deploy Keyfiles	30
Delete Hosts	31
View Host Details	32
Manage Client Registration Profiles	35
Manage SSH Fingerprints	37
Manage the Registry Name Service	38
Manage Registry Name Service Groups	39
Manage Policy Service Groups	40
Manage Sudo Policy Service Groups	41
Manage File Integrity Monitoring Service Groups	42
Manage Privilege Management for Networks Service Groups	43
Manage Log Server Service Groups	44

Manage Log Archive Service Groups	45
Configure Settings and Manage Software	46
Manage BeyondInsight for Unix & Linux Settings	47
Configure Role-Based Access	49
Manage BeyondInsight for Unix & Linux Console Access	51
Integrate Password Safe with BeyondInsight for Unix & Linux	55
Configure the Privilege Management for Unix and Linux Integration	59
Manage Software	60
Add a Directory Service Connection	61
Add SMTP Server Connection	62
Manage Privilege Management for Unix and Linux Policies	63
Manage Privilege Management for Unix and Linux Role Based Policies	66
Manage Role Based Policy Roles	66
Manage Role Based Policy Users and User Groups	70
Manage Role Based Policy Command Groups	72
Manage Role Based Policy Host Groups	73
Manage Role Based Policy Schedule Groups	74
Manage Role Based Policy Backup and Restore	75
Manage Privilege Management for Networks Policies	76
Manage Privilege Management for Unix and Linux Basic Policies	80
Manage File Integrity Monitoring (FIM) Policies	81
Manage Privilege Management for Unix and Linux Script Policies	83
View Privilege Management for Unix and Linux Settings	85
Audit Activity Using BeyondInsight for Unix & Linux	86
Replay Sessions in BeyondInsight for Unix & Linux	88
Enable Session Recording in Script Policy Mode	88
Enable Session Recording in Role Based Policy Mode	88
Play a Recorded Session	89
View Entitlement Reports	89
Manage Credentials in BeyondInsight for Unix & Linux	91
View Tasks and Task Details in BeyondInsight for Unix & Linux	92
Troubleshoot Common Issues with BeyondInsight for Unix & Linux	94
Troubleshoot Password Safe Issues	95

BeyondInsight for Unix & Linux User Guide

This guide shows system administrators and security administrators how to configure and use BeyondInsight for Unix & Linux. It provides an overview of how BeyondInsight for Unix & Linux 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
Privilege Management for Unix and Linux Basic (formerly PowerBroker for Sudo)	PMUL Basic
Solr (formerly PowerBroker Solr)	Solr
File Integrity Monitoring	FIM
Advanced Control and Audit	ACA
Role Based Policy	RBP

Overview of BeyondInsight for Unix & Linux

BeyondInsight for Unix & Linux is a web-based tool that you can use to:

- Manage software for AD Bridge, Privilege Management for Unix and Linux, Privilege Management for Unix and Linux Basic, and Solr.
- 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 Privilege Management for Unix and Linux licenses on policy servers.
- Manage Privilege Management for Unix and Linux Script, Privilege Management for Unix and Linux Basic, File Integrity Monitoring (FIM), and Role Based policies.
- Manage Sudo host groups and FIM policy host assignment.
- View, replay, and audit Privilege Management for Unix and Linux logs.

Core Features

- **Dashboard:** Provides visual insight into host and software metrics.
- **Host Discovery:** Is the first stage of adding any remote hosts to be managed by the console. Hosts available by SSH will be added.
- **Hosts Inventory:** Is the central page of the console. On the **Hosts > Hosts Inventory** page, you can profile targets, install and uninstall AD Bridge, Privilege Management for Unix and Linux, Privilege Management for Unix and Linux Basic, 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 Privilege Management for Unix and Linux Registry Name Service systems.
- **Policy Management:** Allows for management of Privilege Management for Networks, FIM, Privilege Management for Unix and Linux Basic, and Role Based and Script Based policies on Privilege Management for Unix and Linux policy servers.
- **Audit:** View Privilege Management for Unix and Linux event and IO logs. IO logs can be replayed as they occurred. Users can add comments on the logs.
- **Tasks:** Provides 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.

Install BeyondInsight for Unix & Linux



Note: You can install the console on Windows or Linux operating systems.

Requirements

- System firewall configured to allow access on port 4443 (default)

Supported Operating Systems

The following operating systems are supported by BIUL:

- Windows 2012 or later
- Windows 2012 R2 or later
- RHEL/CentOS 5 or later
- Debian/Ubuntu 12.04 or later

Supported Browsers

The following browsers are supported:

- Safari 9 or later
- Chrome 52 or later
- FireFox 48 or later
- Edge

Prepare for the BeyondInsight for Unix & Linux Installation

- Run the install using an account with root or administrator privileges.
- Copy the installers for BeyondInsight for Unix & Linux, Privilege Management for Unix and Linux, AD Bridge, and Privilege Management for Unix and Linux Basic packages to the server.
- If deploying to an HP-UX server, make sure **gzip** is in **/usr/bin** or **/bin**. If it is not, create a symbolic link.

```
ln -s /usr/contrib/bin/gzip /usr/bin/gzip
```

Install BeyondInsight for Unix & Linux on Linux

Use the following syntax to install BeyondInsight for Unix & Linux.

RHEL and CentOS

```
# install, where {version} is the current version
rpm -i biul-{version}.rpm
# optional: verify software is running
service pbsmc status

# configure firewall using OS version appropriate command:
# RedHat Enterprise Linux/CentOS 7:
firewall-cmd --zone=public --add-port=4443/tcp --permanent
firewall-cmd --reload

# or, RedHat Enterprise Linux/CentOS 6:
iptables -A INPUT -p tcp -m tcp --dport 4443 -j ACCEPT
service iptables save
```

Debian and Ubuntu

```
# install, where {version} is the current version
dpkg -i biul-{version}.deb

# optional: verify software is running
service pbsmc status

# configure firewall using OS version appropriate command:
# for ubuntu 14+:
ufw allow 4443

# or other versions:

iptables -A INPUT -p tcp -m tcp --dport 4443 -j ACCEPT
service iptables save
```

Install BeyondInsight for Unix & Linux on Windows

1. Run the msi package and follow the install wizard.
2. After you go through the wizard, configure the firewall.
3. Open **Control Panel > System and Security > Windows Firewall**.
4. Click **Advanced Settings**.
5. Click **Inbound Rules**.
6. Click **New Rule** in the **Actions** window.
7. Click **Rule Type of Port**, and then click **Next**.
8. On the **Protocol and Ports** page, click **TCP**.
9. Select **Specific Local Ports** and type a value of **4443**. Click **Next**.
10. On the **Action** page, click **Allow the connection**. Click **Next**.
11. On the **Profile** page, click the appropriate options for your environment and click **Next**.
12. On the **Name** page, enter a name for BeyondInsight for Unix & Linux. Click **Finish**.

Copy ISO Files to the Console Server

You must copy and extract the ISO files for the Privilege Management for Unix and Linux, AD Bridge, and Privilege Management for Unix and Linux Basic installers.



Note: The installer path folder structures must not be modified.

AD Bridge

Windows:

```
C:\Program Files (x86)\BeyondTrust\PBSMC\software\pbis
```

Unix:

```
/usr/local/bin/software/pbis/
```

Privilege Management for Unix and Linux

Windows:

```
C:\Program Files (x86)\BeyondTrust\PBSMC\software\pmul
```

Unix:

```
/usr/local/bin/software/pmull
```

Privilege Management for Unix and Linux Basic

Windows:

```
C:\Program Files (x86)\BeyondTrust\PBSMC\software\pmbasic
```


Unix:

```
/usr/local/bin/software/pmbasic/
```

Solr**Windows:**

```
C:\Program Files (x86)\BeyondTrust\PBSCMC\software\solr
```

Unix:

```
/usr/local/bin/software/solr/
```

Upload Software

Alternatively, you can upload software for Privilege Management for Unix and Linux, AD Bridge, and Privilege Management for Unix and Linux Basic installers on the **Settings** page.



Note: You cannot upload software on the BeyondTrust UVM appliance. Use BT Updater to update local packages.

To upload software:

1. Click **Settings > Software**, and then click the upload icon.
2. Drag the file to the upload area.

Optionally, click anywhere in the upload area to navigate to the file. The Privilege Management for Unix and Linux ISO files and AD Bridge zip files are large. The upload can take time. A progress bar shows the upload progress. You can resume an upload if an interruption occurs (for example, a session timeout occurs).

3. After the upload is complete, BeyondInsight for Unix & Linux unpacks the files, which can take a few minutes. The software is available after the unpacking is complete.
4. Click the refresh icon to update the status of available software.

Uninstall BeyondInsight for Unix & Linux

RHEL and CentOS

In an escalated shell session, enter:

```
# remove
rpm -e pbsmc

# optional: remove config and db
rm -rf /etc/pbsmc
rm -rf /usr/share/pbsmc/
```

Debian and Ubuntu

In an escalated shell session, enter:

```
# remove
dpkg -r pbsmc

# optional: remove config and db
rm -rf /etc/pbsmc
rm -rf /usr/share/pbsmc
```

Windows

1. Open **Control Panel**.
2. Click the **Add or Remove Software** icon.
3. Remove **BeyondInsight for Unix & Linux**. Configuration and database files can be manually deleted in the **%ProgramFiles%\PBSMC** directory.

Configure BeyondInsight for Unix & Linux

1. You can customize the console using the **pbsmc.toml.default** file located in:
 - Linux: **/etc/pbsmc**
 - Windows: **%ProgramFiles%\PBSMC**
2. Create a copy of the file using the name **pbsmc.toml**. You can include only the settings that you want to customize.
3. Be sure to include the section title in **pbsmc.toml**. For example, if you want to change the default port number, the text will look similar to the following:

```
[server]
port="4443"
```



Note: Apply proper security settings on the **.toml** file. The file owner requires **Read** and **Write** privileges.

4. You can configure the following settings:
 - **SSL:** By default, the console supports encrypted HTTPS connections using automatically generated, self-signed certificates. The console serves only HTTPS traffic on the configured port, unless explicitly configured to fall back to insecure HTTPS in the **pbsmc.html** configuration file. A custom certificate pair may also be provided and placed in the configuration file.
 - **Port:** By default, the console runs on port **4443**. Before changing this value, stop the service.
 - **Database:** By default, the console creates a SQLite database in **/etc/pbsmc/pbsmc.sqlite** or in **%ProgramFiles%\pbsmc** on Windows. This can be changed to another location.
 - **Pool:** Console tasks are run in a concurrent pool of processes. The default number of processes running at a time is **20**. You can increase the pool size to allow jobs to complete faster. However, the server performance might lag, and decreasing the pool size will have the opposite affect.
 - **keys:** Encryption keys for BIUL use base64 encoded AES 256 encryption. The key secures sensitive data stored in the database. More than one key can be used at a time. The **Active** key in the **pbsmc.toml** file is the key currently in use. If you start BeyondInsight for Unix & Linux without an encryption key, one is generated for you. You can review the comments in the **pbsmc.toml.default** file.



Note: You must restart the service to apply changes.

Run BeyondInsight for Unix & Linux

Log into 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.

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 system settings including:

- **Administrator account:** Create the account that you will use to log into the console.
- **Active Directory connection:** Configure a connection to an Active Directory forest. Active Directory users and groups can be used in Privilege Management for Unix and Linux policy and can log into the console.
- **Settings:** Configure default settings, including default policy type, authentication timeout values, and security level.
- **Credentials:** Create credentials for remote hosts. The credentials are used to connect to the remote hosts.

Review the settings and save. You are now able to log into the console using the administrator account you created in the wizard.

View the BeyondInsight for Unix & Linux Home

The **Home** screen allows administrators to view BeyondInsight for Unix & Linux options on the landing page for easy access. The options include:

- **Host Inventory:** Discover, add, and manage hosts for BeyondInsight for Unix & Linux.
- **Settings:** Configure BeyondInsight for Unix & Linux.
- **Audit:** View, replay, and audit Privilege Management for Unix and Linux logs.
- **Policy Management:** Create, edit, and modify policies on managed policy servers.
- **Tasks:** View jobs executed by BeyondInsight for Unix & Linux.

View the BeyondInsight for Unix & Linux 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.

Discover Hosts with BeyondInsight for Unix & Linux

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 BeyondInsight for Unix & Linux](#)" on page 11.

Discover Host Methods

Hosts are discovered through the following methods:

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

Left-Click the **Add Hosts** menu on the **Host Inventory** page to access any of these methods from the drop-down menu.

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, 10.1.100.15.
- **IP Range:** Discover any hosts in the range, 10.1.100.15–10.1.100.20.
- **CIDR Notation:** Discover hosts in a CIDR block, 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**.

SCAN FOR HOSTS



Scan hosts by IP (10.100.1.0), a hyphen-separated IP range (10.100.1.0-10.100.1.20), or CIDR notation (10.100.1.0/24)

Address

SSH Port
22



SSH Host Public Key SHA256 Fingerprint (optional - single IP disc...

☐ Automatically accept SSH fingerprints

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**.

IMPORT HOSTS



Import a CSV file to discover hosts. The format is IP, SSH port, and an optional SSH Fingerprint to authorize communication.

Example:

```
hosts.csv
"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
```

☐ Automatically accept SSH fingerprints from new hosts

Drag CSV files here or click here to browse to upload.

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**.

SCAN REGISTRY NAME SERVICES



Scan the Registry Name Service in order to discover hosts.

SSH Port
22



☐ Automatically accept SSH fingerprints

Primary Registry Servers

pbsmc-centos6-02.one.pbsmc
pbsmc-debian8-03.unix.symark.com

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.

Use the BeyondInsight for Unix & Linux 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.

HOSTS INVENTORY

Hostname ▼ IP Address ▼ Operating System ▼ Tags ▼

+ ADD HOSTS ▼

15 items

<input type="checkbox"/>	Hostname	Alerts	AD Bridge	PMUL	PMUL Basic Edition	Solr	Updated
<input type="checkbox"/>	pbsmc-centos6-01.one.pbsmc 172.20.31.101 CentOS 6.7	1 Agent joined 8.8.0		Policy Log Client FIM License RNS 10.3.0-16	Client Not Ready	Server Client	5 days ago
<input type="checkbox"/>	pbsmc-centos6-02.one.pbsmc 172.20.31.102 CentOS 6.7	Agent joined 8.6.0 ONE.PBSMC		Policy Log Client FIM License RNS 10.3.0-16	Client Ready	Server Client BIUL Managed	5 days ago
<input type="checkbox"/>	pbsmc-centos6-03.one.pbsmc 172.20.31.103 CentOS 6.7	1 Agent joined 10.0.0 ONE.PBSMC		Policy Log Client FIM License RNS 10.3.0-16	Client Ready	Server Client	4 days ago
<input type="checkbox"/>	pbsmc-centos6-04.unix.symark.com 172.20.31.104 CentOS 6.7	Agent joined 8.8.0		Policy Log Client FIM License RNS 10.3.0-14	Client Ready	Server Client	4 days ago
<input type="checkbox"/>	pbsmc-centos6-05.unix.symark.com 172.20.31.105 CentOS 6.9 balrog @guile policy log my	Agent joined 8.8.0		Policy Log Client FIM License RNS 10.1.0-15	Client Ready	Server Client BIUL Managed	4 days ago
<input type="checkbox"/>	pbsmc-centos6-06.one.pbsmc	1 Agent joined		Policy Log Client FIM License RNS	Client	Server Client	5 days ago

1 - 15 of 15 items



For more information, please see the following:

- ["View Tasks and Task Details in BeyondInsight for Unix & Linux" on page 92](#)
- ["Manage Credentials in BeyondInsight for Unix & Linux" on page 91](#)

Use the Hosts 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. Select a host and then select the **View Host Details** menu to view more details about the host.



For more information on adding hosts, please see ["Discover Hosts with BeyondInsight for Unix & Linux" on page 15](#).

Primary Server Columns

The following outcomes are possible:



Privilege Management for Unix and Linux 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 outcomes 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 Privilege Management for Unix and Linux 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

PMUL Basic Edition

If Privilege Management for Unix and Linux Basic is installed, the **PMUL Basic Edition** column displays the version number and an icon for each feature and role the host has enabled.

- **Client:** Sudo Client

Solr

- **Server:** Solr Server
- **Client:** Client (indexed 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 **Perform Host Actions** from the menu to start the **Host Actions** wizard. Host actions include:

- Profile
- Install software for AD Bridge, Privilege Management for Unix and Linux, Privilege Management for Unix and Linux Basic, and Solr
- Manage Solr
- 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 server at a time. On the **Hosts > Hosts Inventory** page, you can select more than one host and select the **Bulk Actions** menu. The **Bulk Actions** menu is only displayed when more than one server is selected.

Use Privilege Escalation for BeyondInsight for Unix & Linux Credentials

Most actions require a credential be supplied in BeyondInsight for Unix & Linux. 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 BeyondInsight for Unix & Linux

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 **/tmp** folder.



You can configure a remote working directory. For more information, please see ["Deployment Settings" on page 47](#).



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

1. Go to the **Hosts > Hosts Inventory** page.
2. Select a host, and then select **Perform Host Actions**.
3. Select **Profile**, and then click **Next Step**.
4. On the **Credential Selection** page, select a logon credential that will 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 may require choosing a second credential.
5. Review the **Summary** page, and then click **Finish**.
6. Review the **Task** page, and verify the completed status of attempted actions under **Task Summary**.
7. Click **Task Details** to view more information about **Task Status**.

Manage AD Bridge Hosts



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

To manage AD Bridge hosts:

1. Go to the **Hosts > Hosts Inventory** page.
2. Select a host, and then 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.
 - **Uninstall:** Remove AD Bridge software.
5. On the **Credential Selection** page, select a logon credential that will 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 may 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. Click **Task Details** to view more information about **Task Status**.

Join a Domain

To join selected AD Bridge hosts to a domain:

1. Go to the **Hosts > Hosts Inventory** page.
2. Select a host, and then select **Perform Host Actions**.
3. On the **Primary Action** page, select **Active Directory Bridge**.
4. On the **Join Domain** page, provide the following information:
 - **Domain Join Arguments:** The CLI arguments to join the domain.
 - **AD Credential:** The credential for the Active Directory domain.
5. On the **Credential Selection** page, select a logon credential that will 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 may 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. Click **Task Details** to view more information about **Task Status**.

Manage Privilege Management for Unix and Linux 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 hosts:

1. Go to the **Hosts > Hosts Inventory** page.
2. Select a host, and then 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 Privilege Management for Unix and Linux installations will use these keys. The keys can be managed on the **Settings** page.

Install the Privilege Management for Unix and Linux Policy Server

To install Privilege Management for Unix and Linux policy server:

1. Go to the **Hosts > Hosts Inventory** page.
2. Select a host, and then select **Perform Host Actions**.
3. Select **Privilege Management for Unix and Linux**, and then select **Next Step**.
4. Click **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 Privilege Management for Unix and Linux components will be installed except for RNS server.
 - **License Server Only:** Only the Privilege Management for Unix and Linux license server will be installed.
 - **Policy and Log Server Only:** All server components of Privilege Management for Unix and Linux will be installed except for RNS server.
 - **Submit and Run Host Only:** The client components of Privilege Management for Unix and Linux will be installed.
 - **Primary Registry Server and All Components:** All Privilege Management for Unix and Linux 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 that will 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 may 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. Click **Task Details** to view more information about **Task Status**.



For more information about installation templates, see "[Privilege Management for Unix and Linux Installation Templates](#)" on page 60. For more information about client registration profiles, see "[Manage Client Registration Profiles](#)" on page 35.

Upgrade the Privilege Management for Unix and Linux Policy Server

To upgrade the policy server to the version loaded in the console:

1. Go to the **Hosts > Hosts Inventory** page.
2. Select a host, and then select **Perform Host Actions**.
3. Select **Privilege Management for Unix and Linux**, and then select **Next Step**.
4. Click **Upgrade**, and then click **Next Step**.
5. In the **Action Requirements** section, select a **License Server**. Select **Current** to set the option to the currently selected server.



Note: If the current host is selected as a **License Server**, this server will be a **Primary License server**.

6. As necessary, check the **Install license server** box to make this host a secondary license server when used with a selected primary.
7. On the **Credential Selection** page, select a logon credential that will 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 may require choosing a second credential.
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. Click **Task Details** to view more information about **Task Status**.

Uninstall the Privilege Management for Unix and Linux Policy Server

To remove the policy server:

1. Go to the **Hosts > Hosts Inventory** page.
2. Select a host, and then 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 that will 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 may 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. Click **Task Details** to view more information about **Task Status**.

Manage Privilege Management for Unix and Linux Basic Hosts

To manage Privilege Management for Unix and Linux Basic hosts:

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

Install the Privilege Management for Unix and Linux Basic Client

To install Privilege Management for Unix and Linux Basic software on the client:

1. Go to the **Hosts > Hosts Inventory** page.
2. Select a host, and then select **Perform Host Actions**.
3. Select a client registration server and a client registration profile. This client registration server list is filtered to known client registration servers with working REST credentials. Click **Next Step**.
4. On the **Credential Selection** page, select a logon credential that will 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 may require choosing a second credential.
5. Review the **Summary** page, and then click **Finish**.
6. Review the **Task** page, and verify the completed status of attempted actions under **Task Summary**.
7. Click **Task Details** to view more information about **Task Status**.

Upgrade the Privilege Management for Unix and Linux Basic Client

To upgrade the sudo client to the version loaded in the console:

1. Go to the **Hosts > Hosts Inventory** page.
2. Select a host, and then select **Perform Host Actions**.
3. Select **Privilege Management for Unix and Linux Basic**, and then click **Next Step**.
4. Select **Upgrade**.
5. On the **Credential Selection** page, select a logon credential that will 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 may 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. Click **Task Details** to view more information about **Task Status**.

Uninstall the Privilege Management for Unix and Linux Basic Client

To remove the sudo client:

1. Go to the **Hosts > Hosts Inventory** page.
2. Select a host, and then select **Perform Host Actions**.
3. Select **Privilege Management for Unix and Linux Basic**, and then click **Next Step**.
4. Select **Uninstall**.

5. On the **Credential Selection** page, select a logon credential that will 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 may 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. Click **Task Details** to view more information about **Task Status**.

Install and Manage Solr

Solr Connectivity

Certificates must be used to communicate between the Solr server and the log servers.

BeyondInsight for Unix & Linux is a certificate signing authority. The console can generate and distribute the required certificates.



Note: Solr must be installed using BeyondInsight for Unix & Linux; otherwise, there is no way to communicate with the Solr server.

Install Solr

To install Solr:

1. Go to the **Hosts > Hosts Inventory** page.
2. Select a host, and then select **Perform Host Actions**.
3. Select **Solr**, and then select **Next Step**.
4. Select **Install**, and then select **Next Step**.
5. Solr tries to detect the location of the Java environment on the server. Otherwise, you can enter the Java Home details.
6. On the **Credential Selection** page, select a logon credential that will 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 may 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. Click **Task Details** to view more information about **Task Status**.

Uninstall Solr

To remove Solr:

1. Go to the **Hosts > Hosts Inventory** page.
2. Select a host, and then select **Perform Host Actions**.
3. Select **Solr**, and then select **Next Step**.
4. Select **Uninstall**, and then select **Next Step**.
5. On the **Credential Selection** page, select a logon credential that will 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 may 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. Click **Task Details** to view more information about **Task Status**.

Assign a Log Server

The log servers selected are indexed by the Solr server.

To assign a log server:

1. Go to the **Hosts > Hosts Inventory** page.
2. Select a host, and then select **Perform Host Actions**.
3. Select **Solr**, and then select **Next Step**.
4. Select **Assign Solr Indexing Server**, and then select **Next Step**.
5. Select a Solr server from the **Solr Server** list, and then select **Next Step**.
6. On the **Credential Selection** page, select a logon credential that will 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 may 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. Click **Task Details** to view more information about **Task Status**.

Deploy Keyfiles

The **Deploy Keyfile** action uses the network and encryption keys configured on the **Settings > Integration** page.

To deploy keyfiles:

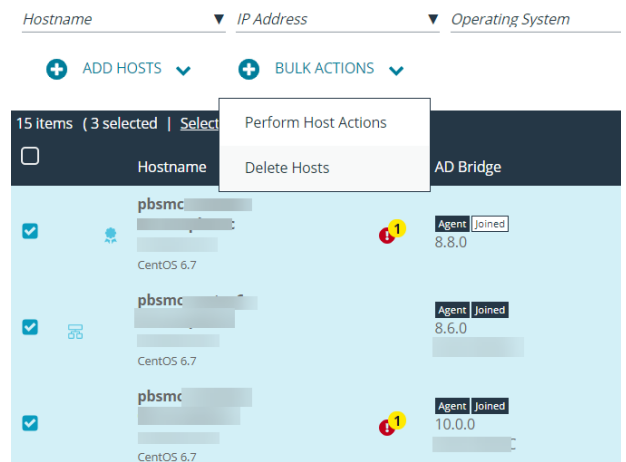
1. Go to the **Hosts > Hosts Inventory** page.
2. Select a host, and then select **Perform Host Actions**.
3. Select Privilege Management for Unix and Linux, and then select **Next Step**.
4. Select **Deploy keyfiles**, and then click **Next Step**.
5. On the **Credential Selection** page, select a logon credential that will 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 may 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. Click **Task Details** to view more information about **Task Status**.

Delete Hosts

The **Delete Host** action can be selected from the menu on the **Hosts > Hosts Inventory** page. It removes the selected hosts from the console database. No action is taken on the host nor on any credentials the console may have stored for it.

To delete more than one host, select the hosts in the list, and then select **Delete Hosts** from the **Bulk Actions** list.

HOSTS INVENTORY



The screenshot shows the 'HOSTS INVENTORY' page. At the top, there are tabs for 'Hostname', 'IP Address', and 'Operating System'. Below the tabs are two buttons: '+ ADD HOSTS' and '+ BULK ACTIONS'. A dropdown menu is open under 'BULK ACTIONS', showing 'Perform Host Actions' and 'Delete Hosts'. The main table lists 15 items, with 3 selected. The table columns are 'Hostname', 'IP Address', 'Operating System', and 'AD Bridge'. The selected hosts are all CentOS 6.7 machines with the hostname 'pbsmc'.

Hostname	IP Address	Operating System	AD Bridge
pbsmc		CentOS 6.7	Agent Joined 8.8.0
pbsmc		CentOS 6.7	Agent Joined 8.6.0
pbsmc		CentOS 6.7	Agent Joined 10.0.0

View Host Details

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


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

- Configure the Privilege Management for Unix and Linux **Rest API Time Correction**, which is the acceptable time offset between BeyondInsight for Unix & Linux and the Privilege Management for Unix and Linux host in seconds.
- Apply licenses and view license details.

To view more information about a host:

1. On the **Hosts > Host Inventory** page, select the **View Host Details** menu for a server. General host details are displayed, including:
 - **Discovered**
 - **Last Profiled**
 - **IP**
 - **Operating System**
 - **Architecture**
 - **Default Gateway**
 - **Tags**
2. Select a product name in the **Host Details** list to view details about the host collected by BeyondInsight for Unix & Linux. Details on errors and warnings are included here.

PBSMC-CENTOS6-01.ONE.PBSMC



Discovered:
Operating System:
Tags:

November 21, 2019
Linux CentOS 6.7

Last Profiled:
Architecture:

5 days ago
x86_64

IP:
Default Gateway:

172.20.31.101

[Host Details](#) | [Client Registration Profiles](#)

HOST DETAILS

General
Privilege Management for Unix & Linux
 PMUL Settings
 Registry Name Service
 PMUL Licensing
 AD Bridge
 Privilege Management for Unix & Linux Basic
 Solr
 Errors & Warnings

GENERAL DETAILS

Tags
 Add tags

Connection Details
 Hostname and IP address are determined by profiling the relevant host. You can profile a host on the [Hosts Inventory](#) page.
 Hostname
pbsmc-centos6-01.one.pbsmc
 IP Address
172.20.31.101
 Port
22

SAVE HOST

REST API Connectivity

BeyondInsight for Unix & Linux automatically configures a REST connection to Privilege Management for Unix and Linux policy servers.

Note the following when using the REST API:

- REST API connections can only be made to a policy server with Privilege Management for Unix and Linux v 9.4 or later.
- REST connectivity does not open any firewall ports. This must be done by the user.
- By default, Privilege Management for Unix and Linux uses self-signed certificates. BeyondInsight for Unix & Linux 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 **Host 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 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 select **View Host Details**.
3. Under **General Details**, left-click in the **Add tags** field and scroll till 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 > Host Inventory** page.
2. Click the **Tags** drop-down 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 select **View Host Details**.

3. Under **General Details**, left-click in the **Add tags** field, and scroll till you find the desired tag.
4. Left-click the **X** that appears beside the tag to delete it from the list.

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.

Manage SSH Fingerprints

You can accept or reject SSH fingerprints. When BeyondInsight for Unix & Linux 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.

SSH FINGERPRINTS

Hostname	Profiled	Fingerprint	Status	Last Updated
10.100.3.6	false	SHA256:HASH... KEY	allowed	4 months ago
pbsmc-centos6-01.on...	true	SHA256:XaQ7X...	unknown	3 months ago
pbsmc-centos6-02.bash	true	SHA256:XaQ7X...	allowed	a month ago

FINGERPRINT DETAILS

Host

10.100.3.6

Fingerprint

SHA256:HASHED-KEY

Status

allowed 4 months ago

ALLOW

DENY

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](https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm) 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**
- **Sudo**
- **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 will be set as a **Primary** RNS server and the previous primary will be 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 RNS server must be demoted to a Secondary role before it can be removed.

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 RNS server in the service group, click **Promote**. The server's role will be set as a **Primary** RNS 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 RNS server must be demoted to a Secondary role before it can be removed.

Manage Sudo Policy Service Groups

Sudo Policy service groups define the policy sources and clients for Privilege Management for Unix and Linux Basic policy. To manage Sudo policy service groups, select **Sudo** 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 RNS server in the service group, click **Promote**. The server's role will be set as a **Primary** RNS 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 RNS server must be demoted to a Secondary role before it can be removed.

Manage File Integrity Monitoring 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 RNS server in the service group, click **Promote**. The server's role will be set as a **Primary** RNS 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 RNS server must be demoted to a Secondary role before it can be removed.

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 RNS server in the service group, click **Promote**. The server's role will be set as a **Primary** RNS 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 RNS server must be demoted to a Secondary role before it can be removed.

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 RNS server in the service group, click **Promote**. The server's role will be set as a **Primary** RNS 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 RNS server must be demoted to a Secondary role before it can be removed.

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 RNS server in the service group, click **Promote**. The server's role will be set as a **Primary** RNS 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 RNS server must be demoted to a Secondary role before it can be removed.

Configure Settings and Manage Software

From the **Settings** menu option, you can configure the following:

- **Console Access:** Add new users and groups to BeyondInsight for Unix & Linux.
- **System:** Manage BeyondInsight for Unix & Linux settings.
- **Integration:** Manage integration settings for external BeyondTrust integrations.
- **Software:** Manage BeyondTrust software versions.

Manage BeyondInsight for Unix & Linux 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 BeyondInsight for Unix & Linux by default upon discovery.
5. Click **Save**.

Authentication Timeout Settings

The following options are available to configure **Authentication Timeout Settings** for the BeyondInsight for Unix & Linux console. The settings are specified in minutes.

- **Total Session Length**
- **Session Timeout Warning**
- **Total Idle Length**
- **Idle Timeout Warning**

Application Settings

Configure application settings if you want to use the password reset feature available on the BeyondInsight for Unix & Linux 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. Enter the base URL for BeyondInsight for Unix & Linux. For a standalone deployment with default port, the URL is <https://<hostname>:4443/>. On the BeyondTrust appliance, the URL is <https://<hostname>/pbsmc/>. The BeyondInsight for Unix & Linux URL is required for password reset and email verification; the URL is used to format links in emails.
2. Turn on **Enforce Email Verification**. This is optional. When this setting is turned on, BeyondInsight for Unix & Linux 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.

Set up Password Reset

A **Reset Password** link is available on the BeyondInsight for Unix & Linux 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 BeyondInsight for Unix & Linux 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. Select 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.



For more information on configuring the SMTP server, please see "[Manage BeyondInsight for Unix & Linux Settings](#)" on [page 47](#).

Configure Role-Based Access

Access control provides a role-based system to authenticate users in BeyondInsight for Unix & Linux. Users are assigned roles based on the level of access they need to do their BeyondInsight for Unix & Linux 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
- **amountadmin:** 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 > Users** page. Provision roles on the details page for users and groups.
- On the **Settings > Roles** 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 51](#).

Assign a Role to User Accounts

1. Select **Settings > Roles**.
2. Select a role from the list.
3. Click the **Users** tab or **Groups** tab.
4. Click the toggle **Show users with/without this role** to see users not currently in the role. Check the boxes for users you want to add.
5. Click **Add Selected Users**.

Assign a Role to Groups

1. Select **Settings > Roles**.
2. Select a role from the list.
3. Click the toggle **Show groups with/without this role** to see groups not currently in the role.

4. Check the boxes for groups you want to add.
5. Click **Add Selected Groups**.

Manage BeyondInsight for Unix & Linux Console Access

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

CONSOLE ACCESS

USERS GROUPS

Username Roles Active Status ADD USERS +

Enabled	Name	Path	Roles
<input checked="" type="checkbox"/>	admin		accountadmin sysadmin
<input checked="" type="checkbox"/>	localuser-test		accountadmin apuser sysadmin
<input checked="" type="checkbox"/>	localuser-testing		accountadmin apuser policyadmin sysadmin
<input checked="" type="checkbox"/>	policy_admin		auditor policyadmin
<input checked="" type="checkbox"/>			
<input checked="" type="checkbox"/>			policyadmin softwareadmin
<input checked="" type="checkbox"/>			auditor policyadmin
<input checked="" type="checkbox"/>			apuser

1 - 8 of 8 items

Add a Local User Account

1. Select the **Settings** menu.
2. Click **Users**.
3. Click **Add Users**.
4. Select **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 **Add Account**.

ADD USERS

Create Local Users or grant access to Active Directory Users or Groups.

Add
Local User

☒ (Enabled)

Username
Local-Test

First Name
Local

Last Name
Test

Email
Local-Test@test.com

Password

Confirm Password

ADD ACCOUNT

Assign a Role to a User Account

1. In the **Console Access** list, click the **Users** tab.
2. Select the edit icon for a local user account to display the **User Details** page.
3. Select the **Roles** tab.

4. 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 49.

Update a Local User Account

1. In the **Console Access** list, click the **Users** tab.
2. Select the edit icon for a local user account to display the **User Details** page.
3. The following configuration options are available:
 - **Enabled:** 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.
4. Select **Save User**.

Update Password for a Local User Account

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

Delete a Local User Account

1. In the **Console Access** list, click the **Users** tab.
2. Select the edit icon for a local user account to display the **User Details** page.
3. Click the trashcan, and then click **OK** to confirm the deletion.

Add an Active Directory User

1. In the **Console Access** list, click the **Users** tab.
2. Click **Add Users**.
3. From the **Add** menu, select **Active Directory**.
4. Select the Active Directory **Forest** and **Domain**.
5. To search in an organizational unit (OU), click **Browse** and select an OU.
6. In the **Search for** box, enter the search criteria for the Active Directory object.
7. Click **Search Active Directory**. Search results are displayed.
8. Select the user or group from the search results and it is added to the **Console Access** list.


ADD USERS

Create Local Users or grant access to Active Directory Users or Groups.

Add
Active Directory × ▾

Forest
two.one.pbsmc × ▾

Domain
one.pbsmc × ▾

 Search in Organizational Unit:

BROWSE

CLEAR

Search for

SEARCH ACTIVE DIRECTORY



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

Add an Active Directory Group

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

1. In the **Console Access** list, click the **Groups** tab.
2. Click **Add Groups**.
3. Select the Active Directory **Forest** and **Domain**.
4. To search in an organizational unit (OU), click **Browse** and select an OU.
5. In **Search for**, enter the search criteria for the Active Directory object.
6. Click **Search Active Directory**. Search results are displayed.
7. Select the group from the search results and it is added to the **Console Access** list.

Assign a Role to a Group

1. In the **Console Access** list, click the **Groups** tab.
2. Select the edit icon for a group to display the **Group Details** page.
3. Select the **Roles** tab.
4. 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 49.

Delete an Active Directory User or Group

1. In the **Console Access** list, click the **Users** or **Groups** tab. The update section is displayed.
2. From the update section, select the user or group and click the trashcan.
3. Click **OK** to confirm the deletion.

Integrate Password Safe with BeyondInsight for Unix & Linux

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](https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/index.htm) 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. This should not have 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 will bypass certificate validation.
4. Click **Test Settings** to ensure the connection works. This is optional.
5. Click **Save Settings**.

Password Safe

Password Safe Server

API Key

RunAs User

Description

☐ Verify certificate

TEST SETTINGS

SAVE SETTINGS

DISCARD

Import Password Safe Managed Accounts

A Password Safe managed account must be imported as a BeyondInsight for Unix & Linux 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 > Credentials**.
2. Click **Add Credential** and select **Import from Password Safe**.

3. Select the managed accounts from the list of results the console can access and click **Import Selected**. The managed accounts can be filtered 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, then choose the **Add/ Edit Password Safe** option for 10.100.10.10 in the **Assets** grid.
 - On the **Local Accounts** tab, select **Add** 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 BeyondInsight for Unix & Linux IP address to the source addresses list.
 - Disable the certificate required option.
 - An API key will be generated when the registration is saved. This key will be 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 BeyondInsight for Unix & Linux:
 - 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 BeyondInsight for Unix & Linux:
 - 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 Privilege Management for Unix and Linux 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 for versions 9.4.5 and later.

To configure Privilege Management for Unix and Linux:

1. In the console, select the **Settings** menu, then click **Integration**.
2. Turn on **Bypass SSL certificate validation** if you do not want to verify certificates.
3. Choose whether to enable or disable **Role entitlement reporting by default**.
4. Choose whether to enable or disable **Prevent role entitlement reporting override**.
5. Upload network or REST key files to the console.



Note: PMUL hosts running 10.1 and above in **Role Based Policy Mode** or Privilege Management for Unix and Linux Basic servers can take advantage of **Entitlement Reporting** to discover who is able to do what, where, and when. Entitlement can be searched by **Run user**, **Run host**, **Submit user**, **Submit host**, and **Commands**. Report levels can be set to provide varying levels of detail, with higher numbers providing more details. Entitlement reporting can be enabled per policy. A default value for reporting can be configured in **Settings**; if enabled, all new role based policies will default 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 will not change the values for existing policies.

Manage Software

View Software Managed by BeyondInsight for Unix & Linux

The **Settings > Software** page details the software managed by BeyondInsight for Unix & Linux. Information includes:

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

Click the refresh icon to update the list.

Upload Software Packages

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



For more information, please see ["Upload Software" on page 9](#).

Privilege Management for Unix and Linux Installation Templates

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

There are templates available that are ready-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 Privilege Management for Unix and Linux Policy Server" on page 24](#).

Create an Installation Template

You can create a custom 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**.

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. Select **Settings > Software**.
2. Click **Manage Installation Templates** in the Privilege Management for Unix and Linux row.
3. Click **Add New Template**.

4. Enter a meaningful name for the template.
5. Select the template options. The template settings are automatically saved.

Add a Directory Service Connection

BeyondInsight for Unix & Linux 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. Click **Test Settings** to ensure the connection between BIUL and the directory service works. This is optional and does not save the settings.
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.

Add SMTP Server Connection

Add SMTP server details if you want to provide local BIUL users access to the **Reset Password** link on the BeyondInsight for Unix & Linux logon page. Using the password reset feature requires a verified email address.

1. Enter the information for the mail server, including: server address, port, and user credentials.
2. Click **Test Settings** to ensure there is a connection to the mail server. This is optional.
3. Click **Save Settings**.



For more information on setting up a local account to use password reset, please see "[Manage BeyondInsight for Unix & Linux Console Access](#)" on page 51.

Manage Privilege Management for Unix and Linux Policies

The **Policy Management** section allows the user to manage creating, updating, and deleting Privilege Management for Unix and Linux policies for the following:

- Sudo
- FIM
- Script Policy
- Role Based Policy
- Privilege Manage for Networks

To manage policies, the user must select the policy server on which the policy resides, and then choose the type of policy they wish to manage. Hosts can be filtered by **Hostname** and **IP Address**. The policy server list is made of known policy servers with working REST connections. If a server is listed in grey, the server has an unsupported version of Privilege Management for Unix and Linux installed and should be upgraded to enable policy management.



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 policies, please see the [Privilege Management for Unix and Linux Administration Guide](#) and the [Privilege Management for Unix and Linux Policy Language Guide](#) at <https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm>.

Role Based vs. Script Based Policies

A Privilege Management for Unix and Linux 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 Policy mode only uses script policies.

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 Policy mode to Role Based mode.



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

To manage policy server mode:

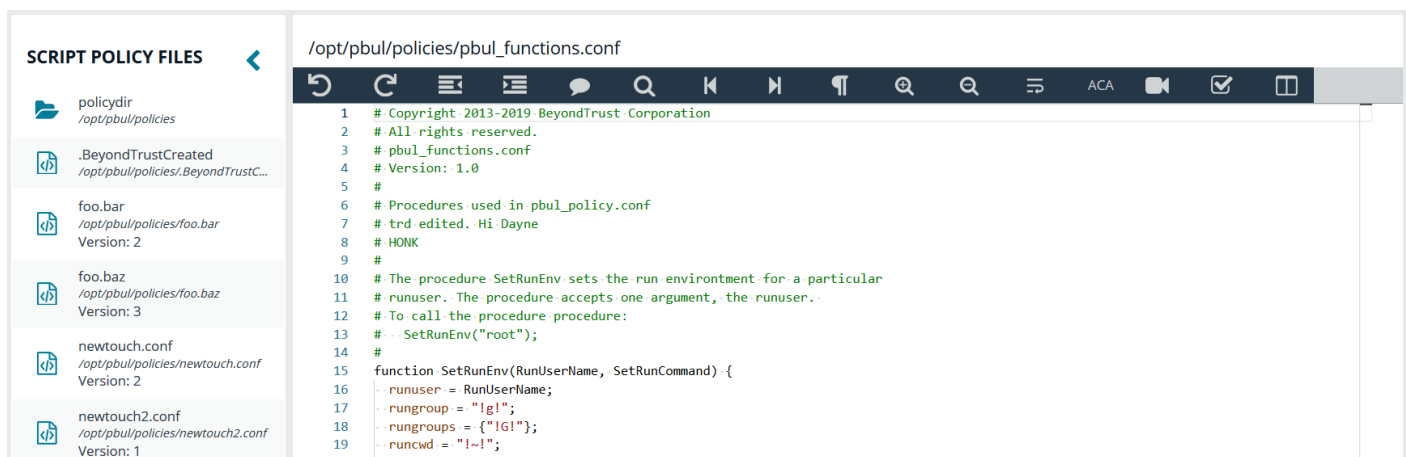
1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry.
3. On the **Server Details** page, select **Quick Actions > Configure Privilege Management for Unix & Linux Settings**.
4. In the **Policy Mode** section, click **Enable Script Based Policy** or **Enable Role Based Policy** to enable the preferred policy mode.

BeyondInsight for Unix & Linux Code Editor

BeyondInsight for Unix & Linux 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.

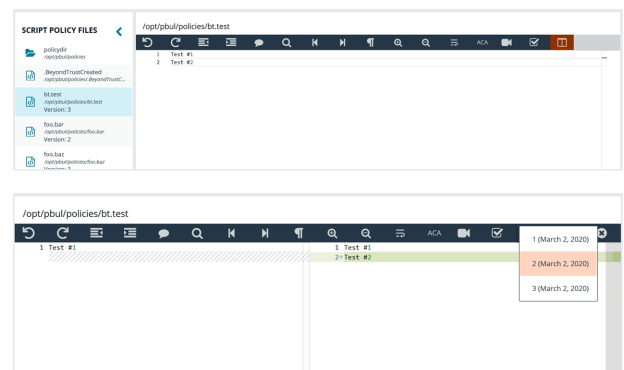


Using the Diff Tool

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, 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 is available to allow the user to choose a specific version to edit.



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

Change Management

BeyondInsight for Unix & Linux 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 Management** page.
2. In the **Hostname** list, select a server entry.
3. On the **Server Details** page, select **Quick Actions > Configure Privilege Management for Unix & Linux Settings**.
4. Click the **Enable Change Management** button.

Change Management

Enabling Change Management will allow you to track file changes across versions of Sudo, Script and Role based Policies.

Note: Once Change Management is enabled, it cannot be disabled

ENABLE CHANGE MANAGEMENT







Manage Privilege Management for Unix and Linux Role Based Policies



Role Based Policy management will be disabled on hosts configured to use Script Based Policy. For more information, please see ["Role Based vs. Script Based Policies"](#) on page 63.

A Privilege Management for Unix and Linux 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 Privilege Management for Unix and Linux role based policy option and an appropriate policy server from the selection lists to load the **Role Based Policy** menu.

ROLES	WHO	WHAT	WHERE	WHEN	BACKUP & RESTORE
					
Roles define core policy behaviour and represent combinations of Users, Hosts, Commands and Schedules to which the policy applies	Users and User Groups determine who the role will be applied to	Command Groups determine which commands will be allowed or rejected	Host Groups determine where the roles will be applied	Schedule Groups determine when the roles will be applied	Backup, restore, or revert to a specific policy version



Note: Fields may be disabled during policy configuration when the options are not available for the installed version of Privilege Management for Unix and Linux.

Entitlement Reporting

You can access the Entitlement Report from a link on the Role Based Policy page.



For more information about the report, please see ["View Entitlement Reports"](#) on page 89.

Manage Role Based Policy Roles

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

ROLES

Enabled

Name

Description

Action

ADD ROLE

Role Order	Enabled	Name	Description	Comment	Action
		devs			Accept
		demo role	simple demo role for demo	this role is to demonstrate the functionality of the RBP editor	Accept
		trd test			Accept

1

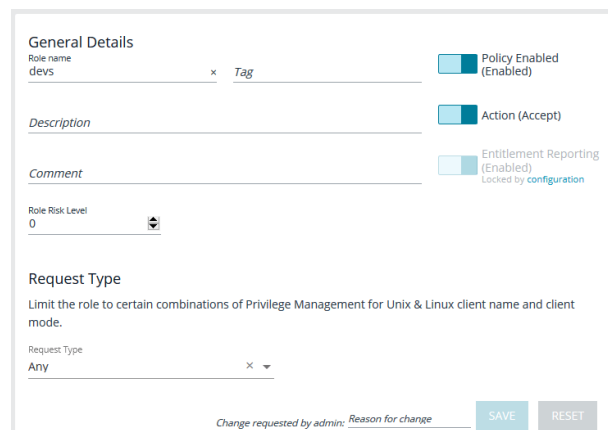
Role Ordering

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 will be saved automatically.

General

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**).



The screenshot shows the 'General Details' form for a role named 'devs'. It includes fields for 'Role name' (devs), 'Tag', 'Description', 'Comment', 'Role Risk Level' (0), and 'Request Type' (Any). On the right, there are three toggle switches: 'Policy Enabled (Enabled)', 'Action (Accept)', and 'Entitlement Reporting (Enabled)'. The 'Entitlement Reporting' toggle is locked by configuration. At the bottom, there are 'SAVE' and 'RESET' buttons, and a note: 'Change requested by admin: Reason for change'.



Note: PMUL hosts running 10.1 and above in **Role Based Policy Mode** or **Privilege Management for Unix and Linux Basic servers** can take advantage of **Entitlement Reporting** to discover who is able to do what, where, and when. Entitlement can be searched by **Run user**, **Run host**, **Submit user**, **Submit host**, and **Commands**. Report levels can be set to provide varying levels of detail, with higher numbers providing more details. Entitlement reporting can be enabled per policy. A default value for reporting can be configured in **Settings**; if enabled, all new role based policies will default 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 will not change the values for existing policies.



For more information on locking the Entitlement Reporting setting, please see "[Configure the Privilege Management for Unix and Linux Integration](#)" on page 59.

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**

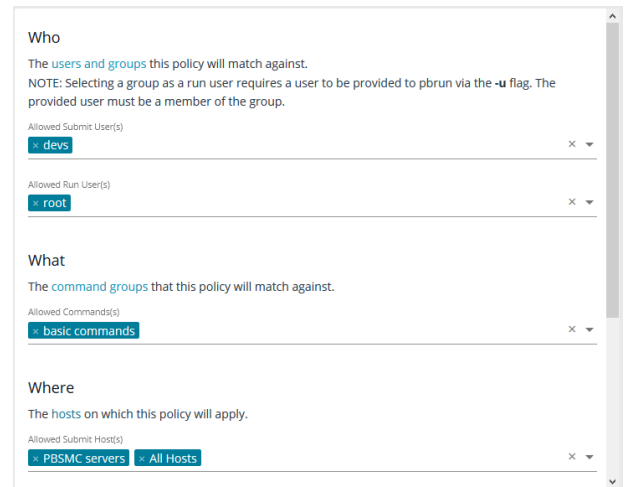
These lists will contain the user entities.

- **What:** Defines which commands the policy applies to. This list will contain the command entities.
- **Where:** Defines which hosts the policy applies to. This item is divided into two user types:

- **Submit Hosts**
- **Run Hosts**

These lists will contain the host entities.

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



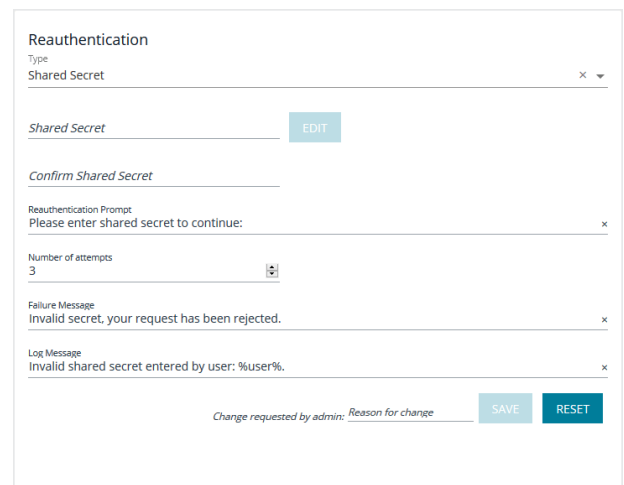
Reauthentication

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.
- **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 enable reauthentication, choose the **Type** from the dropdown menu; this opens an appropriate editor for the selected type.

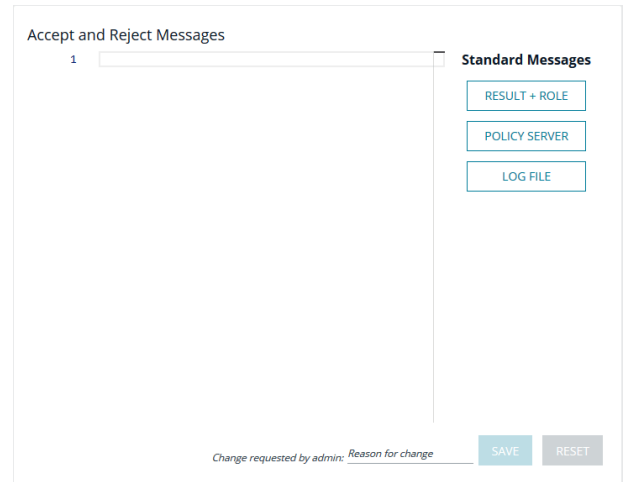
To configure this option:

1. Use the **Type** dropdown to select the desired type of reauthentication. Depending on the selected type, fill in the requested information.
2. Type in a message to prompt the user on how to proceed.
3. Enter the number of retries before reauthentication locks up.
4. Enter the message the user sees if reauthentication fails.
5. Enter the message that is recorded in the log when reauthentication fails.
6. 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.



Accept and Reject Messages

1

Standard Messages

RESULT + ROLE

POLICY SERVER

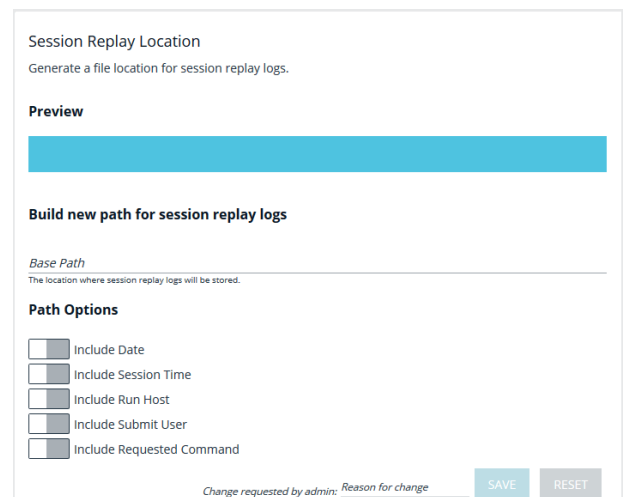
LOG FILE

Change requested by admin: Reason for change

SAVE RESET

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.



Session Replay Location

Generate a file location for session replay logs.

Preview

Build new path for session replay logs

Base Path

The location where session replay logs will be stored.

Path Options

☐ Include Date

☐ Include Session Time

☐ Include Run Host

☐ Include Submit User

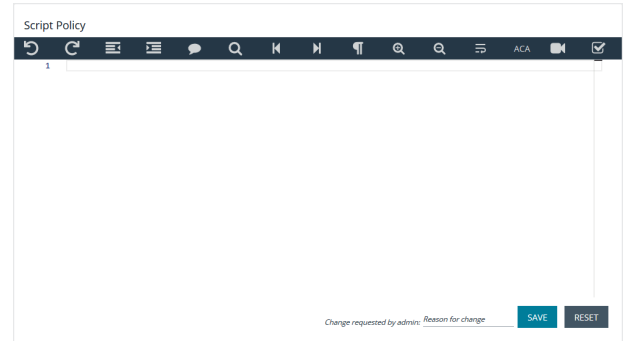
☐ Include Requested Command

Change requested by admin: Reason for change

SAVE RESET

Script Policy

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



Manage Role Based Policy Users and User Groups

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

USERS					ADD USER / GROUP +	
Enabled	Name	Description	User Type	Read Only		
<input checked="" type="checkbox"/>	Administrator		Active Directory	Built-in account for administering the computer/domain		
<input checked="" type="checkbox"/>	Everyone		Secure	All Users	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/>	PBSMC_API		Active Directory			
<input checked="" type="checkbox"/>	PBSMC_CLIENT		Active Directory			
<input checked="" type="checkbox"/>	Steve		Secure			
<input checked="" type="checkbox"/>	TestGroup1		Active Directory			
<input checked="" type="checkbox"/>	TestGroup3		Active Directory			
<input checked="" type="checkbox"/>	abrt		System			
<input checked="" type="checkbox"/>	adm		System			
<input checked="" type="checkbox"/>	audio		System			
<input checked="" type="checkbox"/>	bin		System			



Role Based Policy management will be disabled on hosts configured to use Script Based Policy. For more information, please see ["Role Based vs. Script Based Policies"](#) on page 63.

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.
- **Active Directory:** The users and groups are retrieved from Active Directory. Create a connection to Active Directory on the **Settings > Integration** page.



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

Add a Secure User

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry.
3. Click **Role Based 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.
3. Click **Role Based 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.
3. Click **Role Based 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.
3. Click **Role Based 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.
3. Click **Role Based 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 an Active Directory User or Group

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry.
3. Click **Role Based Policy**.
4. Click **Who**.
5. Click **Add User / Group** and select **Active Directory 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 Active Directory**.
10. Check the box to import Active Directory users or user groups. The imported users or user groups are displayed in the **Users** list.

Remove an Active Directory User or Group

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry.
3. Click **Role Based Policy**.
4. Click **Who**.
5. Select an Active Directory 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.

Manage Role Based Policy Command Groups

Command Groups determine which commands will be allowed or rejected.

COMMAND GROUPS		
Enabled	Name	Description
ADD COMMAND GROUP +		
Enabled	Name	Description
●	basic commands	simple commands for demo
●	smancon	smancon
●	test commands	the group
●	trdtest	

i Role Based Policy management will be disabled on hosts configured to use Script Based Policy. For more information, please see ["Role Based vs. Script Based Policies"](#) on page 63.

Add a Command Group

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry.
3. Click **Role Based 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 will be 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.
3. Click **Role Based Policy**.
4. Click **What**.
5. Select an existing entry from the **Command Groups** list.
6. Click **Delete**.

Manage Role Based Policy Host Groups

Host Groups determine where the roles will be applied.

HOST GROUPS			
Enabled	Name	Description	Read Only
<input checked="" type="checkbox"/>	All Hosts	All Hosts	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	PBSMC servers		
<input type="checkbox"/>	Rob's Servers		
<input checked="" type="checkbox"/>	newhostname	newhostdesc	
<input checked="" type="checkbox"/>	search engines		
<input checked="" type="checkbox"/>	smoists		

i Role Based Policy management will be disabled on hosts configured to use Script Based Policy. For more information, please see ["Role Based vs. Script Based Policies"](#) on page 63.

Add a Host Group

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry.
3. Click **Role Based 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.
3. Click **Role Based Policy**.
4. Click **Where**.
5. Select an existing entry from the **Host Groups** list.
6. Click **Delete**.

Manage Role Based Policy Schedule Groups

Schedule Groups determine when roles will be 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 will start 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.

SCHEDULE GROUPS			
Enabled	Name	Description	Read Only
Any Time	Any Time	Any Time	✓
Hello Schedule	Multiple Configured		
Working Day	Working Day		✓



Role Based Policy management will be disabled on hosts configured to use Script Based Policy. For more information, please see ["Role Based vs. Script Based Policies"](#) on page 63.

Add a Schedule Group

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry.
3. Click **Role Based 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.
3. Click **Role Based Policy**.
4. Click **When**.
5. Select an existing entry from the **Schedule Groups** list.
6. Click **Delete**.

Manage 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**.



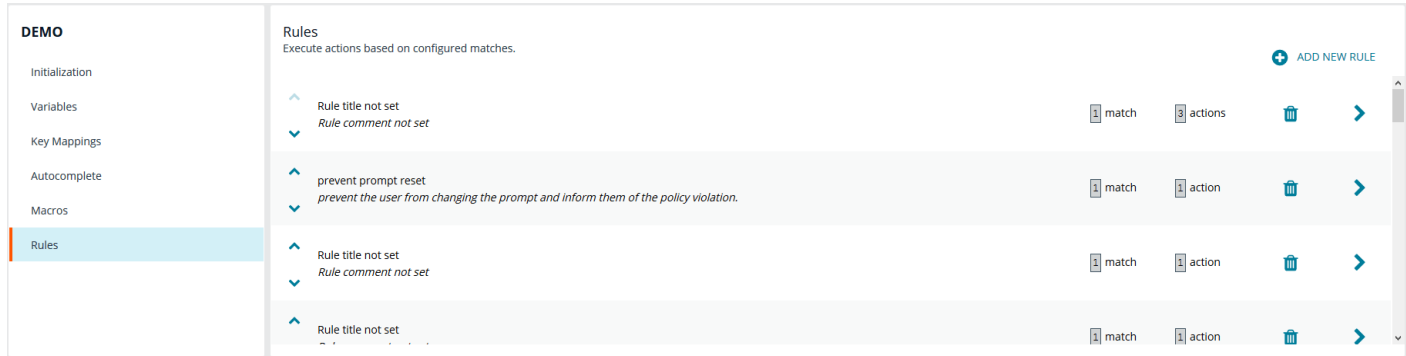
Role Based Policy management will be disabled on hosts configured to use Script Based Policy. For more information, please see ["Role Based vs. Script Based Policies"](#) on page 63.

<p>Backup Role Based Policy Download the Role Based Policy database for later restoration</p> <p>BACKUP ROLE BASED POLICY DATABASE</p>	<p>Restore Role Based Policy Import a Role Based Policy database to restore a previously saved state</p> <p>Drag JSON file to upload (or click to open file browser)</p>	<p>Version Control Restore the Role Based Policy database to a specific version. All roles and group data will be reset to the selected version.</p> <p>Version ▼</p> <p>RESTORE VERSION</p>
---	---	--

Manage Privilege Management for Networks Policies

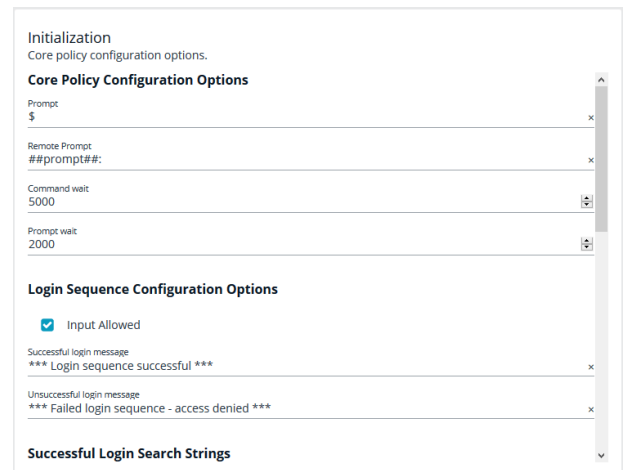
Privilege Management for Networks policy is managed from the **Policy Management > Server Details > Privilege Management for Networks** section. From here, you can add, delete, or clone a policy, as well as configure the settings for Privilege Management for Networks.

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.



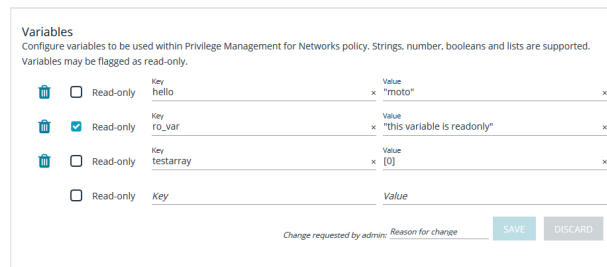
The following configuration options are available:

- 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 into 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**.



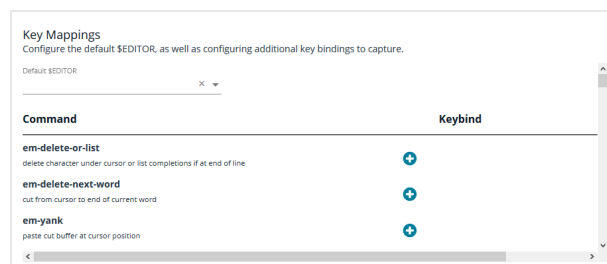
Variables
Configure variables to be used within Privilege Management for Networks policy. Strings, number, booleans and lists are supported. Variables may be flagged as read-only.

	Key	Value
<input type="checkbox"/> Read-only	hello	"moto"
<input checked="" type="checkbox"/> Read-only	ro_var	"this variable is readonly"
<input type="checkbox"/> Read-only	testarray	[0]
<input type="checkbox"/> Read-only	Key	Value

Change requested by admin: Reason for change SAVE DISCARD

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**.



Key Mappings
Configure the default \$EDITOR, as well as configuring additional key bindings to capture.

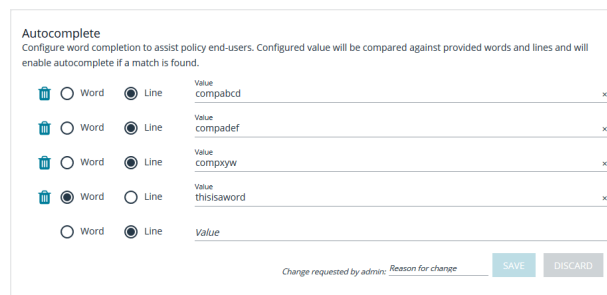
Default \$EDITOR: vi

Command	Keybind
em-delete-or-list delete character under cursor or list completions if at end of line	+
em-delete-next-word cut from cursor to end of current word	+
em-yank paste cut buffer at cursor position	+

X

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**.



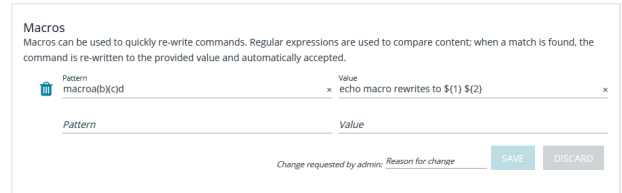
Autocomplete
Configure word completion to assist policy end-users. Configured value will be compared against provided words and lines and will enable autocomplete if a match is found.

	Word	Line	Value
<input type="radio"/> Word <input checked="" type="radio"/> Line			compabcd
<input type="radio"/> Word <input checked="" type="radio"/> Line			compadef
<input type="radio"/> Word <input checked="" type="radio"/> Line			compayw
<input checked="" type="radio"/> Word <input type="radio"/> Line			thisisaword
<input type="radio"/> Word <input checked="" type="radio"/> Line			Value

Change requested by admin: Reason for change SAVE DISCARD

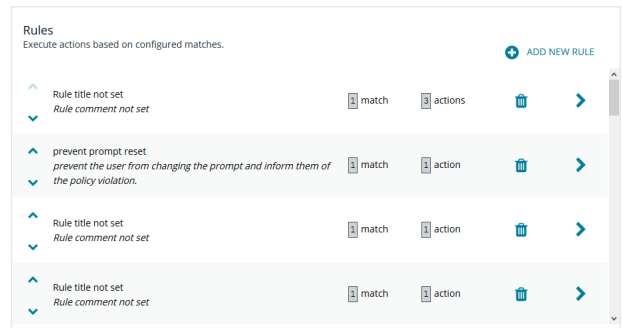
Macros

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**.



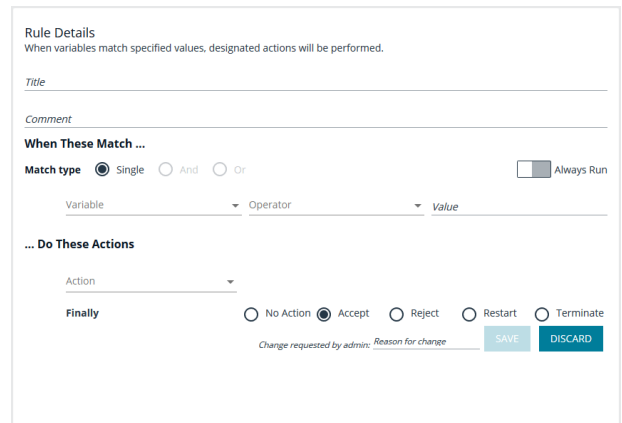
Rules

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

On the **Privilege Management for Networks** page, click **Create New Policy**, enter the **Policy name**, and 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.
3. Click the **Quick Actions** menu and select **Configure Privilege Management for Networks**.
4. Configure the following options:
 - **Password Safe Runfile**
 - **Certificate path**
 - **Password Safe Servers**
5. When the configuration is complete, click **Save**.

Manage Privilege Management for Unix and Linux Basic Policies

Manage Privilege Management for Unix and Linux Basic Policies

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry.
3. Select **Sudo Policy**. A list of available Privilege Management for Unix and Linux Basic policies is displayed.
4. Select a policy file to open for editing. Alternatively, click **Create New Policy** to create a policy.
5. If you are creating a policy, enter a **Hostgroup or Hostname** and **File path**. The file path can be a relative or absolute path. If a relative path is provided, the path will be preceded by **/etc/**.
6. Click **Save** to save the file to the policy server.

Delete a Sudo Policy File

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry.
3. Select **Sudo Policy**. A list of available Privilege Management for Unix and Linux Basic policies is displayed.
4. Select a policy file to open for editing.
5. Click **Delete Policy File**.

Manage Sudo Policy Assignment

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry.
3. Click the **Quick Actions** menu and select **Manage Sudo policy assignment**.
4. Select an **Alias name** from the drop-down menu. If no Alias name has been created, options include **No alias assignment/Use own hostname** and **Create new**.



Note: To create a new alias, select **Alias name > Create new** and enter a value in **Create new Alias**.

5. Use the check boxes to select servers for Sudo alias assignment
6. Click **Apply**.



Note: If you want to remove an **Assigned Sudo Alias**, select the **Alias name** called **No alias assignment/Use own hostname** and apply it to the server.

Manage File Integrity Monitoring (FIM) 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

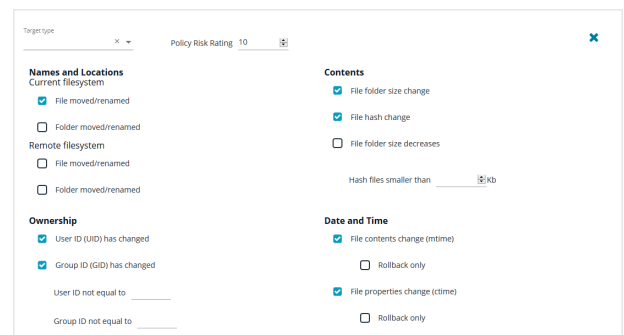
To create a FIM policy:

1. Go to **Policy Management > Server Details > File Integrity Monitoring**.
2. Click **Create New FIM Policy** and enter a name for the policy.
3. Click **Add New FIM Rule** to create a policy definition and enter a **Rule name**.



Note: To delete an 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.

4. Click **Add New FIM Target** to add more targets to the definition.
5. Select a **Target type**, and set attributes you want to monitor.



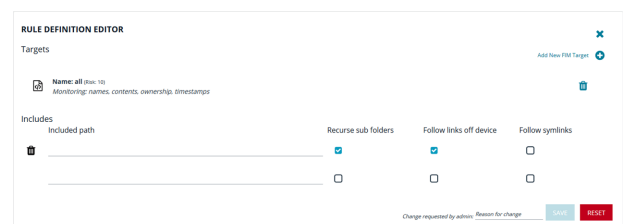
The screenshot shows the 'Rule Definition Editor' for a File Integrity Monitoring (FIM) policy. It features a 'Target type' dropdown menu and a 'Policy Risk Rating' of 10. The editor is divided into several sections for selecting attributes to monitor:

- Names and Locations:** Includes 'Current filesystem' and 'Remote filesystem'. Under 'Current filesystem', 'File moved/renamed' is checked. Under 'Remote filesystem', 'File moved/renamed' and 'Folder moved/renamed' are listed.
- Ownership:** 'User ID (UID) has changed' and 'Group ID (GID) has changed' are checked. There are also fields for 'User ID not equal to' and 'Group ID not equal to'.
- Contents:** 'File folder size change' and 'File hash change' are checked. There is a checkbox for 'File folder size decreases' and a field for 'Hash files smaller than' set to 8kb.
- Date and Time:** 'File contents change (mtime)' is checked. There are checkboxes for 'Rollback only' and 'File properties change (ctime)'.

6. A risk rating value can be assigned. The accepted values are between **1** to **10**. A risk rating weights the severity of the monitored actions configured for the targets.
7. On the **Rule Definition Editor** page, enter **Included path** entries. Optionally, check the boxes:

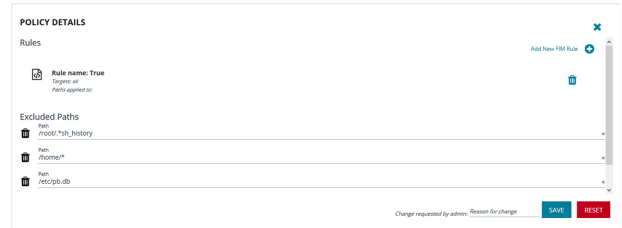
- **Recurse sub folders**
- **Follow symlinks**
- **Follow links off device**

The policy will apply to all files in the path.



This screenshot shows the 'Rule Definition Editor' with the 'Included path' field populated. Below the path field, there are three checkboxes: 'Recurse sub folders' (checked), 'Follow links off device' (checked), and 'Follow symlinks' (unchecked). At the bottom right, there are buttons for 'Cancel' and 'Save', along with a 'Revert for change' link.

- Enter paths that you do not want to monitor in the **Exclude Paths** section.



- 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:

- Go to **Policy Management > Server Details > File Integrity Monitoring**.
- In the **FIM Policies** list, click the trash bin icon on the policy you want to remove and confirm by clicking **Delete**.

Manage FIM Policy Assignment

To manage FIM policy assignment:

- Go to the **Policy Management** page.
- In the **Hostname** list, select a server entry.
- Click the **Quick Actions** menu and select **Manage FIM policy assignment**.
- Select a **Policy name** from the drop-down menu.
- Use the check boxes to select servers for FIM policy assignment.
- Click **Apply**.



Note: If you want to remove an **Assigned FIM Policy**, select the **Policy name** called **No policy assignment** and apply it to the server.

Manage Privilege Management for Unix and Linux Script Policies



Note: Script 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 63.

To manage script policies:

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry.
3. Select **Script Policy**.
4. Select an existing script to open it in the editor. Alternatively, click **Create New Script** and provide a **Filename** to create a script policy.
5. 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.



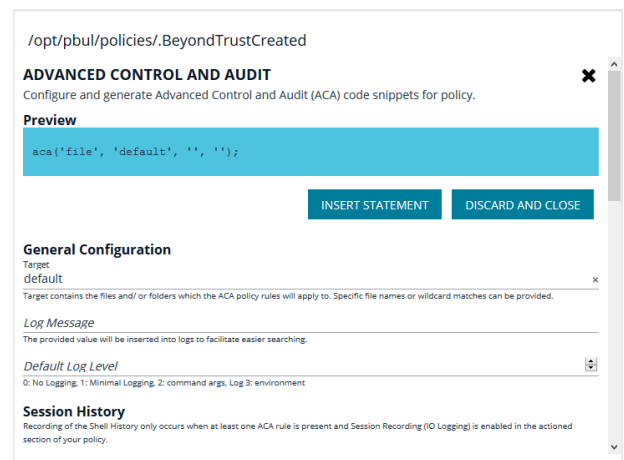
Note: Script policies can reside in either the file system under the folder defined as the **policydir** in Privilege Management for Unix and Linux settings or as objects in the change management database. Files that are in the database support version control. Files that are not in the database can 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 (ACA)

The 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](https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm) at <https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm>.


View Privilege Management for Unix and Linux Settings

1. Go to the **Hosts > Host Inventory** page and select the **View Host Details** menu for a policy server.
2. On the **Host Details** page, select **PMUL Settings**. **Privilege Management for Unix & Linux Settings** are displayed.



Note: Values entered in the **Policy Submit Servers (submitmasters)**, **Policy Accept Servers (acceptmasters)**, and **Log Servers** fields are freely entered and as a result are not verified.

PBSMC-XXXXXXXXXX



Discovered: November 21, 2019

Operating System: Linux CentOS 6.7

Tags:

Last Profiled: 5 days ago

Architecture: x86_64

IP: XXXXXXXXXX

Default Gateway:

[Host Details](#) | [Client Registration Profiles](#)

HOST DETAILS

General
Privilege Management for Unix & Linux
PMUL Settings
Registry Name Service
PMUL Licensing
AD Bridge
Privilege Management for Unix & Linux Basic
Solr
Errors & Warnings

PRIVILEGE MANAGEMENT FOR UNIX & LINUX SETTINGS

REST API Time Correction sets the acceptable time variance between the PMUL and BIUL Host.

REST API Time Correction
60

Policy Submit Servers (submitmasters)
pbsmc-XXXXXXXXXX@XXXXXXXXXX.com x

Policy Accept Servers (acceptmasters)
pbsmc-XXXXXXXXXX x

Log Servers
pbsmc-XXXXXXXXXX x

SAVE

DISCARD

↶

↷

☰

☷

💬

🔍

⏮

⏭

⏪

⏩

🔍

🔍

🔍

🔍

🔍

☑

```

1 # This file was reformatted by pbdutil on 2020/07/13 06:03:06
2
3 ### Global.
4 databasedir ...../opt/pbul/dbs
5 #tempfilepath ...../tmp
6 #lockfilepath ...../opt/pbul/locks

```

Audit Activity Using BeyondInsight for Unix & Linux

On the **Audit** page, you can view event logs, replay IO logs, and leave feedback about IO logs. Hosts can be filtered by **Hostname** and **IP Address**.

View Event Logs in BeyondInsight for Unix & Linux

You can view high level details of a log and search for specific details.

To view event logs:

1. Go to the **Audit** page.
2. In the **Hostname** list, select a server entry.
3. On the **Server Details** page, select **Event Log**.
4. Select a database or logfile from the **Event Source** dropdown menu and filter as necessary.
 - When a database is selected, the following filtering and sorting options apply:
 - Filtering options:
 - **Date Range**
 - **Submit User**
 - **Run Command**
 - **Event Type**
 - **Run Host**
 - **Submit Host**
 - **Run User**
 - Sorting options:
 - **Date/Time**
 - **Submit User**
 - **Run Command**
 - **Event**
 - **Run Host**
 - **Submit Host**
 - **Run User**
 - **Exit Status**
 - When a logfile is selected, the following filtering options apply:
 - Filtering options:
 - **Date Range**
 - **Event Log File**
5. Select a result to view the contents of the event.



Note: As of *Privilege Management for Unix and Linux 10.3*, event log information is retrieved from databases. Previous versions of *Privilege Management for Unix and Linux* support log files.



Note: A minimum version of *Privilege Management for Unix and Linux 10.0* is required to view log contents. In earlier versions, the log must be downloaded to view.

Replay Sessions in BeyondInsight for Unix & Linux

Using session replay, you can view and replay IO logs.

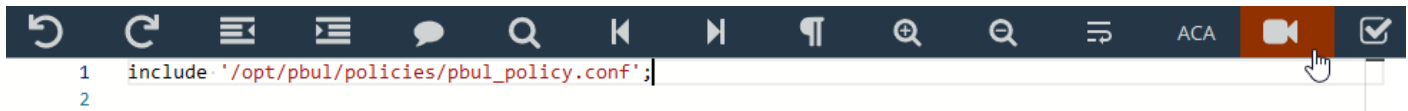
Enable Session Recording in Script Policy Mode

! IMPORTANT!

To turn on session recording, Solr must be installed using BeyondInsight for Unix & Linux and log servers must be assigned to a Solr server. For more information, please see *"Install and Manage Solr" on page 28*.

To turn on session recording in Script Policy Mode:

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry.
3. Select **Script Policy**. The **Script Policy Files** list is displayed.
4. Select a script policy file to edit. The file is displayed in an editor.
5. Select the **Session Replay Path** button from the toolbar.
6. Enter a **Base Path** for the log file.
7. Optionally, configure **Path Options**, such as **Display Warnings** and **Limit Size**.
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.



Enable Session Recording in Role Based Policy Mode

! IMPORTANT!

To turn on session recording, Solr must be installed using BeyondInsight for Unix & Linux and log servers must be assigned to a Solr server. For more information, please see *"Install and Manage Solr" on page 28*.

To turn on session recording in Role Based Policy Mode:

1. Go to the **Policy Management** page.
2. In the **Hostname** list, select a server entry.
3. Select **Role Based Policy**, and then select **Roles**.
4. On the **Roles** page, select a role entry, and then click **Edit**.
5. On the **Edit Role** page, select **Session Replay**.
6. Enter a **Base Path** for the log file.

7. Optionally, configure **Path Options**, such as **Include Requested Command**.
8. Click **Save**.

Play a Recorded Session

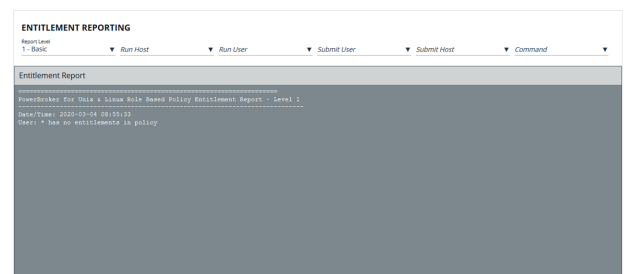
To play an IO log session:

1. Go to the **Audit** page.
2. In the **Hostname** list, select a server entry.
3. On the **Server Details** page, select **Session Replay**. Logs indexed by BeyondInsight for Unix & Linux are displayed.
4. 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 IO log immediately.
 - **Playback**: replays the IO 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 IO Log.
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.

View Entitlement Reports

You can access the Entitlement Report in two places:

- On the **Server Details** page, click **Entitlement Report** to view reports. This feature is enabled from the **Role Based Policy** page.
- On the **Role Based Policy** page. Select **Policy Management > Server Details > Role Based Policy**, and then click **View Entitlement Report**.



For more information, please see "[Manage Privilege Management for Unix and Linux Role Based Policies](#)" on page 66.



Note: PMUL hosts running 10.1 and above in **Role Based Policy Mode** or **Privilege Management for Unix and Linux** Basic servers can take advantage of **Entitlement Reporting** to discover who is able to do what, where, and when. Entitlement can be searched by **Run user**, **Run host**, **Submit user**, **Submit host**, and **Commands**. Report levels can be set to provide varying levels of detail, with higher numbers providing more details. Entitlement reporting can be enabled per policy. A default value for reporting can be configured in **Settings**; if enabled, all new role based policies will default 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 will not change the values for existing policies.

Manage Credentials in BeyondInsight for Unix & Linux

On the **Hosts > 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 55](#).

Add Credentials

On the **Credentials** page:

1. Select **Add Credential**.
2. Click **Create Credential**.
3. Enter the following required information:
 - **Username**
 - **Description**
 - **Password**
 - **Confirm Password**
4. Click **Save**.

Update Credentials

On the **Credentials** page:

1. In the **Credentials** list, select the credential to be updated. The **Update Credential** section is displayed.
2. Update any of the below 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. The **Update Credential** section is displayed.
2. Select **Delete Credential** and confirm by clicking **OK**.

View Tasks and Task Details in BeyondInsight for Unix & Linux

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. In the console, select **Tasks** from the menu.
2. Select a task. A **Task Summary** is displayed.
3. From the **Task Summary**, click the **View Task Details** button.

TASKS

Task Type

Date Range

Username

Pending Status

Success Status

Failure Status

Type	Tasks	Pending	Succeeded	Failed	Username	Updated
Profile	22	0	18	4	admin	a day ago
Profile	3	0	3	0	admin	a day ago
Profile	2	0	0	2	admin	5 days ago
Profile	2	0	2	0	admin	8 days ago
Profile	2	0	2	0	admin	8 days ago
Profile	21	0	17	4	admin	13 days ago

1

2

3

4

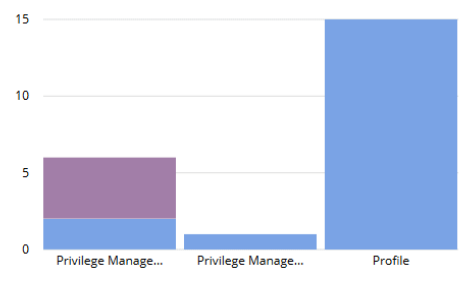
5

6

7

1 - 25 of 171 items

TASK SUMMARY



Task Status

Pending

Succeeded

Failed

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.

TASK DETAILS

✓ ~\$ Profile - pbsmc-centos6-01.one.pbsmc

Profile on 172.20.31.101 was successful.
Local PBSMC pb.key file checksum did not match checksum on host.
Local REST pb.key file checksum did not match checksum on host.

✓ ~\$ Profile - pbsmc-centos6-02.bash

Profile on 172.20.31.102 was successful.

✓ ~\$ Profile - pbsmc-centos6-03.one.pbsmc

Profile on 172.20.31.103 was successful.
Local PBSMC pb.key file checksum did not match checksum on host.
Local REST pb.key file checksum did not match checksum on host.

✓ ~\$ Profile - pbsmc-centos6-04.unix.symark.com

Profile on 172.20.31.104 was successful.
Local PBSMC pb.key file checksum did not match checksum on host.
Local REST pb.key file checksum did not match checksum on host.
Could not get RMUL REST API status. Creating new REST key.

✓ ~\$ Profile - pbsmc-centos6-05.unix.symark.com

Profile on 172.20.31.105 was successful.
Local PBSMC pb.key file checksum did not match checksum on host.
Local REST pb.key file checksum did not match checksum on host.
ERROR: Warning -- unexpected output: ER80[2020-03-03T11:01:48-08:00] Error deleting temp settings file err="remove /tmp/settings893546727: no such file or directory" file=/tmp/settings893546727

Troubleshoot Common Issues with BeyondInsight for Unix & Linux

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" on page 8](#).

Unable to install PMUL, AD Bridge, or PMUL Basic



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.