AD Bridge

Quick Start Guide

Table of Contents

Introduction

This guide provides information on setting up AD Bridge Open Edition.

> If you experience issues when deploying AD Bridge Open, visit https://github.com/BeyondTrust/pbis-open/issues.

Overview

AD Bridge Open Edition is an agent-based tool that allows you to connect Linux, Unix, and macOS computers to Microsoft Active Directory for consistent security policy across your entire environment.

To get started with AD Bridge Open:

- Install the AD Bridge Open agent
- Join a domain
- Log on using Active Directory credentials

Depending on your environment, you might also need to set common options and give your domain account admin rights.

> For more information, please see the following:
>
> - "Set Common Options" on page 7
> - "Assign Admin Rights to the Domain Account" on page 8

If you already have a previous version of AD Bridge Open or Likewise Open installed, upgrade to the latest version.

> For more information, please see "Upgrade to the Latest Version" on page 7.

Install the Agent, Join a Domain, and Log On

This section provides the installation steps for deploying AD Bridge Open:

- Install AD Bridge Open Edition on a Linux or Mac computer.
- Connect the Linux or Mac computer to an Active Directory domain.
- Log on with your domain credentials.

If you experience issues during the agent deployment, refer to the AD Bridge Open product documentation available on BeyondTrust's website.

Step 1: Download AD Bridge Open

1. Go to: https://github.com/BeyondTrust/pbis-open.
2. Click **Releases**.
3. Right-click the download link for your platform, and then save the installer to the desktop of your Linux computer.

Step 2: Install AD Bridge Open

Install AD Bridge Open using a shell script that contains a self-extracting executable, an SFX installer with a file name that ends in *sh*.

Example: **pbis-open-version number.build number-linux-i386-rpm.sh**

Linux

To deploy the agent to a Linux computer:

1. As root, run the installer, substituting the file name of the installer:

   ```
   sh ./pbis-open-version number.build number-linux-i386-rpm.sh
   ```

   Example:

   ```
   sh ./pbis-open-8.8.0.506.linux-i386-rpm.sh
   ```

   Alternatively, run the installer as a regular user:

   ```
   sudo sh ./pbis-open-version number.build number-linux-i386-rpm.sh
   ```

2. Follow the instructions in the installer.

macOS

> ***Note:*** *To access a Mac using* ***ssh****, turn on remote login.*

For more information on activating remote login on a Mac, please see the Apple website.

To deploy the agent to a Mac computer:

1. Log on to the Mac computer using a local account with administrator privileges.
2. On the desktop, double-click the AD Bridge Open .dmg file, and then double-click the AD Bridge Open .pkg file.
3. Go through the wizard.

Step 3: Join Active Directory

To join a computer to a domain, you must use the root account and have credentials for an Active Directory account that has privileges to join computers to a domain:

```
/opt/pbis/bin/domainjoin-cli join <Domain> <ADMIN>
```

4. (Optional). To set whether the user should type their domain prefix before their user or group name every time they log in, use either of the following command line options:

```
--assumeDefaultDomain {yes|no}
```

```
--userDomainPrefix <short domain name>
```

5. (Optional). To join a computer to a specific Organizational Unit (OU) path, use the following command line option:

```
--ou <organizational unit>
```

Note: *The OU path is from the top of the Active Directory domain down to the OU.*

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

Example:

```
/opt/pbis/bin/domainjoin-cli join --ou automation/default --assumeDefaultDomain yes --
userDomainPrefix pbisqa pbisqa.com pbisadmin
```

Step 4: Log On with AD Credentials

After the computer is joined to the domain and restarted, log on using one of the following formats:

- User principal name (UPN)
- Down-level logon

For more information, please see User Name Formats at https://msdn.microsoft.com/en-us/library/windows/desktop/aa380525(v=vs.85).aspx.

1. Log out of the current session.
2. Log on the system console using your Active Directory user account.

   If you did not set a default domain, log on the system console by using an Active Directory user account in the form of **DOMAIN\username** or **username@domain.com**, where **DOMAIN** is the Active Directory domain name.

   Example:

   example\kathy

   kathy@example.com

IMPORTANT!

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

Active Directory account logons can be restricted by setting **RequireMembershipOf**. For more information, please see Set Common Options and the AD Bridge Configuration Tool Reference Guide at https://www.beyondtrust.com/docs/ad-bridge/documentation.htm.

Upgrade to the Latest Version

With AD Bridge Open Edition 6 or later, seamlessly upgrade preserving your local configuration and maintaining the Active Directory state.

***Note:** You do not need to leave the domain and uninstall the old version before an upgrade. After installation, you are still connected to your domain.*

To upgrade install the latest version of AD Bridge Open while the previous version is running and the computer is joined to a domain.

Set Common Options

This section shows you how to quickly modify two common AD Bridge Open settings, the default domain and the shell, by running the following **config** command-line tool as root:

/opt/pbis/bin/config

To view the config settings, execute the following command:

```
/opt/pbis/bin/config --list
```

The syntax to change the value of a setting is as follows, where **setting** is replaced by the AD Bridge Open option and **value** by the new value that you want to set:

```
/opt/pbis/bin/config setting value
```

Here is an example of how to use **config** to change the **AssumeDefaultDomain** setting:

```
[root@rhel5d bin]# ./config --detail AssumeDefaultDomain ❶
Name: AssumeDefaultDomain
Description: Apply domain name prefix to account name at logon
Type: boolean
Current Value: false
Accepted Values: true, false
Current Value is determined by local policy.

[root@rhel5d bin]# ./config AssumeDefaultDomain true ❷

[root@rhel5d bin]# ./config --show AssumeDefaultDomain ❸
boolean
true
local policy
```

❶ Use the **--detail** argument to view the setting's current value and to determine the values that it accepts.

❷ Set the value to **true**.

❸ Use the **--show** argument to confirm that the value was set to **true**.

Here is another example. To set the shell for a domain account, run **config** as root with the **LoginShellTemplate** setting followed by the path and shell:

```
[root@rhel5d bin]# /opt/pbis/bin/config LoginShellTemplate /bin/ksh
```

Assign Admin Rights to the Domain Account

To run commands with superuser privileges and perform tasks as a superuser, assign local administrative rights to the Active Directory account.

On Ubuntu, add the domain account to the **admin** group in the **/etc/group** file by entering a line like the following as root:

```
admin:x:115:EXAMPLE\kathy
```

On other Linux systems, add an entry for your Active Directory group to the **sudoers** file, typically, **/etc/sudoers**, by editing the file with the **visudo** command as root.

> ***Note:** Editing the **sudoers** file is recommended only for advanced users. Improperly configured **sudoers** files can lock out administrators, create permissions issues for important accounts, or create security issues.*

Example entry of an AD user account:

```
% EXAMPLE\\domain^admins ALL=(ALL) ALL
```

Note: *The example assumes that you are a member of the Active Directory domain administrators group.*

For information about how to format the sudoers file, see the computer's man page for sudo.

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.

Install the AD Bridge 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 11.

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 the linuxmafia.com FAQ *When Should I Set LB_LIBRARY_PATH?*

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 500 KB and 2MB each
- CPU: On a 2.0GHz single-core processor under heavy load with authentication requests is about 2 percent.

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.

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
```

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs 13

©2003-2019 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority. TC: 1/8/2020

Install the Agent on a macOS Computer

To install the AD Bridge agent on a computer running macOS, you must have administrative privileges on the Mac.

1. Log on to the Mac with a local account that has administrative privileges.
2. Obtain the AD Bridge agent installation package for your Mac from BeyondTrust Corporation, and save it to your desktop.
3. On the **Apple** menu, click **System Preferences**.
4. Under **Internet & Network**, click **Sharing**, and then check the **Remote Login** box.

> ***Note:*** *Turn on Remote Login to access the Mac with SSH after you install AD Bridge.*

5. On the Mac computer, go to the **Desktop** and double-click the AD Bridge .dmg file.
6. In the **Finder** window, double-click the AD Bridge .pkg file.
7. Follow the instructions in the installation wizard.

After the agent is installed, you are ready to join the Mac computer to an Active Directory domain.

Install the Agent on a Mac in Unattended Mode

The AD Bridge command-line tools can remotely deploy the shell version of the AD Bridge agent to multiple macOS computers. You can automate the installation of the agent using the installation command in unattended mode.

The commands in this procedure require administrative privileges. Replace **x.x.x.xxxx** with the version and build number indicated in the file name of the SFX installer.

1. Use SSH to connect to the target macOS computer and then use SCP to copy the .dmg installation file to the desktop of the Mac or to a location that can be accessed remotely.

> ***Note:*** *This procedure assumes that you copied the installation file to the desktop.*

2. On the target Mac, open **Terminal** and then use the **hdiutil mount** command to mount the .dmg file under **Volumes**:

```
/usr/bin/hdiutil mount Desktop/pbis-enterprise-x.x.x.xxxx.dmg
```

3. Execute the following command to open the .pkg volume:

```
/usr/bin/open Volumes/pbis-enterprise
```

4. Execute the following command to install the agent:

```
sudo installer -pkg /Volumes/pbis-enterprise/pbis-enterprise-x.x.x.xxxx.pkg -target LocalSystem
```

> ***Note:*** *For more information about the* ***installer*** *command, in Terminal execute the* ***man installer*** *command.*

5. To join the domain, execute the following command in **Terminal**, replacing **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:

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

Example:

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

Terminal prompts you for two passwords:

- the user account on the Mac that has admin privileges
- the user account in Active Directory that you set in the join command

> ***Note:*** *You can also add the password for joining the domain to the command. However, it is not recommended as another user can view and intercept the full command that you are running, including the password:*
>
> ```
> sudo /opt/pbis/bin/domainjoin-cli join domainName joinAccount joinPassword
> ```
>
> *Example:*
>
> ```
> sudo /opt/pbis/bin/domainjoin-cli join example.com Administrator YourPasswordHere
> ```

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.*

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**.

Leave a Domain and Uninstall the AD Bridge 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 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 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" on page 18.

If you installed the agent on a Linux or Unix computer by using the shell script, you can uninstall the AD Bridge Open 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 Open 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 Open by using a command, run the following command:

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

To completely remove all files related to AD Bridge Open 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 Open 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" on page 18.

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
   ```

   .