AD Bridge
Group Policy Reference Guide

Table of Contents

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

3

Introduction to the AD Bridge Group Policy Reference Guide

AD Bridge (AD Bridge Enterprise) joins Unix and Linux computers to Active Directory so that you can centrally manage all your computers from one source, authenticate users with the highly secure Kerberos 5 protocol, control access to resources, and apply group policies to non-Windows computers.

This guide describes how to manage Unix and Linux computers using Group Policy settings provided with AD Bridge Enterprise Edition.

Additional Resources

For release notes, please see the Product Changelog at https://www.beyondtrust.com/support/changelog.

Work with AD Bridge Enterprise Group Policy Settings

This section contains general information about AD Bridge Enterprise Group Policy settings.

- About Group Policy Settings
- Managing GPOs
- Apply a Group Policy to a Cell
- View a Report on a Group Policy's Settings
- Create and Test a sudo Group Policy

About Group Policy Settings

AD Bridge Enterprise enables you to configure Group Policy settings for computers running Linux and Unix. AD Bridge Enterprise includes more than 100 policy settings that are designed to manage non-Windows computers.

All the policy settings are integrated with the Microsoft Group Policy Management Editor, part of the Microsoft Group Policy Management Console (GPMC).

For example, you can use a group policy setting to control who can use sudo for access to root-level privileges by specifying a common **sudoers** file for target computers. You could create an Active Directory group called **SudoUsers**, add **Active Directory** users to the group, and then apply the sudo group policy setting to the container, giving those users sudo access on their Linux and Unix computers. In the **sudoers** file, you can specify Windows-style user names and identities. Using a group policy setting for sudo gives you a powerful method to remotely and uniformly audit and control access to Unix and Linux resources.

AD Bridge Enterprise stores its Unix and Linux policy settings in Group Policy Objects (GPOs) in the same location and in the same format as the default GPOs in Windows Server: in the system volume (**sysvol**) shared folder. Unix and Linux computers that are joined to an Active Directory domain receive GPOs in the same way that a Windows computer does:
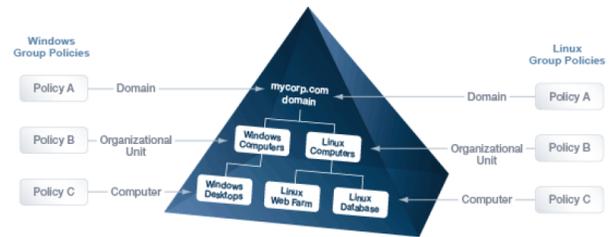
The following topics are covered:

-
-
-
-
-

AD Bridge Group Policy Agent

The AD Bridge Group Policy Agent is automatically installed when you install the AD Bridge Enterprise agent.

To apply and enforce policy settings, the AD Bridge Group Policy Agent runs continuously as a daemon processing user policy and computer policy:

- **Computer policy processing**: The agent traverses the computer's distinguished name (DN) path in Active Directory.
- **User policy processing**: Occurs when a user logs on; the agent traverses the user's DN path in Active Directory.

The AD Bridge Group Policy Agent connects to Active Directory, retrieves changes, and applies them once every 30 minutes, when a computer starts or restarts, or when requested by the GPO refresh tool.

The AD Bridge Group Policy Agent uses the computer account credentials to securely retrieve policy template files over the network from the domain's protected system volume shared folder.

The AD Bridge Group Policy Agent applies only AD Bridge Enterprise Group Policy settings: those in the Unix and Linux Settings collection in the Group Policy Management Editor; it does not apply any other group policy settings that may be specified in the GPOs.

Inheritance

There are two types of policy settings:

- File-based: File-based policy settings, such as sudo and automount, typically replace the local file. File-based policy settings are not inherited and do not merge with the local file.
- Property-based: Property-based policy settings are inherited, meaning that the location of a GPO in the Active Directory hierarchy can affect its application. Property-based settings merge with local policy settings. Local policy settings are not replaced by property-based settings.

Most policy settings are based on properties.

Filter by Target Platform

You can set the target platforms for a GPO. The GPO is applied only to the platforms that you select. You can select the target platforms by operating system, distribution, and version. For example, you can target a GPO at:

- Only computers running SUSE Linux Enterprise Server
- A mixture of operating systems and distributions, such as Red Hat Linux, Sun Solaris, Ubuntu Desktop, and HP-UX

Some policy settings, however, apply only to specific platforms.

> For more information, please see the **Help** for the policy setting that you want to use.

Target Platforms		
CentOS Linux	Debian Linux	Fedora Linux
Hewlett-Packard HP-UX	IBM AIX	OpenSUSE Linux
Red Hat Linux	Red Hat Enterprise Linux (ES and AS)	Sun Solaris
SUSE Linux	SUSE Linux Enterprise Desktop	
SUSE Linux Enterprise Server	Ubuntu Linux	

Go to the **Target Platform Filter** policy to select targets for the GPO.
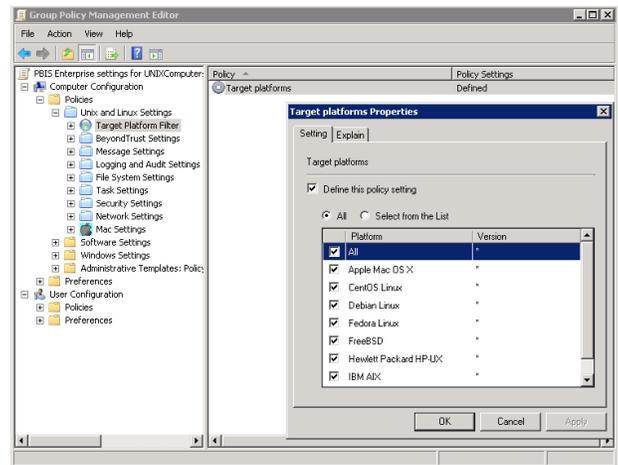
AD Bridge EnterpriseGPO Update Tool

Use the AD Bridge Enterprise GPO update tool to force a computer to pull the latest version of group policy settings. The tool includes the following options:

Option	Description	Example
help	Displays the help for the tool .	**gpupdate --help**
verbose	Displays information on the policies that were added, updated, removed.	**gpupdate --verbose**
rsop	Displays the Resultant Set of Policy (RSoP) information. The RSoP is the set of group policy settings the group policy agent will apply, either when it runs as part of periodically applying settings or when gpupdate is run. **gpupdate --rsop** does not apply group policy settings.	**gpupdate --rsop**
no-pager	Do not page output. By default, **gpupdate** automatically pages output using the command set in the PAGER environment variable.	**gpupdate --no-pager**

The **--verbose** command provides details on the group policy extensions being run, whether settings were added, modified or removed and whether those changes were successfully applied.

Run the following command at the shell prompt: **/opt/pbis/bin/gpupdate --verbose**

The command returns a success or failure result similar to the following:

- On success: **GPO Update succeeded**
- On failure: **GPO Update was unsuccessful, error code <code> (<error message>)**

On target computers, AD Bridge Enterprise stores policy settings in **/var/lib/pbis/grouppolicy**.

Manage Group Policy Objects (GPOs)

You can create or edit Group Policy Objects (GPOs) and configure policy settings for computers running Linux and Unix by using the Group Policy Management Console (GPMC).

> **Note:** To manage a GPO, you must log on as a member of the Domain Administrators security group, the Enterprise Administrators security group, or the Group Policy Creator Owners security group.

> **Tip:** You can download the Microsoft Group Policy Management Console at https://www.microsoft.com/en-us/downloads/.

To create a GPO using GPMC:

1. Navigate to **Start > Administrative Tools** and click **Group Policy Management**.
2. Right-click the organizational unit, and then select **Create a GPO in this domain, and Link it here**.
3. Type a name for your GPO.
4. Click **OK**.
5. Right-click the GPO that you created, and then click **Edit**.

> **Note:** The AD Bridge Enterprise Group Policy settings are in the **Unix and Linux Settings** collection. For more information about each policy, see the **Help** for the policy setting that you want to use.
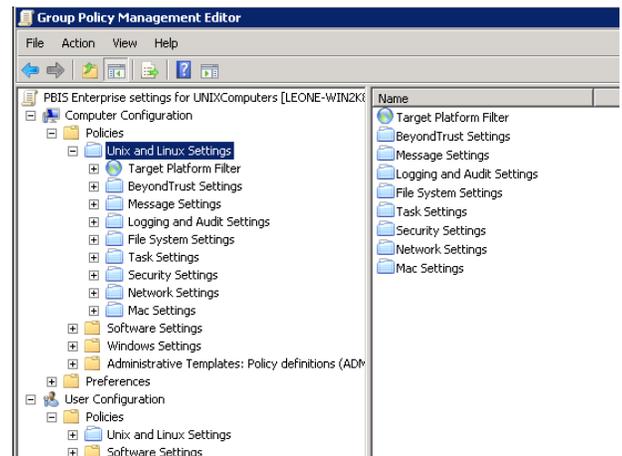
View a Report on a GPO's Policy Settings

In GPMC, you can view details on AD Bridge Enterprise policy settings defined in a GPO. Go to the GPO and select the **Settings** tab. The image depicts an example.
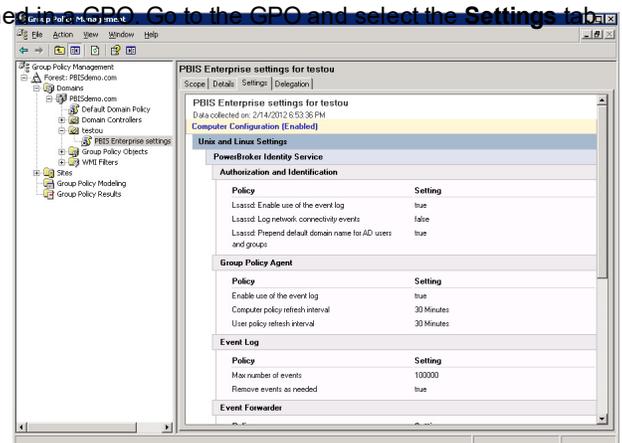
Walkthrough: Create a sudo GPO

You can create a GPO to specify a sudo configuration file for target computers. **Sudo**, or **superuser do**, allows a user to run a command as root or as another user. You can use this GPO to control sudo access in a centralized and uniform way.

The sudo configuration file is copied to the local computer and replaces the local **sudoers** file. A sudo file can reference Active Directory users and groups. For more information about sudo, see the man pages for your system.

When you define the GPO, you can also set its target platforms. The GPO settings are applied only to the operating systems, distributions, and versions that you choose.

> *Note: The AD Bridge Enterprise entries in your **sudoers** file must conform to the rules set in "Configure Entries in Your Sudoers Files" in the AD Bridge Enterprise Edition Administration Guide.*

Create a sudo GPO

> *Note: To create or edit a GPO, you must log on as a member of the Domain Administrators security group, the Enterprise Administrators security group, or the Group Policy Creator Owners security group.*

1. In the Group Policy Management Editor, expand either **Computer Configuration** or **User Configuration**, expand **Policies > Unix and Linux Settings**.
2. Expand **Security Settings**, and then select **SUDO command.**
3. Double-click **Define Sudoer file**.
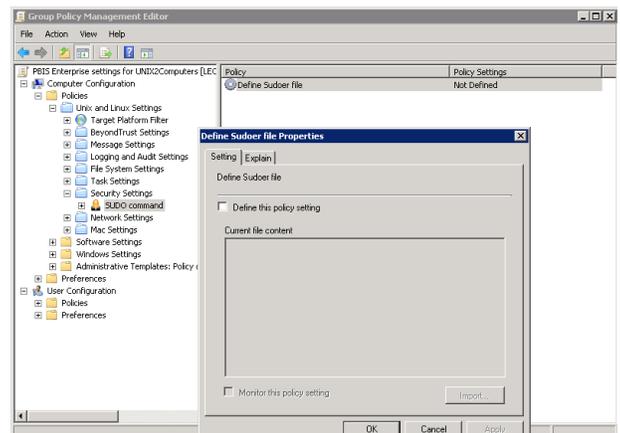
4. Check the **Define this Policy Setting** box, and then in the **Current file content** box, type your commands. Or, to import a sudo configuration file, click **Import**.
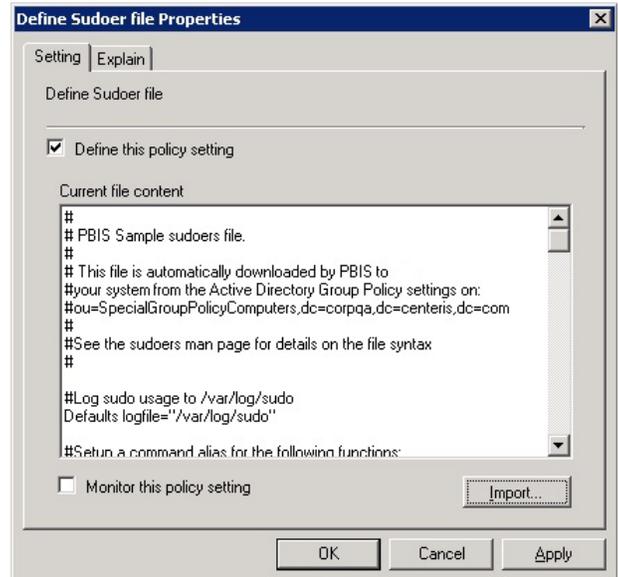
5. Select **Target Platform Filter**.
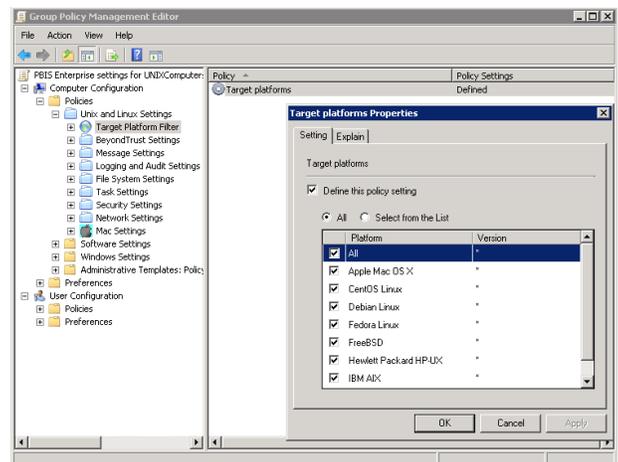
6. Double-click **Target platforms**.

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

10

7. To target all the platforms, select **All**. To choose platforms, click **Select from the List**, and then select the platforms.

Test the sudo GPO

After you set the sudo GPO, you can test it on a target computer. The target computer must be in a cell associated with the organizational unit where you linked the sudo GPO.

1. On a target Linux or Unix computer, log on as an administrator and execute the following command to force AD Bridge Enterprise Group Policy settings to refresh:

```
/opt/pbis/bin/gpupdate
```

2. Check whether your sudoers file is on the computer:

```
cat /etc/sudoers
```

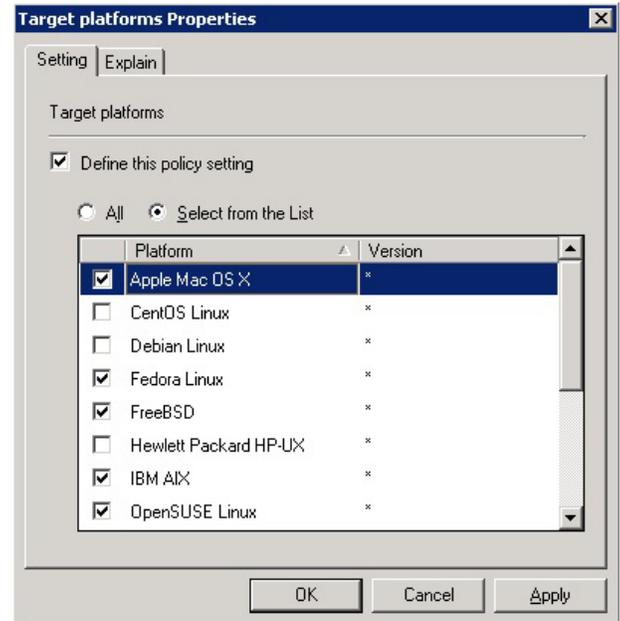> *Note: The location of the sudoers file varies by platform. For example, on Solaris it is in **/opt/sfw/etc** or **/opt/csw/etc**. On other platforms, it is in **/usr/local/etc**.*

3. Log on to the Unix or Linux computer as a regular user who has sudo privileges as specified in the sudoers configuration file.
4. Try to access a system resource that requires root access using sudo. When prompted, use the password of the user you are logged on as, unless **targetpw** is set in the **sudoers** file. Verify that the user was authenticated and that the user can access the system resource.

Test sudo Security

1. Log on as a user who is not enabled with sudo in the **sudoers** file that you used to set the Group Policy Object (GPO).
2. Verify that the user cannot perform root functions using sudo with their Active Directory credentials.

AD Bridge Enterprise Settings and Descriptions

Authorization and Identification

GPO Name	Description
Lsassd: Enable use of the event log	Turns on event logging, includes: log on and off events, authentication and identification events.
Lsassd: Log network connectivity events	Turns on event logging for network connection failures.
Lsassd: Prepend default domain name for AD users and groups	Turns on the feature to add a domain name to user and groups. Use this policy with **Lsassd: Default domain name to prepend for AD user and groups**.
Lsassd: Default domain name to prepend for AD users and groups	Set the domain name to add to the user and group names. Use **Lsassd: Prepend default domain name for AD users and groups** policy to turn this feature on.
lsassd: System time synchronization	Synchronizes the lsass service computer with the Active Directory Domain Controller.
Home Directory Template and Path Prefix	Use the home directory path template and path prefix policy settings together to customize the way that the home directory path is determined for a user account.
Remote directory path template	Sets the network connected share (Home Folder) location defined in the Active Directory user account profile.
Login shell template	Defines the login shell for an AD account only when it is not set on the **AD Bridge Cell Settings** tab in Active Directory.
Local account login shell template	Use for a local AD Bridge account.
Local account home directory path prefix	Use for a local AD Bridge account.
Local account home directory path template	Sets the **homedir-template** setting of the user home directory path on target systems running lsassd.
Lsassd: Enable signing and sealing for LDAP traffic	Sign and seal LDAP traffic to certify and encrypt it so that others cannot see your LDAP traffic on your network as it travels between a AD Bridge client and a domain controller.
Lsassd: Enable user credential refreshing	Sets if the credentials must be refreshed.
Lsassd: Enable user group membership trimming	Specifies whether to discard cached information from a Privilege Attribute Certificate (PAC) entry when it conflicts with new information retrieved through LDAP. Otherwise, PAC information, which does not expire, is updated the next time the user logs on. It is turned on by default.
Lsassd: Enable cache only group membership enumeration for NSS	Specifies whether to return only cached information for the members of a group when queried through the name service switch, or **nsswitch**. The setting determines whether nsswitch-based group APIs obtain group membership information exclusively from the cache, or whether they search for additional group membership data through LDAP.

GPO Name	Description
Lsassd: Enable cache only user membership enumeration for NSS	When set to enabled, enumerates the groups to which a user belongs using information based solely on the cache. When set to disabled, it checks the cache and searches for more information over LDAP. It is turned off by default.
Lsassd: Enable NSS enumeration	Controls whether all users or all groups can be incrementally listed through NSS. On Linux computers and Unix computers, the default setting is set in the registry as **0**, or turned off. To allow third-party software to show Active Directory users and groups in lists, you can turn on this setting, but performance might be affected.
Lsassd: Force authentication to use unprovisioned mode	To use the AD Bridge agent to join a computer to a domain that has not been configured with cell information, you must set this group policy to unprovisioned mode.
Lsass: User names to ignore	User account names to ignore on target AD Bridge clients. The policy can contain a comma-separated list of account names. 📌 *Note: If **Apply Policy** is set to **Always** (default), any changes to managed system files on the agent system will be replaced when group policy is next applied. If a managed system file is edited or removed, **gpupdate** will recreate the file on policy refresh. If set to **Once**, any changes to managed system files on the agent system will only be replaced when the policy is updated or **gpagent** is restarted.* *Backups of existing system files are performed before initial policy application.*
Lsass: Group names to ignore	Group names to ignore on target AD Bridge clients. The policy can contain a comma-separated list of group names. 📌 *Note: If **Apply Policy** is set to **Always** (default), any changes to managed system files on the agent system will be replaced when group policy is next applied. If a managed system file is edited or removed, **gpupdate** will recreate the file on policy refresh. If set to **Once**, any changes to managed system files on the agent system will only be replaced when the policy is updated or **gpagent** is restarted.* *Backups of existing system files are performed before initial policy application.*
Lsass: Ignore all trusts during domain enumeration	Determines whether the authentication service discovers domain trusts. In the default configuration of disabled, the service enumerates all the parent and child domains and forest trusts to other domains. For each domain, the service establishes a preferred domain controller by checking for site affinity and testing server responsiveness, a process that can be slowed by WAN links, subnet firewall blocks, stale AD site topology data, or invalid DNS information. When it is unnecessary to enumerate all the trusts – for example, the intended users of the target computer are only from the forest that the computer is joined to – turning on this setting can improve startup times of the authentication service.
Lsass: Domain trust enumeration include list	When turned on, only the domain names in the include list are enumerated for trusts and checked for server availability.
Lsass: Domain trust enumeration exclude list	When turned off (default setting), the domain names in the exclude list are not enumerated for trusts and not checked for server availability.

GPO Name	Description
Lsass: Require trust enumeration to complete during startup	Sets the AD Bridge authentication service (Lsass) to finish enumerating all the domain trusts before the service indicates that it has started. You can use this policy to help sequence services, such as **crond**, that depend on Lsass for user and group object lookups. Default is turned off.
Domain Separator Character	Configures the domain separator used by the AD Bridge agent for user and group account name lookups witha character that you choose.
Cache Expiration Time	You can use this policy to improve the performance of your system by increasing the expiration time of the cache.
Machine account password expiration time (machine password timeout)	Set the machine account password expiration time on target computers. The expiration time specifies when machine account passwords are reset in Active Directory.
Replacement character for names with spaces	Replace spaces in Active Directory user and group names with a character that you choose. For example, when you set the replacement character to caret (**^**), the group **DOMAIN\Domain Users** in ActiveDirectory appears as **DOMAIN\domain^users** on target computers.
Maximum Tolerance for Kerberos Clock Skew (clockskew)	You can create a group policy to set the maximum amount of time that the clock of the Kerberos Distribution Center (KDC) can deviate from the clock of target hosts.

For security, a host rejects responses from any KDC whose clock is not within the maximum clock skew, as set in the host's **krb5.conf** file.

The default clock skew is 300 seconds, or 5 minutes. This policy changes the clock skew value in the **krb5.conf** file of target hosts. |

Logon

GPO Name	Description
Allow Logon Rights	Set the Active Directory users and groups allowed to log on to target computers. Users and groups who have logon rights can log on to the target computers either locally or remotely.

You can also use this policy to enforce logon rules for local users and groups. To use this policy, you must grant the users access to the AD Bridge cell that contains the target computer object. By default, all Unix and Linux computers are joined to the default cell, and all members of the Domain Users group are allowed to access the default cell. AD Bridge checks requiremembershipof information in both the authentication phase and the account phase. |
| Cumulative Allow Logon Rights | Sets logon rights to child OUs. |
| Denied logon rights message | Sets a message to display when a user cannot log on because the allow logon right policy is not set. |
| Create a home directory for a User Account at Logon | You can automatically create a home directory for an AD user account or a local AD Bridge user account on target AD Bridge clients. When the user logs on the computer, the home directory is created if it does not exist.

For AD accounts, the location of the home directory is specified in the AD Bridge settings of the user account in Active Directory Users and Computers. |
| Template files for a new user home directory | AD Bridge can add the contents of **skel** to the home directory created for an AD user account or a AD Bridge local user account on target AD Bridge clients.

Using the **skel** directory ensures that all users begin with the same settings or environment. |

GPO Name	Description
Home Directory Creation Mask	AD Bridge can set permissions for the home directory that is created when a user logs on target AD Bridge clients. The home directory and all the files in the directory are preset with the ownership settings of the file creation mask, or **umask**. There is a **umask** policy for local accounts and a **umask** policy for AD accounts.
Local account password expiration	Sets the number of days a local account is notified before a password expires.
Local account password lifespan	Sets the number of days a password is valid.
Create a .k5Login file in user home directory	Creates a **.k5Login**.
Log PAM debugging information	Logs winbind debugging information.
Ignore group alias	When turned on, group names are displayed using the NT4 format (**DOMAIN\SAMaccountname**).

Smart Card

GPO Name	Description
Smart card removal policy	Sets the action to take when a smart card is removed from a target. For example, lock out the computer.
Require smart card for login	Turns on the requirement to use Smart Card two-factor authentication.

Reaper Syslog Settings

GPO Name	Description
Unmatched Error Events	Sets the policy to capture Error class events from syslog reaper service.
Unmatched Warning Events	Sets the policy to capture Warning class events from syslog reaper service.
Unmatched Info Events	Sets the policy to capture Information class events from syslog reaper service.

Group Policy Agent

GPO Name	Description
Enable use of event log	Turns on logging for group policy events on target computers. You can use this policy to help improve security and to troubleshoot group policies by capturing information in the AD Bridge event log about the application and processing of group policy objects, including such events as errors, adding a new GPO, updating a GPO for a new version, and removing a GPO that no longer applies to a user or computer.
Computer Policy Refresh Interval	Sets how often a computer's group policies are updated while the computer is in use. By default, when this policy is undefined, a computer's group policies are updated when the system starts and every 30 minutes while the computer is in use. The updates take place in the background without interrupting the user.

GPO Name	Description
User Policy Refresh Interval	Sets how often the user settings are updated while the user is logged on. By default, when this policy is undefined, a user's settings are updated when the user logs on and every 30 minutes while the user is logged on. The updates take place in the background without interrupting the user. Only applies to AD Bridge group policies.
User Policy Loopback Processing Mode	The policy is designed for special-use computers, such as those in public places, laboratories, and classrooms, where you must modify the user setting based on the computer that is being used. By default, the user's group policy objects determine which user settings apply. If this setting is enabled, when a user logs on to this computer, the computer's group policy objects determine which set of group policy objects applies.
Enable user logon group policies	By default, the AD Bridge group policy agent processes and applies user policies when a user logs on with an Active Directory account, a process that can delay logon. If no user group policy objects apply to a target set of computers and the users who access them, defining this group policy and setting it to disabled stops the AD Bridge group policy agent from attempting to process user policies, resulting in faster logons.

Event Log

GPO Name	Description
Max disk usage	Set the maximum event log size.
Max number of events	Set the maximum number of events that can be saved in the event log.
Max event lifespan	Set the number of days that pass before events are deleted.
Remove events as needed	Deletes events when the Max disk usage policy reaches the size threshold configured. Used with the **Max disk usage** policy.
Allow read-event access	Set the Active Directory users that can read events from the AD Bridge event log.
Allow write-event access	Set the Active Directory users and groups allowed to write events in to the AD Bridge event log.
Allow delete-event access	Set the Active Directory users and groups allowed to delete events from the AD Bridge event log of target computers.

Event Forwarder

GPO Name	Description
Event log collector	Sets the event log collector for the target computers.
Service principal for collector	Set the service principal account name that the event forwarder daemon process uses to contact the collector.

User Monitor

GPO Name	Description
Enable monitoring of users and groups	AD Bridge includes a **User Monitor** service for entitlement reports. This feature is designed to support computers that are critical to regulatory compliance and for which restricted access by only essential staff is vital. A computer that is openly accessible to hundreds of users would be a source of unnecessary audit activity in such a situation and would significantly increase resource requirements, such as for Auditing Database sizing. This policy setting turns on the **User Monitor** service to monitor account and group changes. The service queries all local user accounts, local groups, and Active Directory users and groups. The service detects additions, deletions, and modifications that occur. Information is then sent to the **Eventlog** service for reporting purposes.
Monitoring check interval	Sets the frequency with which the **User Monitor** service attempts to detect user and group changes on target computers.

SNMP Settings

GPO Name	Description
Configure SNMP	The following groups of SNMP trap settings can be applied using a GPO: • Account • Domain • Logon Authentication • SUDO • System Services To use SNMP policies, you must also turn on **Lsassd: Enable use of the event log** in the **Authorization and Identification** group policy.

Account Override

GPO Name	Description
User Account Attributes (to override)	You can override the following user attributes: • Login Name • UID Number • Primary GID • GECOS • Home directory • Login shell *Note: If **Apply Policy** is set to **Always** (default), any changes to managed system files on the agent system will be replaced when group policy is next applied. If a managed system file is edited or removed, **gpupdate** will recreate the file on policy refresh. If set to **Once**, any changes to managed system files on the agent system will only be replaced when the policy is updated or **gpagent** is restarted.* *Backups of existing system files are performed before initial policy application.*
Group Account Attributes (to override)	You can override the following group attributes: • Group Alias • GID Number *Note: If **Apply Policy** is set to **Always** (default), any changes to managed system files on the agent system will be replaced when group policy is next applied. If a managed system file is edited or removed, **gpupdate** will recreate the file on policy refresh. If set to **Once**, any changes to managed system files on the agent system will only be replaced when the policy is updated or **gpagent** is restarted.* *Backups of existing system files are performed before initial policy application.*

AD BridgeMessage Settings and Descriptions

GPO Name	Description
Login Prompt	Set a message in the **/etc/issue** file on target computers. The message, which appears before the login prompt, can display the name of the operating system, the kernel version, and other information that identifies the system. In the message text, you can use characters, numbers, and special characters; there is no limit to the length of the message. *Note: If **Apply Policy** is set to **Always** (default), any changes to managed system files on the agent system will be replaced when group policy is next applied. If a managed system file is edited or removed, **gpupdate** will recreate the file on policy refresh. If set to **Once**, any changes to managed system files on the agent system will only be replaced when the policy is updated or **gpagent** is restarted.* *Backups of existing system files are performed before initial policy application.*
Message of the Day	Set a message of the day in the **/etc/motd** file on target computers. The message of the day, which appears after a user logs in but before the logon script executes, can give users information about a computer. For example, the message can remind users of the next scheduled maintenance window. The policy replaces the **motd** file on the target computer. *Note: If **Apply Policy** is set to **Always** (default), any changes to managed system files on the agent system will be replaced when group policy is next applied. If a managed system file is edited or removed, **gpupdate** will recreate the file on policy refresh. If set to **Once**, any changes to managed system files on the agent system will only be replaced when the policy is updated or **gpagent** is restarted.* *Backups of existing system files are performed before initial policy application.*
Password Prompts	Users can set password prompts to indicate which account is prompting for the password. There are three types of password prompts that can be configured: • Local Account passwords • Active Directory passwords • Other account passwords

Logging and Audit Settings and Descriptions

GPO Name	Description
SELinux	SELinux puts in place mandatory access control using the Linux Security Modules, or LSM, in the Linux kernel. The security architecture, which is based on the principle of least privilege, provides fine-grained control over the users and processes that are allowed to access a system or execute commands on it. SELinux can secure processes from each other. For example, if you have a public web server that is also acting as a DNS server, SELinux can isolate the two processes so that a vulnerability in the web server process does not expose access to the DNS server.
SysLog	A syslog policy can help you manage, troubleshoot, and audit your systems. You can log different facilities, such as **cron**, **daemon**, and **auth**, and you can use priority levels and filters to collect messages. The policy can import syslog, rsyslog, and syslog-ng configuration files. There are options to replace or append to the current configuration. *Note: If **Apply Policy** is set to **Always** (default), any changes to managed system files on the agent system will be replaced when group policy is next applied. If a managed system file is edited or removed, **gpupdate** will recreate the file on policy refresh. If set to **Once**, any changes to managed system files on the agent system will only be replaced when the policy is updated or **gpagent** is restarted.* *Backups of existing system files are performed before initial policy application.*
LogRotate	To help you manage, troubleshoot, and archive your system's log files, you can create a group policy to configure and customize your log-rotation daemon. For example, you can choose to use either a **logrotate** or **logrotate.d** file, specify the maximum size before rotation, compress old log files, and set an address for emailing log files and error messages. You can also enter commands to run before and after rotation. *Note: If **Apply Policy** is set to **Always** (default), any changes to managed system files on the agent system will be replaced when group policy is next applied. If a managed system file is edited or removed, **gpupdate** will recreate the file on policy refresh. If set to **Once**, any changes to managed system files on the agent system will only be replaced when the policy is updated or **gpagent** is restarted.* *Backups of existing system files are performed before initial policy application.*

File System Settings in AD Bridge

GPO Name	Description
Files, Directories and Links	You can define a group policy to create directories, files, commands, and symbolic links on target computers. This policy can be applied to either computers or users. The policy, which is not inherited, does not concatenate a series of settings across multiple group policy objects in different locations in the Active Directory hierarchy. Instead, the closest local policy object is applied. You can add more than one script when setting up scripts using this policy setting. All scripts will automatically merge and run. Note that a script can be applied at the system level using the Run Scripts policy. For example, you might want to run a common script (for example, **/etc/resolv.config**) on all systems but then configure other scripts that are different depending on the system (for example, **/etc/sysconfig/iptables**). Configure the system specific policies using a Files, Directories and Links policy setting. *Note: When setting up the local user or local group, you can prefix the ID with a number sign (#). AD Bridge Enterprise does not validate a user or group ID prefixed by a number sign; you must provide a valid user or a valid group. To use the ID of 0 for the root account, however, do not use the # prefix.*
AutoMount	Starts a daemon that automatically mounts a file system on target computers. When a user tries to access an unmounted file system, the file that you associate with this policy automatically mounts it. *Note: If **Apply Policy** is set to **Always** (default), any changes to managed system files on the agent system will be replaced when group policy is next applied. If a managed system file is edited or removed, **gpupdate** will recreate the file on policy refresh. If set to **Once**, any changes to managed system files on the agent system will only be replaced when the policy is updated or **gpagent** is restarted.* *Backups of existing system files are performed before initial policy application.*

GPO Name	Description
Files System Mounts (fstab)	Create a group policy for the file systems table, or **fstab**, on target computers and add mount entries to it by using a graphical user interface. **Fstab**, typically located in **/etc/fstab**, is a configuration file that specifies how a computer is to mount partitions and storage devices. The mount entries are appended to the contents of **/etc/fstab** (**/etc/vfstab** on Solaris), but the file systems are not mounted until you explicitly mount them using a command such as **mount -a** even though the group policy has been polled by the target computer. To mount the file systems, you can do one of the following: • Log on to the target computer and execute the **mount -a** command (or a similar command, depending on your operating system) or restart the computer. • Run a cron job that resets the mounts remotely or restarts the computer. *Note: If **Apply Policy** is set to **Always** (default), any changes to managed system files on the agent system will be replaced when group policy is next applied. If a managed system file is edited or removed, **gpupdate** will recreate the file on policy refresh. If set to **Once**, any changes to managed system files on the agent system will only be replaced when the policy is updated or **gpagent** is restarted.* *Backups of existing system files are performed before initial policy application.*

Task Settings and Descriptions

GPO Name	Description
Run script	Use a GPO to execute a text-based script file on target computers. The script file runs under the root account when the target computer first receives the GPO or when the policy object's version changes. When a target system is restarted, the script runs again. This policy replaces the local file. It is not inherited and does not merge with the local file. The default ordering of the script policy is as follows: 1. Default domain policy 2. Higher-level OU policies 3. Current-level OU policies Within an OU, the ordering is from highest link number to the lowest link order number.
Crontab/Cron.d	Schedules commands, or cron jobs, that are executed at a set time on target computers. *Note: If **Apply Policy** is set to **Always** (default), any changes to managed system files on the agent system will be replaced when group policy is next applied. If a managed system file is edited or removed, **gpupdate** will recreate the file on policy refresh. If set to **Once**, any changes to managed system files on the agent system will only be replaced when the policy is updated or **gpagent** is restarted.* *Backups of existing system files are performed before initial policy application.*

Network and Security Settings Reference

GPO Name	Description
DNS	Sets the DNS servers and search domains on target computers.
	The search domains are automatically appended to names that are typed in Internet applications.
	*Note: Setting this group policy can lead to a conflict with the settings in the **resolv.conf** file on some target computers, especially those running newer versions of Linux that include NetworkManager.*
	*NetworkManager's dynamic maintenance of **resolv.conf** will likely conflict with this policy's resolver options. When turned on, NetworkManager typically leaves a comment in **resolv.conf** to indicate that it generated the file:*
	``` [root@bvt-rad12-32 ~]# cat /etc/resolv.conf # Generated by NetworkManager search corpqa.pbisdemo.com corp.pbisdemo.com nameserver 10.100.1.24 nameserver 10.100.1.45 nameserver 10.100.1.51 ```
	When the GPO is processed, a new **resolv.conf** file is generated and named **resolv.conf.gp**. The old **resolv.conf** file is saved as **resolv.conf.lwidentity.orig**, and then the new **resolv.conf.gp** is renamed **resolv.conf**. When the network interface is restarted, however, the updated **resolv.conf** settings can be overwritten with values from other configuration repositories, even if NetworkManager is not turned on.
	We recommend that you use a target platform filter to apply the policy only to Unix platforms or other systems on which **resolv.conf** is not dynamically modified.
Sudoers	This policy specifies a sudo configuration file for target computers running Linux or Unix. The sudo configuration file is copied to the local machine and replaces the existing sudo file.
	A sudo file can reference local users and groups or Active Directory users and groups. Sudo, or superuser do, allows a user to run a command as root or as another user.
	Example: DOMAIN\\adminuser ALL=(ALL) ALL %DOMAIN\\domain^admins ALL=(ALL) ALL
	Note: User and group need to be entered as they appear on the target computer.
	Note: Related Policy/Settings: ***Lsassd: Prepend default domain name for AD user**: Changes accounts to use only shortname*

GPO Name	Description
Certificates Autoenrollment	AD Bridge autoenrollment policy is used to automatically enroll domain, root, and select certificate templates. The following Windows server roles are required. Ensure the roles are properly configured before setting the policy in AD Bridge. - Active Directory Certificate Services (AD CS) - Web Server (IIS) with Certificate Enrollment Web service and Certificate Enrollment Web Service (CES) The auto enrollment service is managed by the **lwsm** service manager. When the autoenrollment group policy is downloaded, **gpagentd** will start up the autoenroll daemon and download the certificates. The **autoenroll** service will renew expired or revoked certificates and remove revoked certificates if configured. As of 8.5.4, root certificates are downloaded from: **CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,DC=ForestRoot,DC=com** to the local directory: **/etc/pbis/security/certs/<DOMAIN>/** If the computer leaves the domain, then the autoenrollment of certificates stops. However, certificates on the system will remain on the system. This policy was tested on: - RHEL 6, 7 x86_64 - Ubuntu 16.04, 18.04 LTS x86_64 *Note:* *The autoenrollment policy only enrolls computer certificates.* *Templates with **Publish certificate in Active Directory** enabled will fail to enroll.*
Wireless	The AD Bridge wireless policy configures a wireless interface using Network Manager. When the policy is downloaded to the workstations, the policy automatically enrolls in this certificate template and configures a wireless interface. The name of the certificate template must match the name as stated in the certificate authority template list. This policy is tested on: - Ubuntu 14.04 LTS x86_64 - RHEL 6.6, 7.0 x86_64 - CentOS 6.6, 7.0 x86_64

Privilege Management for Unix & Linux Servers Settings

This section describesThese topics describe how to use Privilege Management for Unix & Linux Servers to configure policy settings to support Privilege Management for Unix & Linux Servers.

Using the Privilege Management for Unix & Linux Servers Rule Editor and configuration file, you can create and change simple Privilege Management for Unix & Linux Servers policy rules.

Using the Rule Editor, you can enable or disable specific rules.

Privilege Management for Unix & Linux Servers policy data can be exported to a local file, edited manually, and imported to Active Directory from a local file.

Policy Rules Data

The policy data is saved to a .csv file. When the client-side agent applies the data from this Group Policy setting to a Privilege Management for Unix & Linux Servers Policy Server, the resulting collection of policy rules data will be at the following location: **/etc/pb/Policy.csv**.

If more than one Group Policy Object (GPO) has defined Policy Rules Data in the Active Directory policy hierarchy that applies to a given Privilege Management for Unix & Linux Servers Policy Server computer, the client-side agent determines which of all the policy settings should be applied based on targeting (filtering by host, system type), and precedence (link order and hierarchy). The resultant set of policy rules data is combined and written to the final **/etc/pb/Policy.csv** file to represent the union of all rules.

> ℹ️ For more information, please see "Export, Manually Edit, and Import PMUL Rules" on page 31.

Priority of Rules Within a GPO

Priority of rules within a GPO is defined in the Privilege Management for Unix & Linux Servers GPO Properties dialog box. If multiple GPOs containing Privilege Management for Unix & Linux Servers policy settings are applicable to a Privilege Management for Unix & Linux Servers Policy Server, the processing order of the GPOs is defined by their relative position in the Active Directory hierarchy. The closer a GPO is to the Privilege Management for Unix & Linux Servers Policy Server, the higher priority it has.

Configure Policy Rules Data in the Group Policy Management Editor

The process of defining a Privilege Management for Unix & Linux Servers rule begins by creating a GPO in an Active Directory (AD) hierarchy leading to a **pbmaster** computer object.

> 📌 *Note: Before Privilege Management for Unix & Linux Servers rules can be deployed, a Privilege Management for Unix & Linux Servers configuration file must be defined.*

> ℹ️ For more information, please see "Privilege Management for Unix & Linux Servers Configuration" on page 32.

To configure policy rules data:

1. In Group Policy Management Console, right-click an existing Group Policy Object (GPO) and click **Edit** to open the Group Policy Management Editor.

2. In Group Policy Management Editor, expand **Computer Configuration > Policies > Unix and Linux Settings > BeyondTrust Settings > PowerBroker Servers > PowerBroker Policy Rules Data**.
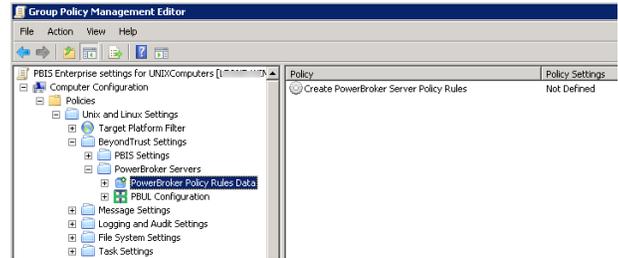
3. Double-click the **Create PowerBroker Server Policy Rules** policy setting to open the **Create Server Policy Rules Properties** dialog.

> 💡 **Tip:** *If a rule includes multiple commands, submitters, or Submit Hosts, a summary of the number of each is displayed in the row. To display an itemized list of commands, submitters, or hosts in a tool tip, point to the **Commands**, **Submitters**, or **Submit Hosts** cell in the row for that rule.*
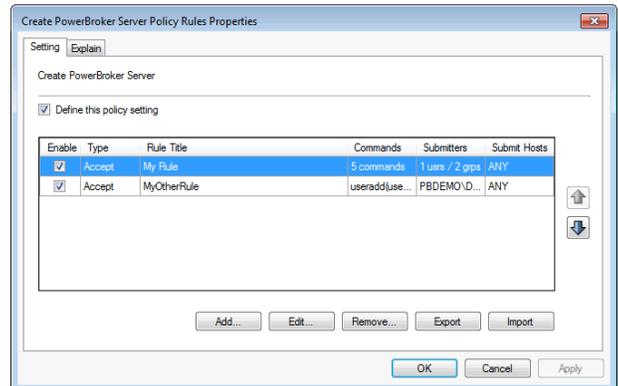
4. Using the rule properties dialog box, you can create or modify a Privilege Management for Unix & Linux Servers rule, change the priority of Privilege Management for Unix & Linux Servers rules, disable or enable a Privilege Management for Unix & Linux Servers rule, and export, manually edit, and import Privilege Management for Unix & Linux Serverspolicy data.

> ℹ️ For more information, please see the following:
> - "Create or Modify a PMUL Servers Rule" on page 27
> - "Change the Priority of PMUL Servers Rules" on page 30
> - "Disable or Enable PMUL Servers Rules" on page 31
> - "Export, Manually Edit, and Import PMUL Rules" on page 31
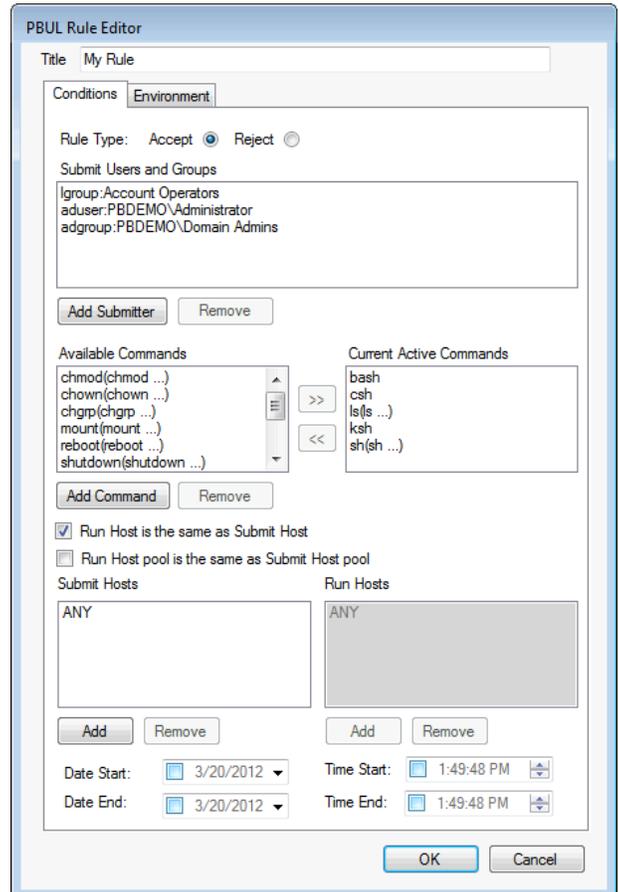
Create or Modify a PMUL Servers Rule

> 📌 **Note:** *Before Privilege Management for Unix & Linux Servers rules can be deployed, a Privilege Management for Unix & Linux Servers configuration file must be defined.*

> ℹ️ For more information, please see "Privilege Management for Unix & Linux Servers Configuration" on page 32.

To create a Privilege Management for Unix & Linux Servers rule or to modify an existing Privilege Management for Unix & Linux Servers rule, do the following:

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

©2003-2020 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

27

TC: 10/16/2020

1. In the **Create Policy Rules Properties** dialog box:
   - To create a new Privilege Management for Unix & Linux Servers rule, click **Add**.
   - To modify an existing Privilege Management for Unix & Linux Servers rule, select the rule and then click **Edit**.

2. Enter a name for the rule.

3. On the **Conditions** tab, select the rule type radio button. Choose from **Accept** or **Reject**.

4. To add a user or group to be managed by the rule, click **Add Submitter**.

5. Select a type of user or group to add. If adding an Active Directory user or group, click **OK**, enter the name of the user or group, and then click **OK**.
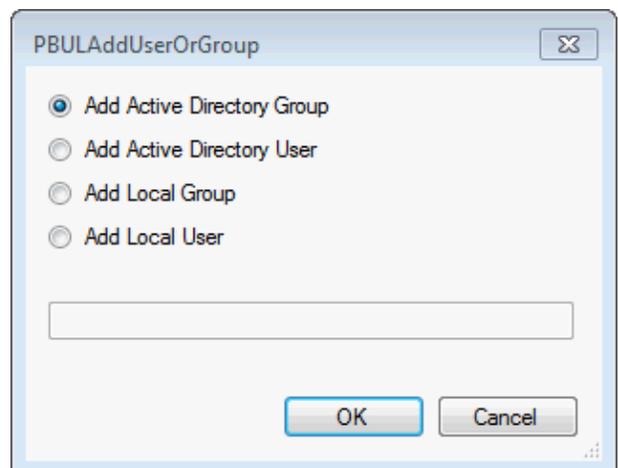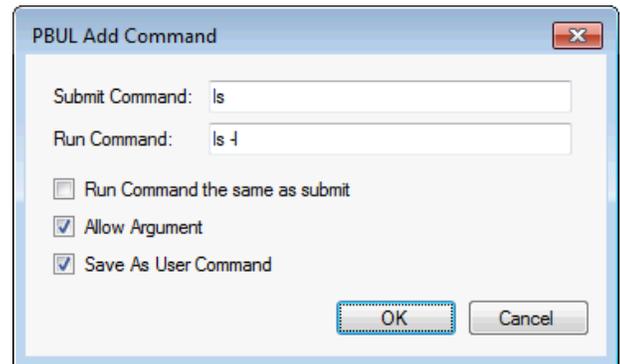

6. If adding a local user or group, type the name in the box and click **OK**.

7. Click **Add Command** and select from the following:

    - **Submit Command**: Enter the command as a submitter would type it. You can include arguments. If you want to allow the user to include additional arguments with the command at runtime, check the **Allow Argument** box.

    - **Run Command**: Enter the command that runs when a submitter types the **Submit Command**. You can include arguments.

    - **Run Command the same as submit**: Check the box when you want the command the same as **Submit Command**.

    - **Run Command the same as Submit**: If this is not selected, you can effectively create an alias for a command for submitters.

    - **Save As User Command**: Check the box to use the command with other PBUL rules.

8. Click **OK** to add the command.

> 📌 *Note: You can remove commands that you add, but you cannot remove the default commands provided with AD Bridge Enterprise.*

9. Select the commands that you want to run when the rule is activated.

    - Click **>>** to move the command to the **Current Active Commands** list.

    - To remove the command from the **Current Active Commands** list, click **<<**.

10. Select the computers that will be **Submit Hosts** (commands in the rule are run by submitters) and **Run Hosts** (commands entered by submitters are run).

    - **Run Host is the same as Submit Host**: (Optional). The computer used as the Run Host must be the same computer used as the Submit Host; check the box.

    - **Run Host pool is the same as Submit Host pool**: (Optional). The selected computers are used as both Submit Hosts and Run Hosts; check the box.

    - **Submit Hosts** and **Run Hosts**: In the **Submit Hosts** or **Run Hosts** areas, click **Add**. Type a computer name or click **ADD** to search Active Directory for a computer. You can enter multiple computer names separated by commas.
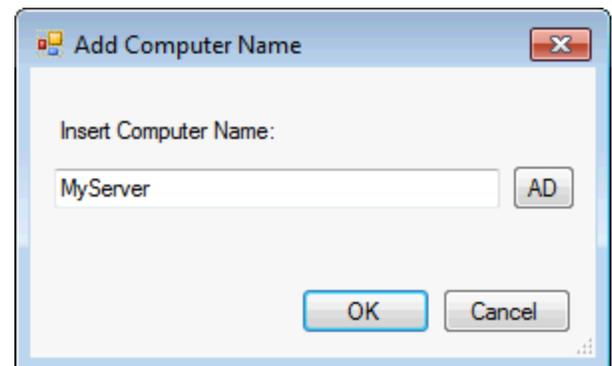
11. (Optional). You can limit when the rule is active to between specified dates or times of day, delay when a rule will become active, or specify an expiration for a rule. For example, to make the rule active only between 8:00AM and 7:00PM, check the **Time Start** box and enter **8:00:00 AM**. Then check the **Time End** box and enter **7:00:00 PM**.

12. Optional. Click the **Environment** tab, and then enter information for the following:

- **Run User**: Enter the user account to use to run the commands in this rule on the Run Host. The default account is **root**. If you change the account, ensure that the account has the permissions necessary to run the commands in the rule and that the account exists on the Run Hosts.
- **Preserve Environment** : (Optional). List any Unix or Linux environment variables that you want to remain unchanged by the effect of this rule when commands are run. Environment variables can alter which libraries are loaded for the session.
- **Define Environment**: (Optional). Enter the names and values of any Unix or Linux environment variables that you want to explicitly define when this rule is used to run commands.
- **Enable Keystroke Logging**: (Optional). To enable keystroke logging, check this box. If selected, by default, keystrokes are logged to a separate log file for each command instance. Advanced administrators can change the path and file name format of these log files by changing the **pb.conf** file. If the default **pb.conf** file is used, keystroke log files are saved to file names beginning with **/var/adm/pb.iolog**.
- **Authenticate User**: (Optional). To display a password prompt to the user and authenticate the user before a command is run, check this box. Select where authentication occurs: **Submit Host**, **Run Host**, or the **Master** Server. This setting can provide additional protection against unauthorized users if an authorized user neglects to lock their computer before stepping away from it.
- **Idle Timeout**: (Optional). To force a timeout so that a long-running command cannot continue indefinitely, check this box and enter the maximum number of minutes. For example, if you are configuring rules that allow users to create a shell session using pbsh or pbksh, you can use this setting to ensure that this elevated access eventually expires if idle.
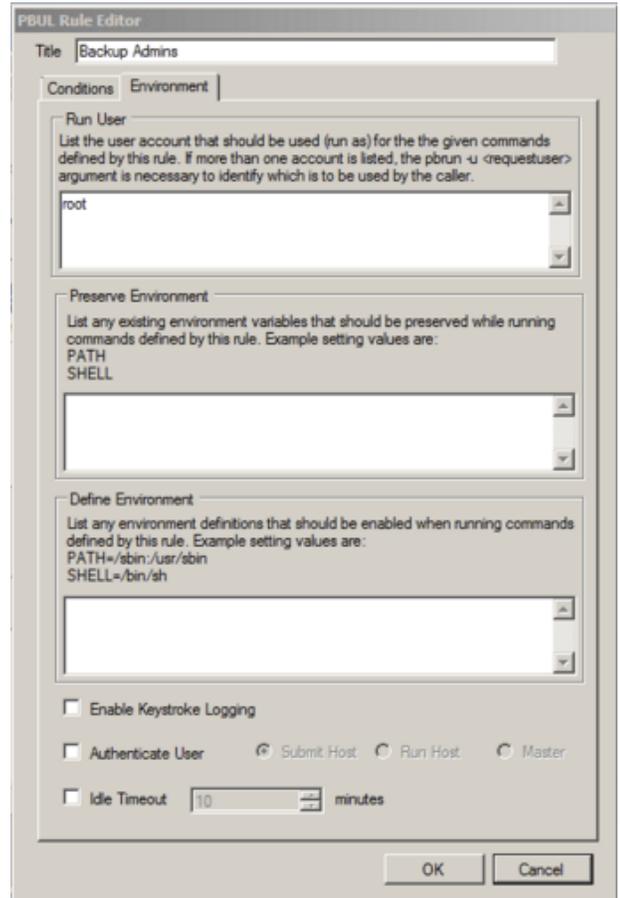
13. Click **OK**.

Change the Priority of PMUL Servers Rules

The priority of Privilege Management for Unix & Linux Servers rules in a GPO is determined by their order in the list on the **Create PowerBroker Server Policy Rules Properties** dialog box.

To change the priority of Privilege Management for Unix & Linux Servers rules, on the **Create PowerBroker Server Policy Rules Properties** dialog box, select a rule and click one of the arrows to move the rule to a higher or lower priority.

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

30

Disable or Enable PMUL Servers Rules

You can enable and disable Privilege Management for Unix & Linux Servers rules from the **Create PowerBroker Server Policy Rules Properties** dialog box. Check the **Enable** box to enable the rules you want to be active. Clear the **Enable** box to disable a rule.
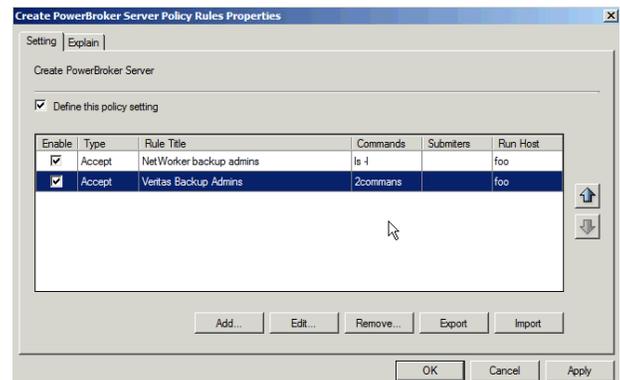
Export, Manually Edit, and Import PMUL Rules

You can export Privilege Management for Unix & Linux Servers rules from Active Directory to a local file, manually edit the rules, and then import the edited rules from a local file into Active Directory.

Export Privilege Management for Unix & Linux Servers Rules to a Local File

You can export Privilege Management for Unix & Linux Servers rules from Active Directory to a local file so that you can manually edit the rules or to archive the rules.

To export Privilege Management for Unix & Linux Servers rules from Active Directory to a local .csv file:

1. On the **Create PowerBroker Server Policy Rules Properties** dialog box, select the rules that you want to export.

*Tip: Use the **CTRL** key to select more than one rule.*

2. Click the **Export** button.
3. Indicate where to save the .csv file, enter a name for the file, and click **Save**.

Import Privilege Management for Unix & Linux Servers Rules to Active Directory

If you manually edited PBUL rules or previously saved PBUL rules to a .csv file, you can import those rules to Active Directory.

To import PBUL rules from a local .csv file to Active Directory:

1. On the **Create Server Policy Rules Properties** dialog box, click the **Import** button.
2. Select a local .csv file from which to import data and click **Open**.
3. Click **Apply** to save the data to Active Directory.

*Tip: To ensure that rules are not inadvertently overwritten, rules in the .csv file that you import will not overwrite existing rules, even if the rule names are the same. If you want a rule that you imported to replace an existing rule, select the existing rule and click **Remove**.*

Privilege Management for Unix & Linux Servers Configuration

The Privilege Management for Unix & Linux Servers Configuration policy setting is designed to install a **pb.conf** file on target computers that are running Privilege Management for Unix & Linux Servers as a Policy Server, enabling Privilege Management for Unix & Linux Servers rules to function. The given computer's **/etc/pb.settings** file determines the placement of the PowerBroker configuration policy file by using the two settings **policyfile** and **policydir**. These values indicate the file and path that the given Policy Server is configured to use for determining policy (typically **/etc/pb.conf**). If there is a previous file at the given location, it is backed up prior to being updated by the new policy configuration installed by Group Policy.

Before Privilege Management for Unix & Linux Servers rules can be deployed using Group Policy, you must define a Privilege Management for Unix & Linux Servers configuration file (**pb.conf**) that will be deployed to PB Masters.

There are several sources from which you can obtain a configuration file.

- If you are already using Privilege Management for Unix & Linux Servers, you can import your existing configuration file.
- If you have not previously used Privilege Management for Unix & Linux Servers or do not have a configuration file, you can import a copy of the default configuration file that is installed with AD Bridge Enterprise. We recommend that you use this file without modification unless you are an advanced administrator of Privilege Management for Unix & Linux Servers.
- If you are an advanced administrator of Privilege Management for Unix & Linux Servers and familiar with Privilege Management for Unix & Linux Servers syntax, you can import a copy of the default configuration file to serve as a template and modify it as needed to use advanced Privilege Management for Unix & Linux Servers functionality.

> **Tip:** If keystroke logging is enabled in a Privilege Management for Unix & Linux Servers rule, keystrokes are logged to a separate file for each command instance. The path and file name format for these files are specified in the **pb.conf** file. The path and file prefix are defined in the **_iolog_file_** variable. The file name is defined by the **iolog** variable.

The default **pb.conf** file is installed in the AD Bridge software installation directory. This **pb.conf** file is designed to process the Privilege Management for Unix & Linux Servers Policy Rules Data (**/etc/pb/Policy.csv**) that is created and maintained by the **Create PowerBroker Server Policy Rules** policy setting. It will apply all of the fields that the Privilege Management for Unix & Linux Servers Rule Editor supports when running on target PB Master computers.

To import a copy of a Privilege Management for Unix & Linux Servers configuration file so that you can deploy Privilege Management for Unix & Linux Servers rules:

1. In Group Policy Management Console (GPMC), right-click an existing GPO and click **Edit** to open the Group Policy Management Editor.

2. In the Group Policy Management Editor, expand **Computer Configuration > Policies > Unix and Linux Settings > BeyondTrust Settings > PowerBroker Servers > PBUL Configuration**.
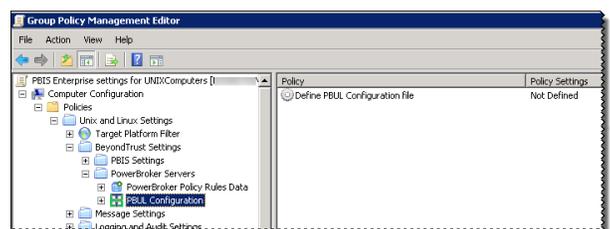
3. Double-click the **Define PBUL Configuration file** policy setting to open the **Define PBUL Configuration file Properties** dialog.

4. Click **Import** to import a copy of a Privilege Management for Unix & Linux Servers configuration file (**pb.conf**). The default **pb.conf** file is located in the AD Bridge software installation directory (typically **C:\Program Files\BeyondTrust\PBIS\Enterprise\Resources\Configuration\pb.conf**).

Note: *You do not need to make any changes to the file. However, if you are an advanced administrator of PBUL who is familiar with PBUL syntax, you can edit the imported file on this dialog box.*
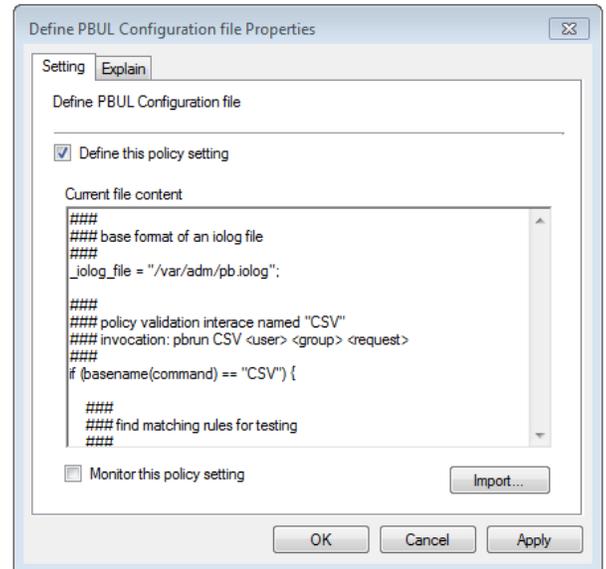
5. Optional. To turn on monitoring for local **pb.conf** files, check the **Monitor this policy setting** box. If the Group Policy agent detects local tampering of the **pb.conf** file, audit event warnings are logged and the local file is replaced by the **pb.conf** file specified in this policy setting.

6. Click **OK**.

Tip: *The **pb.conf** file that you have imported is a copy of the one installed in the AD Bridge software installation directory (typically **C:\Program Files\BeyondTrust\PBIS\Enterprise\Resources\Configuration\pb.conf**). If an administrator inadvertently alters the **pb.conf** file that has been imported, you can replace it by repeating this procedure to import a new copy of the default **pb.conf** file.*

Log a Trouble Ticket With 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

34

- 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
> www.beyondtrust.com/docs/ad-bridge/how-to/troubleshoot.

- 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 www.beyondtrust.com/docs/ad-bridge/getting-started/linux-admin.

- 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:

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