BeyondTrust

AD Bridge
Mac Administration Guide 9.0

Powered by PowerBroker

TC:5/7/2019

Table of Contents

AD Bridge Mac Administration Guide

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

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

Install the AD Bridge Agent on a Mac OS X Computer

1. Obtain the AD Bridge agent installation package for your Mac from BeyondTrust Technical Support, and save it to your desktop.
2. Log into the Mac with a local account that has administrative privileges.
3. On the **Apple** menu, click **System Preferences**.
4. Under **Internet & Network**, click **Sharing**, and then select the **Remote Login** check box.
5. Turn on remote login to access the Mac with SSH after you install 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.
8. 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 Mac OS X 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 Mac OS X computer.
2. Use SCP to copy the DMG installation file to the desktop of the Mac or to a location that can be accessed remotely.

Note: *The steps below assume that you copied the installation file to the desktop.*

3. On the target Mac, open **Terminal**.
4. Use the **hdiutil mount** command to mount the DMG file under **Volumes**:

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

5. Execute the following command to open the PKG volume:

```
/usr/bin/open Volumes/pbis
```

6. Execute the following command to install the agent:

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

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

7. To join the domain, execute the following command in **Terminal**, replacing **domainName** with the fully qualified domain name (FQDN) of the domain that you want to join and **joinAccount** with the username 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
```

8. 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, but we recommend that you do not use this approach. If you do so, another user could view and intercept the full command that you are running, including the password. Should you choose to send the password, the command is:

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

Example:

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

Join a Mac Computer to an Active Directory Domain

You can join the Mac OS X to a domain using either the user interface or the command line. Before joining a domain:

- Make sure that the computer's name server can find the domain. To check, run the command:

  ```
  nslookup domainName
  ```

- Make sure that the computer can reach the domain controller. To check, run the command:

  ```
  ping domainName
  ```

Join from the User Interface

To join a computer running Mac OS 10.6 or later to an Active Directory domain, you must have administrative privileges on the Mac and privileges on the Active Directory domain that allow you to join a computer.

IMPORTANT!

Apple's built-in service for inter-operating with Active Directory must not be bound to any previous domains for AD Bridge to work properly. If you are migrating from Open Directory or Active Directory, please see "Turn Off OS X Directory Service Authentication" on page 7.

1. In **Finder**, click **Applications**.
2. In the list of applications, double-click **AD Bridge Utilities**, and then click **Domain Join**.
3. Enter a name and password of a local machine account with administrative privileges.
4. In the **Computer name** box, type the local host name of the Mac without the **.local** extension.

***Note:** The local host name cannot be more than 15 characters (this is a limitation with Active Directory). Also, **localhost** is not a valid name.*

***Tip:** To find the local host name of a Mac, on the **Apple** menu, click **System Preferences**, and then click **Sharing**. Under the **Computer Name** box, click **Edit**. Your Mac's local host name is displayed.*

5. In the **Domain to join** box, type the fully qualified domain name (FQDN) of the Active Directory domain.
6. To join the computer to an organizational unit in the domain, select **OU Path** and then type a path in the **OU Path** box.

***Note:** To join the computer to an OU, you must be a member of the Domain Administrator security group.*

7. To join the computer to the **Computers** container, select **Default to "Computers" container**.
8. Click **Join**.

After you join the domain, you can set the display login window preference on the Mac:

1. On the **Apple** menu, click **System Preferences**.
2. Under **System**, click **Accounts**.
3. Click the lock, and enter an administrator's name and password to unlock it.
4. Click **Login Options**.
5. Under **Display login window as**, select **Name and password.**

With AD Bridge, the domain join utility includes a tool to migrate a Mac user's profile from a local user account to the home directory specified for the user in Active Directory. For more information, please see "Migrate a User Profile on a Mac" on page 8.

Join from the Command Line

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

Using sudo, execute the following command in **Terminal**. Replace **domainName** with the FQDN of the domain to join and **joinAccount** with the user account that has privileges to join computers to the domain.

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

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

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

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

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

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, a correct FQDN must exist in **/etc/hosts**.

You can determine the FQDN of a computer running Linux, Unix, or Mac OS X 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.

As an example, the correct entry for the hostname **qaserver** in **/etc/hosts** is **10.100.10.10 qaserver.corpqa.example.com qaserver**. If the entry in **/etc/hosts** is incorrect in its order or format, such as **10.100.10.10 qaserver qaserver.corpqa.example.com**, the computer's FQDN would be read as and would become **qaserver**.

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**.

Turn Off OS X Directory Service Authentication

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

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

Migrate a User Profile on a Mac

On a Mac OS X computer, the AD Bridge domain join utility includes a tool to migrate a user's profile from a local user account to the home directory specified for the user in Active Directory.

When you migrate the user's profile, you can either copy or move it from the local account to the user's Active Directory account. Copying the profile leaves a copy of the user's files in their original location, but it doubles the space on the hard disk required to keep the user's files.

You can migrate a user through the user interface or the command line. In addition, you can customize the migration shell script to suit your requirements.

IMPORTANT!

To migrate a user's profile, you must have a local or AD account with administrative privileges. The account that you use must not be the account that you are migrating.

Migrate from the User Interface

The user interface is no longer supported either for Mac OS 10.8 and later or for AD Bridge 7.0 and later on any version of Mac. Instead, please see "Migrate from the Command Line" on page 9.

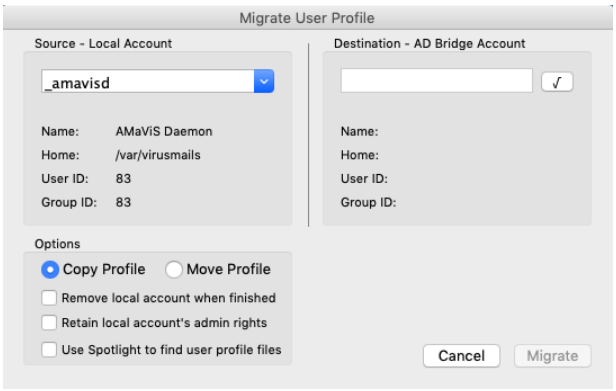
1. Save and close any documents that the user has open.
2. Log in with an administrator account that is not being migrated.
3. In **Terminal**, execute the following command to open the AD Bridge **Domain Join** dialog box:

```
open /opt/pbis/bin/Domain\ Join.app
```

4. If prompted, enter a name and password of an account with administrative privileges. The account can be either a local machine account or an AD account, but it must not be the account that you are migrating.
5. In the **Domain Join** dialog box, click **Migrate**.

***Note:** The **Domain Join** dialog box might be behind your Terminal window or behind another window.*

6. Under **Source - Local Account**, select the user that you want from the dropdown.
7. In the box under **Destination - AD Bridge Account**, type the name of the Active Directory user account that you want to migrate the local account to, and then click the check mark button to verify that the account is in Active Directory.
8. In the **Options** section, select one of the following:
    - **Copy Profile:** Copy a user's files and data from the user's home directory to a home directory specified in Active Directory.
    - **Move Profile:** Move the user's files and data from the user's home directory to a home directory specified in Active Directory.



Note: *Copying the profile doubles the amount of hard disk space required to store the user's files and data on the computer.*

9. Select any additional options, as needed:
    - **Remove local account when finished:** Deletes the account after the account is migrated to AD.
    - **Retain local account's admin rights:** Maintains the permissions of the account after migration.
    - **Use Spotlight to find user profile files**.
10. Click **Migrate**.

Migrate from the Command Line

You can migrate a user's profile using the command line. On a Mac OS X, the migration shell script is located at **/opt/pbis/bin/lw-local-user-migrate.sh**.

You can run the script locally or remotely. To remotely migrate users from another computer, connect to a Mac using SSH and then run the migration script.

For information about the command's syntax and arguments, execute the following command in **Terminal**:

```
/opt/pbis/bin/lw-local-user-migrate.sh --help
```

If you need to modify the migration script, you can open and edit it. The script is written in Bash shell.

IMPORTANT!

BeyondTrust Technical Support does not assist with customizing scripts or provide support for modified scripts.

Remove a Computer from an Active Directory Domain

When you remove a computer from a domain, AD Bridge retains the settings that were made to the computer's configuration when it was joined to the domain.

Remove through the User Interface

The user interface is no longer supported for Mac OS 10.8 and later. Instead, please use the command line.

1. Log in with an administrator account.
2. In **Finder**, click **Applications**.
3. In the list of applications, double-click **AD Bridge Utilities**, and then click **Domain Join**.
4. Click **Leave**.

Remove the Computer Account in Active Directory

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

To disable the computer account, include the user name as part of the **leave** command.

```
domainjoin-cli leave userName
```

Example:

```
domainjoin-cli leave brsmith
```

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

Remove through the Command Line

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

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

Uninstall AD Bridge

Execute the following command in **Terminal**:

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

Configure Group Policy Settings

When you install the Group Policy Management Console component during the AD Bridge install, the following Mac features are available in Group Policy Management Console. Use these features to manage Mac OS X targets that are managed by AD Bridge.

- **Mac System Preferences:** Offers a subset of the System Preferences available with the native Mac tools.
- **DS Plugin Settings:** Offers policies that can be applied if you use Apple's directory services tools to manage users.
- **Profile Manager Settings:** Allows you to upload configuration settings to deploy to Mac OS X computers when they join the domain.

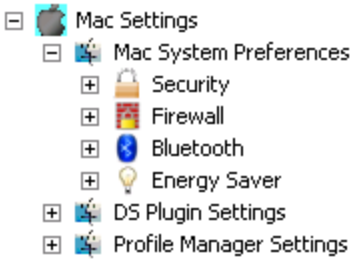
Mac System Preferences

Using Group Policy Management Console, you can deploy certain Mac System Preferences to target Mac OS X systems that are managed by AD Bridge.

Access Mac System Preferences

To access Mac System Preferences in Group Policy Management Console:

1. Create or edit a group policy for the organizational unit you want, and then open it with the **Group Policy Management Editor**.
2. Expand **Computer Configuration > Policies > Unix and Linux Settings > Mac Settings**.
3. Expand **Mac System Preferences**, and then configure a policy.



Security

The policies in **Security preferences** are inherited. The policies will merge with Local policies.

Group Policy Name	Description
Secure system preferences with password	Enable the policy to lock system preferences on target computers so that only administrators with the password can change the preferences.
Automatic logout from user inactivity	Turn on to automatically log a user off a target computer when the computer is idle. Use this policy to prevent unauthorized access to Mac computers that have been inactive for a set period of time. ***Note:*** *If a document with unsaved changes is open on a target computer running Mac OS 10.5 (and possibly other versions), the application cancels logout.*

Firewall

The policies in **Firewall preferences** are inherited. The policies will merge with Local policies.

Group Policy Name	Description
Use firewall protection	Enable to turn on the built-in firewall on target computers.
Block all incoming connections	Turn on to set the built-in firewall on target computers to block UDP traffic. Blocking UDP traffic can help secure target computers.
Use firewall stealth mode	Turn on stealth mode to cloak the target computer behind its firewall. Uninvited traffic gets no response, and other computers that send traffic to the target computer get no information about it.

Bluetooth

Group Policy Name	Description
Turn Bluetooth on or off	Enable or disable Bluetooth power on target computers. When Bluetooth power is off, other Bluetooth devices, such as wireless keyboards and mobile phones, cannot connect to the computer.
Open Bluetooth Setup Assistant at startup when no input device is present	Turn on to open the Bluetooth Setup Assistant if an input device (such as a keyboard or mouse) is not detected when the computer starts.  ***Note:*** *This settings works with computers running Mac OS 10.5.*

Energy Saver

Sleep Preferences

Group Policy Name	Description
System Sleep Timer	Turn on to put a target computer to sleep after it has been idle for a set number of minutes. To set the computer to never sleep, enter **0**.
Display Sleep Timer	Turn on to put the screen of a target computer to sleep after it has been idle for a set number of minutes. To set the computer to never sleep, enter **0**.
Disk Sleep Timer	Turn on to put the hard disk of a target computer to sleep when it is not in use.

Options Preferences

Group Policy Name	Description
Wake on LAN	Turn on to wake up a target computer when a network administrator accesses it through a local area network Ethernet connection.
Sleep on Power button	Turn on to set the power button to put a target computer to sleep. When the power button is pressed, the computer goes to sleep instead of shutting down.
Automatic restart on power loss	Turn on to automatically restart a target Mac OS X computer after it loses power. This policy can help recover a workstation or server after a power failure.

Mac DS Plugin Settings

If you are using Apple's directory services tools to manage users, you can use the DS Plugin Settings to apply policies on home directory and local administration settings.

Group Policy Name	Description
Use UNC path from Active Directory to create home location	Connects the computer to the network share defined in the Active Directory user account. The UNC path is converted to **SMB protocol** when the target file server is running Windows or **AFP protocol** when the target file server is running Mac OS X. If the policy for forcing the home directory on the startup disk is enabled, the UNC path is used to create a folder in the user's dock, and the home directory is set to the user's local home directory path. To set the path for the home directory, go to the **Profile** tab of the user's properties in **Active Directory Users and Computers**. Under the **Home** folder, select **Connect**, choose a drive (which is ignored by a Mac OS X computer), and type the UNC path in the **To** box. Path format: **\\server\share\folder** Example: **\\lwdemo01\homes\fanthony**
Force home directory on startup disk	Sets a computer to use a local home directory path. When a user with a home folder connection defined in Active Directory logs on, the connection is created in the dock under **/Network/Servers/homeFolderName**. The home directory is set on the **AD Bridge Cell Settings** tab in Active Directory.
Allow administration by	Set the administrators included in the local admin group (group ID 80) on a target computer. Local entries are overwritten unless you also set the policy to **Allow admins group local entries**. Select the Active Directory users and groups to add to the list of administrators. You can select users and groups, or you can enter a comma-separated list of short domain names with Active Directory account names or group names. ***Note:*** *The users and groups that you select must be enabled in the AD Bridge cell containing the target computer.*
Allow admins group local entries	Preserves members of the admin group who are defined locally but are not specified in the **Allow administration by** policy.

Profile Manager Settings

You can upload Profile Manager configuration settings to Group Policy Management Console and deploy the settings to your Mac OS X computers. When the Mac OS X computer joins the domain, then the policies defined in the Profile Manager settings are deployed to the computer.

> ***Note:*** *Profile Manager polices are applied on computers running Mac OS 10.7 and later. If both Profile Manager and Workgroup Manager policies are in place, then the group policy agent tries to apply both types of policy. Therefore, we recommend that you do not use Workgroup Manager and Profile Manager in the same AD Bridge environment, as results might not be reliable.*

Requirements

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Import a Policy

1. In **Group Policy Management Editor**, go to the **Mac Settings**.
2. Select **Profile Manager Settings**.
3. Double-click the policy.
4. Select the **Define this policy** check box.
5. Click **Import**, and then navigate to the **mobileconfig** file.
6. Click **Apply**.

> ***Note:*** *Only one* ***mobileconfig*** *file is permitted per group policy.*

> ***Tip:*** *If the policy is deployed but not applied, try restarting the computer and restarting* ***gpagent****.*

Remove a Policy

1. In **Group Policy Management Editor**, go to the **Mac Settings**.
2. Select **Profile Manager Settings**.
3. Double-click the policy.
4. Clear the **Define this policy** check box.
5. Click **Apply**.
6. The next time you open the policy, the **mobileconfig** contents are no longer displayed. You can import a new or updated mobileconfig file if needed.

Use the Mac OS X Config Tool

Command Name	Description
AllowAdministrationBy	Allows Active Directory users to be set as local admins without setting the permission via group policy. Local entries are overwritten unless users set the **enablemergeadmins** config option.
EnableForceHomedirOnStartupDisk	Sets a computer to use a local home directory path. When a user with a home folder connection defined in Active Director logs in, the connection is created in the dock under **/Network/Servers/homefoldername**. The default value is **0**.
EnableMergeAdmins	Preserves members of the admin group who are defined locally but are not defined in the **AllowAdministrationBy** setting. The default value is **false**.
UncProtocolForHomeLocation	Enables use of the UNC protocol for a home directory. This setting is used with the **UseADUncForHomeLocation** to connect to network servers. The default value is **smb**.
UseADUncForHomeLocation	Connects the computer to the network share defined in the Active Directory user account. The UNC path is converted to **SMB protocol** when the target file server is running Windows or **AFP protocol** when the target file server is running Mac OS X. If the setting for forcing the home directory on the startup disk is enabled, the UNC path is used to create a folder in the user's dock, and the home directory is set to the user's local home directory path. The default value is **false**.

Contact BeyondTrust Technical Support

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

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

Before Contacting BeyondTrust Technical Support

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

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

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

Segmentation Faults

Provide the following information when contacting BeyondTrust Technical Support:

- Core dump of the AD Bridge application:
  `ulimit - c unlimited`
- Exact patch level or exact versions of all installed packages

Program Freezes

Provide the following information when contacting BeyondTrust Technical Support:

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

Domain-Join Errors

Provide the following information when contacting BeyondTrust Technical Support:

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

All Active Directory Users Are Missing

Provide the following information when contacting BeyondTrust Technical Support:

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

All Active Directory Users Cannot Log On

Provide the following information when contacting BeyondTrust Technical Support:

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

> For more information, please see *Generate Debug Logs* in the *AD Bridge Troubleshooting Guide*.

- 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*.

- tcpdump

Generate a Support Pack

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

Installed location:

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

Download location:

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