BeyondTrust

# AD Bridge 22.3
# Installation Guide



TC:5/10/2023

# Table of Contents

# AD Bridge Enterprise Installation Guide

AD Bridge Enterprise connects Linux and Unix 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. 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 and Linux.*

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:

- Applies policy settings to Unix computers from the Group Policy Management Console (GPMC), including policy settings to define desktop and application preferences for Linux computers.
- Generates a range of reports to help improve regulatory compliance. The result: lower operating costs, better security, enhanced compliance.
- 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.

# Software Components in AD Bridge

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 or Unix computer to connect it to Active Directory.

| Component | Function |
|---|---|
| Agent | • Runs on a Linux or Unix computer to connect it to Active Directory with the AD Bridge Enterprise command-line interface or GUI.<br>• Communicates with an Active Directory domain controller to authenticate and authorize users and groups with the AD Bridge Enterprise Identity Service.<br>• Pulls and refreshes policy settings by using the Group Policy service, which is included only with the AD Bridge Enterprise agent. |
| Enterprise Console | • Runs on a Windows administrative workstation that connects to an Active Directory domain controller to help manage Linux and Unix computers in Active Directory.<br>• Migrates users, checks status, and generates reports. |
| MMC Snap-Ins for ADUC and GPMC | • Extends Active Directory Users and Computers to include Unix and Linux users.<br>• With AD Bridge Enterprise, it also extends the Group Policy Management Console (GPMC) to include Linux or Unix 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. |

*For more information, please see the following:*


- *"The AD Bridge Enterprise Agent" on page 7*
- *"Join Active Directory from the Command Line" on page 43*
- *"Log On with Domain Credentials" on page 51*
- *"Install the Management Console" on page 22*

# The AD Bridge Enterprise Agent

The AD Bridge Enterprise agent is installed on a Linux or Unix 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:*


- *"Daemon Services and Architecture in AD Bridge" on page 7*
- *"Caches and Databases in AD Bridge" on page 13*
- *"Cached Credentials" on page 14*
- *"Synchronize Time Between AD Bridge and the Domain Controller" on page 14*
- *"Use a Network Time Protocol Server" on page 14*
- *"Auto-Detection of Offline Domain Controller and Global Catalog" on page 15*
- *"AD Bridge Agent Active Directory Trust Support" on page 15*
- *"Supported Platforms for AD Bridge" on page 16*


## Daemon Services and Architecture in AD Bridge

The AD Bridge Enterprise agent is composed of the service manager daemon (**/opt/pbis/sbin/lwsmd**). At startup, the operating system (OS) is configured to start the service manager daemon. It is then instructed (by the OS) to start all desired services with the command **/opt/pbis/bin/lwsm autostart**. The service manager daemon keeps track of the services already started and ensures the services are started and stopped in the appropriate order.

The following options are available on the service manager daemon:

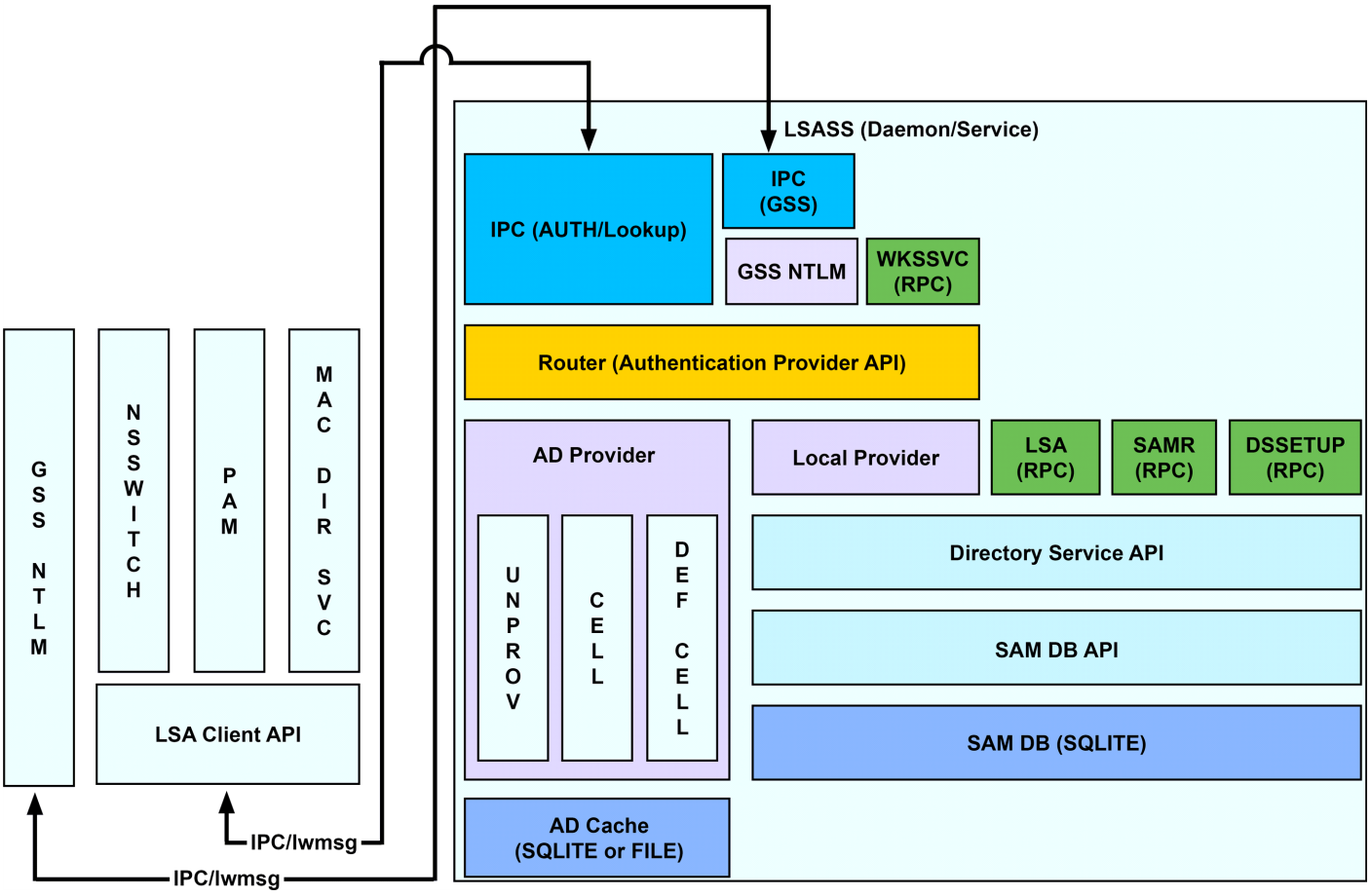
```
/opt/pbis/sbin/lwsmd -help
Usage: /opt/pbis/sbin/lwsmd [options ...]
OPTIONS:

--start-as-daemon              Start as a background process
--syslog                       Log to syslog (default when starting as daemon)
--logfile                      Log to file
--loglevel <level>             Set log level to <level>
                               (error, warning, info, verbose, debug, trace)
--container <group>            Start as a container for service group <group>
--ignoresmf                    Do not start ADBridge daemons using Solaris SMF
--help                         Show usage information
```

The service manager daemon (**/opt/pbis/sbin/lwsmd**) includes the following services:

| Service | Description | Dependencies |
|---|---|---|
| **lsass** | Handles authentication, authorization, caching, and idmap lookups. You can check its status or restart it.<br><br>***Note:*** *To view the lsass architecture, see the diagram following the tables.* | **netlogon**<br>**lwio**<br>**rdr**<br>**lwreg**<br>Usually **eventlog**. This can be disabled after installation.<br>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** |
| **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**<br>**lwreg** |
| **dcerpc** | Handles communication between Linux or Unix computers and Microsoft Active Directory by mapping data to endpoints. Disabled by default. | |
| **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**<br>**eventlog** |
| **gpagent** | Pulls Group Policy Objects (GPOs) from Active Directory and applies them to the computer. | **lsass**<br>**netlogon**<br>**lwio**<br>**rdr**<br>**lwreg**<br>**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

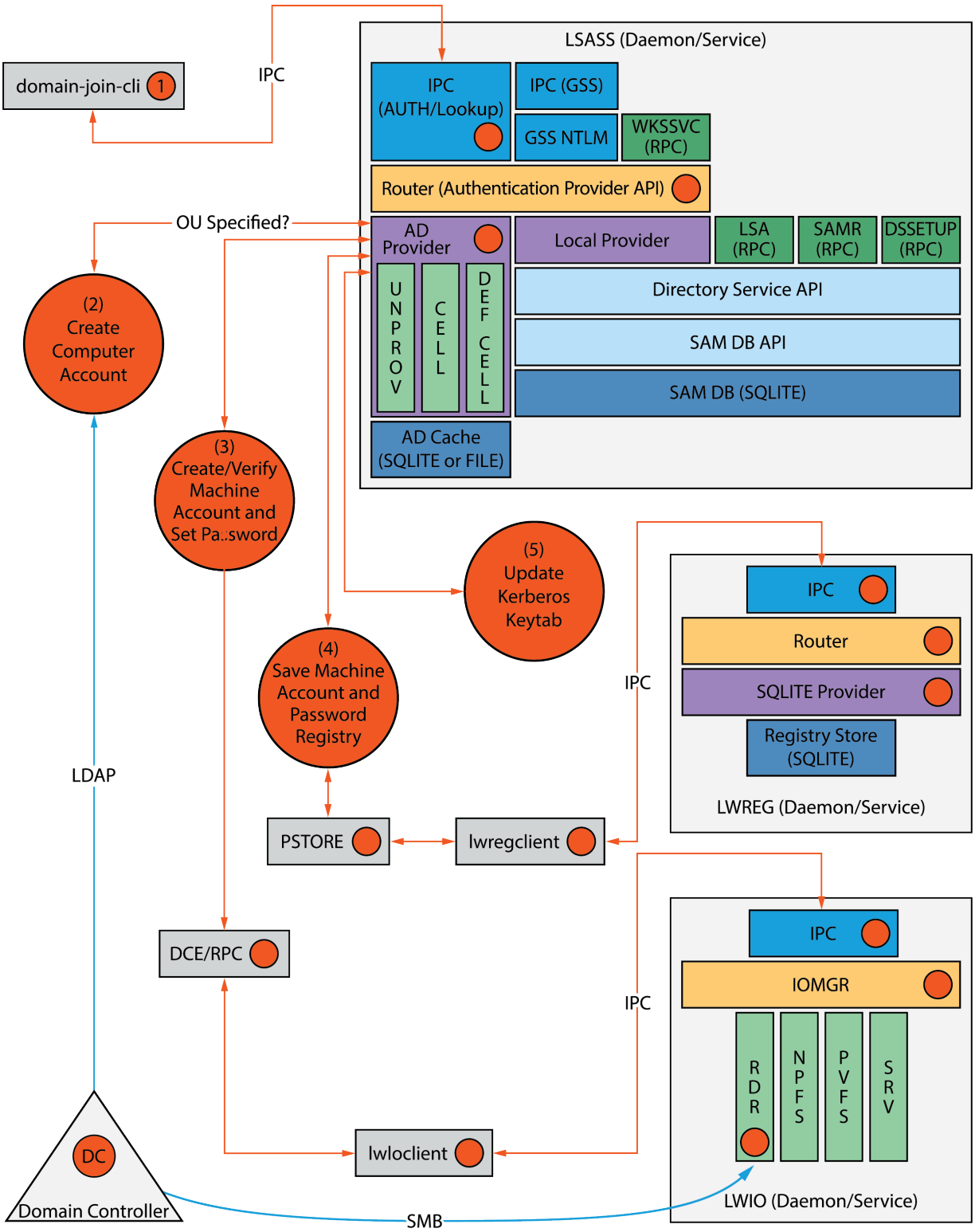
The **lwio** service multiplexes input and output by using SMB1 or SMB2. The service's plugin-based architecture includes several drivers, the most significant of which is coded as **rdr**, the redirector.

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 a trust 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 smart card 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 Enterprise Services at https://www.beyondtrust.com/docs/ad-bridge/getting-started/linux-admin/manage-services.htm in the AD Bridge Enterprise Linux Administration Guide.*

# Caches and Databases in AD Bridge

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 an SQLite database.

> *For more information, please see the AD Bridge Enterprise Administration Guide at www.beyondtrust.com/docs/ad-bridge/getting-started.*

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 are not cause for 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)

For optimal efficiency, disable **nscd**.

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**.

### Cached Credentials

AD Bridge caches credentials so that users can log on when their Linux or Unix computer is disconnected from the network or if their Active Directory services are unavailable.

## Synchronize Time Between AD Bridge and the Domain Controller

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.

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 does 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 or Unix 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.

> *For more information, please see the MIT article Clock Skew at http://web.mit.edu/kerberos/krb5-1.17/doc/admin/appl_servers.html?highlight=clock%20skew#clock-skew.*

### 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.

# Auto-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.

# AD Bridge Agent Active Directory Trust Support

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

| Trust Type | Transitivity | Direction | Default Cell | Named Cells |
|---|---|---|---|---|
| Parent and child | Transitive | Two-way | Yes | Yes |
| External | Nontransitive | One-way | No | Yes |
| External | Nontransitive | Two-way | Yes | Yes |
| Forest | Transitive | One-way | No | Yes |
| Forest | Transitive | Two-way | Yes | Yes |

***Note:*** *In all default cell scenarios, you must enable the default cell in both forests.*

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

## Notes on Trusts

The following is general information about working with trusts.

- To access a trust, users or groups must be added to a cell.
- In a two-way trust, AD Bridge Enterprise searches across all trusted global catalogs. Each domain must opt in by creating the default cell object within that domain.
- If there is a UID conflict across two domains, only the user provisioned to the cell authenticates. If both are provisioned, a true conflict occurs and the users are not allowed access until it is resolved.
- 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 named cell, 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 joining a domain with an administrative account from a different domain, you must provide the account's UPN:

***Example:***

```
domainjoin-cli join domainA.com administrator@domainB.com
```

### 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 in to 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 user or group attributes in the forest's global catalog. 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 Linux or Unix 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** and **Group** objects 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 is stored locally in a named cell, that is, a cell associated with an organizational unit.

> *For information about cells, please see "Plan Your AD Bridge Deployment" on page 21.*

## Supported Platforms for AD Bridge

AD Bridge Enterprise runs on a broad range of Linux or Unix platforms. BeyondTrust frequently adds new vendors and distributions.

> *For the list of supported platforms, see AD Bridge Supported Platforms, at https://www.beyondtrust.com/docs/ad-bridge/getting-started/supported-platforms/index.htm.*

## SELinux Support

The AD Bridge Enterprise SELinux implementation supports many operating systems.

> ***Note:*** *When you install on RedHat Enterprise Linux, AD Bridge runs under the* ***unconfined_t*** *domain.*

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**) is 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 in AD Bridge" on page 39**.*

# Storage Modes in Active Directory

AD Bridge Enterprise has three operating modes:

- Directory Integrated mode
- ID Range mode
- Unprovisioned 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 to 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 information by using the **keywords** attribute.

For example, when you create a cell in Directory Integrated mode, AD Bridge creates a container object, **CN=$LikewiseIdentityCell**, in the domain root, or in the OU where you created the cell. If the container is created in an OU, which is called a *named cell*, the Unix-specific data is stored in **CN=Users** and **CN=Groups** in the **$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.

## ID Range Mode

ID Range mode improves conflict avoidance by expanding the number of available UIDs and GIDs in AD Bridge from 524,288 to 2,147,483,647. There are three places in which ID ranges may be configured:

- Active Directory Users and Computers
- Group Policy Management Editor

- The **config** tool

ID ranges are assigned by the following order of precedence:

1. Forest root
2. Group policy
3. Config tools

ObjectSids are hashed by the agent to create user IDs and group IDs. ID Range introduces a mechanism to support the configuration of ID ranges for domains. Each domain is assigned a starting base ID and a maximum ID, where an ID refers to both user ID and group ID to be used by the AD Bridge agent.

The entire range can be defined for a single domain within a forest or split between domains. ID range overlaps are not allowed. There are no default settings for ID Ranges.

The ID is calculated by adding the object's RID to the ID Base. Careful planning is required when defining the range of each domain to make sure the range of RIDs matches the ID Range. If the calculated ID falls outside the ID range, the agent considers the object as not defined in the domain.

> ***Note:*** *ID range is mutually exclusive from having cells defined. ID Range and either default cells or named cells may not be defined at the same time.*

> ***Note:*** *ID Range is designed for very large environments in specific use cases. If Directory Integrated mode does not meet your requirements, please contact BeyondTrust Technical Support to discuss whether ID Range is feasible for your environment.*

## Unprovisioned Mode

The simplest AD Bridge deployment alternative is Unprovisioned mode. In this mode, no additional user data is stored in Active Directory. Because Unprovisioned mode requires no UNIX data to be stored in AD, it does not require any Windows tools to administer this data.

ID mapping in Unprovisioned mode is performed by mathematically hashing Active Directory SIDs into UNIX identifiers. When hashing SIDs into UIDs and GIDs, AD Bridge can supply uniqueness up to 524,288 AD objects, after which hash collision can start to occur.

The advantage of unprovisioned mode is that all devices (computers and appliances) using AD Bridge hashes AD users and groups into the same UID and GID numbers without requiring any repository of mapping information.

The disadvantage of this mode is that administrators have no control over the ID mapping process; they cannot designate that specific users and groups be mapped to particular UNIX identifiers. An additional disadvantage is that all AD users and groups become *visible* to devices using AD Bridge (there is no way to indicate that an AD user or group not be mapped and available in UNIX).

> ***Note:*** *Visibility does not necessarily imply authorization or access as AD Bridge can prevent an AD user from logging onto a machine via its* ***RequireMembershipOf*** *configuration setting.*

# Schemaless Mode

**IMPORTANT!**

*Schemaless mode is **deprecated**. The content below is for information only.*

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 AD Bridge 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 ID Range. When you configure your domain with the AD Bridge Enterprise domain configuration wizard, you must choose the mode to use.

**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 or Unix users to Active Directory. 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.
- 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. ID Range cannot be used with cells.

*For more information on Directory Integration and ID Range, please see "Storage Modes in Active Directory" on page 18.*

# Install the Management Console

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

## Requirements to Use AD Bridge with Active Directory

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 Red Hat, SUSE Linux, CentOS, Debian, Sun Solaris, IBM AIX, and Ubuntu

> *For agent requirements (the software that runs on the Linux or Unix computers that you want to connect to AD), please see "Install the AD Bridge Enterprise Agent" on page 31.*

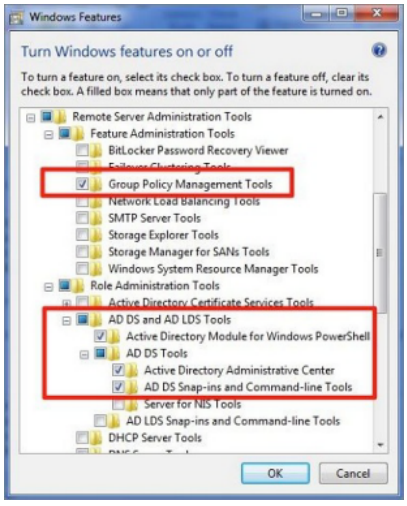
### Microsoft Management Tools

AD Bridge Enterprise works with ADUC, 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**




> *For more information, please see Remote Server Administration Tools for Windows, at https://docs.microsoft.com/en-US/troubleshoot/windows-server/system-management-components/remote-server-administration-tools.*

## Administrator Privileges

To add Linux or Unix computers to an AD domain, the following admin privileges are required:

- Root access or sudo permission on the Linux or Unix 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

> *For the list of supported platforms, see AD Bridge Supported Platforms, at https://www.beyondtrust.com/docs/ad-bridge/getting-started/supported-platforms/index.htm.*

## Windows Requirements for the Console

These are the minimum requirements for the console:

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

> *For the list of supported platforms, see AD Bridge Supported Platforms, at https://www.beyondtrust.com/docs/ad-bridge/getting-started/supported-platforms/index.htm.*

## Requirements to Run AD Bridge Enterprise in Directory Integrated Mode

To run AD Bridge Enterprise in Directory Integrated Mode, you must meet the following requirements:

- Active Directory installations that comply with RFC 2307
- Domain and forest functional levels have been raised to Windows Server 2012 or later

> *For more information, please see "Storage Modes in Active Directory" on page 18.*

## Networking

The subnets with your Linux or Unix 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.

- **DCDiag**: Part of Microsoft's support tools for Windows Server 2012, **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.

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

## Supported Platforms and Applications

### Platforms

AD Bridge Enterprise supports many Linux or Unix and virtualization platforms.

> *For the list of supported platforms, see AD Bridge Supported Platforms, at https://www.beyondtrust.com/docs/ad-bridge/getting-started/supported-platforms/index.htm.*

### Applications

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

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 **ADBridge64-*.exe** install file to your Windows workstation. The installer file includes the version and build number.
2. Run **ADBridge64-*.exe**.
3. On the **Installation Wizard** page, check the box to accept the license agreement and click **Next**.
4. Unless you need to place the files elsewhere, accept the default **Install Location Destination Folder** and click **Next**.
5. Select the features to install and click **Next**.

6. To begin the installation, on the **Install Steps** window, click **Next**.
7. Once the installation is complete, click **Finish**.

   At the end of the installation, you can start the configuration wizard to configure Directory Integrated mode, and follow best practices for configurations. You can also choose to run this wizard later from the default install location **C:\Program Files\BeyondTrust\PBIS\Enterprise**.

*For more information, please see the following:*

- *"Requirements to Use AD Bridge with Active Directory" on page 22.*
- *On Microsoft management tools, "Requirements to Use AD Bridge with Active Directory" on page 22.*
- *For the Configuration wizard, see "Use the Configuration Wizard" on page 26.*
- *For best practices, see AD Bridge Best Practices, at https://www.beyondtrust.com/docs/ad-bridge/how-to/best-practices/index.htm.*

# Use msiexec.exe

## Silent Install or Uninstall

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

***Example:***

```
msiexec.exe /i ADBridge64-##.#.#.###.msi /quiet /qn
```

```
msiexec.exe /x ADBridge64-##.#.#.###.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 ADBridge64-##.#.#.###.msi ADDLOCAL=BaseInstall /qn
```

## Upgrade the Console

AD Bridge supports in-place upgrades. Run the latest installer on the computer where AD Bridge is already installed.

## Use the Configuration Wizard

At the end of the installation, you can start the Configuration wizard to configure Directory Integrated mode, and follow best practices for configurations. The Configuration wizard is designed to simplify AD Bridge deployments. The essential components for a successful deployment can all be set up using the wizard.

You can also choose to run this wizard later from the default install location (see "Access the Configuration Wizard" on page 26).

Use the Configuration wizard to:

- **Set up Directory Integrated Mode and Promote Attributes to Global Catalog**
  - Schema Admin rights are required to promote attributes to the global catalog. This does not extend the schema and is reversible.
- **Create Default Cell**
  - Create a default cell at the root of the domain. Named cells are still supported but cannot be created in the Configuration wizard.
- **Provision Group to Default Cell**
  - Provision an Active Directory group to the Default cell. If you do not select an AD group, the Domain Users group is provisioned by default.
- **Create a License Container and Import a License**
  - Create a license container at the root of the domain.
  - Import a license file to the license container.
- **Create Default Group Policy object with Specific Group Polices**
  - The following Group Policies can be created using the Default Group Policy:
    - Enable audit and forward events to
    - Prepend default domain name to AD users and groups
    - Disable user logon GPO processing

At the end of the wizard, you can launch Cell Manager, BMC, ADUC, and Group Policy Management.

### Access the Configuration Wizard

If you haven't used the wizard from the last window of the Windows installer, you can run it from the command line:

```
C:\Program Files\BeyondTrust\PBIS\Enterprise\ConfigurationWizard.exe
```

# Change to Directory Integrated Mode

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

1. Go to the install directory **C:\Program Files\BeyondTrust\PBIS\Enterprise**.
2. Run **ConfigurationWizard.exe**.
3. On the **Promote Attributes** page, click **Promote Attributes**.
4. After the attributes are promoted, click **Finish**.

The necessary attributes are updated.

## Changes Applied 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 2012 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**).

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 or Unix 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, 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 200MB, which is expected to 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, group names are truncated when enumerated through the **groups** command.

To increase the max user name length on AIX, 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
```

# 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 or Unix 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 "Install Requirements for the AD Bridge Agent" on page 31.*

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
```

### Downgrade AD Bridge Agent to Earlier Version

Before downgrading to an earlier AD Bridge version, a domain leave and uninstall purge are required to ensure configuration settings not supported by previous releases are removed. Otherwise, the previous release may not work properly.

*For more information, please see "Leave a Domain and Uninstall the AD Bridge Enterprise Agent" on page 53.*

## Install Requirements for the AD Bridge 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.

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.

> *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.*

## Uninstall SSSD and Centrify

AD Bridge is not compatible with System Security Services Daemon (SSSD) or Centrify. Uninstall SSSD and Centrify from any Linux computers where you want to deploy the AD Bridge agent.

## 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 https://www.oracle.com/solaris/technologies/network-patching-center.html to ensure the latest patches are deployed to Solaris targets.*

## 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 Linux or Unix 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 "Install Requirements for the AD Bridge Agent" on page 31.*

### 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 "Synchronize Time Between AD Bridge and the Domain Controller" 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):

```
./adbridge-##.#.#.###.linux.x86_64.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 adbridge-##.#.#.###.linux.x86_64.rpm.sh
```

3. As root, run the installer:

```
./adbridge-##.#.#.###.linux.x86_64.rpm.sh
```

4. Follow the instructions in the installer.

## Install the Agent on Linux in Silent Install Mode

Install the agent in silent install mode using the **install** command. For example, on a 64-bit RPM-based Linux system, the installation command would look like the following:

```
./adbridge-##.#.#.###.linux.x86_64.rpm.sh install
```

## Install the Agent on Unix from the Command Line

Install the AD Bridge agent on Sun Solaris 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:***

```
adbridge-##.#.#.###.solaris.sparc.pkg.sh
```

The examples shown here are for Solaris Sparc systems. For other Unix platforms, use the appropriate 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* ***adbridge-##.#.#.###.solaris.sparc_64.pkg.sh****.*

To view a list of command-line options, run the following command on 32-bit OS:

```
./adbridge-##.#.#.###.solaris.sparc_32.pkg.sh --help
```

On a 64-bit OS

```
./adbridge-##.#.#.###.solaris.sparc_64.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 adbridge-##.#.#.###.solaris.sparc_32.pkg.sh
   ```

   On a 64-bit OS:

   ```
   chmod a+x adbridge-##.#.#.###.solaris.sparc_64.pkg.sh
   ```

4. As root, run the installer:

   ```
   ./adbridge-##.#.#.###.solaris.sparc_32.pkg.sh
   ```

   On a 64-bit OS:

   ```
   ./adbridge-##.#.#.###.solaris.sparc_64.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 | **./adbridge-##.#.#.###.solaris.x86_64.pkg.sh -- --help** |
| Install to all zones (default) | **./adbridge-##.#.#.###.solaris.x86_64.pkg.sh -- --all-zones** |
| Install to only current zone | **./adbridge-##.#.#.###.solaris.x86_64.pkg.sh -- --current-zone** |

## Post Install

To complete the installation after a new child zone is installed, booted, and configured, run the following command in the zone as root:

```
/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 AD Bridge on Solaris 11

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

## What's New with the AD Bridge 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.

## Upload the Packages with the P5P file

If using the **pkgrecv** command.

***Example:***

```
pkgrecv -s ./adbridge-##.#.#.###-solaris11-<ARCH>.p5p -d <repository> adbridge.<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 ADBridge\*
```

# Upgrade an Operating System Using AD Bridge

Follow the steps to upgrade an operating system:

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

> *For more information about uninstalling agents, please see the AD Bridge Enterprise Administration Guide at www.beyondtrust.com/docs/ad-bridge/getting-started.*

# Configure SELinux in AD Bridge

> ***Note:*** *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**.
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 the command line utility (CLI):

> *For more information about the Domain Join tool CLI commands, please see the AD Bridge Linux Administration Guide at www.beyondtrust.com/docs/ad-bridge/getting-started/linux-admin.*

## 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 for Active Directory Accounts

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.

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, please see the following:*
>
> - *Error: Access is denied when non-administrator users who have been delegated control try to join computers to a domain controller at https://docs.microsoft.com/en-US/troubleshoot/windows-server/identity/access-denied-when-joining-computers*
> - *Active Directory Privileges at https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc740217(v=ws.10)*

- *Active Directory Object Permissions* at *https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc728117(v=ws.10)*
- *Active Directory Users, Computers, and Groups* at *https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/bb727067(v=technet.10)*
- *Securing Active Directory Administrative Groups and Accounts* at *https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc700835(v=technet.10)*

## Create Local Accounts in AD Bridge

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:***

```
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 or Unix 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 44.*

### 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 agent machines, execute the* ***sudo su*** *command before you run the* ***domainjoin-cli*** *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
```

***Example:*** *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 --nohosts domainName joinAccount
```

***Example:***

```
/opt/pbis/bin/domainjoin-cli join --nohosts 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 or Unix 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
```

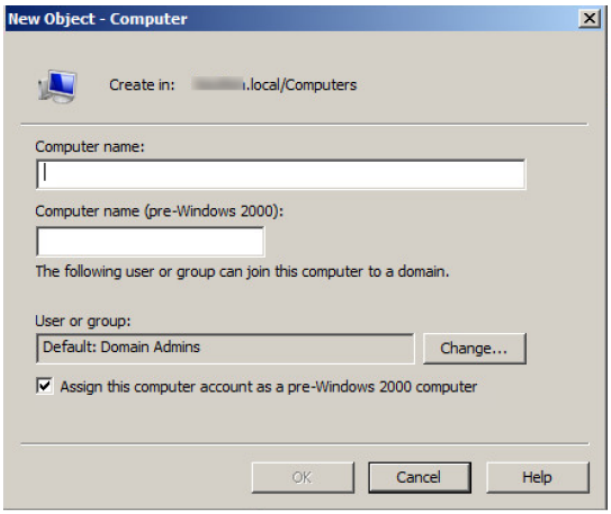
If the host entry cannot be found in **/etc/hosts**, the computer looks for the results in DNS instead. This means that the computer must have a correct A record in DNS. If the DNS information is wrong and you cannot correct it, add an entry to **/etc/hosts**.

## Automatically Join an Agent to a Domain

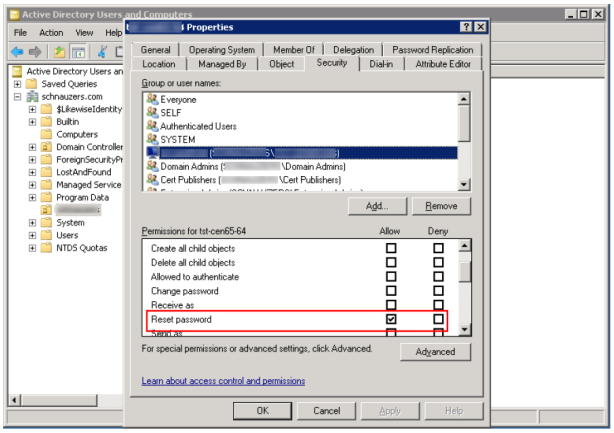
The following sections show you how to prepare a computer account and automate the domain join process.

## 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 that is based on the new computer name.




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




## 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 and Solaris
- **/etc/pam.d/*** on Linux
- **/etc/ssh/{ssh_config,sshd_config}** (or wherever sshd configuration is located)
- **/etc/hosts**
- **/etc/{hostname,HOSTNAME,hostname.*}**
- **/etc/krb5.conf**
- **/etc/krb5/krb5.conf**

*For information on how to join a domain without modifying **/etc/hosts**, please see "Join Active Directory without Changing /etc/hosts" on page 44.*

# Join an Azure AD Tenant

You can set up to authenticate to Active Directory or Azure AD or both, in a hybrid format.

## Requirements

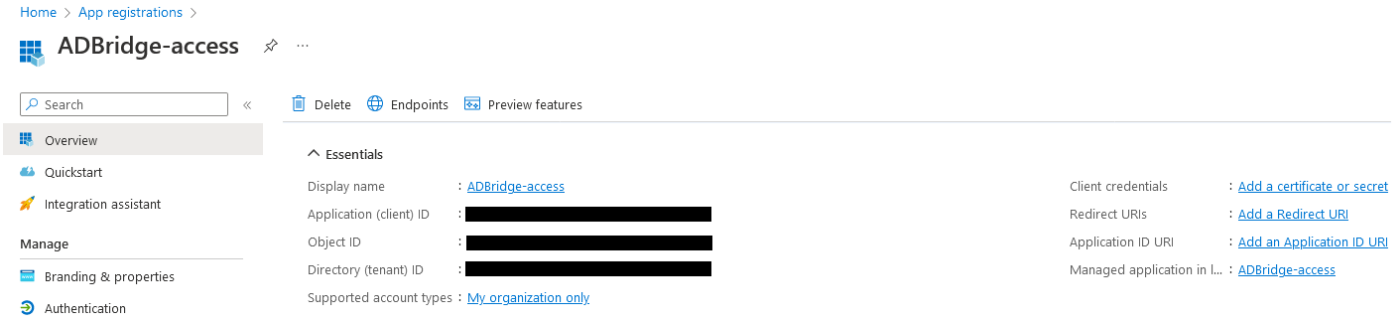
These are the required components to use for Azure AD authentication:

- **Azure AD**
- **On-prem AD environment with Azure AD Connect:** Required for licensing and syncing accounts to Azure. Authentication is supported for AD Connect synced accounts. Authentication is not supported for Azure-only accounts.
- **Azure Application Service:** To join a tenant, an application **client ID** and **secret** are required. The application also defines the access permissions for the endpoint. For configuration information, see "Application Registration and IDs" on page 48.
- **RPM based linux endpoint:** Joined to on-prem AD with 22.3+.

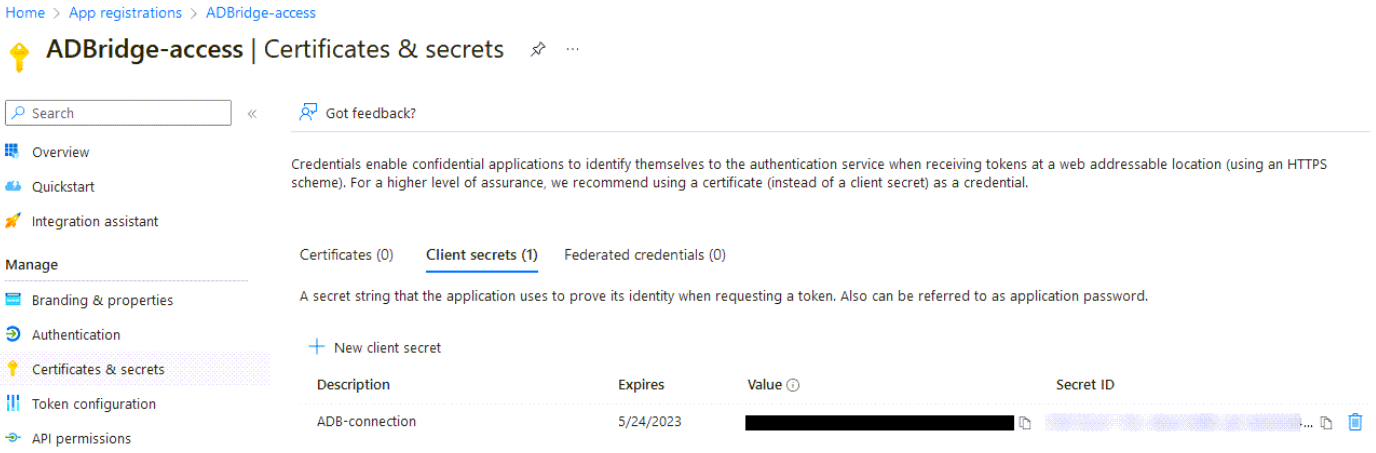
## Application Registration and IDs

To set up app registration and IDs:

1. Create an app registration, and gather the **Client ID** and **Directory (tenant) ID** from it.



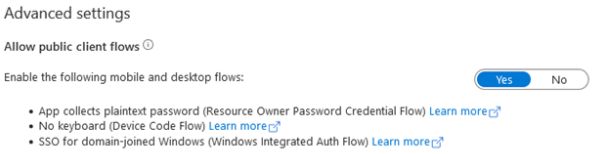

2. Go to **Certificates & secrets** > **Client secrets**.
3. Generate a secret for the app registration. The value is available to copy after you generate it. Copy the secret value and save in a file. It is required to join a tenant. After a period of time, the value is hidden.




4. Set up the app registration rights. The app requires the rights for the endpoint to look up the required information.

| API / Permissions name | Type | Description | Admin consent requ... | Status |
|---|---|---|---|---|
| Microsoft Graph (3) | | | | |
| Group.Read.All | Application | Read all groups | Yes | Granted for ADBridge D... |
| User.Read | Delegated | Sign in and read user profile | No | Granted for ADBridge D... |
| User.Read.All | Application | Read all users' full profiles | Yes | Granted for ADBridge D... |

5. Go to **Authentication** > **Advanced Settings** and enable **Allow public client flows**.




# Endpoint Setup

To connect AD Bridge to Azure AD:

1. Join the Linux endpoint to the on-prem Active Directory that is syncing accounts to Azure AD.

```
/opt/pbis/bin/domainjoin-cli join <DOMAIN> <DOMAINADMIN>
```

2. Create a local file with the app registration secret value.

```
touch azure-secret-file; vi azure-secret-file
```

3. Join Azure tenant with **tenantjoin-cli**.

```
/opt/pbis/bin/tenantjoin-cli join --tenant-id ########-####-####-####-############ --tenant-
name <PRIMARY.TENANT.DOMAIN> --app-id ########-####-####-####-############--app-secret-file
azure-secret-file
```

4. **pbis status** displays the domain, the tenant, and the provider that the agent is joined to.

```
pbis status
```

5. Log in to the endpoint with the Azure user. This displays a device code and a URL.
6. In a browser, navigate to the URL and follow the prompts. You must enter the device code.

```
ssh USER@TENANT@HOSTNAME
```

The authorization polling interval is every 5 secs with 12 tries (60 seconds total).

## Authentication Requirements

Here are a few things to understand regarding authentication.

- The user must be synced from the on-prem Active Directory. This is needed in order to get the user's SID (stored in Azure AD as on-premises security identifier).
- On-prem AD users must have a generated ID from the **Suggest** button. This is to match it with the ID generated as part of the Azure AD login.
- The user that initiates the SSH session must be the same user that authenticates with the device code.
- The User Principal Name (UPN) of the Azure AD user needs to match the on-prem AD user's UPN. This is normally addressed by having a *tenantname* that matches the on-prem AD *domainname*.

# 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 to a Linux or Unix 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 an 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 signon 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, your Active Directory forest functional level must be set to Windows Server 2012.

*For more information, please see "Storage Modes in Active Directory" on page 18.*

## 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**).

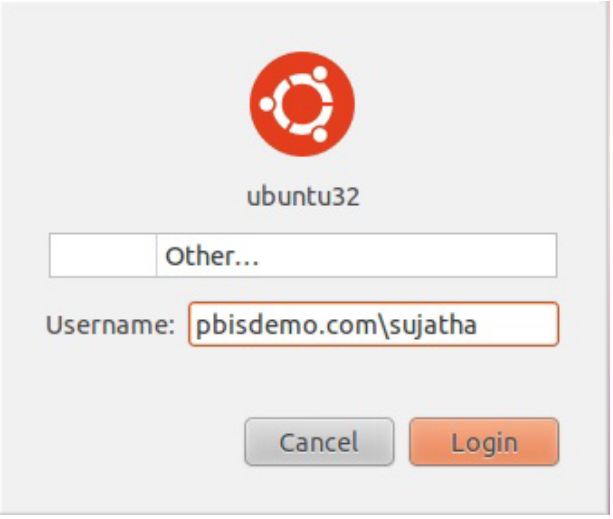
***Example:*** *Example with SSH*

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

Log in to the system console or the text logon 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 in to Ubuntu using AD credentials.




## 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
```

### Delete 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
```

## 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.*

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:*
>
> ```
> ./adbridge-##.#.#.###.linux.x86_64.rpm.sh uninstall
> ```
>
> *For information about the script's options and commands, execute the following command:*
>
> ```
> ./adbridge-##.#.#.###.linux.x86_64.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
```

> ***Note:*** *Using the command to uninstall, as above, leaves the AD Bridge Enterprise configuration files in place on the operating system (OS).*

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
```

# Communicate With 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 www.beyondtrust.com/docs/ad-bridge/how-to/troubleshoot.*

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

## AD Users or Groups are Missing

Provide the following information when contacting BeyondTrust Technical Support:

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

## Poor Performance When Logging On or Looking Up Users

Provide the following information when contacting BeyondTrust Technical Support:

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

> *For more information about the file name and location of the cache files, please see the AD Bridge Linux Administration Guide, at www.beyondtrust.com/docs/ad-bridge/getting-started/linux-admin.*

- tcpdump

# Generate a Support Pack

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

Installed location:

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