BeyondTrust

AD Bridge 9.1

Installation Guide

Table of Contents

AD Bridge Enterprise Edition

AD Bridge Enterprise Edition connects Linux, Unix, and macOS computers to Microsoft Active Directory so you can centrally manage all your computers and users from a single identity management system.

This guide describes how to install and manage AD Bridge Enterprise Edition. The target audience is system administrators who manage access to workstations, servers, and applications with Active Directory.

IMPORTANT!

The guide assumes that you know how to administer computers, users, and Group Policy settings in Active Directory and that you know how to manage computers running Unix, Linux, and macOS.

AD Bridge Enterprise is installed on a Windows administrative workstation connected to a domain controller so you can set user identifiers and group identifiers in **Active Directory Users and Computers**. Once the UIDs and GIDs are set, the AD Bridge Enterprise agent uses the identifiers to authenticate users and groups and to control access to computers and applications.

AD Bridge Enterprise includes additional features:

- Apply policy settings to Unix computers from the Group Policy Management Console (GPMC), including policy settings based on the Gnome GConf project to define desktop and application preferences for Linux computers.
- Integrates Apple's Workgroup Manager with the group Group Policy Management Editor to apply managed client settings to macOS computers with Group Policy Objects (GPOs).
- Generate a range of reports to help improve regulatory compliance. The result: lower operating costs, better security, enhanced compliance.
- AD Bridge Enterprise provides graphical tools to manage Linux and Unix information in Active Directory. However, it can be useful to access and modify the information programmatically. For this purpose, AD Bridge Enterprise provides scripting objects that can be used by any programming language that supports the Microsoft Common Object Model, or COM. The scripting objects provide dual interfaces that can be used by languages that use COM early binding, such as C++ and C#, and by languages that use Idispatch, such as VBScript and Jscript.

AD Bridge Open Edition

AD Bridge Open Edition is available as a free and open source version of AD Bridge. AD Bridge Open authenticates domain users with the highly secure Kerberos 5 protocol by hashing their security identifiers from Active Directory.

AD Bridge Open does not, however, process user identifiers or group identifiers even if they are set in Active Directory.

For more information, visit the BeyondTrust website.

Components

There are two installation packages that you need to install AD Bridge Enterprise:

- **Management tools for Active Directory:** Install on a Windows computer that connects to an Active Directory domain controller.
- **Agent:** Install on a Linux, Unix, or macOS computer to connect it to Active Directory.

Component	Function
Agent	• Runs on a Linux, Unix, or macOS computer to connect it to Active Directory with the AD Bridge Enterprise command-line interface or GUI. • Communicates with an Active Directory domain controller to authenticate and authorize users and groups with the AD Bridge Enterprise Identity Service. • Pulls and refreshes policy settings by using the Group Policy service, which is included only with the AD Bridge Enterprise agent. For more information, please see the following: • "AD Bridge Enterprise Agent" on page 7 • "Join Active Directory from the Command Line" on page 40 • "Log on with Domain Credentials" on page 52
Enterprise Console	• Runs on a Windows administrative workstation that connects to an Active Directory domain controller to help manage Linux, Unix, and macOS computers in Active Directory. • Migrates users, checks status, and generates reports. For more information, please see "Install the Console" on page 22.
MMC Snap-Ins for ADUC and GPMC	• Extends Active Directory Users and Computers to include Unix and Linux users. • With AD Bridge Enterprise, it also extends the Group Policy Management Console (GPMC) to include Linux, Unix, and macOS Group Policy settings as well as a way to target them at specific platforms.
Cell Manager	A snap-in for the Microsoft Management Console to manage cells associated with Active Directory Organizational Units.
Reporting Database	Stores security events and access logs for compliance reports.
Operations Dashboard	A management application, or plug-in, for the BeyondTrust Management Console. The dashboard retrieves information from the AD Bridge Enterprise reporting database to display authentication transactions, authorization requests, network events, and other security events that take place on AD Bridge Enterprise clients.

AD Bridge Enterprise Agent

The AD Bridge Enterprise agent is installed on a Linux, Unix, or macOS computer to connect it to Microsoft Active Directory and to authenticate users with their domain credentials.

The agent integrates with the core operating system to implement the mapping for any application, such as the logon process (**/bin/login**), that uses the name service (NSS) or pluggable authentication module (PAM). As such, the agent acts as a Kerberos 5 client for authentication and as an LDAP client for authorization. In AD Bridge Enterprise , the agent also retrieves Group Policy Objects (GPOs) to securely update local configurations, such as the sudo file.

For more information, about the AD Bridge Enterprise agent, also known as the AD Bridge Enterprise client software, please see the following:

- "Services" on page 8
- "AD Bridge Enterprise Registry" on page 1
- "Caches and Databases" on page 13
- "Time Synchronization" on page 14
- "Use a Network Time Protocol Server" on page 15
- "Automatic Detection of Offline Domain Controller and Global Catalog" on page 15
- "UID-GID Generation in AD Bridge Cells" on page 1
- "Cached Credentials" on page 15
- "Trust Support" on page 15
- "Integrating with Samba" on page 1
- "Supported Platforms" on page 17

Services

Prior to AD Bridge 6.5, the agent was composed of separate daemon processes, and each was started in sequence by the operating systems at start up.

In AD Bridge 6.5+, the daemons are replaced by libraries loaded by the service manager daemon, **/opt/pbis/sbin/lwsmd**. The service **lsass** replaces the daemon **lsassd**.

At start up, the operating system is configured to start the service manager daemon. It is then instructed by the operating system with the command **/opt/pbis/bin/lwsm autostart** to start all desired services.

The service manager daemon keeps track of the services already started and ensures the services are started and stopped in the appropriate order.

AD Bridge Open and AD Bridge Enterprise

The AD Bridge Open agent and the AD Bridge Enterprise agent are composed of the service manager daemon (**/opt/pbis/sbin/lwsmd**) and include the following services:

Service	Description	Dependencies
lsass	Handles authentication, authorization, caching, and idmap lookups. You can check its status or restart it. To view the lsass architecture see the diagram following the tables.	**netlogon** **lwio** **rdr** **lwreg** Usually **eventlog**. This can be disabled after installation. Sometimes **dcerpc**. This can be enabled after installation for registering TCP/IP endpoints of various services.
netlogon	Detects the optimal domain controller and global catalog and caches them.	**lwreg**

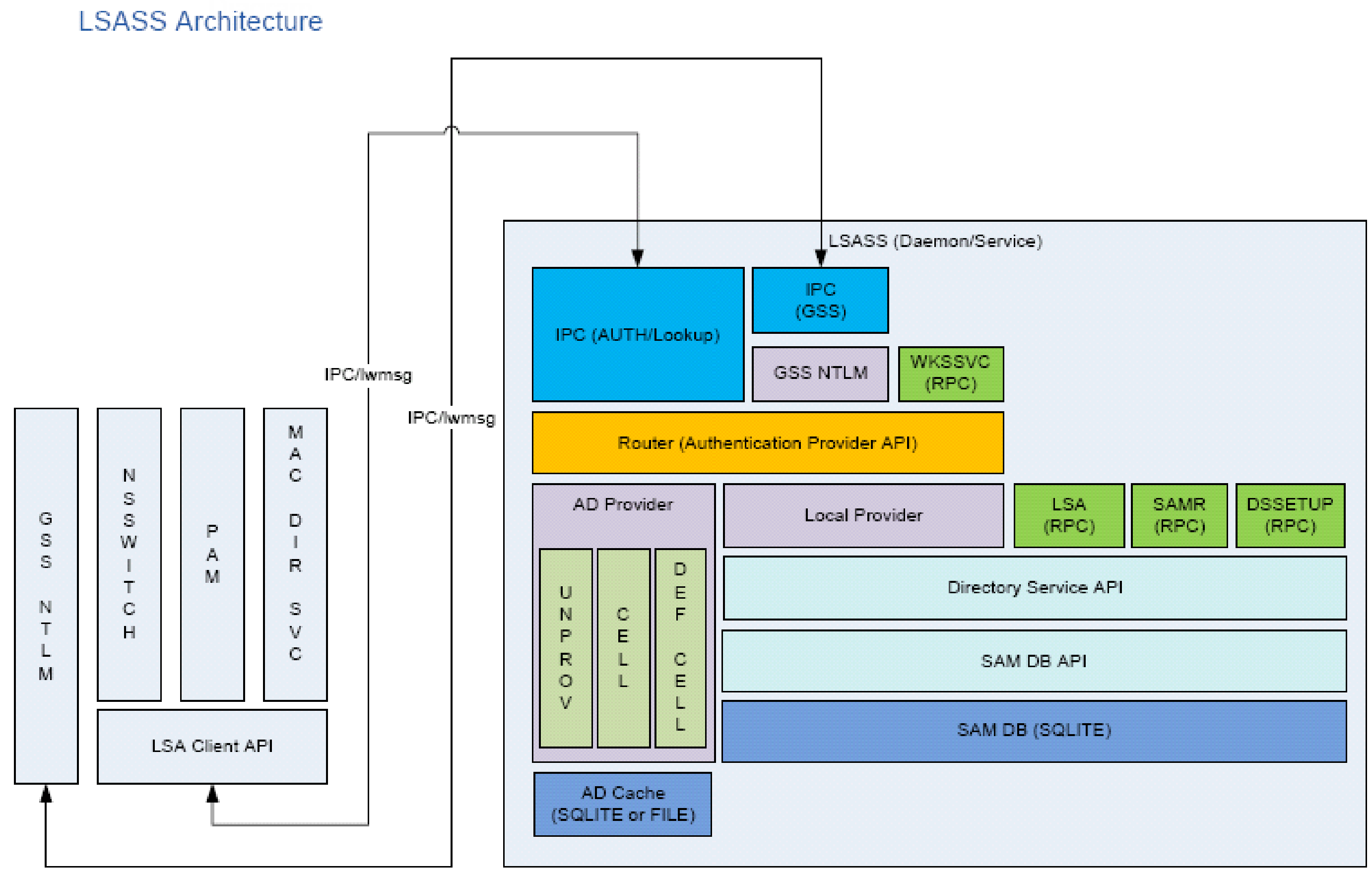
Service	Description	Dependencies
lwio	An input-output service used to communicate through DCE-RPC calls to remote computers, such as during domain join and user authentication.	**lwreg**
rdr	A redirector that multiplexes connections to remote systems.	**lwio** **lwreg**
dcerpc	Handles communication between Linux, Unix, and macOS computers and Microsoft Active Directory by mapping data to end points. By default, it is disabled.	
eventlog	Collects and processes data for the local event log and can be disabled.	
lwreg	The registry service that holds configuration information about both the services and the information provided by the services.	
reapsysl	The syslog reaper that scans syslog for events of interest and records them in the eventlog.	**eventlog**
usermonitor	The service scans the system for changes to users, groups, and authorization rights and records the changes in the eventlog.	**lsass** **eventlog**

AD Bridge Enterprise Only

Additionally, AD Bridge Enterprise also includes the following services to apply Group Policy settings, handle smart cards, and monitor security events:

Service	Description	Dependencies
gpagent	Pulls Group Policy Objects (GPOs) from Active Directory and applies them to the computer.	**lsass** **netlogon** **lwio** **rdr** **lwreg** **eventlog**
eventfwd	Forwards events from the local event log to a remote computer.	**eventlog**
lwsc	Smart card service.	**lwpkcs11**
lwpkcs11	Aids **lwsc** by supporting PKCS#11 API.	
lwpkcs11r	Smart card redirector service for windows client.	**lwsc**

LSASS Architecture:



AD Bridge Enterprise Input-Output Service

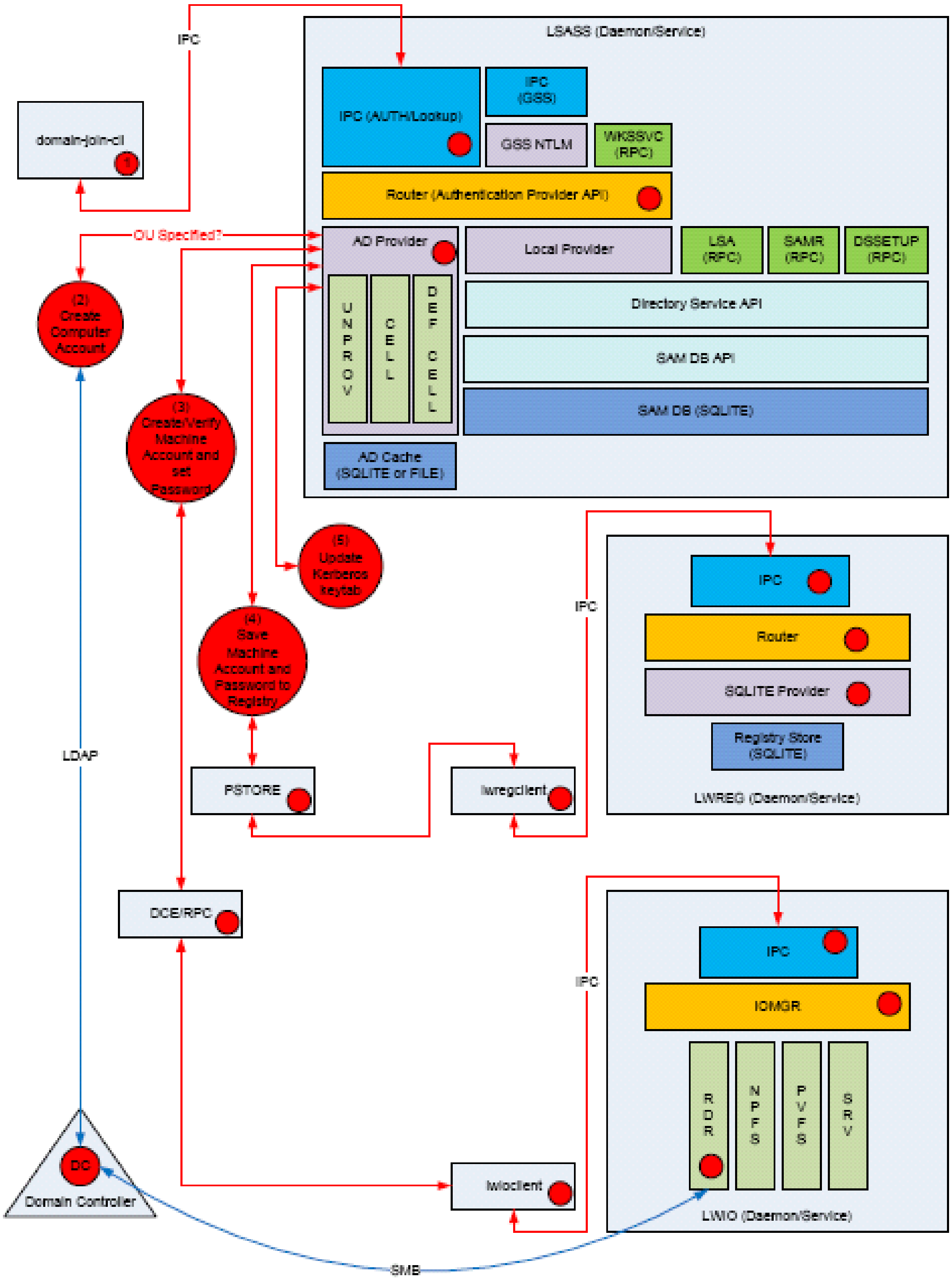
The **lwio** service multiplexes input and output by using SMB1 or SMB2. The service's plugin-based architecture includes several drivers, the most significant of which is coded as **rdr**, the redirector.

The redirector multiplexes Common Internet File System (CIFS) and Server Message Block (SMB) connections to remote systems. For instance, when two different processes on a local Linux computer need to perform input-output operations on a remote system by using CIFS and SMB, with either the same identity or different identities, the preferred method is to use the APIs in the **lwio** client library, which routes the calls through the redirector. In this example, the redirector maintains a single connection to the remote system and multiplexes the traffic from each client by using multiplex IDs.

The input-output service plays a key role in the AD Bridge Enterprise architecture because AD Bridge Enterprise uses Distributed Computing Environment/Remote Procedure Calls (DCE/RPC). DCE/RPC uses SMB. Thus, the DCE-RPC client libraries use the AD Bridge Enterprise input-output client library, which in turn makes calls to **lwio** with Unix domain sockets.

When you join a domain, AD Bridge Enterprise uses DCE-RPC calls to establish the machine password. The AD Bridge Enterprise authentication service periodically refreshes the machine password by using DCE-RPC calls. Authentication of users and groups in Active Directory takes place with Kerberos, not RPC.

Domain Join Component Interaction



In addition, when a joined computer starts up, the AD Bridge Enterprise authentication service enumerates Active Directory trusts by using DCE-RPC calls that go through the redirector. With one-way trusts, the authentication service uses RPC to look up domain users, groups, and security identifiers. With two-way trusts, lookup takes place through LDAP, not RPC.

Because the authentication service registers trusts only when it starts up, you should restart **lsass** with the AD Bridge Enterprise Service Manager after you modify a trust relationship.

The AD Bridge Enterprise Group Policy agent also uses the input-output client library and the redirector when it copies files from the **sysvol** share of a domain controller.

To troubleshoot remote procedure calls that go through the input-output service and its redirector, use a Wireshark trace or a TCP dump to capture the network traffic.

> ***Note:*** *We recommend Wireshark, a free open-source packet analyzer.*

Privileged Access Managment (PAM) Options

AD Bridge Enterprise Edition uses the following standard PAM options:

- **try_first_pass**
- **use_first_pass**
- **use_authtok**
- **debug**

Additionally, there are non-standard options to the PAM configuration on some systems:

- **unknown_ok:** Allows local users to continue down the stack while blocking domain users who do not meet group membership requirements.
- **remember_chpass:** Prevents the AIX computer on AIX systems, which have both PAM and LAM modules, from trying to change the password twice and prompting the user twice.
- **set_default_repository:** used to make sure password changes work as expected on Solaris systems.
- **smartcard_prompt:** Enables smartcard prompts.
- **no_require_membership:** Allows the require membership check to be skipped.

Manage the AD Bridge Enterprise Services

Using the AD Bridge Enterprise Service Manager, you can:

- Track and troubleshoot all the AD Bridge Enterprise services with a single command-line utility. For example, check the status of the services, view their dependencies, and start or stop them. The service manager is the preferred method for restarting a service because it automatically identifies a service's dependencies and restarts them in the correct order.
- Use the service manager to set the logging destination and the log level.

> For more information, please see "Manage AD Bridge Services (lwsm)" in the *AD Bridge Enterprise Windows Administration Guide*.

To list status of the services, run the following command with superuser privileges at the command line:

/opt/pbis/bin/lwsm list

Example:

```
[root@bvt-rhe55-32s ~]# /opt/pbis/bin/lwsm list
lwreg           running (container: 4916)
dcerpc          stopped
eventfwd        stopped
eventlog        running (container: 4929)
gpagent         stopped
lsass           running (container: 4963)
lwio            running (container: 4951)
lwpkcs11        stopped
lwsc            stopped
netlogon        running (container: 4941)
rdr             running (io: 4951)
reapsysl        running (container: 4978)
usermonitor     stopped
[root@bvt-rhe55-32s ~]#
```

Caches and Databases

To maintain the current state and to improve performance, the AD Bridge Enterprise authentication service (**lsass**) caches information about users and groups in memory.

You can change the cache to store the information in a SQLite database.

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

The AD Bridge Enterprise site affinity service, **netlogon**, caches information about the optimal domain controller and global catalog in the AD Bridge Enterprise registry.

The following files are in **/var/lib/pbis/db**:

File	Description
registry.db	The SQLite 3.0 database in which the AD Bridge Enterprise registry service, **lwreg**, stores data.
sam.db	Repository managed by the local authentication provider to store information about local users and groups.
lwi_events.db	The database in which the event logging service, **eventlog**, records events.
lsass-adcache.filedb.FQDN	Cache managed by the Active Directory authentication provider to store user and group information. The file is in **/var/lib/pbis/db**. In the name of the file, FQDN is replaced by your fully qualified domain name.

Since the default UIDs that AD Bridge Enterprise generates are large, the entries made by the operating system in the **lastlog** file when AD users log in make the file appear to increase to a large size. This is normal and should not cause concern. The **lastlog** file (typically **/var/log/lastlog**) is a sparse file that uses the UID and GID of the users as disk addresses to store the last login information. Because it is a sparse file, the actual amount of storage used by it is minimal.

Additional information about a computer's Active Directory domain name, machine account, site affinity, domain controllers, forest, the computer's join state, and so forth is stored in the AD Bridge Enterprise registry. Here is an example of the kind of information that is stored under the **netlogon** key:

```
[HKEY_THIS_MACHINE\Services\netlogon\cachedb\example.com-0]
"DcInfo-ClientSiteName"="Default-First-Site-Name"
"DcInfo-DCSiteName"="Default-First-Site-Name"
```

```
"DcInfo-DnsForestName"="example.com"
"DcInfo-DomainControllerAddress"="192.168.92.20"
"DcInfo-DomainControllerAddressType"=dword:00000017
"DcInfo-DomainControllerName"="w2k3-r2.example.com"
"DcInfo-DomainGUID"=hex:71,c1,9e,b5,18,35,f3,45,ba,15,05,95,fb,5b,62,e3
"DcInfo-Flags"=dword:000003fd
"DcInfo-FullyQualifiedDomainName"="example.com"
"DcInfo-LMToken"=dword:0000ffff
"DcInfo-NetBIOSDomainName"="EXAMPLE"
"DcInfo-NetBIOSHostName"="W2K3-R2"
"DcInfo-NTToken"=dword:0000ffff
"DcInfo-PingTime"=dword:00000006
"DcInfo-UserName"=""
"DcInfo-Version"=dword:00000005
"DnsDomainName"="example.com"
"IsBackoffToWritableDc"=dword:00000000
"LastDiscovered"=hex:c5,d9,86,4b,00,00,00,00
"LastPinged"=hex:1b,fe,86,4b,00,00,00,00
"QueryType"=dword:00000000
"SiteName"=""
```

Name Service Caching Daemon (NSCD)

Disable **nscd** for optimal efficiency.

AD Bridge best practice is to disable the nscd cache from the configuration file **/etc/nscd.conf**.

If **nscd** is not disabled, clear the cache after a domain join by restarting the service: **service nscd restart/reload**.

Time Synchronization

For the AD Bridge Enterprise agent to communicate over Kerberos with the domain controller, the clock of the client must be within the domain controller's maximum clock skew, which is 300 seconds, or 5 minutes, by default.

> For more information, please see the MIT article Clock Skew at http://web.mit.edu/kerberos/krb5-1.4/krb5-1.4.2/doc/krb5-admin/Clock-Skew.html.

The clock skew tolerance is a server-side setting. When a client communicates with a domain controller, it is the domain controller's Kerberos key distribution center that determines the maximum clock skew. Since changing the maximum clock skew in a client's **krb5.conf** file does not affect the clock skew tolerance of the domain controller, the change will not allow a client outside the domain controller's tolerance to communicate with it.

The clock skew value that is set in the **/etc/pbis/krb5.conf** file of Linux, Unix, and macOS computers is useful only when the computer functions as a server for other clients. In such cases, you can use an AD Bridge Enterprise Group Policy setting to change the maximum tolerance.

The domain controller uses the clock skew tolerance to prevent replay attacks by keeping track of every authentication request within the maximum clock skew. Authentication requests outside the maximum clock skew are discarded. When the server receives an authentication request within the clock skew, it checks the replay cache to make sure the request is not a replay attack.

Use a Network Time Protocol Server

If you set the system time on your computer with a Network Time Protocol (NTP) server, the time value of the NTP server and the time value of the domain controller could exceed the maximum skew. As a result, you will be unable to log on your computer.

If you use an NTP server with a cron job, there will be two processes trying to synchronize the computer's time, causing a conflict that will change the computer's clock back and forth between the time of the two sources.

We recommend that you configure your domain controller to get its time from the NTP server and configure the domain controller's clients to get their time from the domain controller.

Automatic Detection of Offline Domain Controller and Global Catalog

The AD Bridge Enterprise authentication service, **lsass**, manages site affinity for domain controllers and global catalogs and caches the information with **netlogon**. When a computer is joined to Active Directory, **netlogon** determines the optimum domain controller and caches the information.

If the primary domain controller goes down, **lsass** automatically detects the failure and switches to another domain controller and another global catalog within a minute.

However, if another global catalog is unavailable within the forest, the AD Bridge Enterprise agent will be unable to find the Unix and Linux information of users and groups. The AD Bridge Enterprise agent must have access to the global catalog to function. Therefore, we recommend that each forest has redundant domain controllers and redundant global catalogs.

Cached Credentials

Both AD Bridge Open and AD Bridge Enterprise cache credentials so users can log on when the computer is disconnected from the network or Active Directory is unavailable.

Trust Support

The AD Bridge Enterprise agent supports the following Active Directory trusts:

Trust Type	Transitivity	Direction	AD Bridge Enterprise Default Cell Support	Named Cells
Parent and child	Transitive	Two-way	Yes	Yes
External	Nontransitive	One-way	No	Yes
External	Nontransitive	Two-way	No	Yes
Forest	Transitive	One-way	No	Yes
Forest	Transitive	Two-way	Yes: Must enable default cell in both forests.	Yes

For more information on the types of trusts, please see the Microsoft article Trust Types at technet.microsoft.com/en-us/library/cc775736(WS.10).aspx.

For more information about trusts, please see the following:

- "Notes on Trusts" on page 1
- "Trusts and Cells in AD Bridge" on page 1

Notes on Trusts

The following is general information about working with trusts.

- You must place the user or group that you want to give access to the trust in a cell other than the default cell.
- In a two-way forest or parent-child trust, AD Bridge Enterprise merges the default cells. When merged, users in one domain can log on computers in another domain, and vice-versa.
- To put a user in a child domain but not the parent domain, you must put the user in a named cell, which is a cell associated with an organizational unit.
- If there is a UID conflict across two domains, one domain will be dropped.
- In a cross-forest transitive one-way or two-way trust, the root of the trusted forest must have a default cell.
- In a one-way trust in which Forest A trusts Forest B, a computer in Forest A cannot get group information from Forest B, because Forest B does not trust Forest A. The computer in Forest A can obtain group information if the user logs on with a password for a domain user, but not if the user logs on with Kerberos single sign-on credentials. Only the primary group information, not the secondary group information, is obtained.
- To support a one-way trust without duplicating user accounts, you must use a cell associated with an OU, not a default cell. If Domain A trusts Domain B (but not the reverse) and if Domain B contains all the account information in cells associated with OUs, then when a user from Domain B logs on a machine joined to Domain A, Domain B will authenticate the user and authorize access to the machine in Domain A.

> ***Note:*** *In such a scenario, you should also add a domain user from the trusted domain to an administrative group in the trusting domain so you can manage the trusting domain with the appropriate level of read access to trusted user and group information. However, before you add the domain user from the trusted domain to the trusting domain, you must first add to the trusting domain a group that includes the user because Unix and Linux computers require membership in at least one group and Active Directory does not enumerate a user's membership in foreign groups.*

- If you have a network topology in which the "front" domain trusts the "back" domain, and you join a machine to the front domain using a back domain administrator, as in the following example, the attempt to join the domain will fail: **domainjoin-cli join front.example.com back\\administrator password**. However, the attempt to join the domain will succeed if you use the following nomenclature: **domainjoin-cli join front.example.com administrator@BACK.example.COM password**.
- With AD Bridge Enterprise, aliased user names are supported in the default cell and in named cells.

Trusts and Cells in AD Bridge

In AD Bridge Enterprise, a cell contains Unix settings, such as a UID and a GID, for an Active Directory user. When an AD user logs into an AD Bridge Enterprise client, AD Bridge Enterprise searches Active Directory for the user's cell information and must find it to operate properly. Thus, your AD topology and your trust relationships may dictate where to locate a cell in Active Directory so that your AD Bridge Enterprise clients can access their Unix settings.

With 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. In a multi-domain topology, a default cell must exist in the domain where user and group objects reside in addition to the default cell that exists in the domain to which Unix, Linux, and Mac computers are joined.

> ***Note:*** *In a multi-domain topology, be sure to create a default cell in each domain.*

Ideally, Unix information is stored on the user object in default cell Directory Integrated mode. If the client computer does not have the access rights to read and write the information to the user object, as in an external one-way trust, the Unix information cannot be stored on the user object. It can, however, be stored locally in a named cell, that is, a cell associated with an organizational unit.

Since a named cell can be linked to the default cell, you can store Unix information on the user object in default cell Directory Integrated mode when possible, and otherwise in a named cell that represents the external user.

For information about cells, please see "Plan Your Deployment" on page 19

Supported Platforms

AD Bridge Open and AD Bridge Enterprise run on a broad range of Unix, macOS, and Linux platforms. BeyondTrust frequently adds new vendors and distributions.

SELinux Support

The AD Bridge Enterprise SELinux implementation supports the following operating systems:

- Fedora 13 - Fedora 17
- RedHat Enterprise Linux and CentOS versions 6.x - 7.x

***Note:** When you install on RedHat Enterprise Linux, AD Bridge runs under the **unconfined_t** domain (as of 8.3.4).*

The AD Bridge post install script checks if **/usr/sbin/semodule** and **/etc/selinux/targeted/policy** are present. If both checks pass, the targeted policy file (**pbis.pp**) will get installed if found in **/opt/pbis/share/<os>/<version>/pbis.pp**.

Unsupported Operating Systems

If SELinux is enabled and you are installing to an unsupported operating system, the installation is stopped. You must place SELinux in permissive mode to continue.

- SELinux enabled is only detected with the RPM package.
- SELinux enabled is not detected with the self-extracting installer or domainjoin.

For more information, please see "Configure SELinux" on page 37.

Storage Modes

AD Bridge Enterprise has two operating modes: Directory Integrated mode and Schemaless mode.

***Note:** Directory Integrated mode is the preferred mode.*

The modes provide a method for storing Unix and Linux information in Active Directory, including UIDs and GIDs, so that AD Bridge can map SIDs to UIDs and GIDs and vice versa.

The mapping lets AD Bridge use an Active Directory user account to grant a user access to a Unix or Linux resource that is governed by a UID-GID scheme. When an AD user logs on a Unix or Linux computer, the AD Bridge agent communicates with the Active Directory Domain Controller through standard LDAP protocols to obtain the following authorization data:

- UID
- Primary GID
- Secondary GIDs

- Home directory
- Login shell

AD Bridge uses this information to control the user's access to Unix and Linux resources.

Directory Integrated Mode

Directory Integrated mode takes advantage of the Unix- and Linux-specific RFC 2307 object classes and attributes to store Linux and Unix user and group information, namely the **posixAccount** and **posixGroup** object classes.

For example, the **posixAccount** and **posixGroup** object classes include attributes (**uidNumber** and **gidNumber**) that AD Bridge Enterprise uses for UID and GID mapping. In addition, AD Bridge uses **serviceConnectionPoint** objects to store the same information as in Schemaless by using the **keywords** attribute.

For example, when you create a cell in Directory Integrated mode, AD Bridge creates a container object, **CN=$LikewiseIdentityCell**, in the domain root, or in the OU where you created the cell. If the container is created in an OU, which is called a named or named cell, the Unix-specific data is stored in **CN=Users** and **CN=Groups** in the **$LikewiseIdentityCell** container object. The objects point to the Active Directory user or group information with a backlinked security identifier.

If the container is created at the level of the root domain, it is known as a default cell. In this case, the Unix-specific data is stored directly in the AD user or group account.

Upgrade Your Schema

You must upgrade your schema if your schema does not comply with RFC 2307 (Windows Server 2003 R2 or later complies with RFC 2307).

Use the Active Directory Domains and Trusts tool to raise the forest functional level.

AD Bridge does not change the schema, but you still must run the **Directory Integrated Mode Wizard** to include the RFC 2307 attributes in the global catalog and to index them for faster searches.

Schemaless Mode

In contrast, Schemaless mode stores Linux and Unix data without requiring RFC 2307 object classes and attributes and without modifying the schema. Instead, Schemaless mode uses existing object classes and attributes to store its data.

- To store information about a cell, AD Bridge Enterprise creates a container object and stores data in its **description** attribute.
- To store information about a group or user, AD Bridge Enterprise creates a **serviceConnectionPoint** object and stores data in its **keywords** attribute. Both **keywords** and **description** are multi-valued attributes that can have multiple values while still allowing AD searches for specific values.

In Schemaless mode, AD Bridge Enterprise uses RFC 2307 attribute names to store values in the **keywords** and **description** attributes in the form **name=value**, where **name** is the attribute name and **value** is its value.

Plan Your Deployment

The key to a successful deployment is planning. Before you begin deploying AD Bridge Enterprise in an enterprise environment, develop a plan that addresses at least the following aspects of installation and deployment:

- Review the AD Bridge Enterprise Release Notes to ensure your environment meets the deployment requirements.
- Set up a test environment. We recommend that you first deploy AD Bridge Enterprise in a test environment so that you can identify and resolve any issues specific to your mixed network before you put the system into production.
- Determine whether to use AD Bridge Enterprise in Directory Integration or Schemaless mode. When you configure your domain with the AD Bridge Enterprise domain configuration wizard, you must choose the mode to use.

> For more information on Directory Integration and Schemaless mode, please see "Storage Modes" on page 17.

IMPORTANT!

Back up Active Directory before you run the AD Bridge Enterprise domain configuration wizard.

- Decide whether to configure AD Bridge Enterprise to manage a single forest or multiple forests. If you manage multiple forests, the UID-GID range assigned to a forest should not overlap with the range of another forest.
- Determine how you will migrate Linux, Unix, and macOS users to Active Directory. For example, if you are using NIS, decide whether you will migrate those accounts to Active Directory and whether you will migrate local accounts and then delete them or leave them. It is usually recommended that you delete interactive local accounts other than the root account.
- Identify the structure of the organizational units or cell topology that you will need, including the UID-GID ranges. If you have multiple NIS servers in place, your users may have different UID-GID maps in each NIS domain. You may want to eliminate the NIS servers but retain the NIS mapping information in Active Directory. To do so, you can use AD Bridge Cells.
- Determine whether you will use aliasing. If you plan to use aliasing, you must associate users with a specific AD Bridge cell; you cannot use the default cell.

Install the Management Console

This section provides information on management console requirements and installing the console.

> For more about installing and using the console, see the following topics:
> - "Requirements" on page 20
> - "Install the Console" on page 22
> - "Change to Directory Integrated Mode" on page 26

Requirements

This section lists the requirements to use AD Bridge Enterprise with Active Directory.

You must have at least the following components:

- An Active Directory domain controller.
- A Windows administrative workstation that is running ADUC and is connected to your Active Directory domain controller.
- One or more Unix or Linux computers running an operating system that AD Bridge Enterprise supports, such as versions of macOS, Red Hat, SUSE Linux, Fedora, CentOS, Debian, Sun Solaris, IBM AIX, HP-UX, and Ubuntu.

> For agent requirements (the software that runs on the Linux, Unix, and macOS computers that you want to connect to AD), please see "Install the AD Bridge Enterprise Agent" on page 30.

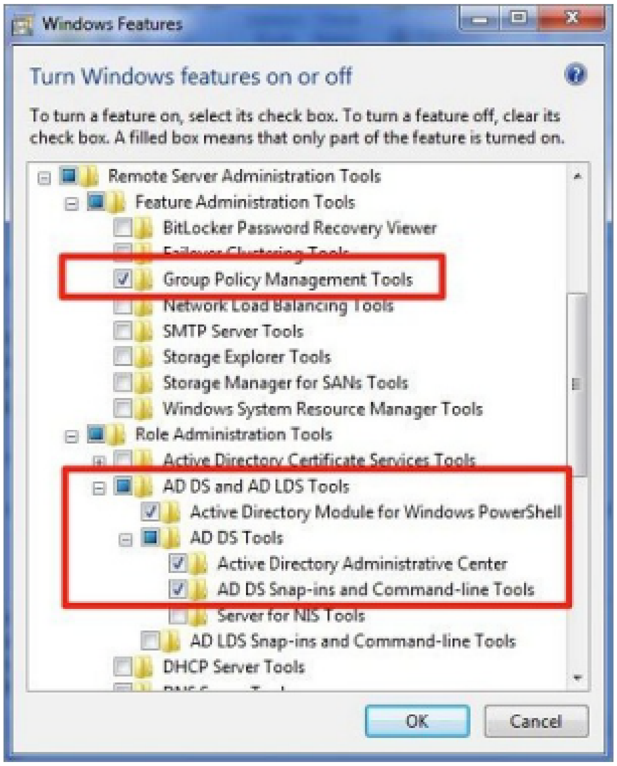
Microsoft Management Tools

AD Bridge Enterprise works with ADUC, GPME, and GPMC. Ensure that the Microsoft management tools are installed before you install AD Bridge Enterprise.

The Microsoft management tools vary by Windows version, but include the Remote Server Administration Tools (RSAT) for Windows.

Turn on the following RSAT features. Go to **Control Panel**, select **Programs**, and then select **Turn Windows features on or off**:

- **Group Policy Management Tools**
- **Active Directory Module for Windows PowerShell**
- **Active Directory Administrative Center**
- **AD DS Snap-ins and Command-Line Tools**



Windows Features

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ■ Remote Server Administration Tools
  - ■ Feature Administration Tools
    - □ BitLocker Password Recovery Viewer
    - □ Failover Clustering Tools
    - ☑ Group Policy Management Tools
    - □ Network Load Balancing Tools
    - □ SMTP Server Tools
    - □ Storage Explorer Tools
    - □ Storage Manager for SANs Tools
    - □ Windows System Resource Manager Tools
  - ■ Role Administration Tools
    - □ Active Directory Certificate Services Tools
    - ■ AD DS and AD LDS Tools
      - ☑ Active Directory Module for Windows PowerShell
      - ■ AD DS Tools
        - ☑ Active Directory Administrative Center
        - ☑ AD DS Snap-ins and Command-line Tools
        - □ Server for NIS Tools
      - □ AD LDS Snap-ins and Command-line Tools
    - □ DHCP Server Tools
    - □ DNS Server Tools

For more information, please see Remote Server Administration Tools for Windows at https://support.microsoft.com/en-us/help/2693643/remote-server-administration-tools-rsat-for-windows-operating-systems.

Administrator Privileges

- Root access or sudo permission on the Unix, Linux, and macOS computers that you want to join to the domain.
- Active Directory credentials that allow you to add computers to an Active Directory domain. For example, membership in the Domain Administrators security group or the Enterprise Administrators security group.

Active Directory Requirements

- Windows Server 2008 R2 or higher

Windows Requirements for the Console

- One of the following operating systems:
  - Windows Professional 7 or higher with RSAT
  - Windows Server 2008 R2 or higher
  - 64-bit versions only

- Microsoft .NET Framework 4.5
- 50 MB of free space

Requirements to Run AD Bridge Enterprise in Directory Integrated Mode

- Active Directory installations that comply with RFC 2307
- Domain and forest functional levels have been raised to Windows Server 2003 or later.

> i For more information, please see "Storage Modes" on page 17.

Networking

The subnets with your Linux, Unix, and macOS computers must be added to Active Directory sites before joining the computers to Active Directory so that the AD Bridge Enterprise agent can detect the optimal domain controller and global catalog.

Replication

Make sure your AD replication system is up to date and functioning properly by using the following diagnostic tools from www.microsoft.com/download to test replication.

> i For instructions, see the Microsoft documentation for each tool.

- **DCDiag**: Part of Microsoft's support tools for Windows Server 2003, **dcdiag.exe** should be run with the **/v /c /e** switches to test the domain controllers in all your sites.
- **FRSDiag**: Use **frsdiag.exe** tool, available from the Microsoft Resource Kit tools, to check the File Replication Service (FRS).

In addition, the following tools can help you review and troubleshoot FRS problems.

- **Sonar**: Use it to perform a quick review of FRS status.
- **Ultrasound**: Use it to monitor and troubleshoot FRS.
- **ReplMon**: Included in the Microsoft Resource Kit Tools. Use it to investigate replication problems across links where DCDiag showed failures.

Supported Platforms and Applications

Platforms

AD Bridge Enterprise supports many Unix, Linux, macOS, and virtualization platforms.

Applications

You can use the Advanced Group Policy Management (AGPM) tool to manage your GPOs. Any AD Bridge Enterprise settings applied to your GPOs will be maintained.

Install the Console

Install the BeyondTrust Management Console on a Windows administrative workstation that can connect to your Active Directory domain controller.

We recommend that you do not install the console on a domain controller.

- Review the requirements before proceeding with the installation.

> For more information, please see "Requirements" on page 20.

- Ensure the account you are using to run the install is a member of the Domain Admins group or Enterprise Admins group. The account needs privileges to change objects and child objects in Active Directory.
- Ensure the Microsoft management tools for Active Directory are installed before you install the console.

> For more information about Microsoft management tools, please see "Requirements" on page 20.

During the installation, checks are in place to ensure that your environment meets successful installation requirements. If you need more information, a log file is created here during the install: **%UserProfile%AppData\Local\PBIS.Logs**.

1. Locate and copy the **SetupPBIS64-*.exe** install file to your Windows workstation. The installer file includes the version and build number.
2. Run **SetupPBIS64-*.exe**.
3. On the **License Agreement** page, click **Accept** to go through the installation.
4. Click **Install**.
5. On the **Directory Integrated Mode Configuration** page, click **Configure** to set up Directory Integrated mode. Otherwise, click **Skip**.
6. On the **Default Cell Creation** page, click **Create Cell** to build the default cell. Otherwise, click **Skip**.
7. On the **Reporting Options** page, configure the following:
   - **Report Viewer**: Click **Install** to install the Report viewer.
   - **SQL Server database instance**: Click **Search Server** to create the AD Bridge database.
   - **Event Collector services**: Click **Install** to go through the wizard to configure the AD Bridge Database utilities.
8. Click **Finish**.

Use msiexec.exe

Silent Install

Run a silent install or uninstall of the console using **msiexec.exe**. To see a complete list of options, run **msiexec.exe**.

Examples

```
msiexec.exe /i PBISEnterprise64-x.x.x.xxx.msi /quiet /qn
```

```
msiexec.exe /x PBISEnterprise64-x.x.x.xxx.msi /quiet /qn
```

Install Individual Modules

Install individual AD Bridge modules using **msiexec.exe**. The following module options are available:

- BaseInstall
- ConsoleInstall
- ReportingToolsInstall
- OperationsDashboard
- DBUpdateTool
- MigrationToolsInstall
- MMCExtensions
- MigrationToolsInstall
- GPMC
- ADUC

Example

```
msiexec /i PBISEnterprise64-x.x.x.xxx.msi ADDLOCAL=BaseInstall /qn
```

Install Active Directory and GPMC Extensions

You can run an installer that only installs the **Active Directory Users and Computers** and **Group Policy Management Console** (GPMC) extensions. The BeyondTrust Management Console and reporting components will not be installed. Run the installer: **SetupExtensions64-x.x.x.xxx.exe**.

Upgrade the Console

To upgrade to the latest version of AD Bridge Enterprise, first uninstall the existing version. Then, before installing the latest version of AD Bridge Enterprise, install the latest version of Group Policy Management Console (GPMC) and run Windows update to make sure your workstation has the latest XML patches.

Upgrade AD Bridge 7.5 to AD Bridge 8.1

If you were using Directory Integrated mode in AD Bridge Enterprise 7.5, updates to the schema need to be applied when you upgrade to AD Bridge Enterprise 8.1. Ensure that the user installing AD Bridge is a member in the **Schema Admins** group. The install must be run on the forest root since the **Schema Admins** group only exists on the domain controller for the forest.

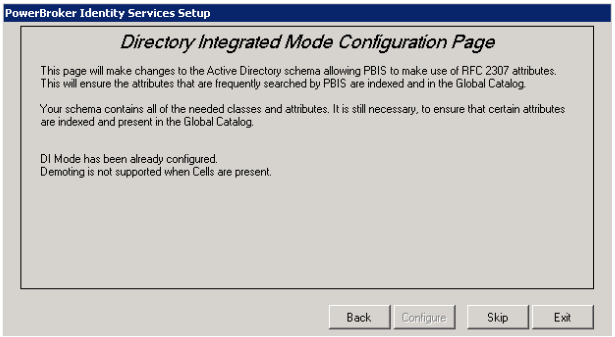
For more information on the **Schema Admins** group, please refer to Microsoft documentation.

When **Schema Admins** permissions are in place, you can upgrade AD Bridge without removing your existing AD Bridge Cells.

***Note:** The **Schema Admins** permissions only apply to an upgrade.*

7.5.3 or earlier you need the schema admin rights to upgrade to 8.1. for this upgrade, you can promote the schema automatically with the cells existing (ie don't have to remove the cells like you did for the 8.0

1. Locate and copy the **SetupPBIS64-*.exe** install file to your Windows workstation. The installer file includes the version and build number.
2. Run **SetupPBIS64-*.exe**.
3. Accept the license agreement, and then click **Next**.
4. To change settings for the AD Bridge Enterprise install, click **Modify**. The installation wizard starts. This is where you select the components to install.
    - set the user name and organization
    - set the installation directory
    - select the AD Bridge components to install:
        - **BT Management Console**
        - **Reporting**
        - **Operations Dashboard**
        - **Database Update and Management tools**
        - **Migration tools**
        - **GPMC support**.
    - click **Finish**
5. If you plan to use Directory Integrated mode, there is no configuration required here. Click **Skip**.



Directory Integrated Mode Configuration Page

This page will make changes to the Active Directory schema allowing PBIS to make use of RFC 2307 attributes.
This will ensure the attributes that are frequently searched by PBIS are indexed and in the Global Catalog.

Your schema contains all of the needed classes and attributes. It is still necessary, to ensure that certain attributes are indexed and present in the Global Catalog.

DI Mode has been already configured.
Demoting is not supported when Cells are present.

6. Click **Skip** on the **Default Cell Create Page**.
7. On the **Advanced Options** page, you can:
    - Remove the report viewer.
    - Create or remove database instances.
    - Run the **AD Bridge Enterprise Database Utilities** wizard.
8. Click **Finish**.

Upgrade from 8.1 - Directory Integrated Mode

This section applies to upgrades from AD Bridge version 8.1 and later if you have met one or more of the following criteria:

- Using Directory Integrated mode in AD Bridge versions 7.5 and earlier, and installing the Management Console.
- In your forest schema, UidNumber, GidNumber and Uid are all indexed and promoted to the Global Catalog.

The installer detects the old Directory Integration mode and updates to the schema needed to be applied to prevent potential issues. Ensure that the user installing AD Bridge is a member in the **Schema Admins** group.

Run the installer on the forest root.

For more information on the **Schema Admins** group, please refer to Microsoft documentation.

When **Schema Admins** permissions are in place, you can upgrade AD Bridge Directory Integration mode without removing your existing AD Bridge Cells.

For changes to the schema, please see "Changes Made by the Directory Integrated Mode Configuration" on page 26.

Change to Directory Integrated Mode

Running the wizard indexes frequently searched attributes in the Active Directory global catalog.

1. Run the AD Bridge installer, and skip to the **Directory Integrated Mode Configuration** page.
2. Click the **Configure** button.

The necessary attributes are updated.

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**

Configure Clients Before AD Bridge Enterprise Agent Installation

Before you install the AD Bridge Enterprise agent, configure client computers as indicated in the following sections.

Configure nsswitch.conf

Before you attempt to join an Active Directory domain, make sure the **/etc/nsswitch.conf** file contains the following line:

```
hosts: files dns
```

The **hosts** line can contain additional information, but it must include the **dns** entry, and we recommend that the **dns** entry appear after the **files** entry.

Computers running Solaris, in particular, may not contain this line in **nsswitch.conf** until you add it.

When you use AD Bridge with Multicast DNS 4 (mDNS4) and have a domain in your environment that ends in **.local**, you must place the **dns** entry before the **mdns4_minimal** entry and before the **mdns4** entry:

```
hosts: files dns mdns4_minimal [NOTFOUND=return] mdns4
```

The default setting for many Linux systems is to list the **mdns4** entries before the **dns** entry, a configuration that leaves AD Bridge Enterprise unable to find the domain.

For AD Bridge Enterprise to work correctly, the **nsswitch.conf** file must be readable by user, group, and world.

For more information on configuring nsswitch, please see the man page for **nsswitch.conf.**

Configure netsvc.conf on AIX

On AIX computers, ensure the **netsvc.conf** file contains the following line:

```
hosts = local,bind
```

Restart Services

After you update **nsswitch.conf** (or **netsvc.conf**), you must restart the AD Bridge Enterprise input-output service (**lwio**) and the authentication service (**lsass**).

Run the following command as root to restart both services:

```
/opt/pbis/bin/lwsm restart lwio
```

Configure resolv.conf

Before you attempt to join an Active Directory domain, make sure that **/etc/resolv.conf** on your Linux, Unix, or Mac client includes a DNS server that can resolve SRV records for your domain.

Example:

```
[root@rhel5d Desktop]# cat /etc/resolv.conf
search example.com
nameserver 192.168.100.132
```

For more information on **resolv.conf**, please see your operating system's man page.

Configure Firewall Ports

If you use local firewall settings, such as **iptables**, on a computer running the AD Bridge Enterprise agent, ensure the following ports are open for outbound traffic.

Note: *The AD Bridge Enterprise agent is a client. It does not listen on any ports.*

Port	Protocol	Use
53	UDP/ TCP	DNS
88	UDP/TCP	Kerberos 5
123	UDP	NTP
389	UDP/TCP	LDAP
443	TCP	AD Bridge Reporting to BeyondInsight
445	TCP	SMB over TCP
464	UDP/TCP	Computer password changes (typically after 30 days)
1433	TCP	Connection to SQL Server. Open the port you are using. The default port for SQL is 1433.
3268	TCP	Global Catalog search

Tip: *To view the firewall rules on a Linux computer using **iptables**, execute the following command:*

```
iptables – nL
```

Extend Partition Size (IBM AIX)

On AIX 5.2 and 5.3, you may need to extend the size of certain partitions to complete the installation.

To change the partition size using IBM'S **chfs** command, use **chfs -a size=+200M /opt**.

The example command increases the size of the **opt** partition by 200 MB, which should be sufficient for a successful installation.

Increase Max User Name Length (IBM AIX)

By default, IBM AIX is not configured to support long user and group names, which might present a conflict when you try to log on with a long Active Directory username.

On AIX 5.3 and AIX 6.1, group names are truncated when enumerated through the **groups** command.

To increase the max user name length on AIX 5.3, use the following syntax:

```
# chdev -l sys0 -a max_logname=MaxUserNameLength+1
```

Example:

```
# chdev -l sys0 -a max_logname=255
```

This command allocates 254 characters for the user and 1 for the terminating null.

The safest value that you can set **max_logname** to is **255**.

You must reboot for the changes to take effect:

```
# shutdown -Fr
```

Note: *AIX 5.2 does not support increasing the maximum user name length.*

Install the AD Bridge Enterprise Agent

The following sections provide details on installing the AD Bridge agent to your computers.

Install the Correct Version for the Operating System

Install the AD Bridge agent, the identity service that authenticates users, on each Linux, Unix, or macOS computer that you want to connect to Active Directory.

IMPORTANT!

Before installing the agent, we recommend that you upgrade your system with the latest security patches. Please see "Requirements for the Agent" on page 30.

The procedure for installing the agent depends on the operating system of the target computer or virtual machine.

Check the Linux Kernel Release Number

To run the AD Bridge agent on a Linux machine, the kernel release number must be 2.6 or later.

To determine the release number of the kernel, run the following command:

```
uname -r
```

Package Management Commands

For an overview of commands such as **rpm** and **dpkg** that can help you manage AD Bridge on Linux and Unix platforms, please see *AD Bridge Package Management Commands*.

Requirements for the Agent

This section lists requirements for installing and running the AD Bridge agent.

Environment Variables

Before you install the AD Bridge agent, make sure that the following environment variables are not set:

- **LD_LIBRARY_PATH**
- **LIBPATH**
- **SHLIB_PATH**
- **LD_PRELOAD**

Setting any of these environment variables violates best practices for managing Unix and Linux computers because it causes AD Bridge to use non-AD Bridge libraries for its services.

> For more information on best practices, please see When Should I Set LB_LIBRARY_PATH? at http://linuxmafia.com/faq/Admin/ld-lib-path.html.

If you must set **LD_LIBRARY_PATH**, **LIBPATH**, or **SHLIB_PATH** for another program, put the AD Bridge library path (**/opt/pbis/lib** or **/opt/pbis/lib64**) before any other path, but keep in mind that doing so may result in side effects for other programs, as they will now use AD Bridge libraries for their services.

If joining the domain fails with an error message that one of these environment variables is set, stop all the AD Bridge services, clear the environment variable, make sure it is not automatically set when the computer restarts, and then try to join the domain again.

Patch Requirements

We recommend that the latest patches for an operating system be applied before installing AD Bridge.

Sun Solaris

All Solaris versions require the **md5sum** utility, which can be found on the companion CD.

> Visit the Oracle Technology Network Patching Center at http://www.oracle.com/technetwork/systems/patches/overview/index.html to ensure the latest patches are deployed to Solaris targets.

HP-UX

> Visit the HP Software Depot to download patches.

Secure Shell: For all HP-UX platforms, we recommend that a recent version of HP's Secure Shell be installed.

Sudo: By default, the versions of sudo available from the HP-UX Porting Center do not include the Pluggable Authentication Module, or PAM, which AD Bridge requires to allow domain users to execute sudo commands with super-user credentials. We recommend that you download sudo from the HP-UX Porting Center and make sure that you use the **with-pam** configuration option when you build it.

HP-UX 11iv1 requires the following patches:

- **PHCO_36229**
- **PHSS_35381**
- **PHKL_34805**
- **PHCO_31923**
- **PHCO_31903**
- **PHKL_29243**

The patches listed here represent the minimum patch level for proper operation. The patches might be superseded by later patches.

Kerberos client libraries: For single sign-on with HP-UX 11.11 and 11.23, install the latest KRB5-Client libraries from the HP Software Depot. By default, HP-UX 11.31 includes the libraries.

Other Requirements for the Agent

Locale

Configure the locale with UTF-8 encoding for every target computer.

Secure Shell

To properly process logon events with AD Bridge, the SSH server or client must support the **UsePam yes** option.

For single sign-on, both the SSH server and the SSH client must support GSSAPI authentication.

Other Software

Telnet, rsh, rcp, rlogin, and other programs that use PAM for processing authentication requests are compatible with AD Bridge.

Networking Requirements

Each Unix, Linux, or macOS computer must have fully routed network connectivity to all the domain controllers that service the computer's Active Directory site. Each computer must be able to resolve A, PTR, and SRV records for the Active Directory domain, including at least the following:

- **A domain.tld**
- **SRV _kerberos._tcp.domain.tld**
- **SRV _ldap._tcp.domain.tld**
- **SRV _kerberos._udp.sitename.Sites._msdcs.domain.tld**
- **A domaincontroller.domain.tld**

Disk Space Requirements

The AD Bridge agent requires 100MB of disk space in the **/opt** mount point.

The agent also creates configuration files in **/etc/pbis** and offline logon information in **/var/lib/pbis**.

The AD Bridge agent caches Group Policy Objects (GPOs) in **/var/lib/pbis**.

Memory and CPU Requirements

- RAM: The agent services and daemons can use between 9MB – 14MB:
  - Authentication service on a 300-user mail server is typically 7MB
  - Other services and daemons require between 500KB and 2MB each
- CPU: On a 2.0GHz single-core processor under heavy load with authentication requests is about 2 percent.

For a description of the AD Bridge Enterprise services and daemons, please see "Requirements for the Agent" on page 30.

Clock Skew Requirements

For the AD Bridge agent to communicate over Kerberos with the domain controller's Kerberos key distribution center, the clock of the client must be within the domain controller's maximum clock skew, which is 300 seconds, or 5 minutes, by default.

For more information, please see "Time Synchronization" on page 14

Additional Requirements for Specific Operating Systems

AIX

On AIX computers, PAM must be enabled. LAM is supported only on AIX 5.x. PAM must be used exclusively on AIX 6.x.

Install the Agent on Linux or Unix with the Shell Script

Install the agent using a shell script that contains a self-extracting executable.

To view information about the installer or to view a list of command-line options, run the installer package using **--help** command. For example (examples here are for RPM-based Linux platform):

```
./pbis-enterprise-x.x.x.xxxx.linux.i386.rpm.sh --help
```

Run the install as root or with a user that has sudo rights.

1. Download or copy the shell script to the computer desktop.

> **IMPORTANT!**
>
> *If you FTP the file, select binary (or BIN), for the transfer as the installer includes some binary code that becomes corrupted in AUTO or ASCII mode.*

2. As root, change the mode of the installer to executable:

   ```
   chmod a+x pbis-enterprise-x.x.x.xxxx.linux.i386.rpm.sh
   ```

3. As root, run the installer:

   ```
   ./pbis-enterprise-x.x.x.xxxx.linux.i386.rpm.sh
   ```

4. Follow the instructions in the installer.

Install the Agent on Linux in Unattended Mode

Install the agent in unattended mode using the **install** command. For example, on a 32-bit RPM-based Linux system, the installation command would look like the following:

```
./pbis-enterprise-x.x.x.xxxx.linux.i386.rpm.sh install
```

Install the Agent on Unix from the Command Line

Install the AD Bridge agent on Sun Solaris, HP-UX, and IBM AIX by using a shell script that contains a self-extracting executable, an SFX installer with a file name that ends in **sh**.

Example:

```
pbis-enterprise-x.x.x.xxxx.solaris.sparc.pkg.sh.
```

The examples shown here are for Solaris Sparc systems. For other Unix platforms, use the correct installer name.

***Note:** The name of a Unix installer for AD Bridge on installation media might be truncated to an eight-character file name with an extension. For example, **I3499sus.sh** is the truncated version of **pbis-enterprise-x.x.1.3499.solaris.sparc.pkg.sh**.*

To view a list of command-line options, run the following command:

```
./pbis-enterprise-x.x.x.xxxx.solaris.sparc.pkg.sh --help
```

1. Download or copy the installer to the computer desktop.
2. Change directories to the desktop.
3. As root, change the mode of the installer to executable:

   ```
   chmod a+x pbis-enterprise-x.x.x.xxxx.solaris.sparc.pkg.sh
   ```

4. As root, run the installer:

   ```
   ./pbis-enterprise-x.x.x.xxxx.solaris.sparc.pkg.sh
   ```

5. Follow the instructions in the installer.

Install the Agent in Solaris Zones

Solaris zones are a virtualization technology created to consolidate servers. Primarily used to isolate an application, Solaris zones act as isolated virtual servers running on a single operating system, making each application in a collection of applications seem as though it is running on its own server. A Solaris Container combines system resource controls with the virtual isolation provided by zones.

Every zone server contains a global zone that retains visibility and control in any installed non-global zones. By default, the non-global zones share certain directories, including **/usr**, which are mounted read-only. The shared directories are writable only for the global zone.

By default, installing AD Bridge in the global zone results in it being installed in all the non-global zones. You can, however, use the following commands to control the zones that you install to.

Install Options for Embedded Scripts

Use the following commands to pass the option to the embedded script.

Help	**./pbis-enterprise-x.x.x.xxxx.solaris.i386.pkg.sh -- --help**
Install to all zones (default)	**./pbis-enterprise-x.x.x.xxxx.solaris.i386.pkg.sh -- --all-zones**
Install to only current zone	**./pbis-enterprise-x.x.x.xxxx.solaris.i386.pkg.sh -- --current-zone**

Post Install

After a new child zone is installed, booted, and configured, you must run the following command as root to complete the installation:

```
/opt/pbis/bin/postinstall.sh
```

You cannot join zones to Active Directory as a group. Each zone, including the global zone, must be joined to the domain independently of the other zones.

Caveats

There are some caveats when using AD Bridge with Solaris zones:

When you join a non-global zone to AD, an error occurs when AD Bridge tries to synchronize the Solaris clock with AD.

The error occurs because the root user of the non-global zone does not have root access to the underlying global system and thus cannot set the system clock. If the clocks are within the 5-minute clock skew permitted by Kerberos, the error will not be an issue.

Otherwise, you can resolve the issue by manually setting the clock in the global zone to match AD or by joining the global zone to AD before joining the non-global zone.

Some group policy settings may log PAM errors in the non-global zones even though they function as expected. The cron group policy setting is one example:

```
Wed Nov 7 16:26:02 PST 2009 Running Cronjob 1 (sh)
Nov 7 16:26:01 zone01 last message repeated 1 time
Nov 7 16:27:00 zone01 cron[19781]: pam_lsass(cron): request failed
```

Depending on the group policy setting, these errors may result from file access permissions, attempts to write to read-only directories, or both.

By default, Solaris displays **auth.notice** syslog messages on the system console. Some versions of AD Bridge generate significant authentication traffic on this facility-priority level, which may lead to an undesirable amount of chatter on the console or clutter on the screen.

To redirect the traffic to a file instead of displaying it on the console, edit your **/etc/syslog.conf** file as follows:

Change this:

```
*.err;kern.notice;auth.notice /dev/sysmsg
```

To this:

```
*.err;kern.notice /dev/sysmsg
auth.notice /var/adm/authlog
```

IMPORTANT!

*Make sure that you use tabs, not spaces, to separate the **facility.priority** information (on the left) from the action field (on the right). Using spaces will cue syslog to ignore the entire line.*

Install Solaris 11

This section is intended for administrators installing AD Bridge Enterprise to Solaris targets.

What's New with the Solaris 11 Installer

There are two ways to install Solaris 11:

- Traditional shell script using the legacy SVR4 packaging mechanism.
- IPS repository install using Oracle's preferred IPS packaging mechanism

There is a p5p file that can be uploaded to your local IPS repository. This is located on the ISO in the following directory: **agents/solaris11-<ARCH>/p5p**

Upload the Packages with the P5P file

You can use the **-ips** option in the install script to upload the AD Bridge p5p archive file to the local repository.

Example:

```
pbis/install.sh --ips <repository>
```

If you only have the p5p file you can use the **pkgrecv** command.

Example

```
pkgrecv -s ./PBISEnterprise-X.X.X.XXXX-solaris11-<ARCH>.p5p -d <repository> PBISEnterprise.<ARCH>
```

Confirm the Package Added to Repository

Verify that the AD Bridge Enterprise package with publisher BeyondTrust has been added to the repository:

```
>pkgrepo list -s <repository>
```

Install the Agent in Solaris 11 Zones

After the files are uploaded to the local IPS repository and the global zone can access the IPS repository, then non-global zones can also access the repository.

In the zone, run the following IPS package command:

```
pkg install PBISEnterprise.<ARCH>
```

Upgrade An Operating System

Follow the steps to upgrade an operating system:

- Leave the domain
- Uninstall the agent

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

- Upgrade the operating system
- Install the correct agent for the new version of the operating system
- Join an Active Directory domain

Configure SELinux

Be sure to review the latest SELinux documentation. You can start with the SELinux wiki, located at http://www.selinuxproject.org/page/Main_Page.

Install SELinux on Unsupported Platforms

If you install SELinux on an unsupported platform, a message similar to the following is displayed:

```
SELinux found to be present, enabled, and enforcing. You may either provide a policy at
/opt/pbis/share/pbis.pp  --OR-- SELinux must be disabled or set to permissive mode by editing the
file /etc/selinux/config and rebooting. For instructions on how to edit the file to disable SELinux,
see the SELinux man page.
```

1. Create a compiled policy. To get started creating an SELinux policy for AD Bridge, use existing policy sources located under version directories: **/opt/pbis/share/rhel** or in **/opt/pbis/share/fedora**.
2. Rename the policy **pbis.pp** and place it in the **\opt\pbis\share** directory.
3. Run the installation again. The **pbis.pp** file is installed.

Configure SELinux After Installation

After installation of AD Bridge with SELinux, security denials might occur. Security denials caused by the current policy are reported in the **/var/log/audit/audit.log** log file.

You can resolve security denial issues automatically or manually.

Automatically Resolve Security Denials

To create a policy to resolve existing denials involving applications and resources with **pbis** in the name:

1. Type **grep pbis /var/log/audit/audit.log | audit2allow -M pbislocal**
2. The file **pbislocal.pp** is a compiled policy module and can be loaded with **semodule -i pbislocal.pp**.

Manually Resolve Security Denials

The procedure is similar to automatically resolving security denials. However, you can edit the policy file **pbislocal.te**:

1. Type **grep pbis /var/log/audit/audit.log | audit2allow -m pbislocal > pbislocal.te**
2. To build a compiled policy, execute the following command in the directory where **pbislocal.te** is located:

   ```
   make -f /usr/share/selinux/devel/Makefile
   ```

3. Load the module with **semodule -i pbislocal.pp**.

Join an Active Directory Domain

You can join computers to Active Directory using one of the following ways:

- Command line utility.
- A GUI-based domain join tool.

For more information, please see Join Active Directory Using the Domain Join GUI Tool.

For more information about the Domain Join tool CLI commands, please see the AD Bridge Linux Administration Guide at https://www.beyondtrust.com/docs/ad-bridge/documentation.htm.

Overview

When AD Bridge Enterprise joins a computer to an Active Directory domain, it uses the hostname of the computer to create the name of the computer object in Active Directory. From the hostname, the AD Bridge Enterprise domain join tool attempts to derive a fully qualified domain name. By default, the AD Bridge Enterprise domain join tool creates the Linux and Unix computer accounts in the default Computers container in Active Directory.

***Note:** After you join a domain for the first time, you must restart the computer before you can log on. If you cannot restart the computer, you must restart each service or daemon that looks up users or groups through the standard nsswitch interface, which includes most services that authenticate users, groups, or computers. You must, for instance, restart the services that use Kerberos, such as **sshd**.*

Pre-Create Accounts in Active Directory

You can create computer accounts in Active Directory before you join your computers to the domain. When you join a computer to a domain, AD Bridge Enterprise associates the computer with the pre-existing computer account when AD Bridge Enterprise can find it.

To locate the computer account, AD Bridge Enterprise first looks for a computer account with a DNS hostname that matches the hostname of the computer. If the DNS hostname is not set, AD Bridge Enterprise then looks for the name of a computer account that matches the computer's hostname, but only when the computer's hostname is 15 characters or less.

Therefore, when the hostname of your computer is more than 15 characters, set the DNS hostname for the computer account to ensure that the correct computer account is found. If no match is found, AD Bridge Enterprise creates a computer account.

Privileges and Permissions

To join a computer to a domain, use credentials for an Active Directory account that has privileges to join computers to the domain and the full name of the domain that you want to join.

For instructions on how to delegate rights to join a computer to a domain, please see Microsoft article 932455 at http://support.microsoft.com/kb/932455.

The level of privileges that you need is set by Microsoft Active Directory and is typically the same as performing the corresponding action on a Windows computer.

For more information about Active Directory privileges, permissions, and security groups, see the following references on the Microsoft TechNet website:

- Active Directory Privileges at http://technet.microsoft.com/en-us/library/cc740217(WS.10).aspx.
- Active Directory Object Permissions at http://technet.microsoft.com/en-us/library/cc728117(WS.10).aspx.
- Active Directory Users, Computers, and Groups at http://technet.microsoft.com/en-us/library/bb727067.aspx#EBAA.
- Securing Active Directory Administrative Groups and Accounts at http://technet.microsoft.com/en-us/library/cc700835.aspx.

Create Local Accounts

After you join a domain, AD Bridge Enterprise creates two local user accounts:

- **ComputerName\Administrator:** The account is disabled until you run **mod-user** with the root account. You are prompted to reset the password the first time you use the account.
- **ComputerName\Guest**

You can view information about these accounts by executing the following command: **/opt/pbis/bin/enum-users**

Example output:

```
User info (Level-2):
====================
Name:                        EXAMPLE-01\Administrator
UPN:                         Administrator@EXAMPLE-01
Generated UPN:               YES
Uid:                         1500
Gid:                         1544
Gecos:                       <null>Shell: /bin/sh
Home dir:                    /
LMHash length:               0
NTHash length:               0
Local User:                  YES
Account disabled:            TRUE
Account Expired:             FALSE
Account Locked:              FALSE
Password never expires:      FALSE
Password Expired:            TRUE
Prompt for password change:  YES
User can change password:    NO
Days till password expires: -149314


User info (Level-2):
====================
Name:                        EXAMPLE-01\Guest
UPN:                         Guest@EXAMPLE-01
Generated UPN:               YES
Uid:                         1501
Gid:                         1546
Gecos:                       <null>Shell: /bin/sh
```

```
Home dir:                   /tmp
LMHash length:              0
NTHash length:              0
Local User:                 YES
Account disabled:           TRUE
Account Expired:            FALSE
Account Locked:             TRUE
Password never expires:     FALSE
Password Expired:           FALSE
Prompt for password change: YES
User can change password:   NO
Days till password expires: -149314
```

Join Active Directory from the Command Line

On Linux, Unix, and macOS computers, the location of the domain join command-line utility is **/opt/pbis/bin/domainjoin-cli**.

When you join a domain by using the command-line utility, AD Bridge Enterprise uses the hostname of the computer to derive a fully qualified domain name (FQDN) and then automatically sets the FQDN in the **/etc/hosts** file.

You can also join a domain without changing the **/etc/hosts** file.

For more information, please see "Join Active Directory Without Changing /etc/hosts" on page 41.

Before You Join a Domain

To join a domain, ensure the following are in place:

- The computer's name server can find the domain. Run the command:

  ```
  nslookup domainName
  ```

- The computer can reach the domain controller. Run the command:

  ```
  ping domainName
  ```

Join a Computer to Active Directory

Run the following command as root.

Replace **domainName** with the FQDN of the domain that you want to join and **joinAccount** with the user name of an account that has privileges to join computers to the domain:

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

Example:

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

> ***Tip:*** *On Ubuntu, execute the* ***sudo su*** *command before you run the* ***domainjoin-cli*** *command.*

Join a Mac Computer

Using sudo, execute the following command in **Terminal**:

```
sudo /opt/pbis/bin/domainjoin-cli join domainName joinAccount.
```

Terminal prompts you for two passwords:

- a macOS user account with administrative privileges
- the Active Directory account that you are using in the join command

Join a Linux or Unix Computer to an Organizational Unit

Run the following command as root.

Replace **organizationalUnitName** with the path and name of the organizational unit 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 target OU:

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

Example:

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

Join a Linux or Unix Computer to a Nested Organizational Unit

Run the following command as root, replacing these values:

- **path** with the AD path to the OU from the top down, with each node separated by a forward slash (/).
- **organizationalUnitName** with the name of the organizational unit that you want to join.
- **domainName** with the FQDN of the domain.
- **joinAccount** with the user name of an AD account that has privileges to join computers to the target OU:

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

Here is an example of how to join a deeply nested OU:

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

Join Active Directory Without Changing /etc/hosts

When you use the AD Bridge Enterprise domain join tool, AD Bridge Enterprise uses the host name of the computer to derive a fully qualified domain name (FQDN) and automatically sets the computer’s FQDN in the **/etc/hosts** file.

To join a Linux computer to the domain without changing the **/etc/hosts** file, run the following command as root. Replace:

- **domainName:** the FQDN of the domain to join
- **joinAccount:** the user account with privileges to join computers to the domain

```
/opt/pbis/bin/domainjoin-cli join --disable hostname   domainName joinAccount
```

Example:

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

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

If the Computer Fails to Join the Domain

Make sure the computer's FQDN is correct in **/etc/hosts**. For the computer to process tickets in compliance with the Kerberos protocol and to function properly when it uses cached credentials in offline mode or when its DNS server is offline, there must be a correct FQDN in **/etc/hosts**.

For more information on GSS-API requirements, please see RFC 2743 at https://tools.ietf.org/html/rfc2743.

You can determine the FQDN of a computer running Linux, Unix, or macOS by executing the following command:

```
ping -c 1 `hostname`
```

When you execute this command, the computer looks up the primary host entry for its hostname. In most cases, this means that it looks for its hostname in **/etc/hosts**, returning the first FQDN name on the same line. For example, the correct entry for the hostname **qaserver**, in **/etc/hosts**:

```
10.100.10.10 qaserver.corpqa.example.com qaserver.
```

If the entry in **/etc/hosts** incorrectly lists the hostname (or anything else) before the FQDN, the computer's FQDN becomes, using the malformed example below, **qaserver**:

```
10.100.10.10 qaserver qaserver.corpqa.example.com
```

If the host entry cannot be found in **/etc/hosts**, the computer looks for the results in DNS instead. This means that the computer must have a correct A record in DNS. If the DNS information is wrong and you cannot correct it, add an entry to **/etc/hosts**.

Options

The **domainjoin-cli** command-line interface includes the following options:

Option	Description	Example
--help	Displays the command-line options and commands.	**domainjoin-cli --help**
--help-internal	Displays a list of the internal debugging and configuration commands.	**domainjoin-cli --help-internal**

Option	Description	Example
--logfile {.| **path**}	Generates a log file or prints the log to the console.	**domainjoin-cli --logfile /var/log/domainjoin.log join example.com Administrator** **domainjoin-cli --logfile . join example.com Administrator**
--loglevel {error|warning|info|verbose}	Adjusts the logging details generated during a domain join.	

Join Commands

The domain join command-line interface includes the following basic commands:

Command	Description	Example
query	Displays the hostname, current domain, and distinguished name, which includes the OU to which the computer belongs. If the computer is not joined to a domain, it displays only the hostname.	**domainjoin-cli query**
setname computerName	Renames the computer and modifies the **/etc/hosts** file with the name that you enter. **computerName** is a required field. If not provided, you are prompted for it.	**domainjoin-cli setname RHEL44ID**
join [--ou organizationalUnit] domainName userName	Joins the computer to the domain. You can use the **--ou** option to join the computer to a specific OU in the domain by setting the path to the OU. The path to the OU is top down and separated by a **/**. If not provided, you are prompted to enter the domain, user name and password. To be prompted for OU you need to pass in **--ou --** When you use this option, you must use an account that is a member in the Domain Administrators security group.	**domainjoin-cli join --ou Eng/Dev example.com Administrator**
join --notimesync	Joins the computer to the domain without synchronizing the computer's time with the domain controller's. When you use this option, the **sync-system-time** value for lsass is set to **no**.	**domainjoin-cli join --notimesync example.com Administrator**
join --trustEnumerationWaitSeconds 60	The length of time Lsass waits for trust enumeration to finish during startup. The range is 1–1000 seconds.	

Leave Commands

Command	Description	Example
leave [userName]	Removes the computer from the Active Directory domain. If the **userName** is provided, the computer account is disabled in Active Directory. If not provided, you are prompted to enter user name and password.	**domainjoin-cli leave domainjoin-cli leave smithy@example.com**
leave [--enable <module> --disable <module> ...]	Enables or disables the module when you run the leave command.	
leave [-- keepLicense]	Retains the license information after the computer leaves the domain. The license key is released by default when you run the leave command.	**domainjoin-cli leave -- keepLicense**
leave [-- deleteAccount <user name> [<password>]]	Deletes the computer account after the computer leaves the domain.	**domainjoin-cli leave -- deleteAccount Administrator AdminPassword**
leave [--advanced] --preview [user name] [password]	Displays information on the configuration.	**leave --advanced --preview Administrator AdminPassword**
leave --details <module>	Displays the configuration information for the module.	**leave --details pam**

Join Mode Commands

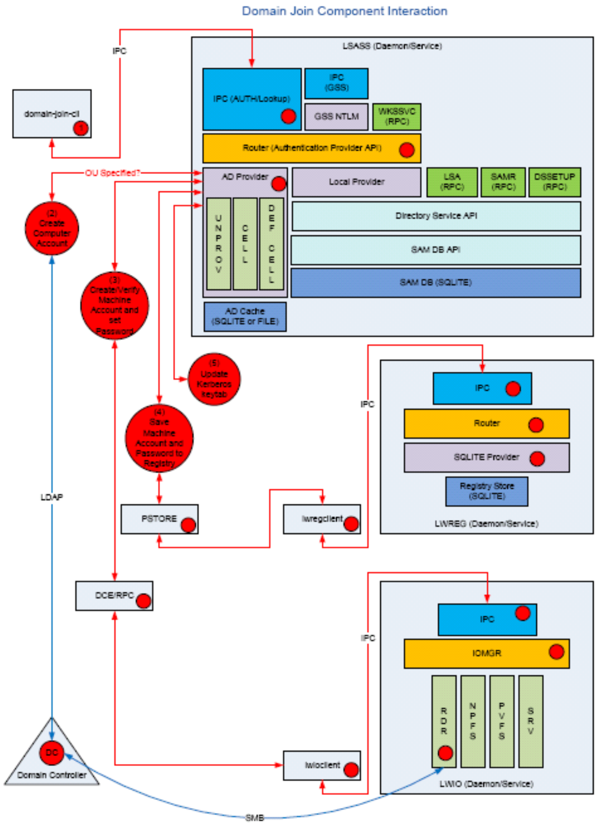
Command	Description
--assumeDefaultCell { auto | no | force }	In Assume Default Cell mode, information is not read from the cells, but from the user/group objects directly. This supports joining to a domain which does not have any named/default cells. If set to **auto**, enable this mode when no cells are found. If set to **force** enable this mode even if named or default cells exist. When this mode is enabled, **get-status** reports the AD authentication provider mode as *Default Cell (Assumed)*. The default setting is **no**. ***Note:*** *This mode is intended for Proof of Concepts (PoC) and small environments. It does not require cells or schema changes. User and group information is read directly from the domain controllers in the forest, no Global Catalog searches are used. Features that rely on items stored in the cell (for example, custom NIS maps) are not supported in this mode.*
--unprovisioned { auto | no | force }	When set the AD provider computes the user/group UIDs from their security identifier and uses local settings for the Unix shell and home directory, ignoring the values set in AD. If set to **auto**, enable this mode when no cells are found. If set to **force** enable this mode even if named or default cells exist. The default setting is **no**.

Advanced Commands

The following advanced commands can be used to troubleshoot issues when configuring a Linux or Unix computer.

- Preview the stages of joining or leaving a domain
- Check configurations required for your system
- View information about a module that will be changed
- Configure a module such as nsswitch

Review the Domain Join Dataflow diagram to see how systems interact when you join a domain.



Preview the Stages of the Domain Join for Your Computer

Command	Description
domainjoin-cli join --preview domainName	Preview the stages of the domain join for a computer, including: domain, DNS name, and configuration stages that will be run after you start the domainjoin process.

Example

```
domainjoin-cli join --preview example.com
```

Here is an example of the results, which can vary by computer:

```
[root@rhel4d bin]# domainjoin-cli join --preview example.com
Joining to AD Domain:   example.com
With Computer DNS Name: rhel4d.example.com

The following stages are currently configured to be run during the domain join:
join           - join computer to AD
krb5           - configure krb5.conf
nsswitch       - enable/disable AD Bridge nsswitch module
start          - start daemons
pam            - configure pam.d/pam.conf
ssh            - configure ssh and sshd
```

Check Required Configurations

To list the modules that apply to your operating system, including those modules that will not be run, execute either the following join or leave command.

Command

```
domainjoin-cli join --advanced --preview domainName
```

```
domainjoin-cli leave --advanced --preview domainName
```

Example

domainjoin-cli join --advanced --preview example.com

The result varies by computer:

```
[root@rhel4d bin]# domainjoin-cli join --advanced --preview example.com
Joining to AD Domain:   example.com
With Computer DNS Name: rhel4d.example.com
[X] [F] stop              - stop daemons
[F] hostname              - set computer hostname
[F] keytab                - initialize kerberos keytab
[X] [N] join              - join computer to AD
[X] [N] nsswitch          - enable/disable AD Bridge nsswitch module
[X] [N] cache             - manage caches for this host
[X] [N] start             - start daemons
[X] [N] krb5              - configure krb5.conf
[F] bash                  - fix bash prompt for backslashes in usernames
[X] [N] pam               - configure pam.d/pam.conf
[X] [S] ssh               - configure ssh and sshd
[F] DDNS                  - Configure Dynamic DNS Entry for this host

Key to flags
[F]ully configured        - the system is already configured for this step
[S]ufficiently configured - the system meets the minimum configuration requirements for this step
[N]ecessary               - this step must be run or manually performed.
[X]                       - this step is enabled and will make changes
[ ]                       - this step is disabled and will not make changes
```

Modules

The AD Bridge Enterprise domain join tool includes the following modules, the components and services that the tool must configure before it can join a computer to a domain:

Module	Description
join	Joins the computer to Active Directory
leave	Deletes the machine account in Active Directory
dsplugin	Enables the AD Bridge Enterprise directory services plugin on a Mac computer
stop	Stops services so that the system can be configured
start	Starts services after configuration
firewall	Opens ports to the domain controller
hostname	sets the computer hostname
krb5	Configures **krb5.conf**
pam-mode	Switches authentication from LAM to PAM
nsswitch	Enables or disables AD Bridge Enterprise nsswitch module
pam	Configures **pam.d** and **pam.conf**
lam-auth	Configures LAM for Active Directory authentication
ssh	Configures ssh and sshd
bash	Fixes the bash prompt for backslashes in usernames
gdm	Fixes gdm presession script for spaces in usernames

Join Commands for the Modules

Command	Description	Example
domainjoin-cli join - - advanced --preview domainName	View the modules that must be configured on your computer.	**domainjoin-cli join --advanced --preview example.com**
domainjoin-cli join - - details module domainName joinAccount	View more information about a module, including the modules that are configured.	**domainjoin-cli join --details nsswitch example.com Administrator**
domainjoin-cli join - - disable module domainName accountName	Turn off a module when you join a domain. Disabling a module can be useful in cases where a module has been manually configured or in cases where you must ensure that certain system files will not be modified.	**domainjoin-cli join --disable nsswitch example.com Administrator**
domainjoin-cli join - - enable module domainName accountName	Turn on a module when you join a domain.	**domainjoin-cli join --enable nsswitch example.com Administrator**

Leave Commands for the Modules

Command	Description	Example
domainjoin-cli leave --details module domainName joinAccount	View more information about a module, including the modules that are configured.	**domainjoin-cli leave -- details pam example.com Administrator**
domainjoin-cli leave --disable module domainName accountName	Turn off a module when you leave a domain.	**domainjoin-cli join --leave --disable pam example.com Administrator**

Example

```
domainjoin-cli join --details nsswitch example.com Administrator
```

The result varies depending on your system's configuration:

```
domainjoin-cli join --details nsswitch example.com Administrator
[X] [N] nsswitch          - enable/disable AD Bridge nsswitch module

Key to flags
[F]ully configured        - the system is already configured for this step
[S]ufficiently configured - the system meets the minimum configuration requirements for this step
[N]ecessary               - this step must be run or manually performed.
[X]                       - this step is enabled and will make changes
[ ]                       - this step is disabled and will not make changes

Details for 'enable/disable AD Bridge nsswitch module':
The following steps are required and can be performed automatically:
* Edit nsswitch apparmor profile to allow libraries in the /opt/pbis/lib and /opt/pbis/lib64
directories
* List lwidentity module in /usr/lib/security/methods.cfg (AIX only)
* Add lwidentity to passwd and group/groups line /etc/nsswitch.conf or
/etc/netsvc.conf

If any changes are performed, then the following services must be restarted:
* GDM
* XDM
* Cron
* Dbus
* Nscd
```

Turn Off a Domain-Join Module

You can turn off a module when you join or leave a domain.

Disabling a module can be useful in cases where a module has been manually configured or in cases where you must ensure that certain system files will not be modified.

> ***Note:*** *If you disable a necessary module and you have not manually configured it, the domain join utility will not join your computer to the domain.*

You can use either **join** or **leave**.

```
domainjoin-cli join --disable module domainName accountName
```

```
domainjoin-cli leave --disable module domainName accountName
```

Example

```
domainjoin-cli join --disable pam example.com Administrator
```

Turn on a Domain-Join Module

You can turn on a module when you join or leave a domain.

Command

```
domainjoin-cli join --enable module domainName accountName
```

Example

```
domainjoin-cli join --enable pam example.com Administrator
```

Configuration and Debugging Commands

The **domainjoin-cli** tool includes commands for debugging the domain-join process and for configuring or preconfiguring a module.

For example, run the **configure** command to preconfigure a system before you join a domain, a useful strategy when you are deploying AD Bridge Enterprise in a virtual environment and you need to preconfigure the nsswitch, ssh, or PAM module of the target computers to avoid restarting them after they are added to the domain.

> ***Note:*** *The* ***--testprefix*** *option supports testing system configuration file changes. If supplied, the* ***--testprefix*** *directory is prepended to the path of the configuration file target.*

For example, the following command changes the **/testconfig/etc/nsswitch.conf** file instead of **/etc/nsswitch.conf**:

```
configure --enable --testprefix testconfig nsswitch
```

Example with nsswitch

```
domainjoin-cli configure --enable nsswitch
```

Example with fixfqdn

```
domainjoin-cli fixfqdn
```

Help Syntax

```
domainjoin-cli --help-internal
```

```
fixfqdn
configure { --enable | --disable } [--testprefix <dir>] pam
configure { --enable | --disable } [--testprefix <dir>] nsswitch
configure { --enable | --disable } [--testprefix <dir>] ssh
configure { --enable | --disable } [--testprefix <dir>]
[--long <longdomain>] [--short <shortdomain>] krb5
configure { --enable | --disable } eventfwdd
configure { --enable | --disable } reapsysld
get_os_type
get_arch
get_distro
get_distro_version
```

Turn Off macOS Directory Service Authentication

If you are migrating from Open Directory or Active Directory and you had set authentication from the command line with **dsconfigad** or **dsconfigldap**, you must run the following commands to stop the computer from trying to use the built-in directory service even if the Mac is not bound to it:

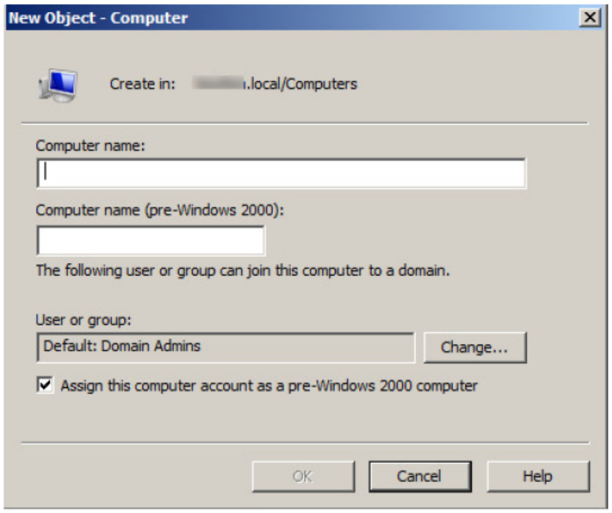
```
dscl . -delete /Computers
dscl /Search -delete / CSPSearchPath /LDAPv3/FQDNforYourDomainController
dscl /Search -delete / CSPSearchPath /Active\ Directory/All\ Domains
dscl /Search/Contacts -delete / CSPSearchPath /Active\ Directory/All\ Domains
dscl /Search/Contacts -delete / CSPSearchPath /LDAPv3/FQDNforYourDomainController
```

Automatically Join an Agent to a Domain

The following sections show you how to prepare a computer account and automate the domain join process.

Create a Computer Account in Active Directory

1. Using **Active Directory Users and Computers**, create a **Computer** account in your preferred OU.
2. The **Computer Name** must be configured to correctly match the AD Bridge agent hostname.
3. Check the **Assign this computer account as a pre-Windows 2000 computer** box to assign this computer a password which is based on the new computer name.



New Object - Computer

Create in: [redacted].local/Computers

Computer name:

Computer name (pre-Windows 2000):

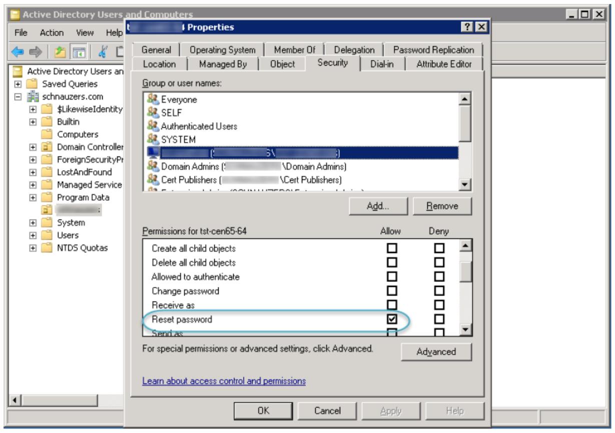
The following user or group can join this computer to a domain.

User or group:

Default: Domain Admins

☑ Assign this computer account as a pre-Windows 2000 computer

4. Select the permissions: **Write** access and **Reset Password** access.



Group or user names:

- Everyone
- SELF
- Authenticated Users
- SYSTEM
- [redacted]
- Domain Admins ([redacted]\Domain Admins)
- Cert Publishers ([redacted]\Cert Publishers)

Permissions for tst-cen65-64	Allow	Deny
Create all child objects	☐	☐
Delete all child objects	☐	☐
Allowed to authenticate	☐	☐
Change password	☐	☐
Receive as	☐	☐
Reset password	☑	☐
Send as	☐	☐

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

Run a Domain Join Script on the Agent

On the AD Bridge agent host, create a script that will run after a reboot (for example, a cron job) and will run the following command:

```
/opt/pbis/bin/domainjoin-cli join <YOUR_DOMAIN> `hostname -s`$ `hostname -s`
```

Files Modified When You Join a Domain

Some system files are changed when a computer is joined to a domain. The files that change depend on the platform, the distribution, and the system's configuration.

Run the following command to see a list of the changes:

```
domainjoin-cli join --advanced --preview domainName
```

***Note:** Not all the following files are present on all computers.*

The following files might be modified.

- **/etc/nsswitch.conf** (on AIX, the file is **/etc/netsvcs.conf**)
- **/etc/pam.conf** on AIX, HP-UX, and Solaris
- **/etc/pam.d/*** on Linux
- **/etc/ssh/{ssh_config,sshd_config}** (or wherever sshd configuration is located)
- **/etc/hosts**

To join a domain without modifying **/etc/hosts**, please see "Join Active Directory Without Changing /etc/hosts" on page 41.

- **/etc/{hostname,HOSTNAME,hostname.*}**
- **/etc/krb5.conf**
- **/etc/krb5/krb5.conf**

Log on with Domain Credentials

AD Bridge Enterprise includes the following logon options:

- Full domain credentials
  - Example: **example.com\\hoenstiv**
- Single domain user name
  - Example: **example\\hoenstiv**
- Alias. Example: **stiv**
- Cached credentials

IMPORTANT!

*When you log on from the command line, you must use a slash to escape the slash character, making the logon form **DOMAIN\\username**.*

When you log on a Linux, Unix, or macOS computer using your domain credentials, AD Bridge Enterprise uses the Kerberos protocol to connect to Active Directory's key distribution center, or KDC, to establish a key and to request a Kerberos ticket granting ticket (TGT). The TGT lets you log on to other computers joined to Active Directory or applications provisioned with a service principal name and be automatically authenticated with Kerberos and authorized for access through Active Directory.

After logon, AD Bridge Enterprise stores the password in memory and securely backs it up on disk. You can, however, configure AD Bridge Enterprise to store logon information in a SQLite database, but it is not the default method. The password is used to refresh the user's Kerberos TGT and to provide NTLM-based single sign-on through the AD Bridge Enterprise GSSAPI library. In addition, the NTLM verifier hash, a hash of the NTLM hash, is stored to disk to handle offline logons by comparing the password with the cached credentials.

AD Bridge Enterprise stores an NTLM hash and LM hash only for accounts in AD Bridge Enterprise's local provider. The hashes are used to authenticate users over CIFS. Since AD Bridge Enterprise does not support offline logons for domain users over CIFS, it does not store the LM hash for domain users.

UPN Names

To use UPN names, you must raise your Active Directory forest functional level to Windows Server 2003, but raising the forest functional level to Windows Server 2003 will exclude Windows 2000 domain controllers from the domain.

For more information, please see "Storage Modes" on page 17

Log on with AD Credentials

After the AD Bridge Enterprise agent is installed and the Linux or Unix computer is joined to a domain, you can log on with your Active Directory credentials.

- Log on from the command line. Use a slash character to escape the slash (**DOMAIN\\username**).

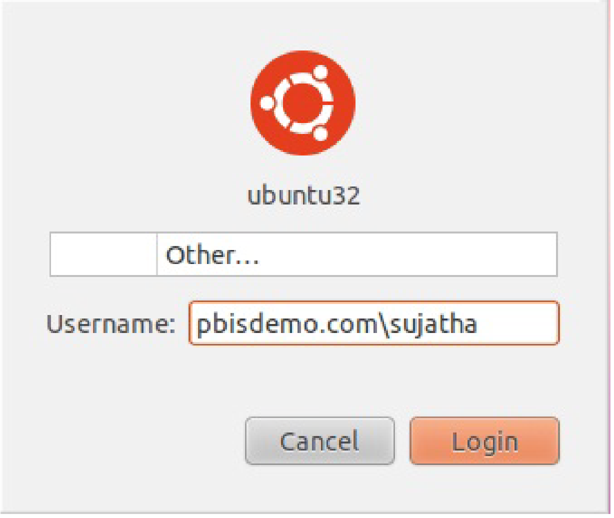
Example with SSH:

```
ssh example.com\\hoenstiv@localhost
```

Log into the system console or the text login prompt using an Active Directory user account in the form of **DOMAIN\username**, where **DOMAIN** is the Active Directory short name.

> ***Note:*** *After you join a domain for the first time, you must restart the computer before you can log on interactively through the console.*

The image depicts an example of logging into Ubuntu using AD credentials.



Username: pbisdemo.com\sujatha

Log on with SSH

You can log on with SSH by executing the **ssh** command at the shell prompt in the following format:

```
ssh DOMAIN\\username@localhost
```

Example:

```
ssh example.com\\hoenstiv@localhost
```

Leave a Domain and Uninstall the AD Bridge Enterprise Agent

You can remove a computer from a domain without necessarily disabling or deleting the computer's account in Active Directory. If needed, you can uninstall the AD Bridge Enterprise agent from a client computer.

Leave a Domain

When a computer is removed from a domain, AD Bridge retains the settings that were made to the computer's configuration when it was joined to the domain. Changes to the **nsswitch** module are also preserved until you uninstall AD Bridge, at which time they are reverted.

Before leaving a domain, run the following command to view the changes that will take place:

```
domainjoin-cli leave --advanced --preview domainName
```

Example:

```
[root@rhel4d example]# domainjoin-cli leave --advanced --preview example.com
Leaving AD Domain:    EXAMPLE.COM
[X] [S] ssh                  - configure ssh and sshd
[X] [N] pam                  - configure pam.d/pam.conf
[X] [N] nsswitch             - enable/disable  nsswitch module
[X] [N] stop                 - stop daemons
[X] [N] leave                - disable machine account
[X] [N] krb5                 - configure krb5.conf
[F] keytab                   - initialize kerberos keytab

Key to flags
[F]ully configured           - the system is already configured for this step
[S]ufficiently configured    - the system meets the minimum configuration requirements for this step
[N]ecessary                  - this step must be run or manually performed
[X]                          - this step is enabled and will make changes
[ ]                          - this step is disabled and will not make changes
```

Remove a Linux or Unix Computer from a Domain

To remove the computer, use a root account to run the following command:

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

Disable the Computer Account in Active Directory

By default, a computer account in Active Directory is not disabled or deleted when the computer is removed from the domain.

To disable but not delete the computer account, include the user name as part of the **leave** command. You will be prompted for the user account password:

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

Remove the Computer Account in Active Directory

To delete the computer account, use the option **--deleteAccount** and include the user name as part of the leave command.

> ***Note:*** *You will be prompted for the password of the user account:*

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

Remove a Mac from a Domain

> ***Note:*** *For Mac OS 10.8 and later, the GUI is no longer supported. For AD Bridge v7.0 and later, GUI on any Mac is not supported. Use the CLI commands.*

To leave a domain on a Mac OS X computer, administrative privileges are required on the Mac.

1. In **Finder**, click **Applications**.
2. In the list of applications, double-click **Utilities**, and then double-click **Directory Access**.
3. On the **Services** tab, click the lock icon and enter an administrator name and password to unlock it.
4. In the list, click **Likewise**, and then click **Configure**.
5. Enter a name and password of a local machine account with administrative privileges.
6. On the menu bar at the top of the screen, click the **Domain Join Tool** menu, and then click **Join or Leave Domain**.
7. Click **Leave**.

Uninstall the Agent on a Linux or Unix Computer

You can uninstall AD Bridge Enterprise by using a shell script or by using a command.

Use a Shell Script to Uninstall

> **IMPORTANT!**
>
> *Before uninstalling the agent, you must leave the domain. Then execute the **uninstall** command from a directory other than **pbis** so that the uninstall program can delete the **pbis** directory and all its subdirectories. For example, execute the command from the root directory.*

> For more information, please see "Leave a Domain and Uninstall the AD Bridge Enterprise Agent" on page 54.

If you installed the agent on a Linux or Unix computer by using the shell script, you can uninstall the AD Bridge Enterprise agent from the command line by using the same shell script with the **uninstall** option.

***Note:** To uninstall the agent, you must use the shell script with the same version and build number that you used to install it.. For example, on a Linux computer running **glibc**, change directories to the location of AD Bridge Enterprise and then run the following command as root, replacing the name of the script with the version you installed:*

```
./pbis-open-x.x.x.xxxx.linux.oldlibc.i386.rpm.sh uninstall
```

For information about the script's options and commands, execute the following command:

```
./pbis-open-x.x.x.xxxx.linux.i386.rpm.sh help
```

Use a Command to Uninstall

To uninstall AD Bridge Enterprise by using a command, run the following command:

```
/opt/pbis/bin/uninstall.sh uninstall
```

To completely remove all files related to AD Bridge Enterprise from your computer, run the command as follows instead. If using this command and option, you do not need to leave the domain before uninstalling.

```
/opt/pbis/bin/uninstall.sh purge
```

Uninstall the Agent on a Mac

On a macOS computer, you must uninstall the AD Bridge Enterprise agent by using **Terminal**.

***Note:** Choose the appropriate action depending on whether you plan to re-install the product.*

- *If you are not planning to re-install the product, leave the domain before uninstalling the agent.*
- *If you are planning to re-install the product, remain in the domain while uninstalling the agent*

For more information, please see "Leave a Domain and Uninstall the AD Bridge Enterprise Agent" on page 54.

1. Log on to the Mac using a local account with privileges that allow you to use **sudo**.
2. Open a **Terminal** window: In **Finder**, on the **Go** menu, click **Utilities**, and then double-click **Terminal**.
3. At the **Terminal** shell prompt, execute the following command:

```
sudo /opt/pbis/bin/macuninstall.sh
```

Contact BeyondTrust Technical Support

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

> 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:

- 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

> 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.

> 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:

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

Download location:

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