BeyondTrust

BeyondInsight for Unix & Linux 22.3 Installation Guide

TC:2/2/2023

Table of Contents

BeyondInsight for Unix & Linux Installation Guide

This guide provides system administrators and security administrators the information to install and configure BeyondInsight for Unix & Linux.

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
Solr (formerly PowerBroker Solr)	Solr
File Integrity Monitoring	FIM
Advanced Control and Audit	ACA
Role Based Policy	RBP

Overview

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, 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, 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:** The first stage of adding any remote hosts to be managed by the console. Hosts available by SSH are added.
- **Hosts Inventory:**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, 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:** Manage Privilege Management for Networks, FIM, and role-based and script-based policies on Privilege Management for Unix and Linux policy servers.
- **Audit:** View, replay, and audit Privilege Management for Unix and Linux events and I/O logs. I/O logs can be replayed as they occur. Users can add comments on the logs. Query and view PMUL and AD Bridge events that have been exported to an external SIEM.
- **License Management:** View and manage license information for Privilege Management for Unix and Linux.
- **Tasks:** View details about results and status of any remote actions performed by the console.
- **Settings:** Configuration settings available to the end user, including integration settings for products like Password Safe.
- **Notifications:** Users with the software administrator role can view notifications that are triggered when given conditions arise within BIUL. The notification details provide options for remediation of the condition.

For information on the use of BeyondInsight for Unix & Linux, see the BeyondInsight for Unix & Linux User Guide at https://www.beyondtrust.com/docs/privilege-management/console/beyondinsight-unix-linux/user/index.htm.

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

Supported Database Versions

The standard Microsoft SQL Server scenario is set up on a U-Series Appliance. The following database versions and platforms are compatible for the BIUL database:

- Microsoft SQL Server 2014, 2016, and 2019
- SQLite versions 3.7.17 to 3.37

> ***Note:*** *The only MS SQL Server configuration that has been tested and approved is with SQL Server running on the same machine as the BIUL installation, which is the standard UVM Appliance setup. Running MS SQL Server on a separate, dedicated database server is not supported.*

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, and AD Bridge 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, and AD Bridge installers.

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

AD Bridge

Windows:

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

Unix and Linux:

/usr/local/bin/software/pbis/

Privilege Management for Unix and Linux

Windows:

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

Unix and Linux:

/usr/local/bin/software/pmul/

Solr

Windows:

C:\Program Files (x86)\BeyondTrust\PBSMC\software\Solr

Unix and Linux:

/usr/local/bin/software/solr/

Upload Software

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

> ***Note:*** *You cannot upload software on the BeyondTrust U-Series 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.

Configure BeyondInsight for Unix & Linux

You can customize the console using the **pbsmc.toml.default** file located in:

- Linux: **/etc/pbsmc**
- Windows: **%ProgramFiles%\PBSMC**

First, you must create a copy of the file using the name **pbsmc.toml**. You can include only the settings that you want to customize.

The BIUL API uses a markup language called **TOML** that is hierarchical. The settings are divided into *sections* and *keys*. 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.*

You can configure the following settings.

Database

By default, the console creates a SQLite database in **/etc/pbsmc/pbsmc.sqlite** on Linux, or in **%ProgramFiles%\pbsmc** on Windows. This can be changed to another location.

```
[database]
dialect="sqlite3"
url="./pbsmc.db"
```

dialect

Default: sqlite3

The *dialect* key allows a user to specify what type of database BIUL will connect to.

url

Default: The default is OS specific, but maps to using an sqlite database file with the following config:

```
pbsmc.db?cache=shared&mode=rwc&_busy_timeout=9999999999999999
```

The url is a key that will allow a user to provide connection information to our database driver.

Example: *MSSQL URLstyle*

```
sqlserver://sa:Hello2018@pbsmc-sqlserver:1433?database=pbsmc
```

Example: *MSSQL ADO Style*

```
server=pbsmc-sqlserver;user id=sa;password=Hello2018;port=1433;database=pbsmc
```

Example: *sqlite*

```
etc/pbsmc/pbsmc.db?cache=shared&mode=rwc&_busy_timeout=9999999999999999
```

Server

By default, the console runs on port **4443**. Before changing this value, stop the service.

```
[server]
disabled=false
port=":4443"
softwarepath="/usr/local/bin/software"
uploads="/tmp/pbsmcUploads"
passwordcost=14
```

port

Default: :4443

The port that BIUL listens for connections on.

disabled

Default: false

A setting to disable BIUL from attempting to initialize.

softwarepath

Default: ""

The path to where installers are stored on disk.

uploads

Default: An OS specific folder where uploads are temporarily stored until they can be moved to the softwarepath.

passwordcost

Default: 14

The bcrypt cost factor for hashing passwords. Values less than 12 use 12. Values greater than 20 use 20.

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.toml** configuration file. A custom certificate pair may also be provided and placed in the configuration file.

```
[ssl]
enabled=true
cert="/usr/local/bin/cert.pem"
key="/usr/local/bin/key.pem"
```

enabled

Default: true

Whether to use TLS 1.2+ to secure connections to BIUL or not.

cert

Default: unset

The location on disk to use as the public key/cert for encrypting communications.

If *key* and *cert* are provided, key pairs stored in the database are not used.

key

Default: unset

The location on disk to use as the private key for encrypting communications.

If *key* and *cert* are provided, key pairs stored in the database are not used.

Worker 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 has the opposite effect.

```
[pool]
size=20
```

size

Default: 20

The number of workers that are allowed to operate performing remote actions simultaneously.

Logging

The logging level configuration.

```
[logging]
loglevel="info"
maxage=365
maxsize=10
```

loglevel

Default: info

The level of logging to write to disk.

maxage

Default: 365

The maximum age of rotated log files. When a logfile is rotated it has the timestamp of when it was rotated added to the logfile's name. Any logfiles that are more than **maxage** days old when the next file is rotated are deleted.

If a logfile happens to be rotated every 10 days, then it is possible for a logfile to exist on disk for more than 365 days.

If set to zero (0), old logfiles are not deleted.

maxsize

Default: 10

The size of a logfile in number of megabytes before the log is rotated.

If set to zero (0), the logfile is not rotated.

Encryption 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.

```
[keys]
active="abcdefg"
revoked= [
    "abcd",
    "efgh"
]
known = [
    "abcde",
    "fghij"

]
```

active

Default: unset

This is the key that is used to encrypt all secrets in the database. If not provided it is created and the settings file mutated.

revoked

Default: dYFnQ8eNHRTnqRahhqwbpizzrEQVK7LK, 8vkb8JJgWRy5h1C421zy2q0sS7i2mdw2

This is a list of keys that are no longer active; any secrets that are encrypted with the keys should be re-encrypted with the **active** key.

known

Default: unset

This is a list of keys that BIUL uses to decrypt secrets. **known** is used as a step in the process of rolling a key. In the event of a cluster of BIUL servers, it is necessary to synchronize keys to all servers before the process of re-encrypting all secrets occurs.

This allows a key to be known by all servers, then you can update **active** to the new key, potentially moving an old key to **revoked**, and then begin the process of moving other servers to update their **active** key to the new key.

This allows all secrets to be readable by all servers.

IMPORTANT!

You must restart the service to apply changes.

SSH Cipher and Key Exchange Configuration

```
[ssh]
ciphers=[
  "aes128-ctr",
  "aes128-gcm",
  "aes128-cbc"
]
```

```
key_exchanges=[
  "curve25519-sha256",
  "ecdh-sha2-nistp256",
  "ecdh-sha2-nistp384"
]
```

ciphers

Default: a list containing the values **aes128-gcm**, **chacha20-poly1305**, **aes128-ctr**, **aes192-ctr**, **aes256-ctr**

This is used to configure the list of allowed ciphers to be used while connecting to remote hosts.

Supported values:

- aes128-ctr
- aes192-ctr
- aes256-ctr
- aes128-gcm
- chacha20-poly1305
- arcfour256
- arcfour128
- arcfour
- aes128-cbc
- 3des-cbc

key exchanges

Default: a list containing the values **curve25519-sha256**, **ecdh-sha2-nistp256**, **ecdh-sha2-nistp384**

This is used to configure the list of allowed key exchange algorithms used to secure the initial connection to remote hosts.

Supported values:

- curve25519-sha256
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521
- diffie-hellman-group14-sha1
- diffie-hellman-group1-sha1
- diffie-hellman-group-exchange-sha256
- diffie-hellman-group-exchange-sha1

Scrypt

Increasing the value of the parameters makes it more difficult for an attacker to crack a given password, but that increase in security slows down the login process for a legitimate user.

IMPORTANT!

Unless you fully understand the implications of adjustments to the parameters below, we recommend using the default parameters. For help with this specific configuration, contact BeyondTrust Support at support.beyondtrust.com.

```
[scrypt]
N-65536
r=8
p=1
```

N

Default: 65536

The *CPU/Memory cost* parameter. N is the most commonly adjusted parameter. N is the main factor governing how much memory the algorithm uses.

Value for N must be:

- Greater than 1
- A power of 2
- Less than 2^(128*r/8)

r

Default: 8

The *block size* parameter.

Value for r must be greater than 0.

p

Default: 1

The *degree of parallelism* parameter.

Value for p must be greater than 0.

Run BeyondInsight for Unix & Linux after Installation

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

IMPORTANT!

If the wizard starts and this is not the first time the console has been run, do not go through the wizard again. All data in the system will be lost. Contact BeyondTrust Technical Support.

Set Up the Console Using the First Run Wizard

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

Configure BeyondInsight for Unix & Linux

The following sections match the layout of the First Run Wizard in BeyondInsight for Unix & Linux. Please follow along for assistance with BIUL's initial configuration and setup.

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

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

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

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.