BeyondTrust

AD Bridge 9.1

Windows Administration Guide

Table of Contents

Introduction

This guide shows system administrators and security administrators how to use BeyondTrust AD Bridge Enterprise Edition.

Use the BeyondTrust Management Console

You can use the console to do the following tasks:

- Run multiple instances of the console and point them at different domains.
- Run the console with a different user account.
- Upgrade your Active Directory schema.
- Obtain status information about your Active Directory forests and domains.
- Migrate Unix and Linux users and groups by importing **passwd** and **group** files and mapping the information to users and groups in Active Directory.
- Remove orphaned objects.
- Generate reports about users, groups, and computers.
- Start **Active Directory Users and Computers (ADUC)**, **Cell Manager**, and the **Migration** tool.

Start the BeyondTrust Management Console

Depending on the options chosen during installation, the console can be started in the following ways:

- Double-click the **BeyondTrust Management Console** shortcut.
- Click **Start > All Programs > BeyondTrust AD Bridge > BeyondTrust Enterprise Console**.
- At the command prompt, execute the following commands:

```
cd %ProgramFiles%\BeyondTrust\PBIS\Enterprise\iConsole.bmc
```

After you start the console, you can navigate to all other pages in the console, including the **BeyondTrust AD Bridge Status** page.
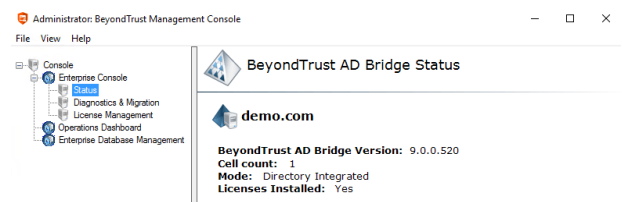
The **BeyondTrust AD Bridge Status** page displays the following information for the selected Active Directory forest. After you start the console, it may take a few moments to retrieve information about your domains.

- **BeyondTrust AD Bridge Version**: The AD Bridge Enterprise version and build number. BeyondTrust technical support personnel may ask you for this information when you contact them for assistance.
- **Cell count**: Displays the number of cells that are associated with organizational units in the selected domain, including the default cell.
- **Mode**: Either Directory Integrated or Schemaless. Directory Integrated indicates that the selected forest is using the RFC 2307-compliant schema. Schemaless indicates that it is not.
- **Licenses Installed:** Indicates if valid product licenses are deployed.

Connect to a Domain

If AD Bridge Enterprise detects more than one Active Directory forest, it displays them on the AD Bridge Enterprise Status page. You can connect to a forest by double-clicking the forest name.

You can connect to another domain as follows:

1. In the **BeyondTrust Management Console** tree, right-click the **Enterprise Console** node, and then click **Connect to Domain**.
2. Enter the FQDN of the domain that you want to connect to.
3. Enter the credentials of an Active Directory administrator.

Changes Made by the Directory Integrated Mode Configuration

The Active Directory schema changes are applied from a set of LDAP Data Interchange Format (LDIF) files. The standard installation places these files in the following directory: **\Program Files\BeyondTrust\PBIS\Enterprise\Resources\LDF**.

After you raise the domain and forest to 2003 functional levels, the AD Bridge Enterprise domain configuration wizard changes the following attributes, which are required for AD Bridge Enterprise to run in Directory Integrated mode.

Promotes and indexes the following attributes to the global catalog:

- **displayName**
- **gidNumber**
- **uid**
- **uidNumber**

Promotes (but does not index) the following attributes to the global catalog:

- **gecos**
- **loginShell**
- **unixHomeDirectory**

Replication in a Large Forest or in Multiple Domains

When you set up AD Bridge Enterprise in an environment with a large forest or multiple domains, it may take some time for the AD Bridge Enterprise objects and the schema update to replicate to the rest of the domain.

Replication must complete before the domain and its child domains are fully enabled for AD Bridge Enterprise. You will be unable to connect to a child domain until replication finishes.

Add a Plug-In

The console includes several plug-ins: **Access and Audit Reporting**, **Enterprise Database Management**, and the **Operations Dashboard**.

1. In the console, on the **File** menu, click **Add/Remove Plug-in**.
2. Click **Add**.
3. Click the plug-in that you want, and then click **Add**.
4. Click **Close**, and then click **OK**.

Work with Cells

You can use the following tools to manage your AD Bridge cells:

- **Active Directory Users and Computers:** An **AD Bridge Cell Settings** tab is added to the dialog box of the following objects in the Active Directory Users and Computers MMC snap-in:
    - Domain
    - Users
    - Groups
    - Organizational Units
- **Cell Manager: Cell Manager** is an AD Bridge Enterprise MMC snap-in for managing your AD Bridge cells. **Cell Manager** is installed when you install the BeyondTrust Management Console.

The AD Bridge Active Directory Users and Computers snap-in can work without cells. The plug-in can manage the RFC2307 attributes on users and groups without using a cell. In this case, a default cell is assumed. The **AD Bridge Cell Settings** tab will display **(Default (Assumed))**.

> ℹ️ For more information, please see "Use the btopt.exe Tool" on page 69

> 📌 *Note: Ensure the account you use to manage AD Bridge cell properties is a member of the **Domain Admins** group or **Enterprise Admins** group. The account needs privileges to create and change objects and child objects in Active Directory.*

Understand AD Bridge Cells

An AD Bridge cell is a container of Unix settings for Active Directory users and groups so they can log into Linux, Unix, and macOS computers.

For each user, the settings include a Unix user identifier (UID), the group identifier (GID) of the primary group, a home directory, and a login shell.

You can use cells to map a user to different UIDs and GIDs for different computers.

Review the details in this section to learn more about how cells work.

Types of Cells

There are two types of AD Bridge cells:

- **Default cell:** A cell associated with a domain or an entire enterprise. In a multi-domain topology, you create a default cell in each domain, and these domain-specific default cells merge into an enterprise-wide default cell.
- **Named cell:** A cell associated with an organizational unit (OU). Associating cells with OUs is a natural way to organize computers and users.

AD Bridge Enterprise lets you define a default cell that handles mapping for computers that are not in an OU with an associated named cell. The default cell for the domain can contain the mapping information for all your Linux and Unix computers. If you use Directory Integrated mode, various attributes are indexed in the global catalog by using the default cell.

In a multi-domain or multi-forest enterprise, the default cells of the domains merge into a single enterprise-wide default cell where users from each domain can authenticate with their credentials. Users' UIDs, GIDs, and other settings are defined separately in each domain, but nothing additional is needed at the domain-level to enable the user to authenticate.

Each forest that has a two-way transitive forest trust with the computer's forest is listed in the default cell. Each domain in each forest can opt in to this enterprise-wide default cell by creating a default cell in that domain. Any user who is listed in the default cell in a domain can be seen by the AD Bridge Enterprise-enabled operating system of any computer joined to the default cell.

How Cells Are Processed

AD Bridge Enterprise Searches Active Directory for Cell Information

When an Active Directory user logs on to an AD Bridge Enterprise client computer, the AD Bridge Enterprise agent searches Active Directory for the user's AD Bridge cell information.

The search typically begins at the node where the computer is joined to Active Directory and can extend to all forests that have a two-way transitive trust with the client computer's forest.

AD Bridge Enterprise Agent Checks the Cell Type

The AD Bridge Enterprise agent determines the OU where the computer is a member and checks whether a named cell is associated with it.

AD Bridge Enterprise Agent Continues Search If No Cell Found for the OU

If a cell is not associated with the OU, the AD Bridge Enterprise agent on the Unix or Linux computer moves up the directory structure, searching the parent and grandparent OUs until it finds an OU that has an AD Bridge cell associated with it.

Named cell found

If a named cell is found, AD Bridge Enterprise searches for a user or group's attributes in the cell associated with the computer.

If an OU with an associated cell is not found, the AD Bridge Enterprise agent uses the default cell for the domain to map the username to UID and GID information.

Default Cell Processing

A default cell is processed differently than a named cell. When processing a default cell, AD Bridge Enterprise searches for a user or group's attributes in the default cell of the domain where the user or group resides. For example, a two-domain topology configured with one domain for users and another domain for computers would require two default cells:

- a default cell in the domain where user and group objects reside
- a default cell in the domain where computer objects are joined

A Linux or Unix computer can be a member of an OU that does not have a cell associated with it. In such a case, the Group Policy Objects (GPOs) associated with the OU apply to the Linux or Unix computer, but user UID and GID mappings follow the policy of the nearest parent cell or the default cell.

AD Bridge Enterprise does not require you to have a default cell, but for AD Bridge Enterprise to operate properly you must ensure that the AD Bridge Enterprise agent can always find a cell.

> ℹ️ For more information about modes, cells, and user rights, please see the AD Bridge Best Practices Guide at https://www.beyondtrust.com/docs/ad-bridge/documentation.htm.

Cell Design

AD Bridge cell technology allows managing overlapping Unix identities in a single Active Directory organization for AD Bridge Enterprise. Cells work in **Directory Integrated** or **Schemaless** mode. Cells do not work with **ID Range**.

Storing Unix Identities

Cells store Unix identity information separate from other cells. This allows a single user or group to have different names or different numerical ID values (UID or GID) in different environments, all associated with the same AD identity.

This also allows multiple users or groups to have overlapping names or numerical ID values (UID or GID) in separate environments. Each cell requires additional overhead for the standard procedure for account management and for troubleshooting end-user logon issues, because both cases require the additional step of determining which cell the operation must be performed against.

> 💡 **Tip:** *To minimize complexity while allowing the flexibility of cells, we recommend that you use no more than four cells.*

Named Cells

Named Cells store Unix identity information (**uid**, **uidNumber**, **gidNumber**, **gecos**, **unixHomeDirectory**, **logonShell**) in a subcontainer of the organizational unit (OU) which is associated with the cell.

Whether a user exists in the local domain or a trusted domain, the Unix identity information exists in an object in the cell. In other words, a Named Cell can reference users or groups from outside the current AD domain.

Default Cells

Default Cell mode refers to how an AD domain is set up. There is one Default Cell, and it is enterprise-wide. All trusted Microsoft Active Directory Global Catalogs are part of the Default Cell. However, individual AD domains participate in the Default Cell by creating the Default Cell object in the root of those domains.

In Default Cell mode, the Unix identity information is stored in the same OU as the user object that the Unix Identity information is related to. This enforces a single Unix identity for a single AD user across the entire enterprise. Therefore, the Default Cell should be viewed as the ultimate authority for Unix information within an enterprise.

Directory Integrated Mode - Default Cell Configurations

In Directory Integrated mode, the Default Cell stores the Unix identity information directly to the user or group object in the same manner as "First Name" (givenName), "Address" (address, city, state), and "Email" (emailAddress) attributes.

Because the Directory Integrated Mode - Default Cell stores the information to the user or group object, existing Identity Management (IDM) products do not need to be modified to provision users for the Default Cell in Directory Integrated Mode. This also allows non-AD Bridge Enterprise computers that use the RFC 2307 attributes (such as Network Appliances ONTAPP Filers and EMC Celerra storage devices) to use the same identity information as AD Bridge Enterprise.

Directory Integrated Mode - Default Cell is the preferred method for all AD Bridge Enterprise installations. In all cases where Unix identity information can be made to be non-overlapping, the Directory Integrated Mode - Default Cell should be used.

Directory Integrated Mode - Named Cell Configurations

In Directory Integrated mode, Named Cells create objects of class **PosixAccount** and **serviceConnectionPoint**, which are linked back to the user or group object associated with the AD Bridge Enterprise object.

Directory Integrated Mode - Named Cells are recommended wherever multiple cells beyond the Default Cell are required.

Schemaless Mode Cells

Schemaless mode is deprecated.

The AD Bridge Enterprise clients determine cell and schema configuration at startup and re-check this configuration periodically. Because of how the data is stored, migration from a Schemaless Default Cell to a Directory Integrated Mode - Default Cell configuration requires more work, more steps, and more potential risks than any other cell migration.

For migration and long-term support purposes, Schemaless Mode Cells should only be created as Named Cells.

> *Note: Directory Integrated mode is preferred for the performance benefits and because Microsoft Active Directory is moving towards Directory Integrated Mode by default.*

Use Multiple Cells

If you have multiple Unix and Linux computers but are not using a centralized scheme to manage UIDs and GIDs, it is likely that each computer has unique UID-GID mappings. You may also have more than one centralized IMS, such as multiple NIS domains. You can use multiple cells to represent the UID-GID associations that the NIS domain provided, allowing those Unix and Linux users to continue to use their existing UID-GID information while using Active Directory credentials.

When using multiple cells, it can be helpful to identify what Unix and Linux objects each cell represents. For example:

- Individual Unix, Linux, or macOS computers
- A single NIS domain
- Multiple NIS domains (which require multiple cells)

Assign Users to Manage Cells

If you want to assign users to help manage AD Bridge cells, ensure the users have the permissions to create container objects in an OU.

> For more information about delegating control, please see [Delegating administration](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778807(v=ws.10)) at https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778807(v=ws.10).

1. In **Active Directory Users and Computers**, right-click an OU, and then select **Delegate Control**.
2. Go through the **Delegation of Control** wizard, and ensure the following permissions are selected:
   - **Read**
   - **Write**
   - **Create All Child Objects**
   - **Delete All Child Objects**

- **Read All Properties**
- **Write All Properties**

3. Click **Finish**.

Assign Users to Manage UNIX Attributes in Directory Integrated Mode

This section applies to AD Bridge administrators that are working in an AD Bridge Directory Integrated - Default Cell mode environment.

> 📌 *Note: In a Named Cell environment, you can use the **Delegation of Control** wizard accessible from the **Cell Manager**.*

1. In **Active Directory Users and Computers**, right-click the OU, and then select **Properties**.
2. Select the **Security** tab.
3. Click **Advanced**, and then click **Add**.
4. Select **Select a Principal**.
5. Select the user or group that you are delegating permissions to, and then click **OK**.
6. From the **Type** menu, select **Allow**.
7. From the **Applies to** menu, select the object type that the permissions will apply to.
8. Go through the list of properties and select the UNIX attributes:

> ℹ️ For a list of the required properties, please see Provision User Accounts and Provision Group Accounts.
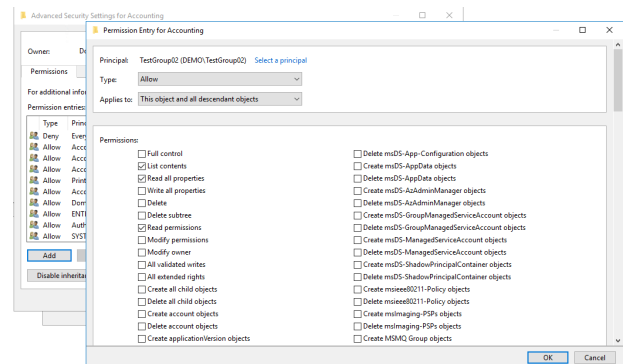
9. Click **OK**.

Provision User Accounts

When provisioning UNIX user accounts, AD Bridge administrators must be able to manage the following RFC2307 attributes:

- **displayName**
- **GECOS**
- **gidNumber**
- **loginShell**
- **uidNumber**
- **uid**
- **unixHomedirectory**

Provision Group Accounts

When provisioning UNIX groups, AD Bridge administrators must be able to manage the following RFC2307 attributes:

- **description**
- **gidNumber**
- **displayName**. You must set the permission in **adsiedit.msc**.

Create a Cell and Associate it with an OU or a Domain

To associate a cell with an OU, for example, you must be a member of the Domain Administrators security group, or you must be assigned permissions to manage container objects in an OU.

> (!) **IMPORTANT!**
>
> *Before you associate a cell with an OU, make sure you chose the schema mode. You cannot easily change the schema mode after you create a cell, including a default cell.*

1. Start **Active Directory Users and Computers**.
2. In the console tree, right-click the OU or the domain for which you want to create a cell, click **Properties**, and then click the **AD Bridge Cell Settings** tab.
3. Under **AD Bridge Cell Information**, select the **Create Associated AD Bridge Cell** check box, and then click **OK**.

You can now associate a user with cells.

> (i) For more information, please see Associate a User with Cells.

Create a Default Cell

You can create a default cell that maps computers that are not in an OU with an associated cell. The default cell can contain the mapping information for all your Linux and Unix computers. AD Bridge Enterprise does not require a default cell.

A Linux or Unix computer can be a member of an OU that does not have a cell associated with it. In such cases, the group policies associated with the OU apply to the Linux and Unix computer, but user UID-GID mappings follow the policy of the nearest parent cell, or the default cell.

To create a default cell:

1. Start **Active Directory Users and Computers**.
2. Right-click the name of your domain, and then select **Properties.**

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

13

TC: 1/31/2020

3. Select the **AD Bridge Cell Settings** tab, and then check the **Create Associated AD Bridge Cell** box.
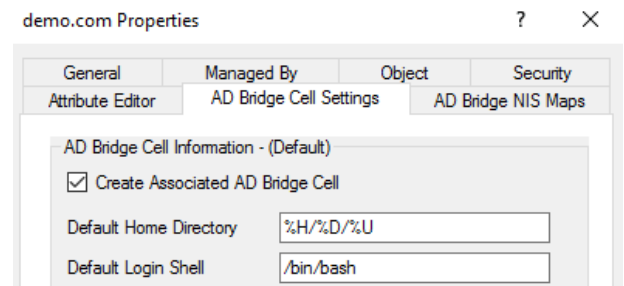
Use Pre-Existing RFC 2307 Data

To recognize and use pre-existing Unix data that is stored in Active Directory with RFC 2307 attributes, make sure AD Bridge is in Directory Integrated mode and then create a default cell.

Associate a User with Cells

You can associate a user with one or more AD Bridge cells to give the user access to the Linux, Unix, and macOS computers that are members of each cell.

1. Start **Active Directory Users and Computers**.
2. In the console tree, click **Users.**
3. In the details pane, right-click a user, and then click **Properties**.
4. Select the **AD Bridge Cell Settings** tab.
5. Under **AD Bridge Cells**, select the check box for the cell that you want to associate the user with. You can select more than one cell.
6. Under **User info for cell**, a default GID value, typically 100000, is automatically populated in the GID box.

> 📌 **Note:** *The user's settings can vary by cell.*

7. To set the UID, click **Suggest**, or type a value in the UID box.

> ⊘ **IMPORTANT!**
>
> *Setting UIDs below 1,000 is not advised, as they can result in a security vulnerability.*

Link Cells

When you link cells, computers in one cell can be accessed by the users in the cell that you linked.

To provide a mechanism for inheritance and to ease system management, AD Bridge can link cells. Users and groups in a linked cell can access resources in the target cell.

For example, if your default cell contains 100 system administrators and you want those administrators to have access to another cell, called **Engineering**, you do not need to provision those users in the **Engineering** cell. Link the **Engineering** cell to the default cell. The **Engineering** cell will inherit the settings of the default cell.

To ease management, in the **Engineering** cell you can set any mapping information that should differ from the default cell.

Although you can use linking to create a hierarchy of cells, linking is not transitive. For example, consider the following linked cells:

- **Civil** cell linked to **Engineering** cell
- **Engineering** cell linked to **Default** cell

In this scenario, the **Civil** cell will not inherit the settings of the default cell.

Link to Multiple Cells

The order of the UIDs controls the search order. Consider the following scenario:

Kathy, a system administrator, has UIDs set in the default cell (100,000) and in the **Engineering** cell (150,000). In the **Civil** cell, however, the UID from the **Engineering** cell must be used to log into **Civil** computers.

If the **Civil** cell is linked to the default cell and the **Engineering** cell, the order is important. If **Engineering** does not precede the default cell in the search order, Kathy will be assigned the wrong UID and will be unable to log on computers in the **Civil** cell.

In the following scenario, a link is created to the **Engineering** cell. With this link, users in the **Engineering** cell can access the computers in the **Accounting** cell:
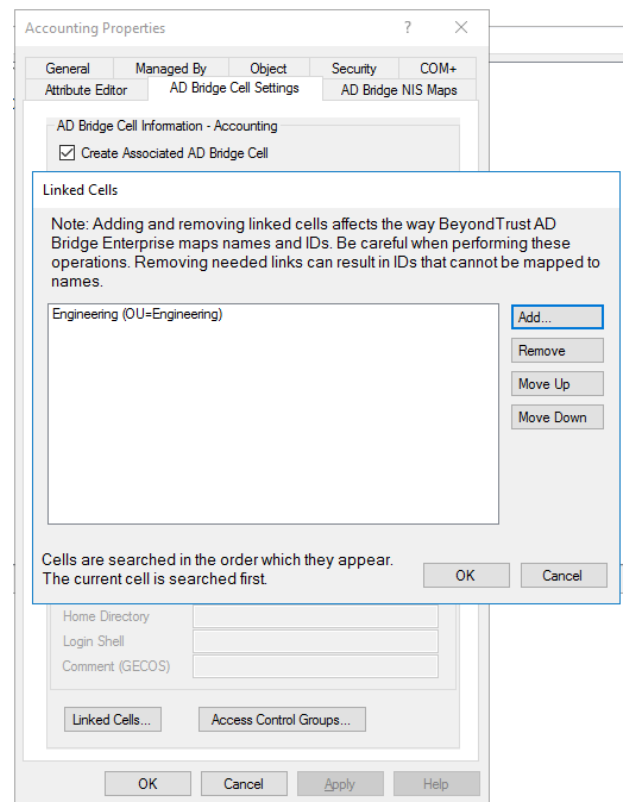
1. Start **Active Directory Users and Computers**.
2. In the console tree, right-click the organizational unit that is associated with the cell you want to link to another cell, and then click **Properties**.
3. Click the **AD Bridge Cell Settings** tab.
4. Click **Linked Cells**, click **Add**, click the cell that you want, and then click **OK**.
5. When you link to multiple cells, the order that you set is important because it controls the search order. The cells are searched in the order listed. Use **Move Up** or **Move Down** to set the order of the cells.

> **i** For more information, please see Link to Multiple Cells.

6. Click **OK**.

Assign Access Control Groups

You can apply access control to UNIX and Linux agents (hosts) using the access control group setting that is available through **AD Bridge Cell Settings**. Using an access control group you can apply restrictive access control to the AD Bridge hosts and users that can access those hosts.

An access control group can be used to supplement existing Group Policy Allow Logon Rights settings and cumulative policy settings. The resultant set of groups will be a combination of the group membership for the AD Bridge host together with the Group Policy Allow Logon Rights settings and cumulative policy.

Configuring and using access control groups is a two-step process:

- Create an Active Directory group: this is a host access group. Create host access groups using a common attribute in the naming convention. For example, prefix all group names with **ADB_**.
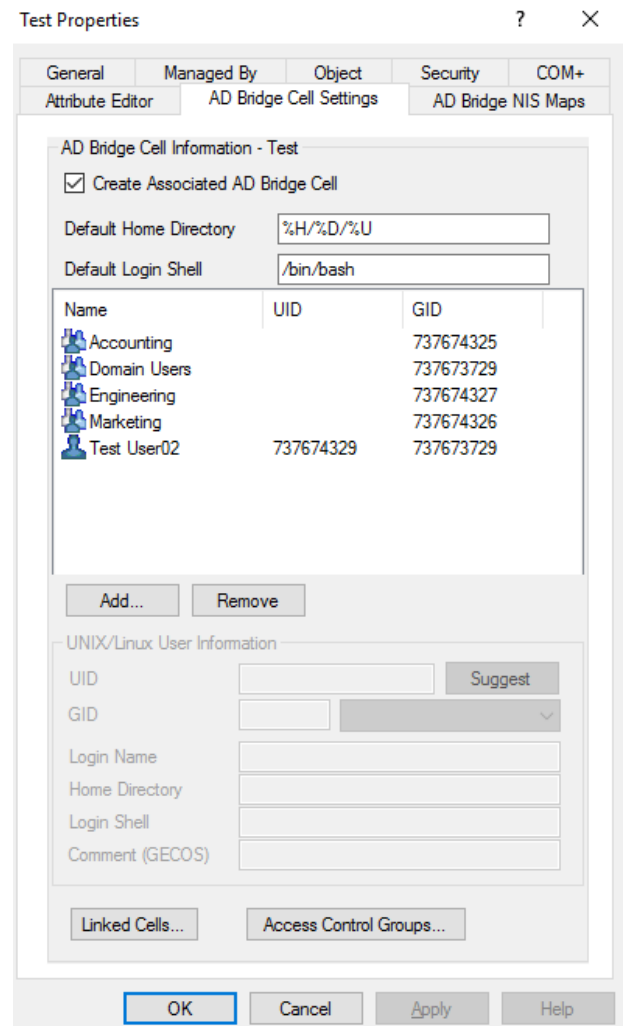
  The groups are added later using a host access template.

  Add the user accounts and the AD Bridge hosts to the group.

  Members can be added directly to the group or through nested group membership. For a user to access an AD Bridge agent, the user and the agent must be a member of the same host access group (directly or through nested groups).

- Add the groups to the Access Control Groups associated with the AD Bridge cell.

  A template is a way to associate the groups with the cell. Host access templates identify the groups to use for the Access Control Group. The host access template can match on group names using wildcards. The name matching is applied to the "Group name (pre-Windows 2000) attribute". This is the **sAMAccountName** attribute.

> 📌 **Note:** *When an AD Bridge agent has no membership in any host access group or any Group Policy Allow Logon Rights, restrictions will be applied to that host. This can be confusing when removing a host from a host access group. If you want the default behavior to disable access to all AD Bridge hosts unless they are a member of a host access group then create a host access template for* **Domain Computers** *where only hosts are defined.*

The **lsass** refresh interval is every 30 minutes. To apply the settings immediately, run the following command:

```
/opt/pbis/bin/lwsm refresh lsass
```

Example Scenario
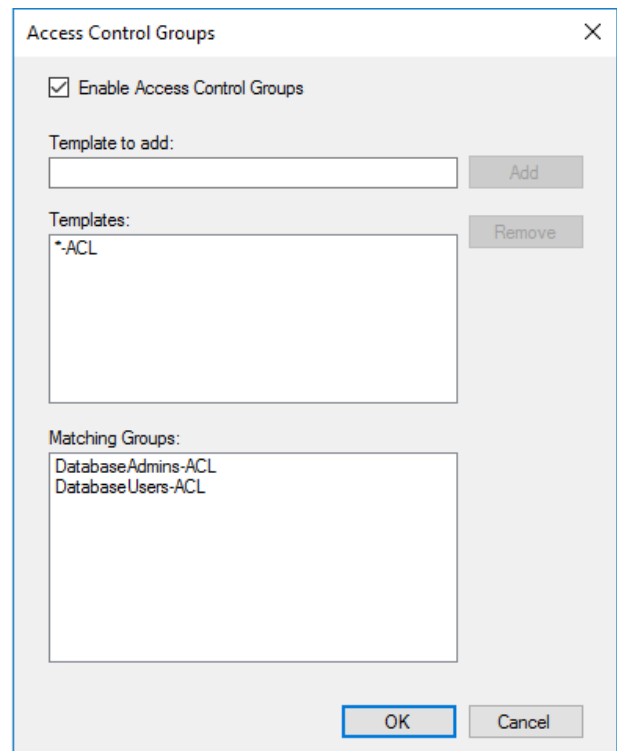
In a database environment, control access is required on a set of hosts running database applications that include the following:

- Group of database server hosts DatabaseServers: dbsrv1, dbsrv2, dbsrv3
- Group of database client hosts DatabaseClients: dbcli1, dbcli2, dbcli3
- Group of database administrator accounts: DatabaseAdmins: dbadm1, dbadm2, dbadm3
- Group of database application user accounts: DatabaseUsers: dbusr1, dbusr2, dbusr3

Database administrators can access all database hosts by creating a DatabaseAdmins-ACL group that includes the following groups as members: DatabaseServers, DatabaseClients and DatabaseAdmins.

Database users can access only database client hosts by creating a DatabaseUsers-ACL group that includes the following groups as members: DatabaseClients and DatabaseUsers.

On the Access Control Groups dialog box, enter the template name similar to the following: *-ACL. The wildcard matching adds all groups that contain -ACL to the list, as shown.

Move a Computer to Another Cell

When you move a computer from one cell to another, you must do the following if you want the cell information to be updated immediately on the client:

- Clear the authentication cache for user and group membership:

```
/opt/pbis/bin/ad-cache --delete-all
```

- Restart the AD Bridge Enterprise authentication service by running this command as root:

```
/opt/pbis/bin/lwsm restart lsass
```

- Force the computer to refresh its Group Policy settings by running this command as root:

```
/opt/pbis/bin/gporefresh
```

Manage Cells with AD Bridge Cell Manager

Using AD Bridge Cell Manager, you can:

- Delegate control of a cell
- Change permissions for a cell
- Add cells, view cells
- Associate cells with OUs to provide users and groups with Linux and Unix access
- Connect to another domain and filter cells to reduce clutter

Start AD Bridge Cell Manager

To start **AD Bridge Cell Manager**:

1. In the **BeyondTrust Management Console**, expand **Enterprise Console** and click **Diagnostics & Migration**.
2. Under **Tasks**, click **Launch Cell Manager**.

   Alternatively, start **Cell Manager** from the **Start** menu. Select **Start > All Programs > BeyondTrust AD Bridge > AD Bridge Cell Manager**.
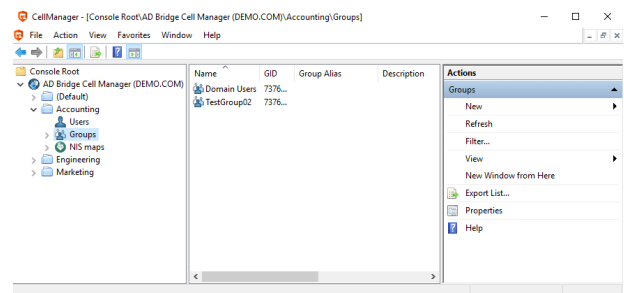
Assign Users to Manage a Cell

You can use **AD Bridge Cell Manager** to create an access control list (ACL) that allows users or groups without administrative privileges to manage AD Bridge cells.

For example, you can assign permissions to particular users to add users or remove users from a cell.

1. In **Cell Manager**, right-click a cell, and then select **Delegate Control**.
2. Click **Start**.
3. Click **Add**, and then choose the users or groups that you are delegating permissions to.
4. Click **Next**, and then select the permissions that you want to assign.
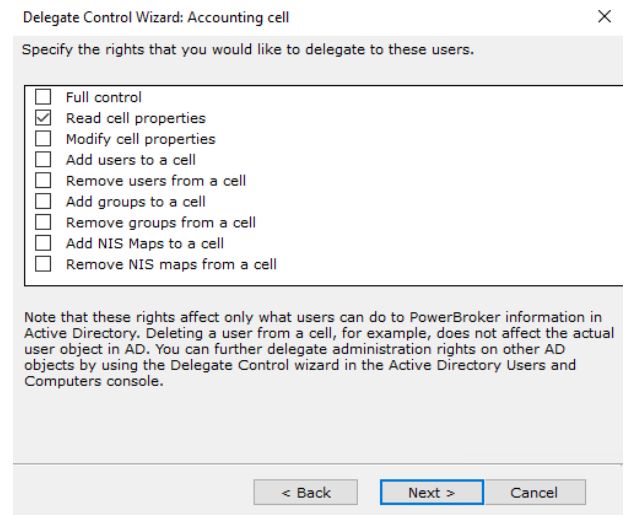
5. Review the information that you entered, and then click **Finish**.

Change Permissions of a Cell, Group, or User

To change the permissions of a cell, a group, or a user:

1. In the **AD Bridge Cell Manager** console tree or in the details pane, right-click the object that you want to change permissions for, and then click **Properties**.
2. Click **Permissions**.
3. Change the permissions, and then click **OK**.

Add a Cell

When you add a cell, you must attach it to an organizational unit (OU) in Active Directory.

To add a cell:

1. In **AD Bridge Cell Manager**, right-click the top-level **Cell Manager** domain node, select **New**, and then click **Cell**.
2. Select the OU to which you want to attach the cell.
3. On the **Cell Defaults** page, select the following:
   - **Default Home Directory:** type the path for the home directory that you want to set for users in the cell. For example, **/home/%D/%U**.

TC: 1/31/2020

> ⚠ **IMPORTANT!**
>
> *When you set the home directory, you must use the default user name variable (**%U**). You can set the default domain name using the domain name variable (**%D**) but it is not required.*

- **Default Login Shell:** type the path to the default shell that you want to use. For example, **/bin/ sh**.
- **Enable Your User Account in the Cell:** select to add your account to the cell.

4. Select the **Create Group Policy Object** check box to create a GPO for the OU and configure the following settings as necessary:
   - **Forward audit event to**
   - **Prepend default domain name to AD users and groups**
   - **Set group policy refresh interval**
5. Click **Start**.

Add a User or Group to a Cell

Default attributes are used when you add a user or group to a cell using **AD Bridge Cell Manager**. You can change the properties later using **Active Directory Users and Computers**.

> ℹ For more information, please see "Configure Cell Settings for Users" on page 21

1. In **Cell Manager**, right-click a cell, select **New**.
2. Select **User** or **Group**.
3. Click **OK**.
4. Enter Search for the user or group that you want to add, and then click **OK**.

Filter Cells

You can use filtering to set the maximum number of cells to display and show only the cells that match a pattern.

1. In **AD Bridge Cell Manager**, right-click the top-level Cell Manager domain node, and then click **Filter**.
2. Set the filtering values that you want to use:
   - Maximum number of cells to display: Enter the number of cells to display. The default is **300**.
   - Only show cells that match pattern.
   - Interpret pattern as regular expression.
3. Click **OK**.

Connect to a Different Domain

Even though users and groups imported from a different domain appear in **AD Bridge Cell Manager**, you cannot modify their settings from outside their original domain. To modify the settings of a user or group imported from another domain, use **Cell Manager** to connect to that domain, and then make the changes that you want.

1. In **Cell Manager**, right-click the top-level Cell Manager domain node, and then click **Connect To Domain**.
2. In the **Domain** box, type the domain. Alternatively, click **Browse**, and then locate the domain.

Manage Users and Groups

Using AD Bridge Enterprise, you can manage the AD Bridge cell settings for Unix, Linux, and macOS users and groups in Active Directory Users and Computers.

Configure Cell Settings for Users

In Active Directory Users and Computers, you can configure AD Bridge cell settings for your users.

> ℹ️ Administrative privileges are required to manage AD Bridge cell settings. Ensure you are logged on as a Domain Administrator, Enterprise Administrator, or you are assigned permissions. For more information, please see "Assign Users to Manage Cells" on page 11.

The following cell settings can be configured to establish connection between Active Directory and your clients:

- **UID:** The Unix user ID. The user's settings can vary by cell.
- **GID:** The Unix primary group ID. By default, you can select any group or enter an arbitrary primary group ID for the user account. If you need to restrict this to only allow groups enabled in the cell and assigned to the user, you can use the **btopt.exe** tool to enforce this validation.

> ℹ️ For more information, please see "Use the btopt.exe Tool" on page 69

- **Login Name:** Provide an alias for an Active Directory user so that the user can log into a bridged client using the alias. An alias only applies to the selected cell.
- **Home Directory:** When you set the default home directory, you must use the default user name variable (**%U**). Using the default domain name using the domain name variable (**%D**) but it is optional.
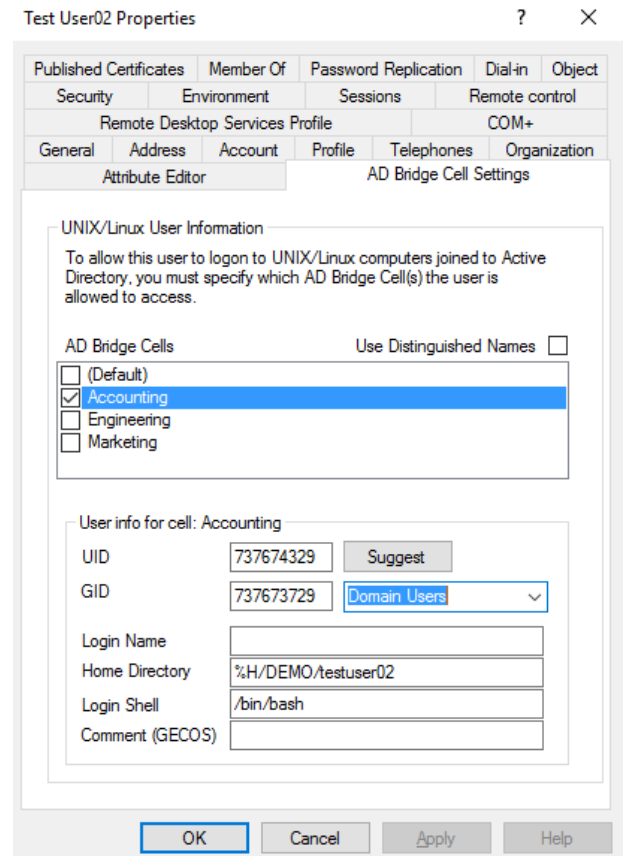
> ⚠️ **IMPORTANT!**
>
> *On Solaris, you cannot create a local home directory in /home, because /home is used by autofs, Sun's automatic mounting service. The standard on Solaris is to create local home directories in /export/home.*

- **Login Shell:** When assigning a login shell, you can select a user or more than one user. You can assign the login shell at the OU level or user level.
- **Comment (GECOS)**

> 💡 *Tip: The Cell Access Report can show you existing values for UID, GID, home directory, and login shells for users. For more information, please see "Run Reports" on page 57 .*

You can configure cell settings at the OU level, user level, or select a range of users in a selected OU. To configure cell settings for your users:

1. Start **Active Directory Users and Computers**.

2. Navigate to the OU where your users reside.

3. Right-click the user and then select **Properties**.

4. Select the cells where you want the settings to apply. When editing the properties for a particular cell, if the box is already checked, then select the cell to activate the settings in the user info section.

5. Enter information for the following:

   - **UID:** Click **Suggest**, or type a value in the box.
   - **GID:** The GID value is automatically populated. Select a group from the list to change the primary group for the user account.

   Note: If you select another group from the list, the GID can be validated. If the group is unavailable, be sure to add the group to the cell. For more information, please see "Configure Cell Settings for a Group" on page 23

   - **Login Name:** Type an alias for the user. The user must log on using the Active Directory account if a login name is not set here.
   - **Home Directory:** To override the default home directory, type the directory that you want to set for the user. For example, **/home/%D/%U**
   - **Login Shell:** Enter a login shell if you want to override the default. For example, **/bin/sh** or **/bin/bash**.
   - **Comment (GECOS):** Enter a comment (Optional).

6. Click **OK**.

SALES: www.beyondtrust.com/contact **SUPPORT:** www.beyondtrust.com/support **DOCUMENTATION:** www.beyondtrust.com/docs

22

Assign Settings to More Than One User

You can assign settings to more than one user at the same time. For example, you can assign users to a cell and then set the home directory. The users must be members of a group already associated to a cell and each user must have a UID-GID mapping.

Configure Cell Settings for a Group

In **Active Directory Users and Computers**, you can configure AD Bridge cell settings for a group. You can configure a GID and group alias.

> **i** Administrative privileges are required to manage AD Bridge cell settings. Ensure you are logged on as a Domain Administrator, Enterprise Administrator, or you are assigned permissions. For more information, please see "Assign Users to Manage Cells" on page 11.

A cell must already be created.

> **i** For more information, please see the following:
> - "Create a Cell and Associate it with an OU or a Domain" on page 13
> - "Create a Default Cell" on page 13

1. Start **Active Directory Users and Computers**.
2. In the console tree, right-click a group, and then click **Properties**.
3. Click the **AD Bridge Cell Settings** tab.
4. In the **AD Bridge Cells** section, select the check box for the cell that you want to provide the group access to.
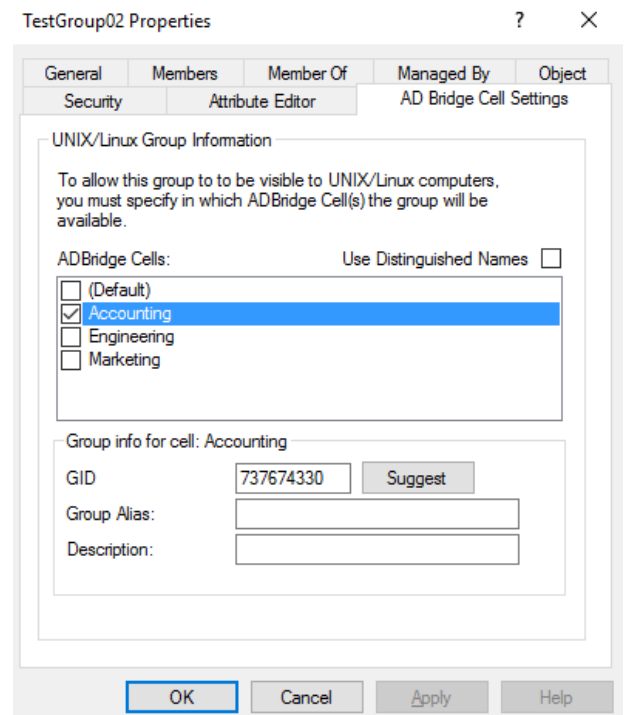
5. In the **Group info for cell** section, set the following:

   - **GID:** Click **Suggest**, or type a value in the **GID** box.

     You can assign a group identifier (GID) to an Active Directory group by associating the group object with a cell and setting a GID value for the group object. The GID information that you enter is applied to all objects in the group. However, the settings are not applied to nested groups; you must apply the GID information to each group.

   - **Group Alias:** Set an alias for the group (Optional). The alias applies only within the cell.

Disable a User

> **Note:** *When a computer cannot communicate with a domain controller, a user whose account was disabled on the domain controller, but who logged on to the computer prior to their account being disabled, can continue to log on until you clear the cache or until the computer regains communication with the domain controller.*
>
> *By default, the cache expires after 4 hours. You can configure the interval using an AD Bridge Enterprise Group Policy setting or, if the policy setting has not been configured, by modifying the registry using the AD Bridge Enterprise config tool.*

1. Start **Active Directory Users and Computers**.
2. Find the user.
3. Right-click the user that you want to disable, and then click **Properties**.
4. Click the **AD Bridge Cell Settings** tab.
5. In the **AD Bridge Cells** section, uncheck the boxes for the cells where you want to disable the user. To disable the user's access to all Linux, Unix, and macOS computers, uncheck all the boxes.

Find Users and Groups in Active Directory Users and Computers

Because of a limitation with the Active Directory Users and Computers snap-in, when you try to find an AD Bridge Enterprise user or group by right-clicking an OU and then clicking **Find**, the user or group will not appear in the results even when the user or group is in the OU. The Find command does, however, work at the domain level.

As an alternative, you can find AD Bridge Enterprise users and groups in an OU using the following procedure:

1. Right-click the OU with an associated cell, select **Properties**, and then click the **AD Bridge Cell Settings** tab.

2. Click **Add**, and then search the user or group.
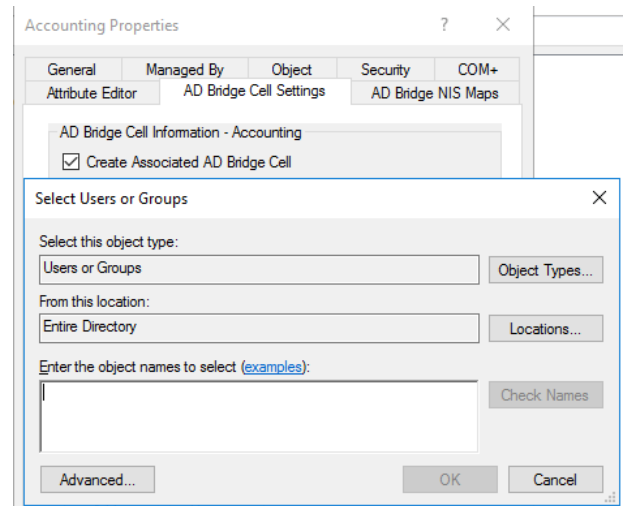
Find Orphaned Objects

You can use the BeyondTrust Management Console to find and remove orphaned objects. An orphaned object is a linked object, such as a Unix or Linux user ID or group ID, that remains in a cell after you delete a group or user's security identifier, or SID, from an Active Directory domain.

Removing orphaned objects from Active Directory can clean up manually assigned user IDs and improve search speed. We recommend that you remove orphaned objects before you use the migration tool with a domain that operates in Schemaless mode.

1. In the BeyondTrust Management Console tree, expand **Enterprise Console**, and then click **Diagnostics & Migration**.
2. From the Tasks list, click **Find Orphaned Objects**.
3. Click **Select Domains**, select the domains that you want to scan, and then click **OK**.
4. Click **Begin Scan**.
5. To remove the objects that appear in the **Orphaned objects to delete** box, click **Delete Objects**.

Migrate Users to Active Directory

The Network Information System (NIS) migration tool imports Linux, Unix, and macOS passwd files and group files and maps them to users and groups in Active Directory. The migration tool includes options to ease your NIS migration to Active Directory, including:

- Migration of account information to the organizational units that you want.
- Creation of groups in Active Directory to match your Linux and Unix groups.
- Generation of scripts to repair file ownership and group settings.
- Changes to the GID of imported users to that of the AD Domain Users group.
- Automatically setting an alias for each migrated user.
- Generation of Visual Basic scripts to migrate users and groups in an automated and custom way.
- Modification of GIDs during migration.
- Selection of only the groups and users that you want to migrate from your full list of groups and users.
- Setting the home directory and shell for migrated users.
- Filtering out standard Unix and Linux accounts, such as mail and news.
- Modification of UID information during migration.
- Use of NIS map files to migrate netgroups, automounts, and other services to Active Directory.

Overview

The AD Bridge Enterprise NIS migration tool can import Linux, Unix, and macOS password and group files (typically **/etc/passwd** and **/etc/group**) and automatically map their UIDs and GIDs to users and groups defined in Active Directory.

You can also generate a Windows automation script to associate the Unix and Linux UIDs and GIDs with Active Directory users and groups. Before you commit the changes, you can resolve ambiguous user names and other conflicts.

⊘ IMPORTANT!

Before you migrate users to a domain that operates in schemaless mode, we recommend that you find and remove orphaned objects. The IDs associated with orphaned objects are reserved until you remove the orphaned objects. For more information, please see

---

Before Running the Migration Tool

Before running the migration tool, obtain the following information:

- The name of the domain where you want to migrate the account information
- Credentials that allow you to modify the domain
- The Unix or Linux **passwd** file and corresponding group file that you want to add to Active Directory. The password and group files can be from a computer or an NIS server.

Run the Migration Tool

To import Linux, Unix, and macOS password and group files and automatically map UIDs and GIDs to users and groups in Active Directory:

1. In the BeyondTrust Management Console tree, expand **Enterprise Console**, and then click **Diagnostics & Migration**.

2. From the **Tasks** list, click **Run Migration Tool**.

3. Click **Next**.

4. In the **Domain** box, type the domain name that you want to migrate the account information to.

5. Select credentials:
   - **Use logon credentials:** Select if your logon credentials allow you to modify the domain.
   - **Use alternate credentials:** Select if your logon credentials are not allowed to modify the domain, and then enter credentials that have the appropriate privileges.

6. Click **Next**.

7. Select your mapping files:
   - Click **Import** to import a Linux/Unix password and group file, and then provide the following information.
     - **Map name:** The migration tool imports the passwd file and group file into the map file, which is then matched to existing Active Directory user and group names.
     - **Passwd file:** Type the path and name of the file that you want to import, or click **Browse** to find the file.
     - **Group file:** Type the path and name of the passwd file's corresponding group file, or click **Browse** and then find the file.
     - To import default Unix or Linux user accounts such as **root and public,** clear the **Omit standard Linux/UNIX user accounts** check box.
     - In the list under **Users**, clear the **Import** check box for any user that you do not want to import, and then click **Next**.
   - Click **Import NIS Map** to import an NIS Map File. You can run the **ypcat** command on the NIS server to create the map file.
     - **NIS Map file:** Click **Browse** to find the map file.
     - **Map type:** Select the map file type: **Netgroups**, **Automounts**, or **Services**.

8. Select the OU where you want to migrate the Linux or Unix account information.

   If you select the top of your domain, the information is migrated to the default AD Bridge cell of your Active Directory forest and UID numbers are automatically assigned within the domain's range.

   If you select an OU, AD Bridge Enterprise creates a cell for the OU and migrates the account information to it. UIDs and GIDs are maintained if the passwd and group files agree, and if the UIDs and GIDs do not conflict with existing users or groups.

   The migrated account information applies only to computers that are members of the OU.

9. Click **Next**.

10. Select from the following list of migration options:
    - **Create groups in Active Directory to match Linux/Unix groups:** Create groups in Active Directory that match your Linux or Unix groups
    - **Create all groups in AD:** Create all groups in Active Directory, not just the referenced ones. To select this option, you must first select the **Create groups in Active Directory to match Linux/UNIX groups** check box.
    - **Generate scripts to repair file ownership and group settings:** Run scripts that can repair ownership issues and group settings issues.
    - **Change GID of imported users to Domain Users**
    - **Always set Login Name (alias), even when same as sAMAcountName**
    - **Generate VBScript to perform migration:** Enter the name of the script in the **Script name** box. Enter the directory where the script is located.

- **Name map file (optional):** File to automatically map Linux and UNIX users and groups to Active Directory accounts and groups in the form of the key/value pairs (delimited by **=** sign). The value can use the LDAP path to the Active Directory user or group or it can use the format **DOMAIN\username**.

  For example, **john=LDAP://CN=jdoe,OU=accounts,DC=thedomain,DC=com** or **john=thedomain\jdoe**, where Unix user with login **john** is matched to AD user with **CN=jdoe**.

  If **[name map file]** is not provided or a successful match is not found, then the Migration tool will try to find the best match in the target domain.

11. Click **Next**.
12. Click the **Users** tab and verify that the information is correct.
13. Click the **Groups** tab and verify that the information is correct.
14. To import the passwd and group files after you verify that the information is correct, click **Next**.

Migrate NIS Domains

If you use AD Bridge Enterprise to migrate all your Unix and Linux users to Active Directory, in most cases you will assign these users a UID and GID that is consistent across all the Unix and Linux computers that are joined to Active Directory. This is a simple approach that reduces administrative overhead.

In cases when multiple NIS domains are in use and you want to eliminate these domains over time and migrate all users and computers to Active Directory, mapping an Active Directory user to a single UID and GID might be too difficult. When multiple NIS domains are in place, a user typically has different UID-GID maps in each NIS domain. With AD Bridge Enterprise, you can eliminate these NIS domains but retain the different NIS mapping information in Active Directory because AD Bridge Enterprise lets you use a cell to map a user to different UIDs and GIDs depending on the Unix or Linux computer that they are accessing.

To move to Active Directory when you have multiple NIS servers, you can create an OU or choose an existing OU, and join to the OU all the Unix computers that are connected to the NIS server. You can then use cells to represent users' UID-GID mapping from the previous identity management system.

Manage Computers

Using AD Bridge Enterprise, you can manage the AD Bridge cell settings for Unix, Linux, and macOS computers in Active Directory Users and Computers.

Use AD Bridge Enterprise with a Single Organizational Unit

You can use AD Bridge Enterprise if you have write privileges for only one OU. Your AD rights to create objects in the OU allow you to join Linux and Unix computers to the OU even though you do not have Active Directory Domain Administrator or Enterprise Administrator privileges.

> ℹ️ For more information, please see "Assign Users to Manage Cells" on page 11

There are additional limitations to this approach:

- You must join the computer to a specific OU, and you must know the path to that OU.
- You cannot use AD Bridge Enterprise in Directory Integrated mode unless you have Enterprise Administrator privileges, which are required to upgrade the schema.

Join a Linux Computer to an Organizational Unit

To join a computer to a domain, you need:

- The user name and password of an account that has privileges to join computers to the OU
- The full name of the domain that you want to join. The OU path is from the top OU down to the OU that you want.

As root, execute the following command, replacing **organizationalUnitName** with the path and name of the OU that you want to join, **domainName** with the FQDN of the domain, and **joinAccount** with the user name of an account that has privileges to join computers to the domain:

```
/opt/pbis/bin/domainjoin-cli join --ou organizationalUnitName domainName joinAccount
```

Example:

```
/opt/pbis/bin/domainjoin-cli join --ou Engineering example.com Administrator
```

Example of how to join a nested OU:

```
domainjoin-cli join --ou topLevelOU/middleLevelOU/LowerLevelOU/TargetOU example.com Administrator
```

After you join a domain for the first time, you must restart the computer before you can log on.

Rename a Joined Computer

To rename a joined computer, you must:

- Leave the domain.
- Rename the computer using the domain join command-line interface.

- Rejoin the computer to the domain.

> ⚠ **IMPORTANT!**
>
> *Do not change the name of a Linux, Unix, or Mac computer using the hostname command because some distributions do not permanently apply the changes.*

Rename a Computer Using the Command-Line Tool

The following procedure removes a Unix or Linux computer from the domain, renames the computer, and then rejoins it to the domain.

> 📌 *Note: Renaming a joined computer requires the user name and password of a user with privileges to join a computer to a domain.*

1. With root privileges, at the shell prompt of a Unix computer, execute the following command:

   ```
   /opt/pbis/bin/domainjoin-cli leave
   ```

2. To rename the computer in **/etc/hosts**, execute the following command, replacing **computerName** with the new name of the computer:

   ```
   /opt/pbis/bin/domainjoin-cli setname computerName
   ```

   Example:

   ```
   /opt/pbis/bin/domainjoin-cli setname RHEL44ID
   ```

3. To rejoin the renamed computer to the domain, execute the following command at the shell prompt, replacing **DomainName** with the name of the domain that you want to join and **UserName** with the user name of a user who has privileges to join a domain:

   ```
   /opt/pbis/bin/domainjoin-cli join DomainName UserName
   ```

   Example:

   ```
   /opt/pbis/bin/domainjoin-cli join example.com Administrator
   ```

   It may take a few moments before the computer is joined to the domain.

4. After you change the hostname of a computer, you must also change the name in the AD Bridge Enterprise local provider database so that the local AD Bridge Enterprise accounts use the correct prefix. Execute the following command as root, replacing **hostName** with the name that you want:

   ```
   /opt/pbis/bin/lsa set-machine-name hostName
   ```

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

30

Remove a Computer from a Domain

You can remove a computer from a domain in the following ways:

- Remove the computer account from ADUC
- Run the domain join tool on the Unix, Linux, or macOS computer

> ℹ️ For more information, please see *Leave Commands* in the AD Bridge Linux Administration Guide at
> https://www.beyondtrust.com/docs/ad-bridge/documentation.htm.

NetworkManager: Use a Wired Connection to Join a Domain

On Linux computers running **NetworkManager**, which is often used for wireless connections, you must make sure before you join a domain that the computer has a non-wireless network connection and that the non-wireless connection is configured to start when the networking cable is plugged in. You must continue to use the non-wireless network connection during the post-join process of restarting your computer and logging on with your Active Directory domain credentials.

After you join the domain and log on for the first time with your AD domain credentials using a non-wireless connection, you can then revert to using your wireless connection because your AD logon credentials are cached (You will not, however, be notified when your AD password is set to expire until you either run a sudo command or log on using a non-wireless connection).

If, instead, you attempt to use a wireless connection when you join the domain, you cannot log into your computer with AD domain credentials after your computer restarts.

Here is why: **NetworkManager** is composed of a daemon that runs at startup and a user-mode application that runs only after you log on. **NetworkManager** is typically configured to auto-start wired network connections when they are plugged in and wireless connections when they are detected. The problem is that the wireless network is not detected until the user-mode application starts, which occurs only after you log on.

> ℹ️ For more information about NetworkManager, please see NetworkManager - GNOME Wiki! at
> https://wiki.gnome.org/Projects/NetworkManager.

AIX: Create Audit Classes to Monitor Events

On AIX computers, after you install the AD Bridge Enterprise agent, you can create audit classes to monitor the activities of users who log on with their Active Directory credentials. You can use the following file as a template to create audit classes for AD users:

/etc/pbis/auditclasses.sample

To create and configure an audit class, copy the file and name it **/etc/pbis/auditclasses**. Edit the file to set the audit classes. After you configure audit classes, the auditing occurs the next time the user logs on.

The sample AD Bridge Enterprise auditclasses file looks like this:

```
#
# Sample auditclasses file.
#
# A line with no label specifies the default audit classes
# for users that are not explicitly listed:
#
```

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

31

```
general, files
#
# A line starting with a username specifies the audit classes
# for that AD user. The username must be specified as the
# "canonical" name for the user: either "DOMAIN\username" or
# just "username" if "--assumeDefaultDomain yes" was passed
# to domainjoin-cli with "--userDomainPrefix DOMAIN".
# In AD Bridge, if the user has an alias specified in
# the cell the alias name must be used here.
#
DOMAIN\user1: general, files, tcpip user2: general, cron
#
# A line starting with an @ specifies the audit classes for
# members of an AD group. These classes are added to the
# audit classes for the user (or the default, if the user is
# not listed here). Whether to specify "DOMAIN\groupname" or
# just "groupname" follows the same rules as for users.
#
@DOMAIN\mail_users: mail group2: cron
```

ℹ️   For more information on AIX audit classes, please see IBM documentation for your version of AIX.
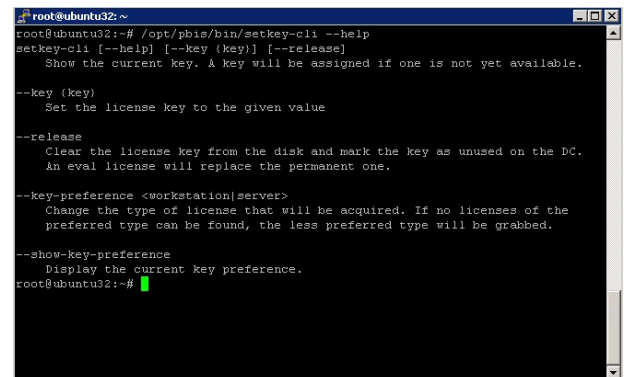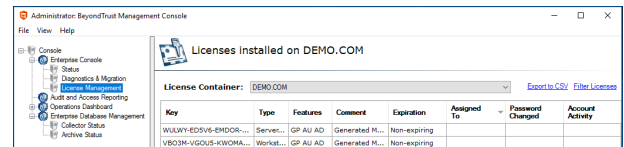
Manage AD Bridge Enterprise Licenses

There are two options to manage the assignment of AD Bridge Enterprise licenses:

- Globally using the **License Management** page in the BeyondTrust Management Console on a Windows administrative workstation connected to Microsoft Active Directory.

  We recommend that you manage your licenses through the BeyondTrust Management Console.

- Locally using an AD Bridge Enterprise command-line utility (**setkey-cli**) on a Linux, Unix, or macOS computer.

Evaluation Licenses and Permanent Licenses

When you install the AD Bridge Enterprise agent without a permanent license on a Unix or Linux computer, a 30-day product evaluation key is automatically generated. If a permanent license key or an extended evaluation license key is unavailable, AD Bridge Enterprise will stop authenticating users and applying Group Policy settings after 30 days. The expiration date of an evaluation license applies only to the computer on which the license is installed.

> 📌 **Note:** To obtain a permanent license or to convert a trial license to a full license, contact a BeyondTrust sales representative at *www.beyondtrust.com/contact*.

You can upgrade an evaluation license to a permanent license by importing the permanent license key into the BeyondTrust Management Console, and applying it to a client computer. If the automatic assignment feature is in use, the AD Bridge Enterprise agent will automatically apply a permanent license when you log on a client with an AD account, restart the AD Bridge Enterprise authentication service, or run the command-line utility for managing licenses.

Site Licenses and Single-Computer Licenses

BeyondTrust offers site licenses and single-computer licenses.

- A site license covers all the computers in a domain and its child domains. To determine whether a computer falls under a site license, AD Bridge Enterprise checks the last two components of the domain name.

  For example, **example.com** is the domain governed by a site license and one of the child domains is named **child.example.com**. The child domain is covered by the site license because the last two components of the domain name match.

- If there are multiple domains, a different license file is required for each domain, regardless of whether you are using a site license or a set of single-computer licenses. To spread a set of single-computer licenses across two or more domains, you can request BeyondTrust sales to distribute the licenses in two or more license files.

Workstation and Server Licenses

BeyondTrust offers two kinds of licenses: workstation and server. Both single-computer licenses and site licenses distinguish between servers and workstations. When a computer joins a domain, AD Bridge Enterprise looks at the version of the operating system to determine whether to assign a workstation or a server license. If a server license is unavailable, a workstation license is automatically used.

A workstation license limits the number of concurrent logins to five discrete user accounts. With a server license, the number of concurrent logins is unlimited.

> 📌 *Note: If the computer is a server but is using a workstation license because no server licenses were available, please contact BeyondTrust sales at* www.beyondtrust.com/contact *to obtain more server licenses. You can adjust the license type that you want the agent to obtain by using the command-line utility for managing licenses.*

The AD Bridge Enterprise agent verifies a license when you run the **setkey-cli** utility, when you start the AD Bridge Enterprise authentication service, and when you log on. To verify a license, the **setkey-cli** utility uses the computer's Active Directory account to search for licenses in the computer's OU hierarchy up to the top of the domain. Other domains in the forest are not searched. When the computers's domain controller is down, the utility loads the license from the disk without verifying its assignment in Active Directory.

The AD Bridge Enterprise Group Policy service also checks for a license when it refreshes the computer's Group Policy Objects (GPOs). If the license is invalid, the service ignores the GPOs. Once the license becomes permanent and valid, the service applies the GPOs when it restarts.

> 📌 *Note: If the message "Invalid computer!" is displayed in the* **Assigned To** *column, revoke the license and return it to the pool of available licenses. This action is performed by right-clicking the license you want to revoke, and then clicking* **Revoke License**.

License Feature Codes

Licenses contain codes that can include or exclude features. When a license is displayed in the console, the codes in the **Features** column indicate the entitlements that the license covers.

License Container: DEMO.COM

Key	Type	Features
WULWY-ED5V6-EMD...	Server...	GP AU AD
VBO3M-VGOU5-KW...	Workst...	GP AU AD

The following table describes each feature code:

Feature Code	Description
SC	Covers the use of two-factor authentication with a smart card
GP	Covers the application of GPOs
AU	Covers the auditing and reporting components
AD	Covers the use of the AD Bridge Enterprise management tools for Active Directory

Create a License Container

You can install AD Bridge licenses manually on each client, or you can install the licenses in Active Directory and manage them from a central location. In Active Directory, you must create a license container before you can import an AD Bridge Enterprise license key file.

Recommendations

Review the following recommendations for creating a license container.

- Manage licenses in Active Directory and create your license container in a common location at the highest level of the organizational unit (OU) hierarchy to which you have write access.

  For instance, if you have separate OUs for your Linux and Mac computers, creating the licensing container in a common location above the OUs for the Mac and Linux computers can simplify license management.

- If you have a default cell, create the license container at the level of the domain.

Any OU may have a license container. The container need not be in the same OU as an AD Bridge cell. The AD Bridge Enterprise agent searches the OU hierarchy for a license container in the same way that it searches for a cell. When a license container is found, the agent stops trying to find a key in another container (even if the container it finds is empty) and checks whether the license is assigned to the computer. When the agent finds a license in Active Directory, it marks it as assigned to the computer.

When you create a license container, computers can automatically acquire a license. You can turn off automatic licensing depending on your requirements. However, after you create the license container you must assign a license to each computer manually.

> ℹ️ For more information, please see "Assign a License to a Computer in AD" on page 37

> 📌 *Note: If needed, you can turn on automatic licensing again at any time after you create the container. For more information, please see Turn on Automatic Licensing.*

If there is no license container in Active Directory, the agent verifies the license locally. This is a scenario reserved for licenses set with **setkey-cli**.

> ⚠️ **IMPORTANT!**
>
> *You must be a member of the **Domain Administrators** security group or have privileges sufficient to create and modify containers where you want to create the licensing container. We recommend that you do not create a license container in the **Domain Controllers** OU.*

To create a license container:

1. In the BeyondTrust Management Console, expand the **Enterprise Console** node, right-click the **License Management** node, and then click **Create License Container**.

2. Uncheck the **Allow Computers to Acquire Licenses Automatically** box to prevent computers from obtaining a license (Optional).

   If you uncheck the box, you must manually assign a license to each computer.

3. Select the location where you want to create a container and then click **OK**.
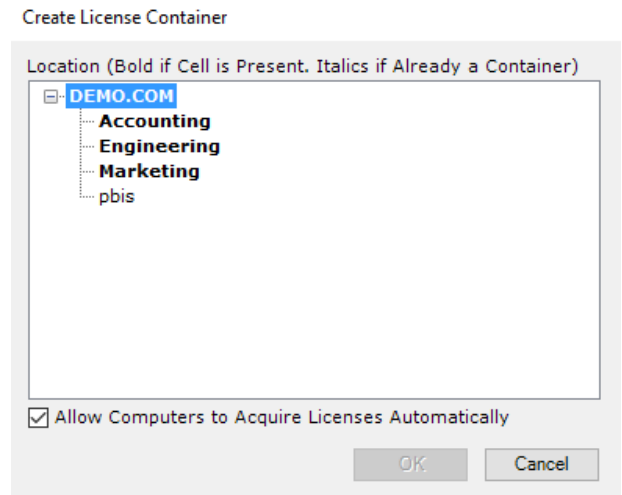
You are now ready to import a license file, which will populate the AD Bridge Enterprise licenses container in Active Directory with licenses for your Unix, Linux, and macOS computers.

Turn on Automatic Licensing

If you turned off automatic licensing when you created the license container, you can turn on the feature at any time.

To turn on automatic licensing:

1. In the BeyondTrust Management Console, expand the **Enterprise Console** node, right-click the **License Management** node, and then click **Assign Policy**.

2. Check the box to allow automatic licensing and click **OK**.
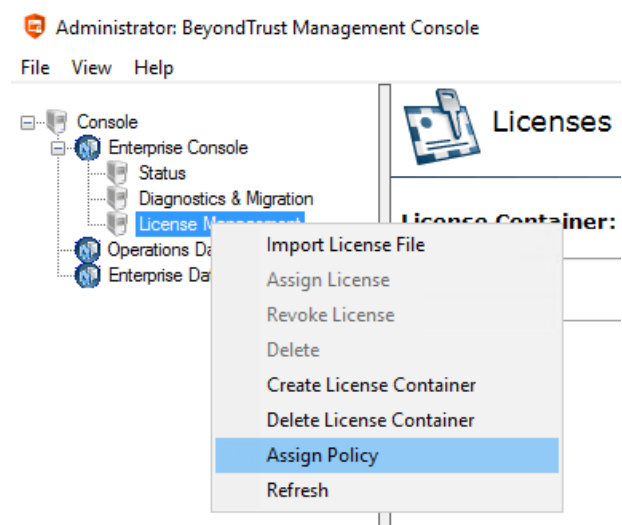
Import a License File

AD Bridge Enterprise license keys and site licenses are distributed in an XML file.Using the BeyondTrust Management Console on your Windows administrative workstation, you can import a license key file containing licenses.

> **Note:** *When you import a license file an Active Directory object is created for every license. For example, if your license XML file contains 100 licenses, then 100 Active Directory objects are created.*

You must create a license container in Active Directory before you can import a license key file.

1. Make sure the XML file containing the licenses is available on your Windows administrative workstation that is running the BeyondTrust Management Console.
2. Under **Enterprise Console**, right-click **License Management**, and then click **Import License File**.
3. Locate the XML file that contains the licenses, and then click **Open**.

Assign a License to a Computer in AD

By default, AD Bridge Enterprise automatically assigns licenses to computers running the AD Bridge Enterprise agent when the computers connect to the domain. If you turn off the default setting, then a computer cannot automatically obtain a license. However, you can manually assign a license using the BeyondTrust Management Console.

To manually assign a license:

1. In the BeyondTrust Management Console, expand **Enterprise Console**, and then click **License Management**.
2. Right-click the license that you want to assign, and then click **Assign License**.
3. In the **Select Computer** dialog box, click **Locations**, select the location that contains the computer you want, and then click **OK**.
4. In the **Enter the object names to select** box, type the name of one or more computers. For example, **AppSrvSeattle-1**.

   Separate multiple entries with semicolons. For a list of examples, click **examples**.

5. Click **Check Names**, and then click **OK**.

> **Tip:** *To use additional criteria to search for and select computers, click **Advanced**. Then, to show more information about a computer in the **Search results** box, click **Columns**, and add or remove columns.*

Manage a License Key from the Command Line

Although we recommend that you manage licenses in the BeyondTrust Management Console, you can also manage a license locally from the command line on a Linux, Unix, or macOS computer.

From the command line of an AD Bridge Enterprise client, you can check the computer's license, set a license key, release a license, and adjust the type of license that you want the computer to obtain.

> **Tip:** *For more information, run the following command:*
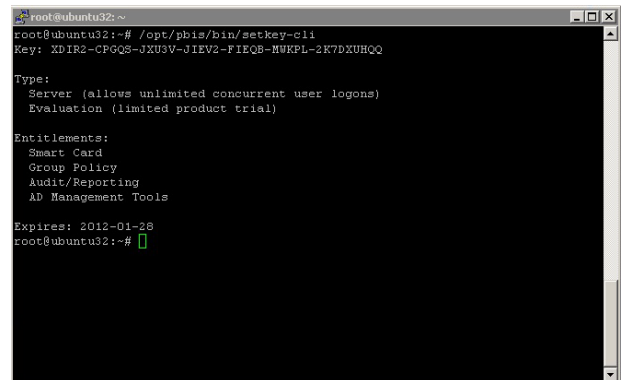>
> ```
> /opt/pbis/bin/setkey-cli --help
> ```

Check the License Key

To view the license key that is installed on a Unix, Linux, or macOS computer, execute the following command at the shell prompt:

```
/opt/pbis/bin/setkey-cli
```

Here is an example:

Set a License Key

You can set a license key for the AD Bridge Enterprise agent by using the command line. You should, however, use this method of setting a key only when there is no licensing container in Active Directory and you want the agent to verify the license locally.

To set a license key, run the following command as root, replacing **LicenseKeyNumber** with a valid license key number:

```
/opt/pbis/bin/setkey-cli --key LicenseKeyNumber
```

> 📌 **Note:** *If there is a license container in Active Directory, you cannot use the command to apply an additional license or to select a license from the license container; instead, assign the license from Active Directory.*

Release a License Key

When you decommision a computer, you can release a computer's license so it can be used by another computer. When you release a permanent license key, it is replaced by a temporary evaluation license.

You can also release a license to apply a different permanent license to the computer.

```
/opt/pbis/bin/setkey-cli --release
```

Change the Type of License

You can change the type of license that the computer obtains when it connects to Active Directory by executing the following command as root, replacing **typeOfLicense** with either **workstation** or **server**.

```
/opt/pbis/bin/setkey-cli --key-preference typeOfLicense
```

If the license type you set is unavailable the non-preferred type is obtained.

Delete a License

When you rename or remove a domain from Active Directory, you might also need to delete AD Bridge Enterprise license keys from Active Directory. If you rename an Active Directory domain, you must obtain new license keys from BeyondTrust.

Licenses are provided on a per-domain basis; domain licenses apply only to the fully qualified domain name or child domain to which they were issued.

1. In the BeyondTrust Management Console, expand **Enterprise Console**, and then click **License Management**.
2. In the list of licenses, under **Key**, right-click the license that you want to delete and then click **Delete**.

> **Tip:** *If you inadvertently delete a license, you can restore it by importing the license file that contains it.*

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

39

Configure Auditing and Reporting

The following AD Bridge Enterprise reporting components depend on the use of the database and the data collectors:

- **Audit and Access Reporting**
- **Operations Dashboard**
- **Enterprise Database Management**

Overview

The reporting system includes the following components. We recommend that you deploy each component to a dedicated server.

- A SQL Server database set up on a dedicated database server.
- A dedicated data collection server set up on a Windows computer. The **Collector** service and **Reaper** service are deployed here.
- A server where AD Bridge is deployed. AD Bridge group policies are configured to allow event forwarding from the agents to the SQL Server database.
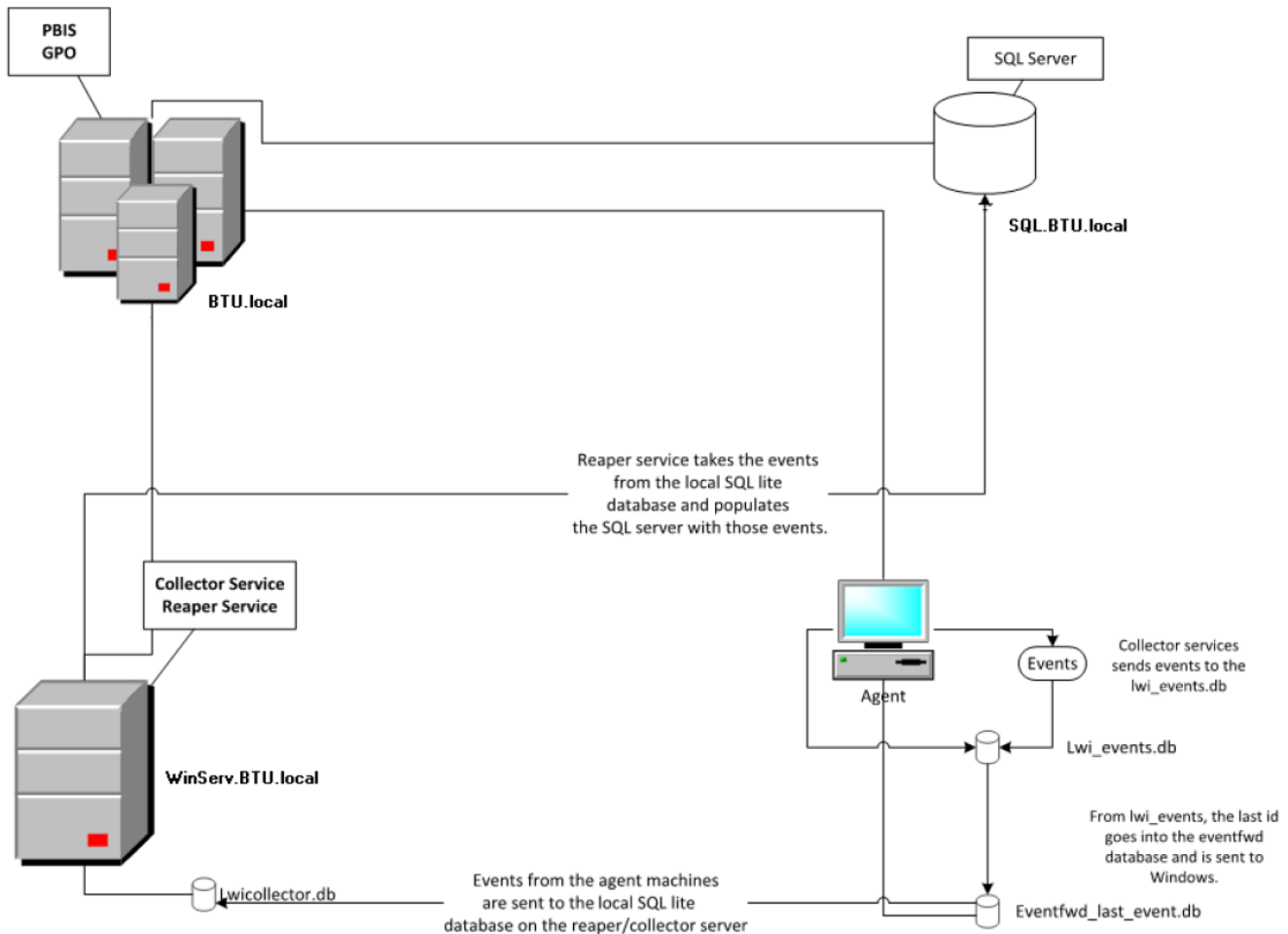
Requirements

The following are the requirements for the reporting system.

General

- A database named **LikewiseEnterprise** running SQL Server 2008 R2 or higher.
- The Microsoft Report Viewer 2015 (**ReportViewer.exe**) must be installed. To download the **Report Viewer**, go to https://www.microsoft.com/en-us/download/details.aspx?id=45496.
- The BeyondTrust Management Console and the reporting components must be installed.

ℹ️ For more information, please see the AD Bridge Enterprise Installation Guide at https://www.beyondtrust.com/docs/ad-bridge/documentation.htm.

- When you install AD Bridge Enterprise, you must install the following components:
    - **Reporting Components**
    - **Database Update and Management Tools**
    - **Operations Dashboard**

SQL Server

- Install SQL Server 2008 R2 or higher so you can create the AD Bridge Enterprise database and set security options.

Data Collector

- .NET Framework version 4.5.
- Microsoft Windows Server 2008 R2 or higher to act as a server for the event collector server.
- The requirements to run the collector in an enterprise are as follows. The requirements might vary with the size of your network. It is suggested that you use a separate collector for every 1,000 computers that are forwarding events to a collector.

Item	Requirement
Memory	8GB
Disk space	10GB free disk space (for local event storage before copying to the central database). The size you require might vary depending on the number of events, the number of systems, and other factors.
Processor	2GHz dual core
Network	1Gb Ethernet (at least, to database server)

Configure SQL Server

This section provides information on configuring a database instance on a Windows Server using SQL Server.

> **⚠ IMPORTANT!**
>
> *This section assumes you are a database administrator who knows how to set up and administer SQL Server, including configuring the database to comply with your IT security policy.*

> ℹ For a complete list of prerequisites for Microsoft SQL Server 2008 R2 or higher, please see Hardware and Software Requirements for Installing SQL Server at https://msdn.microsoft.com/en-us/library/ms143506.aspx.

Plan SQL Server Database Security

Although the SQL Server database will contain no user passwords or other highly confidential information, it will contain a list of user accounts, information about what users are allowed to access what resources, and other information that could be used for nefarious purposes. In considering the security of the database, you should ask yourself several questions:

- Who will be allowed to write to the database?
- Who will be allowed to read from the database?
- What accounts will be used to access the database?

Data is written to the database in several cases:

- When a collector copies events to the database.
- When the **LDBUpdate** process writes information from Active Directory to the database.
- When administrators perform maintenance operations on the database (for example, creating or restoring event archives).

Active Directory Groups and SQL Server Roles

The following tables provide general guidelines on securing reporting components. Create the following Active Directory groups.

Active Directory Group	Description
ADB_DB_Administrators	Contains accounts that are required to configure and maintain the reporting database. We recommend that a minimum number of AD Bridge Enterprise administrators tasked with maintaining the reporting infrastructure are included here.
ADB_Collectors	Contains the service accounts used to run the Collector services.
ADB_DB_Archive_Administrators	Contains the service accounts used for automated archiving.
ADB_Report_Viewers	Contains accounts that need to run reports only.
ADB_LDBUpdate	Contains the service accounts that need to run the **LDBUpdate** tool to import Active Directory information into the database.

Create the following roles with the minimum permissions on the SQL Server database and assign to the corresponding Active Directory groups.

TC: 1/31/2020

Role	Access
ADB_DB_Administrators	dbo
ADB_Collectors	Collectors : insert, select, update CollectorsStat : insert, select, update, delete Events : insert CollectorsView : select
ADB_DB_Archive_Administrators	Archives: insert, select, update, delete Events: select, delete
ADB_Report_Viewers	All Tables: select
ADB_LDBUpdate	dbo

These suggestions are based on using Windows authentication. Windows Authentication simplifies the implementation of database security. To use SQL Server authentication, you must embed user names and passwords in the collector servers and in the BeyondTrust Management Console. This practice is not recommended.

Install and Configure SQL Server

We recommend that you set up the database on a new server.

> ℹ️ For more information on setting up SQL Server, please see SQL Server technical documentation at https://technet.microsoft.com/sqlserver/.

1. Download SQL Server 2008 R2 or higher.
2. Install SQL Server.
3. Using SQL Server Configuration Manager, set the SQL Server Network Configuration protocols to allow external connections with named pipes:
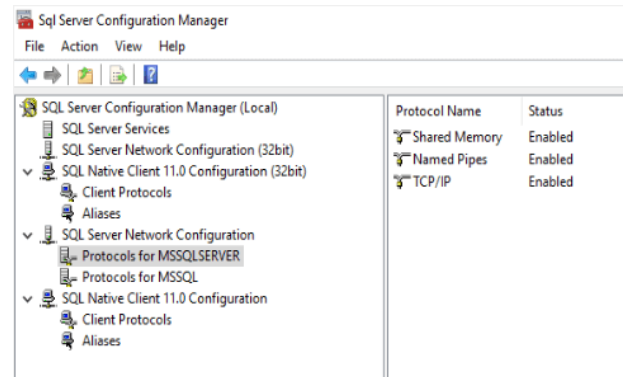
Create the LikewiseEnterprise Database

You can create the database using the AD Bridge Enterprise installer or using SQL Server.

Use the Installer

To create the database using the installer:

1. Run the **install .exe**.

2. Click **Accept** on the license page, and then click **Skip** until you reach the **Reporting Options** page.

3. Click **Search Server** to find existing SQL Server instances.

4. Click **Connect**.

5. Click **Create Database**. The database script runs.

6. Click **OK**, and then click **Finish** to close the installer.

Use SQL Server

To create the AD Bridge Enterprise Reporting Database using SQL Server:
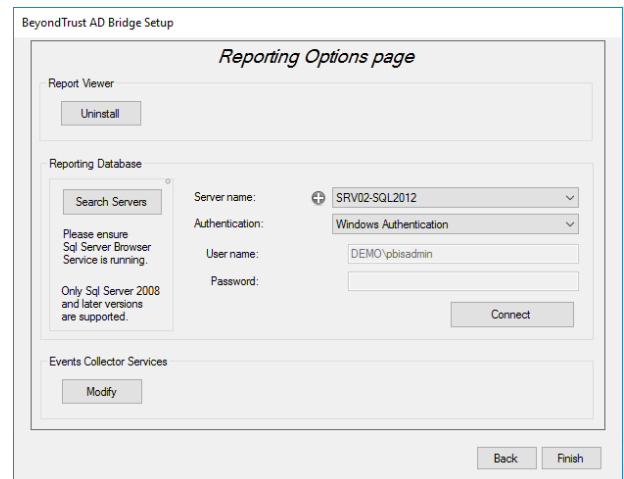
1. Start Microsoft SQL Server Management Studio and connect to the database engine.

2. Create a database named **LikewiseEnterprise**.

3. Copy the SQL Server database creation script from the installation media to a location accessible from SQL Server:

```
CreateLikewiseEnterpriseDatabase.sql
```

4. In SQL Server Management Studio, on the **File** menu, click **Open** and load the AD Bridge Enterprise database creation script:

```
CreateLikewiseEnterpriseDatabase.sql
```

5. Connect to the **LikewiseEnterprise** database, and run the script. If the script executes with errors, run the script again.

Install the Collectors

Use the database utilities package (**PowerBrokerDBUtilities.exe**) to install the following collectors to your data collection server:

- **BTCollector:** Contains RPC server code to enable the agent's forwarding service, **eventfwd**, to upload events to the database server by using secure, authenticated transport protocols. **BTCollector** runs as a Windows autostart service and can be managed from the command line.

- **BTEventDBReaper:** Copies events from the collector server to the central database. The process runs as a Windows auto-start service and can be managed from the command line. **BTEventDBReaper** depends on **BTCollector** to function properly: If **BTCollector** is not running, **BTEventDBReaper** will fail.

In a network with only a few computers or for testing, you can install the collectors on the same server as the AD Bridge Enterprise database.

1. Run the AD Bridge Enterprise Database Utilities installer program (**PowerBrokerDBUtilities-x.x.x.xxxx.exe**) in **C:\Program Files\BeyondTrust\PBIS\Enterprise** or on your AD Bridge Enterprise installation media).

   Follow the instructions in the installer. Install all the database tools listed in the installer.

2. In the **Database Provider Library** box, enter the following string:

   System.Data.SqlClient

3. In the **Connection String** box, enter the following string, where **DBSERVERNAME** is the name of the server running SQL Server and containing the Enterprise database.

   The **Initial Catalog** clause identifies the database to use while **Integrated Security=True** specifies that Windows authentication should be used when connecting to the database server.

   ```
   Data Source=DBSERVERNAME;Initial Catalog=LikewiseEnterprise;Integrated Security=True
   ```

   Example:

   ```
   Data Source=W2K12-R2\SQL;Initial Catalog=LikewiseEnterprise;Integrated Security=True
   ```

4. Click **Next**.
5. Click **Install**.

Set the Start Order for Collector Processes

If the collectors are installed on the same machine as the database, the collector services (**BTCollector** and **BTEventDBReaper**) must start after the Microsoft SQL Engine. **BTCollector** must start before **BTEventDBReaper**.

> ℹ️ For more information on setting dependencies for system services, please see CreateServiceA function at https://msdn.microsoft.com/en-us/library/ms682450(VS.85).aspx.

> ℹ️ For an example of how to create a service dependency, please see Delaying Startup Services at http://www.windowsnetworking.com/kbase/WindowsTips/Windows2003/RegistryTips/DelayingStartupServices.html.

Verify the Collector Processes Are Running

BTCollector and **BTEventDBReaper** are started automatically. You can run the following commands to confirm the processes are running.

Verify BTCollector is Running

1. Run the following command on the Windows computer running the collector:

```
C:\Program Files\BeyondTrust\PBIS\Enterprise>sc query BTCollector

SERVICE_NAME: BTCollector
        TYPE              : 10  WIN32_OWN_PROCESS
        STATE             : 4  RUNNING
                               (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN))
        WIN32_EXIT_CODE   : 0  (0x0)
        SERVICE_EXIT_CODE : 0  (0x0)
        CHECKPOINT        : 0x0
        WAIT_HINT         : 0x0
```

2. Run the following command if the collector is not running:

```
C:\Program Files\BeyondTrust\PBIS\Enterprise>sc start BTCollector
```

Verify BTEventDBReaper is Running

1. Run the following command:

```
C:\Program Files\BeyondTrust\PBIS\Enterprise>sc query BTEventDBReaper

SERVICE_NAME: BTEventDBReaper
        TYPE              : 10  WIN32_OWN_PROCESS
        STATE             : 4  RUNNING
                               (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE   : 0  (0x0)
        SERVICE_EXIT_CODE : 0  (0x0)
        CHECKPOINT        : 0x0
        WAIT_HINT         : 0x0
```

2. Run the following command if the collector is not running:

```
C:\Program Files\BeyondTrust\PBIS\Enterprise>sc start BTEventDBReaper
```

Configure the Collectors Using the Shell Prompt

You can use the shell prompt as an alternative to configuring the collector services using the BeyondTrust Management Console.

ℹ️ For information about configuration using the console, please see Configure the Collectors.

Configure the Collector Service Using the Shell Prompt

You can configure the following performance and security settings on **BTCollector**:

- Set the maximum number of events that an endpoint can send
- Set how frequently the endpoints connect to the collector and send data
- Set permissions on a collector that services more than one domain.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

46

A provider name and a connection string are the only required parameters to run the **BTCollector**, which is auto-started as a Windows process at **C:\Program Files\BeyondTrust\PBIS\Enterprise**.

Run the following command to view the arguments:

```
C:\Program Files\BeyondTrust\PBIS\Enterprise>BTCollector /h
```

Option	Description
/h	Display help.
/p <integer>	Set the maximum number of events that an endpoint can send to a collector per period. A period consists of sending multiple batches and then sleeping until the period is over. This number, in combination with the **/t** parameter, can be set to control the load on endpoints imposed by the event forwarding service (**eventfwd**) sending events to collectors. If this number is large, the event forwarder might consume excessive CPU time and network bandwidth. If the number is small, however, the endpoint might fall behind with the incoming event rate and end up with a large backlog of uncollected events.
/b <integer>	Set the records that the event forwarder can send per batch. A batch is sent with a single RPC call, so setting this too high delays adding any records in the batch until the entire batch is sent. The collector sends events in batches until the number of sent events reaches the value that you set (or until there are no more left to send, whichever number is smaller). If set too high, the network transaction might fail because of a connection that times out. If set too low, the event forwarding service might consume too much CPU time and bandwidth because there are more network transactions.
/t <integer>	Set the forwarding period in seconds. If an event forwarder finishes sending its events before this length of time is up, it will sleep to finish the period. The parameter controls how often the endpoint connects to the collector to forward events. If the forwarding period is set to 300 seconds, for example, the endpoint event forwarder service sends events to a collector once every 5 minutes. The smaller the number is, the more frequently endpoints communicate with collectors and the smaller the latency between the time when an event is generated and when it appears in the database. If the number is too small, however, it can result in excessive load on the endpoints and in excessive network traffic.
/a <string>	Sets the access control list (ACL) of the computers allowed to communicate with the collector. The remote access security descriptor uses SDDL syntax. The default value is **O:LSG:BAD:PAR(A;;CCDCRP;;;BA)(A;;CCDCRP;;;DA)(A;;CC;;;DC)**. The parameter sets configuration information that affects the collector rather than the endpoints that communicate with it. By default, the ACL for the collector's RPC port is set to allow computers in the Active Directory Domain Computers group to write to the collector. This is the permission set by the long SDDL formatted string shown in the usage information for the **/a** parameter. In the case of collectors that are servicing multiple domains, however, this ACL is insufficient as it allows only endpoints joined to the same domain as the collector to write to it. In such cases, you can use the **/a** parameter to specify a more inclusive ACL.

Option	Description
/l *<level>*	Set the log level to **error**, **warning**, **info**, **verbose**, or **debug**.
/s	Show the current settings.

The **/s** parameter shows the default settings:

```
C:\Program Files\BeyondTrust\PBIS\Enterprise>BTCollector /s
Current settings:
Records per period        10000
Records per batch         100
Seconds in a period       10
Database location C:\Program Files\BeyondTrust\PBIS\Enterprise\BTCollector.db
Remote access security descriptor O:LSG:BAD:P(A;;CC;;;DC)(A;;CC;;;DA)(A;;RP;;;DA)(A;;DC;;;DA)
 (A;;CC;;;BA)(A;;RP;;;BA)(A;;DC;;;BA)(A;;CC;;;S-1-5-21-418081286-1191099226-2202501032-515)
```

Remote Access Permissions

The remote access security descriptor shown in the above output is the default. It provides the following group accounts with these permissions:

- Domain Computers are allowed to create children (add events)
- Domain Administrators are allowed to create children (add events)
- Domain Administrators are allowed to read properties (read events)
- Domain Administrators are allowed to delete children (delete events)
- Built-in AD Bridge Enterprise Administrators are allowed to create children (add events)
- Built-in AD Bridge Enterprise Administrators are allowed to read properties (read events)
- Built-in AD Bridge Enterprise Administrators are allowed to delete children (delete events)

The ACL is stored in the Windows registry of the collector server. The AD Bridge Enterprise console writes the ACL to the AD Bridge Enterprise database. The **BTEventDBReaper** service pulls it from the database and writes it to the registry.

Configure the Reaper Service Using the Shell Prompt

BTEventDBReaper gathers events from a collector (forwarded by endpoints) and writes the events to the database. **BTCollector** stores incoming events in a local, intermediate, database while **BTEventDBReaper** writes the events to the central SQL Server database.

BTEventDBReaper runs as a Windows service, but can be run from the command line to set up parameters for the service.

To view **BTEventDBReaper** arguments, execute the following command:

```
C:\Program Files\BeyondTrust\PBIS\Enterprise>BTEventDBReaper /?
```

Option	Description
/?	Display help.
/gui	Opens a GUI where you can set the database provider and connection string. Use as an alternative to command-line.

Option	Description
/d PROVIDER	Sets the database provider: **System.Data.SqlClient** for SQL Server (default) or **MySql.Data.MySqlClient** for MySQL.
/c DBSTRING	Sets the database connection string to connect to the BeyondTrust database.
/f NUMBER	Sets the earliest record id that should be copied when the agent runs. Use this parameter with caution. The **/f** parameter is used to control the point at which the first event in the local collector database is written to the central AD Bridge Enterprise database. Under normal circumstances, it should not be necessary to set this parameter.
/r	Refreshes the agent with new registry settings.
/s	Shows the current status.
/debug	Run as command line application with logging.

Any parameters set from the command line take effect the next time that **BTEventDBReaper** runs. To apply the settings immediately, run **BTEventDBReaper** with the **/r** argument.

The **/s** option is used to display the current configuration settings for the service:

```
C:\Program Files\BeyondTrust\PBIS\Enterprise>BTEventDBReaper /s

Current settings:
    Database provider:     System.Data.SqlClient
    Connection string:     Data Source=RVLN-BUILD;
                           Initial  Catalog=LikewiseEnterprise;
                           Integrated Security=True
    Record id last copied: 1794
    Records per period:    300
    Seconds in a period:   1200
```

Although the settings include **records per period** and **seconds in a period**, the parameters cannot be configured from the command-line. The default values can be changed using the Enterprise Database Management plug-in.

Connect the Management Console to the Database

This section assumes the BeyondTrust Management Console and the following AD Bridge Enterprise components are installed: **Reporting Components**, **Database Update and Management Tools**, **Operations Dashboard**.

To add the Enterprise Database Management plug-in and connect to the database server instance:

1. In the console tree, right-click the **Enterprise Database Management** node and then click **Connect to database**.
2. Click **Change**.
3. Select **Microsoft SQL Server**, and then enter the name of your database server instance in the **Server/Instance** box.
4. Enter the credentials of your database definer account.

Configure the Collectors

You can configure performance and security settings on the **BTCollector**. This section shows you how using the management console.

> ℹ️ For more information on how to use the shell prompt, please see Configure the Collectors Using the Shell Prompt.

On the **BTReaper** service, you must set up the service so that it can send events to the SQL Server database.

Configure Performance Settings on the Collector Service

> ℹ️ For detailed descriptions on the performance parameters, please see Configure the Collector Service Using the Shell Prompt.

To change the parameters on the **Collector** service:

1. In the console tree, expand **Enterprise Database Management**.
2. Right-click **Collector Status**, and then select **Set collector parameters**.

   Alternatively, in the list of collectors, right-click the collector that you want to modify, and then select **Set collector parameters**.

3. Set the following parameters (or use the default values):

   - **Period (seconds):** 15
   - **Maximum events per period:** 5000

   Endpoint Parameters

   - **Period (seconds):** 10
   - **Maximum events per period:** 1000
   - **Events per batch:** 250

Configure Security Settings on the Collector Service

You can configure the access control list (ACL) for the remote procedure calls that take place between the collector and its endpoints.

1. In the console tree, expand **Enterprise Database Management**.
2. Right-click **Collector Status**, and then select **Set collector parameters**.

   Alternatively, in the list of collectors, right-click the name of the collector, and then select **Set collector parameters**.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

50

3. Click **Set Permissions**:
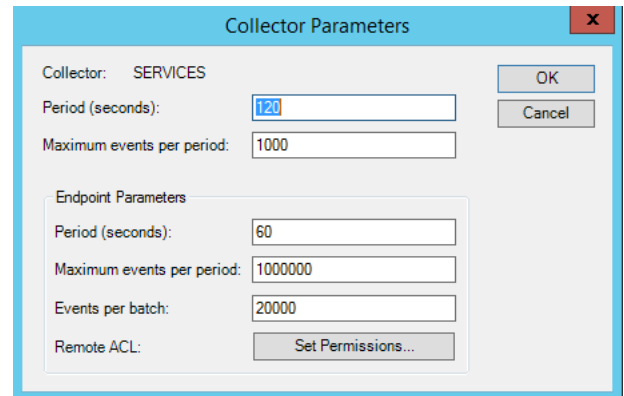
4. Set the following permissions.

   - **ADB_DB_Administrators:** Full Control

     Required to change the **Collector** database using the **btcollector-cli.exe** command.

   - **Domain Computers:** Write Events

     Required for agents to write events to the **Collector** database. When using the **Collector** server cross-domain it is also necessary to add Write Events access to computer accounts from remote domains.

   - **Reaper Service Account:** Full Control

     Required for the **Reaper** to remove events from the **Collector** database after committed to the SQL Server database. Use the account that you create in Configure the Reaper Service.

   - **Collector Server Computer Account:** Full Control

     Required for the system to have full access to the **Collector** database.
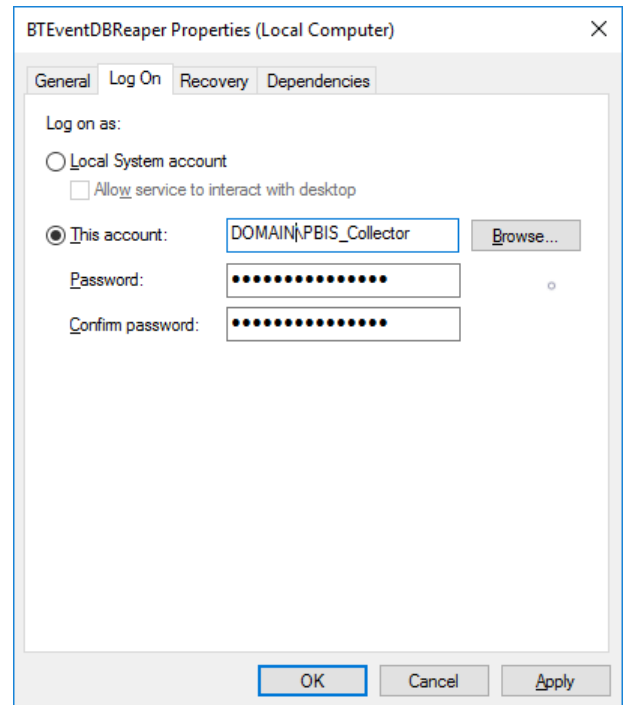
5. Restart the **Collector** service.

Configure the Reaper Service

The **BTEventDBReaper** service needs to write events to the SQL Server database. To do this, the service must be modified to run using a service account that is a member in the **ADB_Collectors** group. The **ADB_Collectors** group was created earlier during the database planning and setup.

> ℹ️ For more information, please see Plan SQL Server Database Security.

1. Create an account to run the **BTEventDBReaper** service under.
2. Add this account to the **ADB_Collectors** group (to grant database access).
3. Grant the account Read and Write access to the following registry keys on the local Collector box:
   - **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\BTEventDBReaper**
   - **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\BTCollector**

4. Modify the **BTEventDBReaper** service to **Log on as** this account.

5. Restart **BTCollector** (which will also restart **BTEventDBReaper**).
6. Review the **Application Log** on the local **Collector** server to ensure the services started without error.

Run the Database Update Script

You can run the **LDBUpdate** script from the command-line or from the BeyondTrust Management Console.

The **LDBUpdate** script is a batch program for Windows that reads information from Active Directory and writes it to the AD Bridge Enterprise database so you can generate reports about computers and users in Active Directory. You can run the update script on demand from the BeyondTrust Management Console, or you can set it up as a scheduled task.

If the information in Active Directory has changed since you last ran the script and if you want those changes included in your reports, run the script before you generate your reports.

To access Active Directory, the **LDBUpdate** script uses the LDAP and RPC ports.

The **Update DB** button will only be enabled if the update utility is available on the current machine. The AD Bridge Enterprise installer allows you to select whether the utility is installed on a machine.

Ensure the following is in place before you run the script:

*   To run the utility, the current user must have privileges to read and write to any table in the Enterprise database.
*   The Windows administrative workstation where you run the script must be connected to Active Directory.
*   The user account that runs the script must have at least read permission for objects and child objects in Active Directory.

To run **LDBUpdate** from the console:

1. In the BeyondTrust Management Console, on the **File** menu, click **Add/Remove Plug-in**.
2. Click **Add**.
3. Click **Audit and Access Reporting**, and then click **Add**.

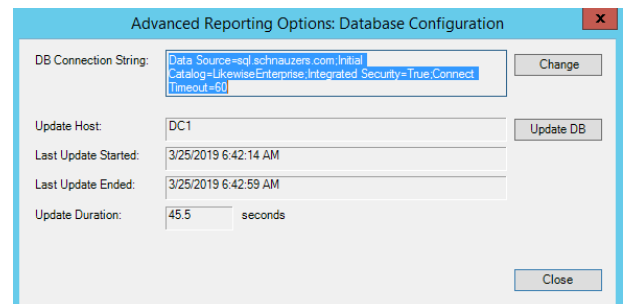4. Click **Close**, and then click **OK**.

5. In the console tree, click the **Audit and Access Reporting** node and then click **Advanced**.
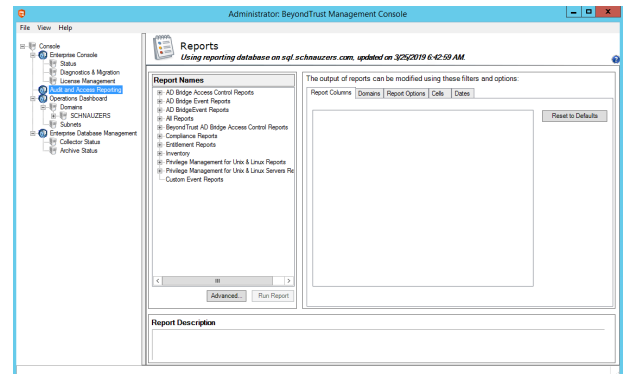
6. Click **Update DB**, and then click **Run**.

7. Click **Close**.

Run the Database Update Script from the Command Line

To view the command-line options for LDBUpdate, run the following command:

```
C:\Program Files\BeyondTrust\PBIS\Enterprise>ldbupdate.exe /? Usage:  LDBUpdate OPTIONS
Where OPTIONS include:
-f LDAPPATH           Path of the forest to synchronize; required
-d FQDN               Domain (in forest or in trusts) to process; can repeat
-o FILE               Send output to FILE
-p PROVIDER           Use PROVIDER as the database type(default: System.Data.SqlClient)
-c STRING             Use STRING as the database connection parameter
-nogpo                Don't analyze GPOs (faster)
-v                    Display verbose output
--force               Ignore the database status and perform update even if marked as busy
--debug               Display debug level output
--transaction         Perform all database operations under a single transaction.
                      Allow interactions to the database with reporting tools while
                      update is performed in the background.
--class STRING        Identify the objects to update, leaving others as is from a
                      previous update.(Examples: Users, Groups, GPOLinks, GPOs, Computers).
                      Can be repeated to identify several class types
                      LDBUpdate --class Users --class Groups -f <domain>...
--help                Displays this usage information
If the -d option is not specified, all the domains in the forest and inany trusted forests will be
processed.
```

Here is an example of how to use the command-line utility to set the provider and the connection string for a SQL Server database:

```
ldbupdate.exe -f dc=example,dc=com -p System.Data.SqlClient -c "Data Source=RVLN-BUILD; Initial
Catalog=LikewiseEnterprise; Integrated Security=True" --force
```

Configure Agents to Forward Events to the Collector Service

You can globally set the agents to forward events by configuring an AD Bridge Group Policy setting. You can also cull events from syslog.

Configure Event Forwarding with Group Policy

The Event Forwarder policy setting modifies the settings in the AD Bridge registry to forward events from agent computers to the **BTCollector** service that resides on a Windows computer.

> ⚠ **IMPORTANT!**
>
> *To use this policy, you must first turn on event logging. For more information, see the* AD Bridge Group Policy Administration Guide *at* https://www.beyondtrust.com/docs/ad-bridge/documentation.htm*. Depending on your network configuration, you may also have to configure a policy setting to specify the service principal of the collector.*

To configure event forwarding using policy settings:

1. In the **Group Policy Management Console**, create a Group Policy Object (GPO) for an organizational unit, and then edit it in the **Group Policy Management Editor**.

2. In the console tree, expand **Computer Configuration > Policies > Unix and Linux Settings > BeyondTrust Settings > AD Bridge Settings**, and then click **Event Forwarder**.
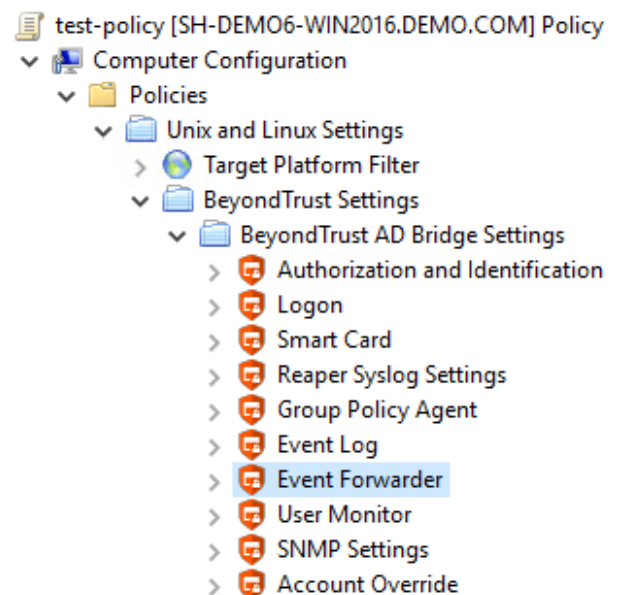
3. Double-click **Event log collector**, and then check the **Define this policy setting** box.
4. Enter the host name of the computer running **BTCollector**. Example: **w2k3-r2.example.com**

Cull Events from Syslog

To collect sudo events and other system events that appear in syslog, you must configure syslog to write data to a location where the AD Bridge Enterprise **reapsysl** service can find it and copy it to the local event log.

> 📌 **Note:** *You can set an AD Bridge Enterprise Group Policy setting to modify /etc/syslog.conf on target computers.*

The **reapsysl** service creates three named pipes and picks up the syslog information written to them:

```
/var/lib/pbis/syslog-reaper/error
/var/lib/pbis/syslog-reaper/warning
/var/lib/pbis/syslog-reaper/information
```

To configure syslog to write to the pipes, add the following lines to **/etc/syslog.conf**:

```
*.err           /var/lib/pbis/syslog-reaper/error
*.warning       /var/lib/pbis/syslog-reaper/warning
*.debug         /var/lib/pbis/syslog-reaper/information
```

The last entry is not analogous to the first two. Some versions of syslog require a tab character instead of spaces to separate the two components of each line.

> ℹ️ For more information, please see your syslog documentation.

After you modify **syslog.conf**, you must restart the syslog service for the changes to take effect:

```
/etc/init.d/syslog restart
```

Troubleshooting Checklist

The checklists in this section can help you troubleshoot problems with the reporting components.

Endpoints

To check for endpoint problems, confirm the following:

- **eventlog** service running
- **eventfwd** service running
- **reapsysl** service running
- **eventfwd** service properly configured
- Collector name resolvable and address reachable
- Collector principal properly set
- **/etc/syslog.conf** properly configured
- Events present in local event log (test with **eventlog-cli**)
- **eventfwd** service seems to forward messages properly (run from command-line to test)
- Firewall not blocking RPC access of collector server

Collector Servers

To check for problems with the collector servers, confirm the following:

- **BTCollector** service running
- **BTEventDBReaper** service running
- Events present in local collector database (test with **BTCollector-cli**)
- **BTEventDBReaper** properly configured (test with **BTEventDBReaper /s**)
- Database provider and connection string properly set
- Collector ACL allows endpoints to write to it (set with Event Management Console)
- Collector machine account has sufficient privileges to write to database
- No unusual errors in Windows event log (run **eventvwr.exe**)
- Firewall not blocking incoming RPC connections or outgoing database connections

Database

To check for problems with the database, confirm the following:

- Can connect to it with SQL Server Management Studio
- **Events** table contains events
- **EventsWithOUName** view contains events
- Database security set to allow writing by collector servers, by **ldbupdate** user, and by administrators
- **ldbupdate** utility recently run to account for new endpoints joined to AD
- Named-pipe client access enabled in SQL Server
- Firewall not blocking incoming database connection

Windows Reporting Components

To check for problems with the Windows reporting components, confirm the following:

- Database connection strings set properly
- User has sufficient privileges to access database
- Firewall not blocking database connections

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

56

TC: 1/31/2020

Run Reports

ℹ️ For a list of reports available in AD Bridge Enterprise, refer to the *AD Bridge Report Book*.

Generate a Sample Report

You can generate reports using the **Audit and Access Reporting** plug-in for the BeyondTrust Management Console.

The following procedure shows how to create a computer access report.

1. In the BeyondTrust Management Console tree, click the **Audit and Access Reporting** node.
2. Under **Report Names**, expand **All Reports**, and then click **Computer Access Report**.
3. Click **Run Report**.
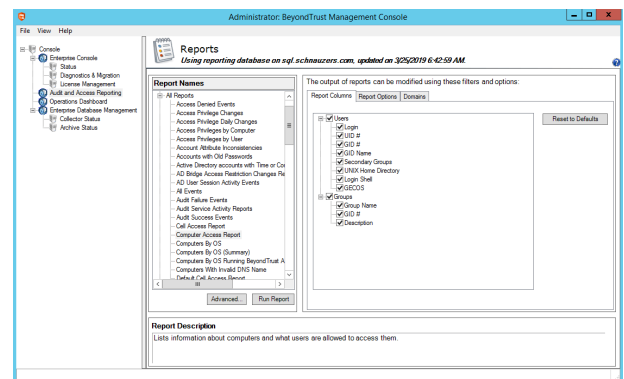
Entitlement Reporting

Entitlement reporting can provide a detailed analysis of accounts. You can use it to help review how group memberships impact access for users. You can also use entitlement reports as part of your regulatory compliance efforts.

The AD Bridge Enterprise agent includes a User Monitor service that logs entitlement changes detected from local accounts and groups on each end-point computer, as well as Active Directory (AD) changes that could affect account access and roles on computers.

All detected changes in entitlement are recorded in the Event Log subsystem for each AD Bridge Enterprise agent. Using event forwarding, this data can be sent to an AD Bridge Enterprise audit collector computer that can provide reporting across a centralized, enterprise-wide database.

📌 *Note: For AD users, the User Monitor reports only the users who have access to the computer due to the **RequireMembershipOf** setting. If **RequireMembershipOf** is not enabled, a special pseudo user is reported. If the computer is running in unprovisioned mode, the pseudo user uses the **All Users accessible from domain %s** format; otherwise the pseudo user uses the **All Users in cell %s** format.*

The User Monitor only reports the AD groups of which at least one of the reported AD users is a member.

The following entitlement reports are available.

Access Privileges by User

This entitlement report, organized by user name, shows which users can log into which computers and how that list has changed over time. The state of access privileges at the start date and end date are compared. Intermediate changes are not shown, so if a

SALES: www.beyondtrust.com/contact **SUPPORT:** www.beyondtrust.com/support **DOCUMENTATION:** www.beyondtrust.com/docs

57

new user is added then deleted in the middle of the reporting time span, no change is shown in the report.

The status date field indicates the date of the last change to the user during the report time span. If a user was added and later the user's UID was changed, the date of the UID change is shown in the report.

When all of the fields in multiple rows match except for **Computer Name** and **Status Date**, those rows are collapsed so that one row is shown with a space separated list of the computers to which it applies.

When the **User Display Name**, **UID**, or **Account Type** is changed, the new value is shown followed by an asterisk.

Access Privileges by Computer

This entitlement report, organized by computer name, shows which users can log into which computers and how that list has changed over time. The state of access privileges at the start date and end date are compared. Intermediate changes are not shown, so if a new user is added then deleted in the middle of the reporting time span, no change is shown in the report.

The status date field indicates the date of the last change to the user during the report time span. If a user was added and later the user's UID was changed, the date of the UID change is shown in the report.

When the **User Display Name**, **UID**, or **Account Type** is changed, the new value is shown followed by an asterisk.

Access Privilege Changes

This entitlement report shows changes to user privileges by date. Every change is shown, including changes that are later undone. This report does not provide a list of all users who can log into the computers, only those users for which there have been changes.

When the **User Display Name**, **UID**, or **Account Type** is changed, the new value is shown followed by an asterisk.

Access Privilege Daily Changes

This entitlement report shows changes to user privileges on a daily basis. Every change is shown, including changes that are later undone. This report does not provide a list of all users who can log into the computers, only those users for which there have been changes.

This report provides the same information as the Access Privilege Changes by User report, but with simplified search criteria.

When the **User Display Name**, **UID**, or **Account Type** is changed, the new value is shown followed by an asterisk.

Account Attribute Inconsistencies

This entitlement report shows conflicts between UID, username, and GECOS.

BeyondInsight Reporting

The AD Bridge GPO, **User Monitor**, sends the following data to the **BTEventDBReaper** service that then forwards the data to BeyondInsight:

- Users that are added, deleted, or changed.
- If the user has the Allow Logon rights GPO set, then changes and deletions are recorded.

No historical data is retained in the BeyondInsight database. Data is overwritten when new updates are sent to the BeyondInsight database.

Requirements

- On the domain controller, turn on **User Monitor**.
- If running an earlier version of **User Monitor**, you must upgrade the **BTEventDBReaper** service before upgrading User Monitor.
- After **BTEventDBReaper** is upgraded, you can upgrade the agent. If the **BTEventDBReaper** service is not updated first, it cannot process the records from the agent which will result in a failure of processing data.
- **Allow Logon Rights** must be turned on and configured for users and groups that you want to log into the agents.
- AD Bridge Enterprise collectors must be installed.

> ℹ️ For more information, please see Install the Collectors.

- BeyondInsight 6.2 or later.

Generate a Certificate

Generate a client certificate using the BeyondInsight Configuration tool. A certificate must be created and copied to the AD Bridge server certificate store to ensure secure communications.

To generate a certificate:

1. Run the configuration tool, and then click **Certificate Management**.
2. Select **Generate Certificate**, and then select **Client Certificate** from the **Certificate type** menu.
3. Enter a password.
4. Click **OK**.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

59

Copy the Certificate to the AD Bridge Enterprise Server

1. Log into the AD Bridge Enterprise server, open MMC and add the Certificates Snap-in for the Local Computer account.
2. Expand **Certificates (Local Computer)**.
3. Right-click **Trusted Root Certificates > All Tasks > Import**.
4. Import the certificates created using the BeyondInsight Configuration tool.
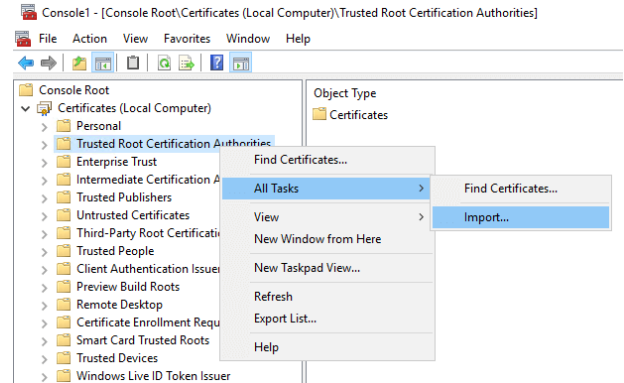

Run the DBUtilities Tool

You must establish a connection to the BeyondInsight server.

To run the **DBUtilities** tool:

1. From the Start menu, select **Reporting Database Connection Manager**. You must run the connection manager as Administrator. Right-click the menu item, and then select **Run as administrator**.

   - Alternatively, you can also run the tool from the command line:

     ```
     bteventdbreaper /gui
     ```


2. Select the **Enable BeyondInsight** check box.
3. Enter the URL to the BeyondInsightserver.
4. Enter the name of the client certificate generated earlier.
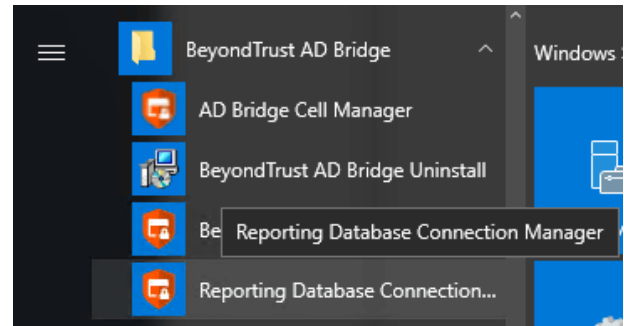
5. Optionally, create a workgroup name. A workgroup name can be used as a unique identifier.
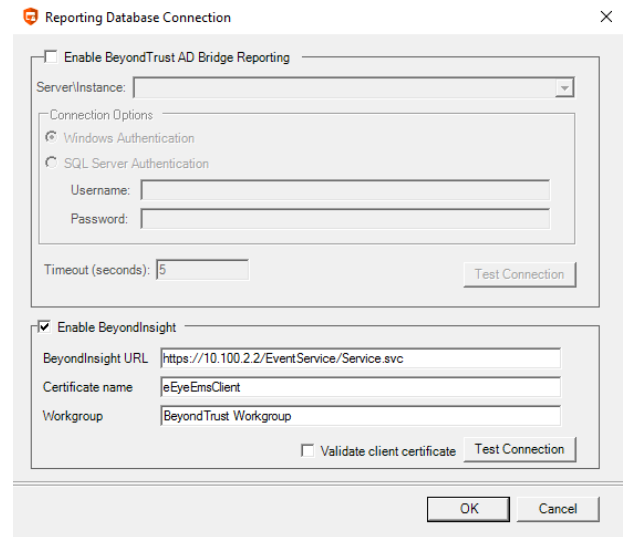
6. Click **Test Connection** to ensure the connection between the servers is successfully established.
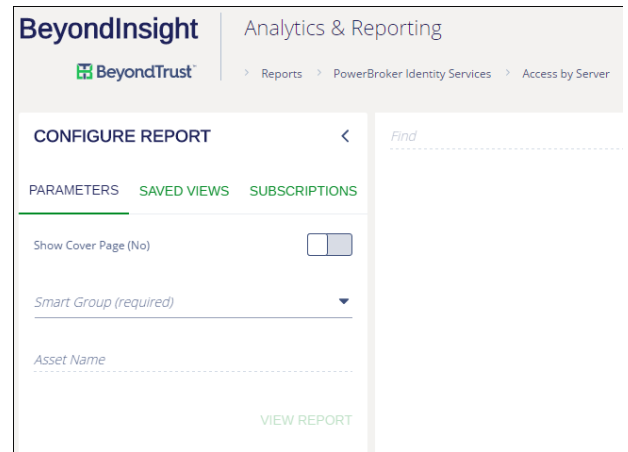7. Click **OK**.

View Reports in BeyondInsight Analytics and Reporting

1. Log into **Analytics and Reporting**.
2. Select **View All Reports** from the menu.
3. Select **AD Bridge**.

4. Select a report.

5. Enter the report parameters, and then click **View Report**.

Monitor Events with the Operations Dashboard

The AD Bridge Enterprise Operations Dashboard is a management plug-in for the BeyondTrust Management Console. The dashboard runs on a Windows administrative workstation connected to the AD Bridge Enterprise Reporting Database and an Active Directory domain controller.

The dashboard retrieves information from the AD Bridge Enterprise database to display authentication transactions, authorization requests, network events, and other security events on Linux, Unix, and macOS computers.

Monitoring events such as failed logon attempts and failed sudo attempts can help prevent unauthorized access to commands, applications, and sensitive resources.
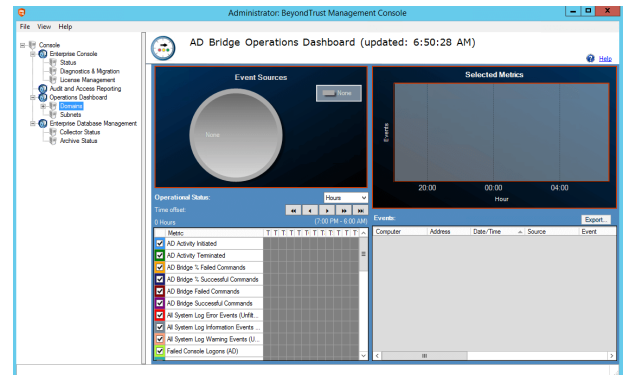
The following are some of the events the dashboard can display. You can also create and monitor custom events.

- All Success Audit Events
- All System Log Error Events
- Console Logons (AD or Local)
- Domain Joins
- Domain Leaves
- Failed Console Logons (AD or Local)
- Failed Group Policy Updates
- Failed Kerberos Refresh
- Failed Password Change
- Failed Root Logons (Local)
- Failed SSH Logons (AD or Local)
- Failed Sudo
- AD Bridge Enterprise Services Failures
- Network Offline Warning
- Root Account Logons (Local)
- SSH Logons (AD or Local)
- Sudo

Configure Settings for the Dashboard

The dashboard, by default, is set to display selected metrics. As you become familiar with the metrics in the dashboard, you can customize settings so you can track critical activities occurring in your clients.

You can change the list of metrics displayed, configure alerting, change the refresh rate for the display, and customize metrics.

Add the Dashboard to the Console

By default, the **Operations Dashboard** node is displayed in the BeyondTrust Management Console. If it is not displayed, you can add the dashboard plug-in to the console.

1. On a Windows administrative workstation, start the BeyondTrust Management Console.
2. From the **File** menu, click **Add/Remove Plug-in**.
3. Click **Add**.
4. Click **Operations Dashboard**, click **Add**, and then click **Close**.
5. Click **OK**.

Connect to a Database

To connect to a database or change your database connection:

1. Log into the BeyondTrust Management Console.
2. Right-click **Operations Dashboard** and then click **Connect to**.
3. Click **Change**.
4. Select the database type.
5. From the **Server/Instance** list, select the instance, and then select the credentials.
6. Click **OK**.

Change the Refresh Rate

You can change the minutes that pass before the information on the dashboard is updated with the latest metrics. The default value is 5 minutes.

To change the refresh rate:

1. Log into the BeyondTrust Management Console.
2. Right-click **Operations Dashboard** and then click **Metric settings**.
3. In the **Refresh Interval** box, enter the minutes that pass before the information on the dashboard is updated with the latest metrics.
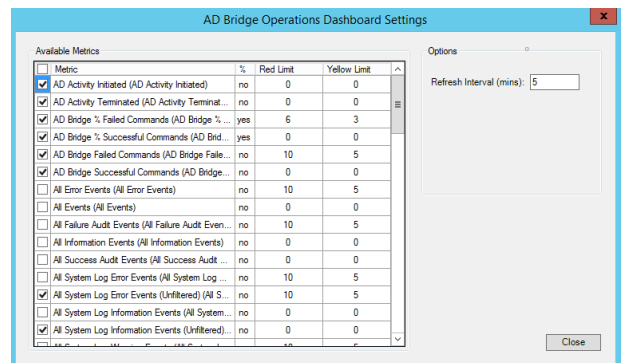

4. Click **Close**.

Change the Metrics to Display

You can change the metrics that you want to display on the **Operations Dashboard**.

1. To change the metrics displayed, log into the BeyondTrust Management Console.

2. Right-click the **Operations Dashboard** node, and then click **Metric settings**.

3. Scroll through the list of metrics and select or clear the check boxes depending on the metrics that you want to display.

   After you change the metrics, the database update program runs to ensure the data between the database and Active Directory is synchronized.
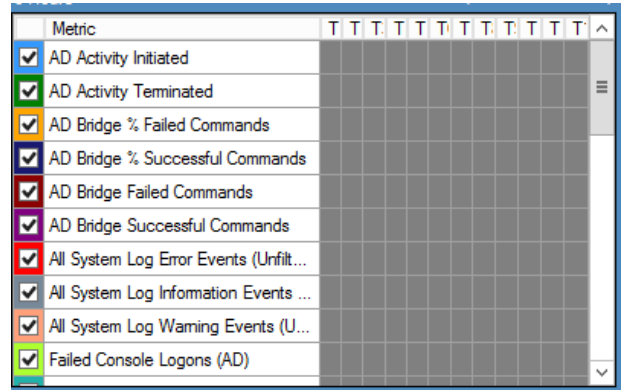
Change the Properties for a Metric

You can configure the following properties for a metric:

- Warning limits

  For example, you might want to set a Red flag limit on a metric. When the activity exceeds that value, a Red flag is issued.

- Alerts

  If you configure the warning limits, you can set an alert that will be issued when the limit is reached.

- Add a query that adds the total number of events.

To set properties for a metric:

1. Log into the BeyondTrust Management Console.

2. Expand the **Operations Dashboard** node.

3. Right-click the **Domains** node, or **Subnets** node, and then select **Metric settings**.

4. Right-click a metric, and then select **Configure metric settings**.

5. Set the warning limits.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

65
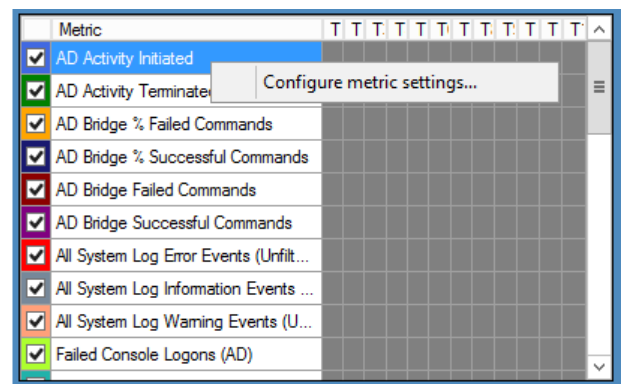
6. Depending on your requirements, select the check boxes to turn on the alerts for the warning limits.
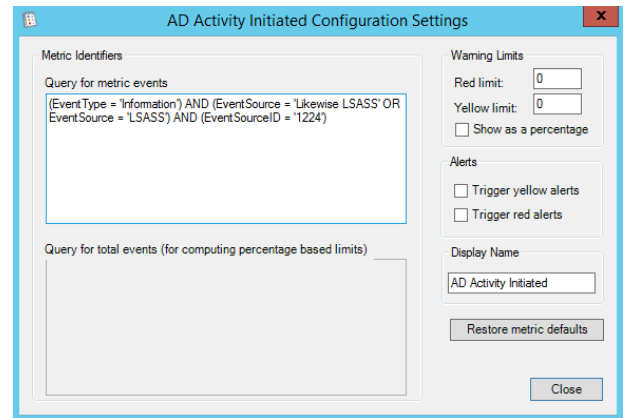
7. Click **Close**.

Analyze Events on the Dashboard

After you configure and customize the view on the dashboard, you can quickly view the results to determine if assets are out of compliance.

To view the number of events:
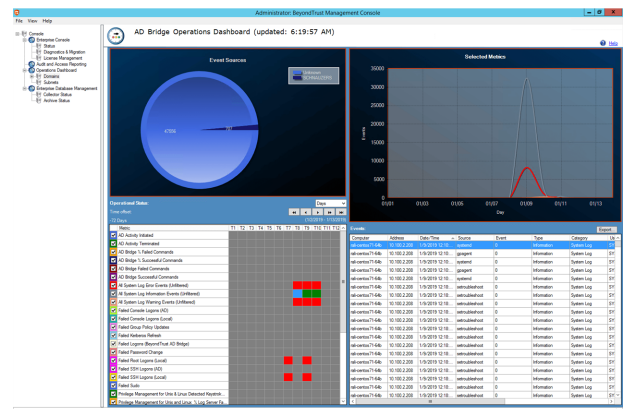
1. Log into the BeyondTrust Management Console.
2. Expand the **Operations Dashboard** node, and then expand the **Domain** node or **Subnets** node.
3. Select the domain that you want to see the events for. The following example shows **Event Sources** and **Selected Metrics**.

- **Event Sources:** Displays the number of events that have been tracked and displays the domain name where the events occurred.
- **Selected Metrics:** Displays the total number of events collected and the selected collection period. You can select the time frame from the **Operational Status** list to analyze trends over the time period.

In the metrics pane, you can view the assets where the events occurred. For example, in the following, select a green rectangle (that represents a period in time), which will display the computers in the right pane where the activity occurred.

Set Alert Notifications

You can track specific activities and receive email alerts when the activity occurs.

To track event activities and configure alerts:

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

66

TC: 1/31/2020

1. Log into the BeyondTrust Management Console.

2. Right-click the **Operations Dashboard**, and then select **Alert Settings**.

3. On the **Operations Dashboard Alert Settings** dialog box, select the following:

   - **Run this program:** Select the check box, and then click **Browse** to navigate to the program that you want to run.

   - **Command Line Arguments** Click to select the activities that you want to monitor. Click **OK**.

   - **Sent email message to:** Select this check box to send email alerts. Click the **Email Settings** button to configure the SMTP server and add the email account that will receive the alerts.
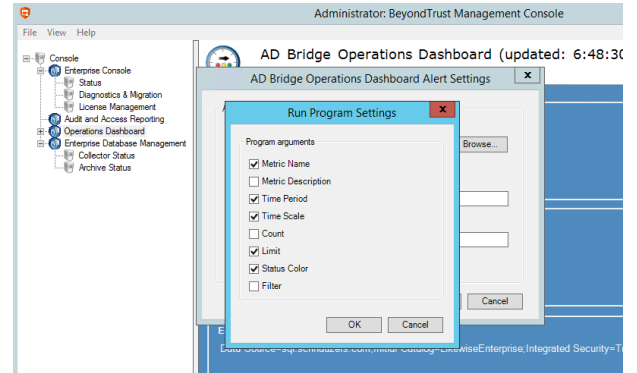
Archive Events

You can archive events in two ways: either with the Enterprise Database Management plug-in or with the command line.

The AD Bridge Enterprise event-archiving utility **BTArchive** combines events older than one year into compressed archives and stores them in a separate database table. A separate archive is created for each month of old event data. After events are archived, they are deleted. The event-archiving utility is intended to be run according to a monthly schedule.

Archive Events using the Console

To archive events using the console:

1. In the console tree, expand **Enterprise Database Management**.
2. Right-click **Archive Status**, and then select **Create archive**.
3. Follow the instructions in the wizard.

Archive Events using the Command Line

To view the arguments of **BTArchive**, execute the following command at the shell prompt on a Windows computer running the AD Bridge Enterprise collectors:

```
C:\Program Files\BeyondTrust\PBIS\Enterprise>btarchive --help
```

- The **–p** and **–c** options identify the database type and connection string of the central AD Bridge Enterprise database.

  The connection string is the same as the one that you used when you configured the connection to the database. With SQL Server, for example, you enter a string like this:

  ```
  Data Source=DBSERVERNAME;Initial Catalog=LikewiseEnterprise;Integrated Security=True
  ```

  Example:

  ```
  Data Source=W2K12-R2\SQL;Initial Catalog=LikewiseEnterprise;Integrated Security=True
  ```

- The **-a** and **–t** options are used to control the archive time unit and the date threshold for archiving.

> 📌 *Note: We suggest you use the default settings, which are **-a monthly** and **-t 12**. These defaults create monthly archives for data older than 12 months.*

- The **–o** option is used to control where the log output of **BTArchive** is written.

  By default, the output is written to the console.

Use the btopt.exe Tool

Using the **btopt.exe** tool, you can manage options for AD Bridge Enterprise from the command-line of a Windows administrative workstation connected to Active Directory.

You can, for example, set an option to use sequential IDs instead of hashed IDs. In addition, after you set the option to use sequential IDs, you can set the initial UID number for a cell.

The **btopt.exe** tool is installed on computers running AD Bridge Enterprise in the following directory:

C:\Program Files\BeyondTrust\PBIS\Enterprise

```
C:\Program Files\BeyondTrust\PBIS\Enterprise> .\btopt.exe --help
btopt - configures local Windows options for
Usage:  btopt OPTIONS
OPTIONS:

--status                      Show current configuration status
--narrowsearch                Only search the default cell on the local domain
--widesearch                  Search the default cell across all domains and two-way forest trust
--sequential                  Use sequential IDs instead of hashed IDs
--hashed                      Use hashed IDs
--foreignaliases              Allow the use of aliases for users and groups from other domains.
--noforeignaliases            Disallow the use of aliases for users and groups from other domains.
--usegc                       Use the Global Catalog to speed up searches (default)
--ignoregc                    Do not use the Global Catalog to speed up searches
--startUID=#                  Sets the initial UID number for a cell (if --sequential)
--startGID=#                  Sets the initial GID number for a cell (if --sequential)
--minID=#                     Sets minimum UID and GID number configurable through the UI
--cell=LDAPPATH               Identifies the cell whose initial IDs (if --sequential)
                              Example: LDAP://somedc/ou=anou,dc=somecom,dc=com
--enableloginnames            Sets the default login names to all the users enabled in all the
                              cells.
--disableloginnames           Disable the enable default login names option to all users enabled
                              in all the cells.
--disablesuggestbutton        Disable "Suggest" button, which is used to suggest UID/GID
                              assignment to users and groups in the cells.
--enablesuggestbutton         Enable "Suggest" button, which is used to suggest UID/GID
                              assignment to users and groups in the cells.
--maxGroupsForUser=#          Sets the maximum number of groups to display for a user on the
                              Properties dialog box.
--maxArchiveEventsPerBatch=#  Sets the maximum number of events that can be used in a batch while
                              archiving.
--enablegidvalidation         The Active Directory user account will be associated with the GID
                              value migrated from the UNIX/Linux account information.
--disablegidvalidation        When turned off, you can set the GID value to any number—the GID
                              value is not associated with a specific group.
                              GID validation is disabled by default.
                              When GID validation is disabled, the --minID option is enforced but
                              there are no other restrictions. Any numerical GID can be selected.
--enableAssumeDefaultCell     Enables Assume Default Cell.
--disableAssumeDefaultCell    Disables Assume Default Cell.
--help                        Displays this usage information

If the --startUID or --startGID options are set, the --cell option must also be set.
```

Contact BeyondTrust Technical Support

BeyondTrust provides an online knowledge base, as well as telephone and web-based support.

ℹ️ For BeyondTrust Technical Support contact information, please visit www.beyondtrust.com/support.

Before Contacting BeyondTrust Technical Support

To expedite support, collect the following information to provide to BeyondTrust Technical Support:

- AD Bridge Enterprise version: available in the AD Bridge Enterprise Console by clicking **Help > About** on the menu bar
- AD Bridge Enterprise Agent version and build number
- Linux or Unix version
- Windows or Windows Server version

If you are contacting BeyondTrust Technical Support about one of the following problems, also provide the diagnostic information specified.

Segmentation Faults

Provide the following information when contacting BeyondTrust Technical Support:

- Core dump of the AD Bridge application:

  ```
  ulimit - c unlimited
  ```

- Exact patch level or exact versions of all installed packages

Program Freezes

Provide the following information when contacting BeyondTrust Technical Support:

- Debug logs
- tcpdump
- An **strace** of the program

Domain-Join Errors

Provide the following information when contacting BeyondTrust Technical Support:

- Debug logs: copy the log file from **/var/log/pbis-join.log**
- tcpdump

All Active Directory Users Are Missing

Provide the following information when contacting BeyondTrust Technical Support:

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

70

TC: 1/31/2020

- Run **/opt/pbis/bin/get-status**
- Contents of **nsswitch.conf**

All Active Directory Users Cannot Log On

Provide the following information when contacting BeyondTrust Technical Support:

- Output of **id <user>**
- Output of **su -c 'su <user>' <user>**
- **lsass** debug logs

> ℹ️ For more information, please see *Generate Debug Logs* in the AD Bridge Troubleshooting Guide at
> https://www.beyondtrust.com/docs/ad-bridge/documentation.htm.

- Contents of **pam.d/pam.conf**
- The sshd and ssh debug logs and syslog

AD Users or Groups are Missing

Provide the following information when contacting BeyondTrust Technical Support:

- The debug logs for lsass
- Output for **getent passwd** or **getent group** for the missing object
- Output for **id <user>** if user
- tcpdump
- Copy of lsass cache file.

Poor Performance When Logging On or Looking Up Users

Provide the following information when contacting BeyondTrust Technical Support:

- Output of **id <user>**
- The lsass debug log
- Copy of lsass cache file.

> ℹ️ For more information about the file name and location of the cache files, please see the AD Bridge Linux Administration Guide at https://www.beyondtrust.com/docs/ad-bridge/documentation.htm.

- tcpdump

Generate a Support Pack

The AD Bridge support script will copy system files that AD Bridge needs to function into an archive. This archive can then be sent to support to assist in the investigation.

Installed location:

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

71

/opt/pbis/libexec/pbis-support.pl

Download location:

http://download.beyondtrust.com/pbis/support-pbis/pbis-support.pl