



# BeyondTrust

## AD Bridge Troubleshooting Guide

# Table of Contents

---

<b>Troubleshoot Common AD Bridge Issues</b> .....	<b>4</b>
Troubleshoot and Solve Domain-Join Problems .....	5
Top 10 Reasons Domain-Join Fail .....	5
Solve Domain-Join Problems .....	5
Ignore Inaccessible Trusts .....	7
Resolve Common Error Messages .....	8
Diagnose NTP on Port 123 .....	10
Turn off Apache to Join a Domain .....	11
Troubleshoot the AD Bridge Agent .....	12
AD Bridge Services and Status .....	12
Generate Debug Logs for AD Bridge Services .....	17
Perform Basic Troubleshooting for the AD Bridge Agent .....	22
Troubleshoot Accounts and Attributes .....	24
Troubleshoot the AD Bridge Cache .....	32
Pluggable Authentication Modules (PAM) .....	34
Perform OS-Specific Troubleshooting .....	35
Troubleshoot Logon Issues with Systems .....	41
Solve Logon Problems from Windows .....	41
Solve Logon Problems on Linux or Unix .....	41
Troubleshoot SSH SSO Login Problems .....	46
Troubleshoot Issues with Kerberos .....	55
Resolve a KRB Error During SSO in a Disjoint Namespace .....	56
Eliminate Logon Delays When DNS Connectivity Is Poor .....	57
Eliminate Kerberos Ticket Renewal Dialog Box .....	57
Troubleshoot the AD Bridge Database .....	58
Check the Endpoints .....	58
Troubleshoot Checklists for Reporting Components .....	60
Check the AD Bridge BTCollector .....	61
Check Events in the AD Bridge Database .....	63
Switch Between Databases in AD Bridge .....	63
Troubleshoot Windows Setup for AD Bridge .....	65

---

RID Pool Error .....	65
Troubleshoot Entra ID Authentication Issues .....	66
Tenant Join Issues .....	66
Troubleshoot Performance Issues .....	67
Configure Max Buffer Size .....	67
Solaris .....	67
Troubleshoot AD Bridge Group Policy .....	69
Autoenrollment GPO .....	69
Wifi GPO .....	69
Force AD Bridge Group Policy Objects to Update .....	69
Check the Status of the AD Bridge Group Policy Daemon .....	70
Restart the AD Bridge Group Policy Daemon .....	70
Generate an AD Bridge Group Policy Agent Debug Log .....	70
Modify or Inspect GPOs from the gp-admin Command .....	70
Log a Support Case With BeyondTrust Technical Support .....	74
Before Contacting BeyondTrust Technical Support .....	74
Segmentation Faults .....	74
Program Freezes .....	74
Domain-Join Errors .....	74
All Active Directory Users Are Missing .....	74
All Active Directory Users Cannot Log On .....	75
AD Users or Groups are Missing .....	75
Poor Performance When Logging On or Looking Up Users .....	75
Generate a Support Pack .....	76

# Troubleshoot Common AD Bridge Issues

The topics listed below cover common problems and issues when installing, setting up, and using AD Bridge.

- ["Troubleshoot and Solve Domain-Join Problems" on page 5](#)
- ["Troubleshoot the AD Bridge Agent" on page 12](#)
- ["Troubleshoot Logon Issues with Systems" on page 41](#)
- ["Troubleshoot Issues with Kerberos" on page 55](#)
- ["Troubleshoot the AD Bridge Database" on page 58](#)
- ["Troubleshoot Windows Setup for AD Bridge" on page 65](#)
- ["Troubleshoot Entra ID Authentication Issues" on page 66](#)
- ["Troubleshoot Performance Issues" on page 67](#)
- ["Troubleshoot AD Bridge Group Policy" on page 69](#)

## Troubleshoot and Solve Domain-Join Problems

Review the sections in this chapter to resolve domain-join problems.

### Top 10 Reasons Domain-Join Fail

Here are the top 10 reasons that an attempt to join a domain fails:

1. Root was not used to run the **domain-join** command (or to run the domain-join graphical user interface).
2. The user name or password of the account used to join the domain is incorrect.
3. The name of the domain is mistyped.
4. The name of the OU is mistyped.
5. The local hostname is invalid.
6. The domain controller is unreachable from the client because of a firewall or because the NTP service is not running on the domain controller.



For more information, see the following:

- [Make Sure Outbound Ports are Open at "Perform Basic Troubleshooting for the AD Bridge Agent" on page 22](#)
- ["Diagnose NTP on Port 123" on page 10](#)

7. The client is running RHEL 2.1 and has an old version of SSH.
8. On SUSE, GDM (**dbus**) must be restarted. This daemon cannot be automatically restarted if the user logged on with the graphical user interface.
9. On Solaris, **dtlogin** must be restarted. This daemon cannot be automatically restarted if the user logged on with the Solaris graphical user interface. To restart **dtlogin**, run the following command:

```
/sbin/init.d/dtlogin.rc start
```

10. SELinux is set to either enforcing or permissive, likely on Fedora. SELinux must be set to disabled before the computer can be joined to the domain.



To turn off SELinux, see the SELinux man page.

### Solve Domain-Join Problems

To troubleshoot problems with joining a Linux computer to a domain, perform the following series of diagnostic tests sequentially on the Linux computer with a root account.

The tests can also be used to troubleshoot domain-join problems on a Unix computer; however, the syntax of the commands on Unix might be slightly different.

The procedures in this topic assume that you have already checked whether the problem falls under the Top 10 Reasons Domain Join Fails (see above). We also recommend that you generate a domain-join log.



For more information, see ["Generate a Domain-Join Log for AD Bridge" on page 19.](#)

## Verify that the Name Server Can Find the Domain

Run the following command as root:

```
nslookup YourADrootDomain.com
```

## Make Sure the Client Can Reach the Domain Controller

You can verify that your computer can reach the domain controller by pinging it:

```
ping YourDomainName
```

## Check DNS Connectivity

The computer might be using the wrong DNS server or none at all. Make sure the nameserver entry in **/etc/resolv.conf** contains the IP address of a DNS server that can resolve the name of the domain you are trying to join. The IP address is likely to be that of one of your domain controllers.

## Make Sure **nsswitch.conf** Is Configured to Check DNS for Host Names

The **/etc/nsswitch.conf** file must contain the following line. (On AIX, the file is **/etc/netsvc.conf**.)

```
hosts: files dns
```

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

## Ensure that DNS Queries Use the Correct Network Interface Card

If the computer is multi-homed, the DNS queries might be going out the wrong network interface card.

Temporarily disable all the NICs except for the card on the same subnet as your domain controller or DNS server and then test DNS lookups to the AD domain.

If this works, re-enable all the NICs and edit the local or network routing tables so that the AD domain controllers are accessible from the host.

## Determine If DNS Server Is Configured to Return SRV Records

Your DNS server must be set to return SRV records so the domain controller can be located. It is common for non-Windows (bind) DNS servers to not be configured to return SRV records.

Diagnose it by executing the following command:

```
nslookup -q=srv _ldap._tcp. ADdomainToJoin.com
```

## Make Sure that the Global Catalog Is Accessible

The global catalog for Active Directory must be accessible. A global catalog in a different zone might not show up in DNS. Diagnose it by executing the following command:

```
nslookup -q=srv _ldap._tcp.gc._msdcs. ADrootDomain.com
```

From the list of IP addresses in the results, choose one or more addresses and test whether they are accessible on Port 3268 using telnet.

```
telnet 192.168.100.20 3268
Trying 192.168.100.20... Connected to sales-dc.example.com (192.168.100.20). Escape character is
'^]'. Press the Enter key to close the connection: Connection closed by foreign host.
```

## Verify that the Client Can Connect to the Domain on Port 123

The following test checks whether the client can connect to the domain controller on Port 123 and whether the Network Time Protocol (NTP) service is running on the domain controller. For the client to join the domain, NTP, the Windows time service, must be running on the domain controller.

On a Linux computer, run the following command as root:

```
ntpdate -d -u DC_hostname
```



**Example:**

```
ntpdate -d -u sales-dc
```



For more information, see ["Diagnose NTP on Port 123" on page 10](#)

In addition, check the logs on the domain controller for errors from the source named **w32tm**, which is the Windows time service.

## FreeBSD: Run Idconfig If You Cannot Restart Computer

When installing AD Bridge on a new FreeBSD computer with nothing in **/usr/local**, run **/etc/rc.d/Idconfig start** after the installation if you cannot restart the computer. Otherwise, **/usr/local/lib** will not be in the library search path.

## Ignore Inaccessible Trusts

An inaccessible trust can block you from successfully joining a domain. If you know that there are inaccessible trusts in your Active Directory network, you can set AD Bridge to ignore all the trusts before you try to join a domain. To do so, use the **config** tool to modify the values of the **DomainManagerIgnoreAllTrusts** setting.

1. List the available trust settings:

```
/opt/pbis/bin/config --list | grep -i trust
```

The results will look something like this. The setting at issue is **DomainManagerIgnoreAllTrusts**

```
DomainManagerIgnoreAllTrusts
DomainManagerIncludeTrustsList
DomainManagerExcludeTrustsList
```

2. List the details of the **DomainManagerIgnoreAllTrusts** setting to see the values it accepts:

```
[root@rhel5d bin]# ./config --details DomainManagerIgnoreAllTrusts
Name: DomainManagerIgnoreAllTrusts
Description: When true, ignore all trusts during domain enumeration.
Type: boolean
Current Value: false
Accepted Values: true, false
Current Value is determined by local policy.
```

3. Change the setting to true so that AD Bridge will ignore trusts when you try to join a domain.

```
[root@rhel5d bin]# ./config DomainManagerIgnoreAllTrusts true
```

4. Check to make sure the change took effect:

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

Now try to join the domain again. If successful, keep in mind that only users and groups who are in the local domain will be able to log on the computer.

In the example output above that shows the setting's current values, **local policy** is listed, meaning that the setting is managed locally through **config** because an AD Bridge Group Policy setting is not managing the setting. Typically, with AD Bridge, you would manage the **DomainManagerIgnoreAllTrusts** setting by using the corresponding Group Policy setting, but you cannot apply Group Policy Objects (GPOs) to the computer until after it is added to the domain. The corresponding AD Bridge policy setting is named **Lsass: Ignore all trusts during domain enumeration**.

For information on the arguments of config, run the following command:

```
/opt/pbis/bin/config --help
```

## Resolve Common Error Messages

This section lists solutions to common errors that can occur when you try to join a domain.

## Configuration of krb5

### Error Message:

```
Warning: A resumable error occurred while processing a module.  
Even though the configuration of 'krb5' was executed, the configuration did not  
fully complete. Please contact BeyondTrust support.
```

### Solution:

Delete `/etc/krb5.conf` and try to join the domain again.

## Chkconfig Failed

This error can occur when you try to join a domain or you try to execute the domain-join command with an option but the `netlogond` daemon is not already running.

### Error Message:

```
Error: chkconfig failed [code 0x00080019]
```

Description: An error occurred while using `chkconfig` to process the `netlogond` daemon, which must be added to the list of processes to start when the computer is rebooted. The problem may be caused by startup scripts in the `/etc/rc.d/` tree that are not LSB-compliant.

Verification: Running the following command as root can provide information about the error:

```
chkconfig --add netlogond
```

### Solution:

Remove startup scripts that are not LSB-compliant from the `/etc/rc.d/` tree.

## Replication Issues

The following error might occur if there are replication delays in your environment. A replication delay might occur when the client is in the same site as an RODC.

### Error Message:

```
Error: LW_ERROR_KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN [code 0x0000a309]  
Client not found in Kerberos database  
[root@rhel6-1 ~]# echo $?  
1
```

```
[root@rhel6-1 ~]# /opt/pbis/bin/domainjoin-cli query  
Error: LW_ERROR_KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN [code 0x0000a309]  
Client not found in Kerberos database
```

## Solution:

After the error occurs, wait 15 minutes, and then run the following command to restart AD Bridge:

```
/opt/pbis/bin/lwsm restart lwreg
```

## Diagnose NTP on Port 123

When you use the AD Bridgedomain-join utility to join a Linux or Unix client to a domain, the utility might be unable to contact the domain controller on Port 123 with UDP. The AD Bridge agent requires that Port 123 be open on the client so that it can receive NTP data from the domain controller. In addition, the time service must be running on the domain controller.

You can diagnose NTP connectivity by executing the following command as root at the shell prompt of your Linux computer:

```
ntpdate -d -u DC_hostname
```



### Example:

```
ntpdate -d -u sales-dc
```

If all is well, the result should look like this:

```
[root@rhel44id ~]# ntpdate -d -u sales-dc  
2 May 14:19:20 ntpdate[20232]: ntpdate 4.2.0a@1.1190-r Thu Apr 20 11:28:37 EDT 2006 (1)  
Looking for host sales-dc and service ntp  
host found : sales-dc.example.com  
transmit(192.168.100.20)  
receive(192.168.100.20)  
transmit(192.168.100.20)  
receive(192.168.100.20)  
transmit(192.168.100.20)  
receive(192.168.100.20)  
transmit(192.168.100.20)  
receive(192.168.100.20)  
transmit(192.168.100.20)  
server 192.168.100.20, port 123  
stratum 1, precision -6, leap 00, trust 000  
refid [LOCL], delay 0.04173, dispersion 0.00182  
transmitted 4, in filter 4  
reference time: cbc5d3b8.b7439581 Fri, May 2 2008 10:54:00.715  
originate timestamp: cbc603d8.df33333 Fri, May 2 2008 14:19:20.871  
transmit timestamp: cbc603d8.dda43782 Fri, May 2 2008 14:19:20.865  
filter delay: 0.04207 0.04173 0.04335 0.04178  
0.00000 0.00000 0.00000 0.00000
```

```
filter offset: 0.009522 0.008734 0.007347 0.005818  
0.000000 0.000000 0.000000 0.000000  
delay 0.04173, dispersion 0.00182  
offset 0.008734  
2 May 14:19:20 ntpdate[20232]: adjust time server 192.168.100.20 offset 0.008734 sec
```

## Output When There is No NTP Service

If the domain controller is not running NTP on Port 123, the command returns a response such as *no server suitable for synchronization found*, as in the following output:

```
5 May 16:00:41 ntpdate[8557]: ntpdate 4.2.0a@1.1190-r Thu Apr 20 11:28:37 EDT 2006 (1)  
Looking for host RHEL44ID and service ntp  
host found : rhel44id.example.com  
transmit(127.0.0.1)  
transmit(127.0.0.1)  
transmit(127.0.0.1)  
transmit(127.0.0.1)  
transmit(127.0.0.1)  
127.0.0.1: Server dropped: no data  
server 127.0.0.1, port 123  
stratum 0, precision 0, leap 00, trust 000  
refid [127.0.0.1], delay 0.00000, dispersion 64.00000  
transmitted 4, in filter 4  
reference time: 00000000.00000000 Wed, Feb 6 2036 22:28:16.000  
originate timestamp: 00000000.00000000 Wed, Feb 6 2036 22:28:16.000  
transmit timestamp: cbca101c.914a2b9d Mon, May 5 2008 16:00:44.567  
filter delay: 0.00000 0.00000 0.00000 0.00000  
0.00000 0.00000 0.00000 0.00000  
filter offset: 0.00000 0.00000 0.00000 0.00000  
0.00000 0.00000 0.00000 0.00000  
delay 0.00000, dispersion 64.00000  
offset 0.00000  
5 May 16:00:45 ntpdate[8557]: no server suitable for synchronization found
```

## Turn off Apache to Join a Domain

The Apache web server locks the keytab file, which can block an attempt to join a domain. If the computer is running Apache, stop Apache, join the domain, and then restart Apache.

## Troubleshoot the AD Bridge Agent

This chapter contains information on how to troubleshoot the AD Bridge agent, including the authentication service, the input-output service, and the network logon service.

This guide contains the following:

- ["AD Bridge Services and Status" on page 12](#)
- ["Generate Debug Logs for AD Bridge Services" on page 17](#)
- ["Perform Basic Troubleshooting for the AD Bridge Agent" on page 22](#)
- ["Troubleshoot Accounts and Attributes" on page 24](#)
- ["Troubleshoot the AD Bridge Cache" on page 32](#)
- ["Pluggable Authentication Modules \(PAM\)" on page 34](#)
- ["Perform OS-Specific Troubleshooting" on page 35](#)



Troubleshooting guidance related to specific subjects is also provided in other guides:

- For information about troubleshooting Samba integration, see the [AD Bridge Integration Guide](#) at [www.beyondtrust.com/docs/ad-bridge/how-to/integration/samba/troubleshoot-samba.htm](http://www.beyondtrust.com/docs/ad-bridge/how-to/integration/samba/troubleshoot-samba.htm).
- For an overview of commands such as **rpm** and **dpkg** that can help troubleshoot AD Bridge packages on Linux and Unix platforms, see [AD Bridge Package Management Commands](#) in the [AD Bridge Installation Guide](#) at [www.beyondtrust.com/docs/ad-bridge/getting-started/installation/index.htm](http://www.beyondtrust.com/docs/ad-bridge/getting-started/installation/index.htm).

## AD Bridge Services and Status

The AD Bridge Service Manager lets you troubleshoot all the AD Bridge services from a single command-line utility. You can, for example, check the status of the services 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 right order.

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

```
/opt/pbis/bin/lwsm list
```



### Example:

```
[root@cent64b62 ~]# /opt/pbis/bin/lwsm list
lwreg          running      (container: 4241)
dcerpc         stopped
eventfwd       running      (container: 4436)
eventlog       running      (container: 4300)
gpagent        running      (container: 4351)
lsass          running      (container: 4335)
lwio           running      (container: 4319)
lwpkcs11       stopped
lwsc           stopped
netlogon       running      (container: 4310)
```



```
rdr          running      (io: 4319)
reapsysl    running      (container: 4400)
usermonitor running      (container: 4447)
```

To restart the **lsass** service, run the following command with superuser privileges:

```
/opt/pbis/bin/lwsm restart lsass
```

To view all the service manager's commands and arguments, execute the following command:

```
/opt/pbis/bin/lwsm --help
```

## Check the Status on AD Bridge Services

### Check the Status of the Authentication Service

You can check the status of the authentication service on a Unix or Linux computer running the AD Bridge agent by executing the following command at the shell prompt as the root user:

```
/opt/pbis/bin/lwsm status lsass
```

If the service is not running, execute the following command:

```
/opt/pbis/bin/lwsm start lsass
```

### Check the Status of the DCE/RPC Service

The DCE/RPC service manages communication between AD Bridge clients and Microsoft Active Directory.

### On Linux and Unix

You can check the status of **dcerpcd** on a Unix or Linux computer running the AD Bridge agent by running the following command as the root user:

```
/opt/pbis/bin/lwsm status dcerpc
```

If the service is not running, run the following command:

```
/opt/pbis/bin/lwsm start dcerpc
```

### Check the Status of the Network Logon Service

The **netlogon** service detects the optimal domain controller and global catalog and caches the data.

## On Linux and Unix

You can check the status of **netlogon** on a computer running the AD Bridge agent by executing the following command as the root user:

```
/opt/pbis/bin/lwsm status netlogon
```

If the service is not running, execute the following command:

```
/opt/pbis/bin/lwsm start netlogon
```



### IMPORTANT!

*If the error message **Failed to verify DC <Domain Controller Name>. (error <number>)** is logged in the agent's syslog files, enable debug logging on the agent. If the incident occurs again, please submit the debug logs to support for review.*

## Check the Status of the Input-Output Service

The AD Bridge input-output service, **lwio**, communicates over SMB with external SMB servers and internal processes.

You can check the status of **lwio** on a Linux or Unix computer running the AD Bridge agent by executing the following command as the root user:

```
/opt/pbis/bin/lwsm status lwio
```

If the service is not running, execute the following command:

```
/opt/pbis/bin/lwsm start lwio
```

## Check the Status of GPAGENT Service

The AD Bridge Group Policy service, **gpagent**, communicates with the AD Bridge domain controller and pulls down group policies.

You can check the status of **gpagent** on a Linux or Unix computer running the AD Bridge agent by executing the following command as the root user:

```
/opt/pbis/bin/lwsm status gpagent
```

If the service is not running, execute the following command:

```
/opt/pbis/bin/lwsm start gpagent
```



*Note: If the agent is not joined to the domain, **gpagent** will not be running.*

## Restart AD Bridge Services

### Restart the Authentication Service

The authentication service handles authentication, authorization, caching, and idmap lookups.

You can restart the AD Bridge authentication service by executing the following command at the shell prompt:

```
/opt/pbis/bin/lwsm restart lsass
```

To stop the service, type this command:

```
/opt/pbis/bin/lwsm stop lsass
```

To start the service, type this command:

```
/opt/pbis/bin/lwsm start lsass
```

### Restart the AD Bridge DEC/RPC Service

The AD Bridge **DCE/RPC** service helps route remote procedure calls between computers on a network by serving as an end-point mapper.



For more information, see **AD Bridge Agent** in the [AD Bridge Installation Guide](#) at [www.beyondtrust.com/docs/ad-bridge/getting-started/installation](http://www.beyondtrust.com/docs/ad-bridge/getting-started/installation).

You can restart the **DCE/RPC** service by running the following command at the shell prompt:

```
/opt/pbis/bin/lwsm restart dcerpc
```

To stop the daemon, type this command:

```
/opt/pbis/bin/lwsm stop dcerpc
```

To start the daemon, type this command:

```
/opt/pbis/bin/lwsm start dcerpc
```

### Restart the Network Logon Service

The **netlogon** service determines the optimal domain controller and global catalog and caches the data.



For more information and a list of start-order dependencies, see [Manage AD Bridge Services](https://www.beyondtrust.com/docs/ad-bridge/getting-started/linux-admin/manage-services.htm) at <https://www.beyondtrust.com/docs/ad-bridge/getting-started/linux-admin/manage-services.htm> in the [AD Bridge Linux Administration Guide](#).

You can restart the AD Bridge network logon service by executing the following command at the shell prompt:

```
/opt/pbis/bin/lwsm restart netlogon
```

To stop the service, type this command:

```
/opt/pbis/bin/lwsm stop netlogon
```

To start the service, type this command:

```
/opt/pbis/bin/lwsm start netlogon
```

## Restart the Input-Output Service

The AD Bridge input-output service, **lwio**, communicates over SMB with SMB servers; authentication is with Kerberos 5.

You can restart the input-output service by executing the following command at the shell prompt:

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

To stop the service, type this command:

```
/opt/pbis/bin/lwsm stop lwio
```

To start the service, type this command:

```
/opt/pbis/bin/lwsm start lwio
```



**Note:** If you start the **lwio** service and the **rdr** service does not also start, use the following command to start the **rdr** service:

## Restart the Group Policy Service

The AD Bridge group policy service communicates with the domain controller and pulls down group policies.

You can restart the group policy service by executing the following command at the shell prompt:

```
/opt/pbis/bin/lwsm restart gpagent
```

To stop the service, type this command:

```
/opt/pbis/bin/lwsm stop gpagent
```

To start the service, type this command:

```
/opt/pbis/bin/lwsm start gpagent
```

## Generate Debug Logs for AD Bridge Services

Logging can help identify and solve problems. There are debug logs for the following services in AD Bridge:

Services	Description
<b>eventfwd</b>	The event forwarding service. Generate a debug log to verify that the service is receiving events and forwarding them to a collector server.
<b>eventlog</b>	The event collection service. Generate a debug log for <b>eventlog</b> to troubleshoot the collection and processing of security events
<b>gpagent</b>	The Group Policy agent. Generate a debug log for <b>gpagent</b> to troubleshoot the application or processing of Group Policy Objects (GPOs).
<b>lsass</b>	The authentication service. Generate a debug log for <b>lsass</b> when you need to troubleshoot authentication errors or failures.
<b>lwio</b>	The input-output service that manages interprocess communication.
<b>lwpkcs11</b>	A service that aids in logging on and logging off with a smart card. Gather logging information about it when there is a problem logging on or logging off with a smart card.
<b>lwreg</b>	The AD Bridge registry service. Generate a debug log for <b>lwreg</b> to troubleshoot ill-fated configuration changes to the registry.
<b>lwsc</b>	The smart card service. Gather logging information for the smart card service when card-insertion or card-removal behavior is other than expected.
<b>lwsm</b>	The service manager.
<b>netlogon</b>	The site affinity service that detects the optimal domain controller and global catalog. Generate a debug log for <b>netlogon</b> when you need to troubleshoot problems with sending requests to domain controllers or getting information from the global catalog.
<b>PAM</b>	The pluggable authentication modules used by AD Bridge. Create a debug log for PAM when you need to troubleshoot logon or authentication problems.
<b>reapsysl</b>	Part of the data collection service. Capture a debug log for <b>reapsysl</b> to investigate the collection and processing of events.

By default, log messages are processed by syslog, typically through the daemon facility. Although the path and file name of the log vary by platform, they typically appear in a subdirectory of **/var/log**. Note that when you change the log level of a AD Bridge service to **debug**, you may also need to update syslog configuration (typically **/etc/syslog.conf**) with the following command and then restart the syslog service:

```
*.debug /tmp/debug.log
```

 Alternatively, you can log directly to a file, as the procedure to change the target illustrates. For more information, see "["Change the Target" on page 18](#).

Log levels can be changed temporarily or permanently.

To temporarily change the log level, you can use **/opt/pbis/bin/lwsm** to specify the log level and whether to log to the syslog or directly to a file.

To permanently change the log level, you must modify the service's entry in the AD Bridge registry.

The following log levels are available for most AD Bridge services:

- **always**
- **debug**
- **error** (default)
- **warning**
- **info**
- **verbose**
- **trace**

To troubleshoot, we recommend that you change the level to debug. However, to conserve disk space, we recommend that you set the log level to the default level when you finish troubleshooting.



**Tip:** The following are the pipes by which su, sudo, and local user (root) sshd logons are captured with the AD Bridge auditing system. They are system pipes created by the **reapsysl** service. AD Bridge cannot start the **reapsysl** service before syslog starts because of a complex series of dependencies on the system. Therefore, these errors are generated and should be ignored. **Reapsysl** will recreate the pipes as necessary.

```
robbie@example:~$ sudo ls -la /var/lib/pbis/syslog-reaper/ total 28
drwx----- 2 root root 4096 Mar  7 12:54 .
drwxr-xr-x  8 root root 4096 May 10 13:27 ..
prwx----- 1 root root     0 Mar  7 12:54 error
prwx----- 1 root root     0 Mar  7 12:54 information
prwx----- 1 root root     0 Mar  7 12:54 warning
```

## Temporarily Change the Log Level and Target for a Service

The service manager supports per-service, per-facility logging. Each service has a default log target (syslog) and level (WARNING).

### Change the Target

You can use the following command to change the log target for a particular service and facility to log to a file:

```
/opt/pbis/bin/lwsm set-log-target <service> <facility> file <path>
```

You can use the following command to change the log target for a particular service and facility to the syslog:

```
/opt/pbis/bin/lwsm set-log-target <service> <facility> syslog
```

The service can be any AD Bridge service except **dcerpc**, which has its own logging mechanism.

The facility is a portion of the service and the default facility is accessed as a hyphen (-). For example, to target the logging messages from default facility of **lsass** to a file **/var/log/lsass.log**:

```
/opt/pbis/bin/lwsm set-log-target lsass - file /var/log/lsass.log
```

If you want to debug the interprocess communications of **lsass** (something rarely required), you can use the **lsass-ipc** facility:

```
/opt/pbis/bin/lwsm set-log-target lsass lsass-ipc file /tmp/lsass-ipc.log
```

## Change the Log Level

To change the level of logging in the default facility of **lsass** to debug:

```
/opt/pbis/bin/lwsm set-log-level lsass - debug
```

The supported log levels are:

- **always**
- **error**
- **warning**
- **info**
- **verbose**
- **debug**
- **trace**

Changing the log level temporarily can help you isolate and capture information when a command or operation fails. For example, if you run a command and it fails, you can change the log level and then run the command again to get information about the failure.

## View Log Settings

To view the current level and target of logging of a service, enter the following command:

```
/opt/pbis/bin/lwsm get-log <service>
```

For example, entering the following command

```
/opt/pbis/bin/lwsm get-log lsass
```

produces the following result

```
<default>: syslog LOG_DAEMON at ERROR
```

This indicates that the **lsass** service's default log level is **error** and is directed to syslog's daemon facility.

## Generate a Domain-Join Log for AD Bridge

To help troubleshoot problems with joining a domain, you can use the command-line utility's **logfile** option with the **join** command. The **logfile** option captures information about the attempt to join the domain on the screen or in a file. When an attempt to join a domain fails, a log is generated by default at **/var/log/domainjoin-cli.log** or **/var/adm/domainjoin-cli.log**.

To display the information in the terminal, execute the following command; the dot after the **logfile** option denotes that the information is to be shown in the console:

```
domainjoin-cli --logfile . join domainName userName
```

To save the information in a log file, execute the following command:

```
domainjoin-cli --logfile path join domainName userName
```



**Example:**

```
domainjoin-cli --logfile /var/log/domainjoin.log join example.com Administrator
```

## Generate a PAM Debug Log for AD Bridge

You can set the level of reporting in the PAM debug log for the AD Bridge authentication service on a Linux or Unix computer. PAM stands for pluggable authentication modules.

The log levels are:

- **disabled**
- **error**
- **warning**
- **info**
- **verbose**

The logged data is sent to your system's syslog message repository for security and authentication. The location of the repository varies by operating system.

Here are the typical locations for a few platforms:

- Ubuntu: **/var/log/auth.log**
- Red Hat: **/var/log/secure**
- Solaris: Check the **syslog.conf** file or **rsyslog.conf** file

The following procedure demonstrates how to change the value of the PAM key's **LogLevel** entry with the **config** command-line utility.

1. Use the **details** option to list the values that the **PAMLogLevel** setting accepts:

```
/opt/pbis/bin/config --details PAMLogLevel
Name: PAMLogLevel
Description: Configure PAM lsass logging detail level
Type: string
Current Value: "disabled"
Acceptable Value: "disabled"
Acceptable Value: "error"
Acceptable Value: "warning"
Acceptable Value: "info"
Acceptable Value: "verbose"
Current Value is determined by local policy.
```

2. As root change the setting to **error** so that AD Bridge will log PAM errors:

```
/opt/pbis/bin/config PAMLogLevel error
```

3. Confirm that the change took effect:

```
/opt/pbis/bin/config --show PAMLogLevel
string
error
local policy
```

For more information on the arguments of **config**, run the following command:

```
/opt/pbis/bin/config --help
```

## Generate a Network Trace in a Session

Execute the following command in a separate session to dump network traffic as the root user and interrupt the trace with **CTRL-C**:

```
tcpdump -s 0 -i eth0 -w trace.pcap
```

The result should look something like this:

```
tcpdump: listening on eth0
28 packets received by filter
0 packets dropped by kernel
```

## Generate Log Service Startup Failures

Generate debug logging when the service manager (**lwsmd**) or registry service (**lwreg**) do not start properly.

1. Define and export the **PBIS\_DEBUG\_BOOTSTRAP** environment variable:

```
export PBIS_DEBUG_BOOTSTRAP=1
```

2. To ensure the service manager sees the defined environment variable, manually start the service manager as other mechanisms for starting **lwsmd** may not pass on the defined environment variable.

```
/opt/pbis/sbin/lwsmd --start-as-daemon
```

3. To stop debugging unset the **PBIS\_DEBUG\_BOOTSTRAP** variable:

```
/opt/pbis/bin/lwsm shutdown
unset PBIS_DEBUG_BOOTSTRAP
/opt/pbis/sbin/lwsmd --start-as-daemon
```

## Perform Basic Troubleshooting for the AD Bridge Agent

The following are basic steps for troubleshooting issues related to the AD Bridge agent.

### Check the Version and Build Number

You can check the version and build number of the AD Bridge agent from computers that are running Linux or Unix, or from a computer that is connected to the domain controller and is running Windows.

#### Check From Linux or Unix

To check the version number of the AD Bridge agent from a computer running Linux or Unix, execute the following command:

```
cat /opt/pbis/data/ENTERPRISE_VERSION
```

Another option is to execute the following command:

```
/opt/pbis/bin/get-status
```

#### Check the Build Number of the Agent

On Linux distributions that support RPM, for example, Red Hat Enterprise Linux, Fedora, SUSE Linux Enterprise, OpenSUSE, and CentOS, you can determine the version and build number of the agent (10.1.0.xxxx in the examples below) by executing the following command at the shell prompt:

```
rpm -qa | grep pbis
```

The result shows the build version after the version number:

```
pbis-enterprise-10.1.0-881.x86_64
```

On Unix computers and Linux distributions that do not support RPM, the command to check the build number varies by platform:

Platform	Command
Debian and Ubuntu	dpkg -S /opt/pbis/
Solaris	pkginfo   grep -i pbis
AIX	lslpp -l   grep pbis

#### Check From Windows

To check the version and build number of the AD Bridge agent from a Windows administration workstation that is connected to your domain controller:

In Active Directory Users and Computers, right-click the Linux or Unix computer that you want, and then click **Properties**.

Click the **Operating System** tab. The build number is shown in the Service pack box.

## Determine a Computer's FQDN

You can determine the fully qualified domain name of a computer running Linux or Unix by executing the following command at the shell prompt:

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

### On Solaris

On Sun Solaris, you can find the FQDN by executing the following command (the computer's configuration can affect the results):

```
FQDN=`/usr/lib/mail/sh/check-hostname|cut -d" " -f7`;echo $FQDN
```



For more information, see [Join Active Directory Without Changing /etc/hosts in the AD Bridge Installation Guide](#), at [www.beyondtrust.com/docs/ad-bridge/getting-started/installation](http://www.beyondtrust.com/docs/ad-bridge/getting-started/installation).

## Make Sure Outbound Ports are Open

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



**Note:** The AD Bridge agent is a client only; 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
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
```

## Check the File Permissions of nsswitch.conf

For AD Bridge to work correctly, the `/etc/nsswitch.conf` file must be readable by user, group, and world. The following symptoms indicate that you should check the permissions of `nsswitch.conf`:

- Running the `id` command with an AD account as the argument (for example, `id example.com\kathy`) works when it is executed as root, but when the same command is executed by the AD user, it returns only a UID and GID without a name.
- You receive an *I have no name!* or *intruder alert* error message for non-root users.

## Configure SSH After Upgrading it

After SSH is upgraded, run the following command as root to make sure that the `sshd_config` file is set up properly to work with AD Bridge:

```
domainjoin-cli configure --enable ssh
```

## Upgrade an Operating System

After upgrading an operating system or installing a kernel patch, you should rerun the domain-join command to:

- Make sure that the files related to the operating system, such as PAM and nsswitch, are configured properly to work with AD Bridge.
- Update the `operatingSystemVersion` value and the `operatingSystemServicePack` value in Active Directory so the AD Bridge reporting tool reflects the correct version numbers.

Another suggestion, nearly universal in scope, is to apply updates to test systems before you apply updates to production systems, giving you the opportunity to identify and resolve potential issues before they can affect production machines.

## Troubleshoot Accounts and Attributes

The following topics provide help with troubleshooting account issues.

- ["Allow Access to Account Attributes" on page 24](#)
- ["User Settings Are Not Displayed in ADUC" on page 25](#)
- ["Enable Logging for ADUC Plugin" on page 27](#)
- ["Resolve an AD Alias Conflict with a Local Account" on page 27](#)
- ["Fix the Shell and Home Directory Paths" on page 28](#)
- ["Troubleshoot with the get-status Command" on page 28](#)
- ["Troubleshoot User Rights with Ldp.exe and Group Policy Modeling" on page 30](#)
- ["Fix Selective Authentication in a Trusted Domain" on page 32](#)

### Allow Access to Account Attributes

AD Bridge is compatible with Small Business Server 2003. However, because the server locks down several user account values by default, you must create a group in Active Directory for your Unix computers, add each AD Bridge client computer to it, and configure the group to read all user information.

On other versions of Windows Server, the user account values are available by default. If, however, you use an AD security setting to lock them down, they will be unavailable to the AD Bridge agent.

To find Unix account information, the AD Bridge agent requires that the AD computer account for the machine running AD Bridge can access the attributes in the following table.

Attribute	Requirement
<b>uid</b>	Required when you use AD Bridge in schema mode.
<b>uidNumber</b>	Required when you use AD Bridge in schema mode.
<b>gidNumber</b>	Required when you use AD Bridge in schema mode.
<b>userAccountControl</b>	Required for Directory Integrated mode and Schemaless mode. It is also required for unprovisioned mode, which means that you have not created an AD Bridge Cell in Active Directory.

To allow access to account attributes:

1. In Active Directory Users and Computers, create a group named **Unix Computers**.
2. Add each AD Bridge client computer to the group.
3. In the console tree, right-click the domain, choose **Delegate Control**, click **Next**, click **Add**, and then enter the group named **Unix Computers**.
4. Click **Next**, select **Delegate the following common tasks**, and then in the list select **Read all user information**.
5. Click **Next**, and then click **Finish**.
6. On the target Linux or Unix computer, restart the AD Bridge agent to reinitialize the computer account's logon to Active Directory and to get the new information about group membership.
7. Run `/opt/pbis/enum-users` to verify that you can read user information.

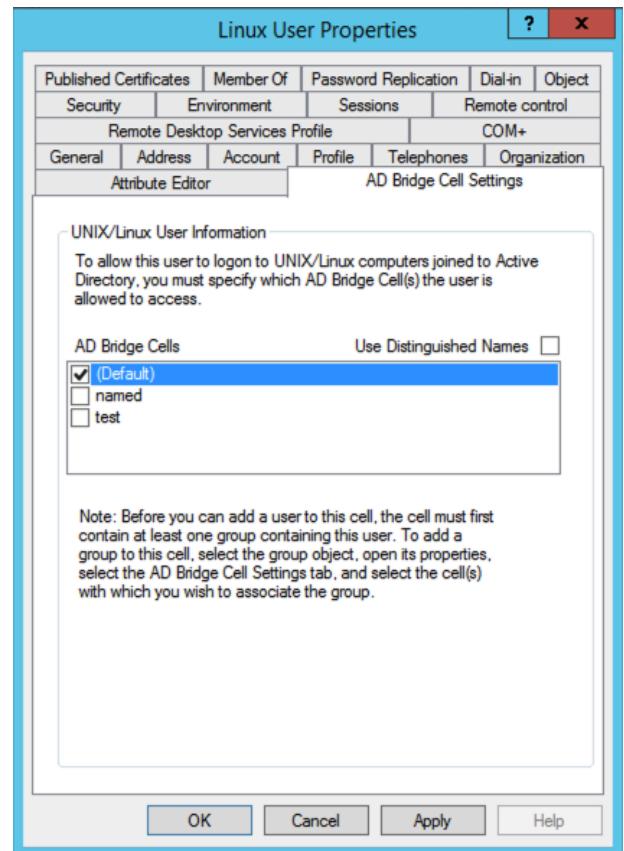


For more information, see *Storage Modes in the AD Bridge Installation Guide* at [www.beyondtrust.com/docs/ad-bridge/getting-started/installation](http://www.beyondtrust.com/docs/ad-bridge/getting-started/installation).

## User Settings Are Not Displayed in ADUC

If there is no group in a cell that can serve as the user's primary GID, for instance, because the default primary group, domain users, has been removed from the cell, the **AD Bridge Cell Settings** tab for a user in **Active Directory Users and Computers (ADUC)** will not display the user or group settings, as shown in the screen shot below.

To display the settings, enable a group that the user is a member of.

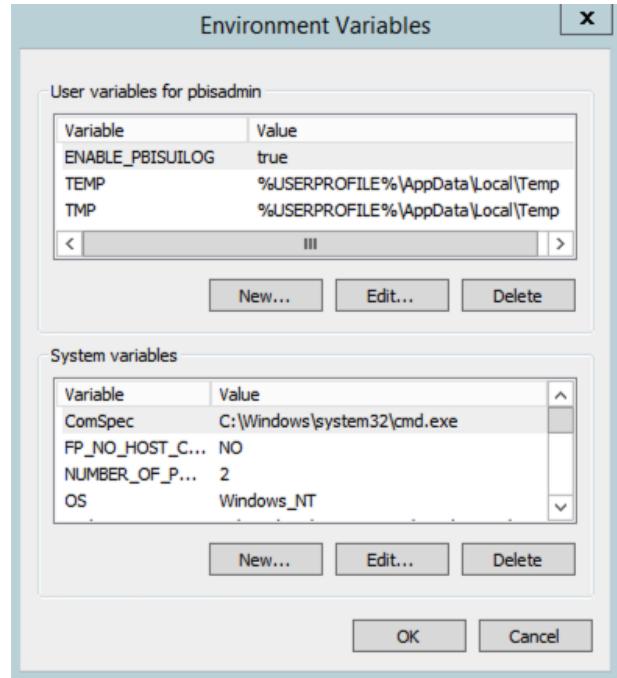


## Enable Logging for ADUC Plugin

Log files can be generated to troubleshoot issues with the ADUC **AD Bridge Cell Settings** tab.

By default, there is no log file generated unless the following environment variable is set: **ENABLE\_PBISUILOG=true**

Set the variable in **Control Panel > System > Advanced System Settings > Advanced > Environment Variables**.



After the setting is turned on, log files are generated the next time ADUC starts. Logs are saved in the C:\Users\username\AppData\Local\PBIS.Logs directory. The plugin displays a dialog box containing the log file path when it opens the log file.

## Resolve an AD Alias Conflict with a Local Account

When you use AD Bridge to set an Active Directory alias for a user, the user can have a file-ownership conflict under the following conditions if the user logs on with the AD account:

- The AD alias is the same alias as the original local account name.
- The home directory assigned to the user in Active Directory is the same as the local user's home directory.
- The owner UID-GID of the AD account is different from that of the local account.

To avoid such conflicts, by default AD Bridge includes the short AD domain name in each user's home directory. If the conflict nevertheless occurs, there are two options to resolve it:

- Make sure that the UID assigned to the user's AD alias is the same as that of the user's local account.
- Log on as root and use the **chown** command to recursively change the ownership of the local account's resources to the AD user alias.

## Change Ownership

Log on the computer as root and execute the following commands:

```
cd <users home directory root>
chown -R <AD user UID>:<AD primary group ID> *.*
```

Alternatively, the following command may be used:

```
chown -R <short domain name>\<account name>:<short domain name>\<AD group name> *.*
```



*Tip: You can generate reports to help identify duplicates and inconsistencies.*

## Fix the Shell and Home Directory Paths

**Symptom:** A local directory is in the home directory path and the home directory path does not match the path specified in Active Directory or in `/etc/passwd`.

**Example:** `/home/local/DOMAIN/USER` instead of `/home/DOMAIN/USER`

The shell might also be different from what is set in Active Directory, for example, `/bin/ksh` instead of `/bin/bash`.

**Problem:** The computer is not in an AD Bridge Cell in Active Directory.

**Solution:** Make sure the computer is in a AD Bridge Cell.



*For more information, please refer to the [AD Bridge Administration Guide](#) at [www.beyondtrust.com/docs/ad-bridge/getting-started](http://www.beyondtrust.com/docs/ad-bridge/getting-started).*

A Default Cell handles mapping for computers that are not in an OU with an associated cell. The Default Cell can contain the mapping information for all your Linux and Unix computers. For instance, a Linux or Unix computer can be a member of an OU that does not have a cell associated with it. In such a case, the home directory and shell settings are obtained from the nearest parent cell or the Default Cell. If there is no parent cell and no Default Cell, the computer will not receive its shell and home directory paths from Active Directory.

## Troubleshoot with the get-status Command

The `/opt/pbis/bin/get-status` command shows whether the domain or the AD Bridge AD provider is offline. The results of the command include information useful for general troubleshooting.

```
/opt/pbis/bin/get-status
```



*Example: Here is an example of the information the command returns:*

```
[root@rhel5d bin]# /opt/pbis/bin/get-status
LSA Server Status:
Compiled daemon version: 6.1.272.54796
```



Packaged product version: 6.1.272.54796  
Uptime: 15 days 21 hours 24 minutes 1 seconds

[Authentication provider: lsa-activedirectory-provider]

Status: Online  
Mode: Un-provisioned  
Domain: EXAMPLE.COM  
Forest: example.com  
Site: Default-First-Site-Name  
Online check interval: 300 seconds  
[Trusted Domains: 1]

[Domain: EXAMPLE]

DNS Domain: example.com  
Netbios name: EXAMPLE  
Forest name: example.com  
Trustee DNS name:  
Client site name: Default-First-Site-Name  
Domain SID: S-1-5-21-3190566242-1409930201-3490955248  
Domain GUID: 71c19eb5-1835-f345-ba15-0595fb5b62e3  
Trust Flags: [0x000d]  
[0x0001 - In forest]  
[0x0004 - Tree root]  
[0x0008 - Primary]  
Trust type: Up Level  
Trust Attributes: [0x0000]  
Trust Direction: Primary Domain  
Trust Mode: In my forest Trust (MFT)  
Domain flags: [0x0001]  
[0x0001 - Primary]

[Domain Controller (DC) Information]

DC Name: w2k3-r2.example.com  
DC Address: 192.168.92.20  
DC Site: Default-First-Site-Name  
DC Flags: [0x000003fd]  
DC Is PDC: yes  
DC is time server: yes  
DC has writeable DS: yes  
DC is Global Catalog: yes  
DC is running KDC: yes

[Authentication provider: lsa-local-provider]

Status: Online  
Mode: Local system  
Domain: RHEL5D

## Troubleshoot User Rights with Ldp.exe and Group Policy Modeling

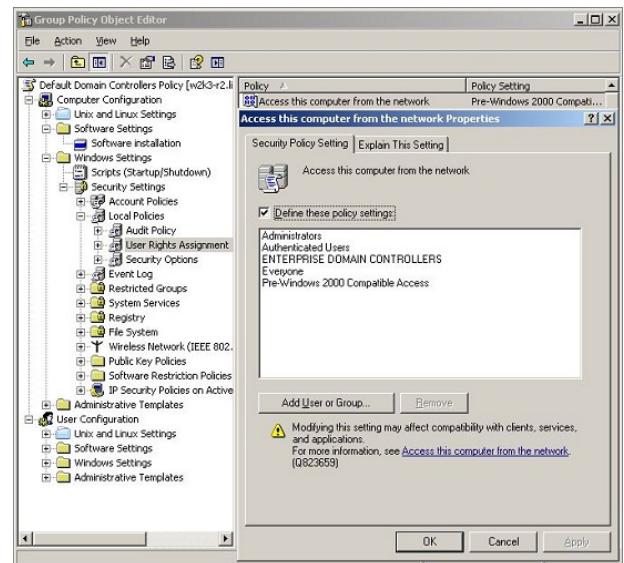
The following Microsoft default domain policy and default domain controller policy can cause an AD Bridge client to fail to join a domain or to fail to enumerate trusts:

- Access this computer from the network:** Users and computers that interact with remote domain controllers require the **Access this computer from the network** user right. Users, computers, and service accounts can lose the user right by being removed from a security group that has been granted the right. Removing the administrators group or the authenticated users group from the policy setting can cause domain join to fail. According to Microsoft, *There is no valid reason for removing Enterprise Domain Controllers group from this user right.*

 For more information, see [Microsoft article 823659](https://support.microsoft.com/en-us/help/823659), at <https://support.microsoft.com/en-us/help/823659>.

- Deny access to this computer from the network:** Including the domain computers group in the policy setting, for instance, causes domain-join to fail.

 For more information, see [Microsoft article cc758316](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc758316(v=ws.10)) at [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc758316\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc758316(v=ws.10)).



The symptoms of a user-right problem can include the following:

- An attempt to join the domain is unsuccessful.
- The AD Bridge authentication service, **lsass**, does not start.
- The **/opt/pbis/bin/get-status** command shows the domain or the AD provider as offline.

You can pin down the issue by using the **Ldp.exe** tool to check whether you can access AD by using the machine account and machine password. **Ldp.exe** is typically included in the support tools (**suptools.msi**) for Windows and located on the Windows installation CD (Support folder, Tools subfolder). You might also be able to download the support tools that contain **Ldp.exe** from the Microsoft website.

 For more information, see [Ldp Overview](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc772839(v=ws.10)), at [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc772839\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc772839(v=ws.10)).

To resolve a user-right issue, you can use Group Policy Modeling in the **Group Policy Management Console (GPMC)** to find the offending policy setting and then modify it with the **Group Policy Management Editor** (or the **Group Policy Object Editor**).



For more information, see [Group Policy Modeling](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc781242(v=ws.10)), at [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc781242\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc781242(v=ws.10)).

- On the AD Bridge client, run the **/opt/pbis/bin/lsa ad-get-machine password** command as root to get the machine password stored in Active Directory:

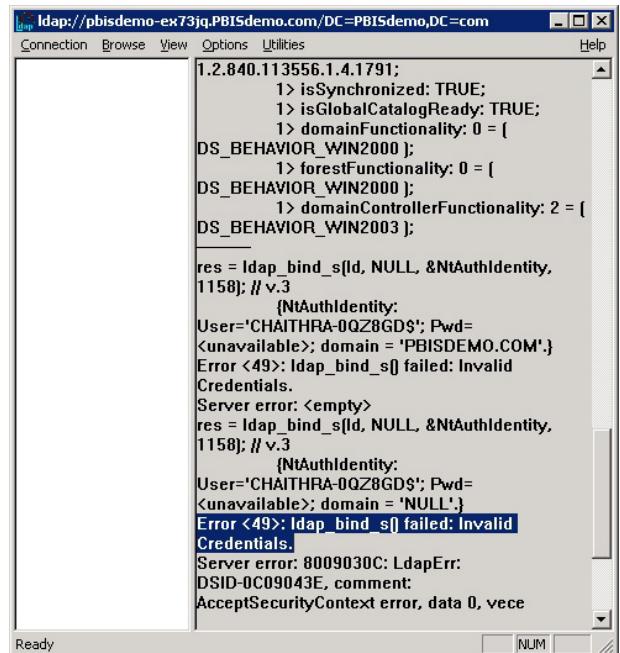
```
/opt/pbis/bin/lsa ad-get-machine password
Machine Password Info:
  DNS Domain Name: EXAMPLE.COM
  NetBIOS Domain Name: EXAMPLE
  Domain SID: S-1-5-21-3190566242-1409930201-3490955248
  SAM Account Name:
RHEL5D$
  FQDN: rhel5d.example.com
  Join Type: 1
  Key Version: 0
  Last Change Time: 129401233790000000
  Password: i(2H2e41F7tHN275
```

- On a Windows administrative workstation that can connect to AD, start **ldp.exe** and connect to the domain.



For more information, see [LDP UI](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc756988(v=ws.10)), at [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc756988\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc756988(v=ws.10)).

- In LDP, on the **Connection** menu, click **Bind**, and then use the AD Bridge client's SAM account name and machine password from the output of the **lsa ad-get-machine password** command to bind to the directory.
- If the attempt to bind with the machine account and the machine password fails because of invalid credentials, as in the LDP output image shown, go to the GPMC and use **Group Policy Modeling** to try to identify the policy setting causing the problem.



- In the **GPMC**, run **Group Policy Modeling** to pinpoint the offending policy setting and then modify the policy setting to grant the correct level of user right to the computer or user.

**i** For more information, see [Group Policy Modeling](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc781242(v=ws.10)), at [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc781242\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc781242(v=ws.10)).

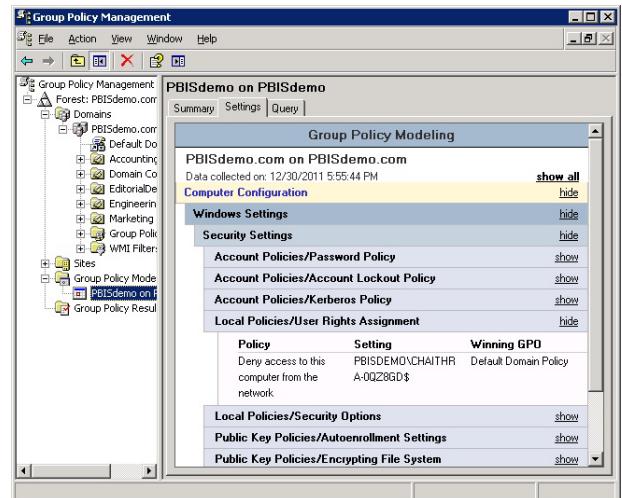
In the screen shot, for example, the cause of the problem is that the **Deny access to this computer from the network** policy setting in the Default Domain Policy GPO contains the domain computers group.

## Fix Selective Authentication in a Trusted Domain

When you turn on selective authentication for a trusted domain, AD Bridge can fail to look up users in the trusted domain because the machine account is not allowed to authenticate with the domain controllers in the trusted domain. Here is how to grant the machine account access to the trusted domain:

- In the domain the computer is joined to, create a global group and add the computer's machine account to the group.
- In the trusted domain, in **Active Directory Users and Computers**, select the **Domain Controllers** container and open **Properties**.
- On the **Security** tab, click **Advanced**, click **Add**, enter the global group, and then click **OK**.
- In the **Permission Entry** box, under **Apply onto**, check **Computer objects**. Under **Permissions**, find **Allowed to Authenticate** and check it. Click **OK** and then click **Apply** in the **Advanced Security Settings** box.
- If you have already joined the AD Bridge client computer to the domain, restart the AD Bridge authentication service:

```
/opt/pbis/bin/lwsm restart lsass
```



**i** For more information, see [Configuring Selective Authentication Settings](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc755844(v=ws.10)), at [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc755844\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc755844(v=ws.10)).

## Troubleshoot the AD Bridge Cache

If a cache becomes corrupted or if certain conditions occur, you may need to clear caches.

### Clear the Authentication Cache

There are certain conditions under which you might need to clear the cache so that a user's ID is recognized on a target computer.

By default, the user's ID is cached for 4 hours. If you change a user's UID for an AD Bridge Cell with AD Bridge, during the 4 hours after you change the UID you must clear the cache on a target computer in the cell before the user can log on. If you do not clear the cache after changing the UID, the computer will find the old UID until the cache expires.

One AD Bridge Group Policy setting can affect the cache time: Cache Expiration Time. This policy setting stores UID-SID mappings, user and group enumeration lists, **getgrnam()**, and **getpwnam()**. Its default expiration time is 4 hours.



For more information about this policy setting, see the [AD Bridge Group Policy Reference Guide](#) at [www.beyondtrust.com/docs/ad-bridge/how-to/group-policy](http://www.beyondtrust.com/docs/ad-bridge/how-to/group-policy).



**Tip:** While you are deploying and testing AD Bridge, set the cache expiration time of the AD Bridge agent's cache to a short period of time, such as 1 minute.

## Clear the Cache on a Unix or Linux Computer

To delete all the users and groups from the AD Bridge AD provider cache on a Linux or Unix computer, execute the following command with superuser privileges:

```
/opt/pbis/bin/ad-cache --delete-all
```

You can also use the command to enumerate users in the cache, which may be helpful in troubleshooting.



### Example:

```
[root@rhel5d bin]# ./ad-cache --enum-users
TotalNumUsersFound:      0
[root@rhel5d bin]# ssh example.com\\hab@localhost
Password:
Last login: Tue Aug 11 15:30:05 2009 from rhel5d.example.com
[EXAMPLE\hab@rhel5d ~]$ exit
logout
Connection to localhost closed.
[root@rhel5d bin]# ./ad-cache --enum-users
User info (Level-0):
=====
Name:      EXAMPLE\hab
Uid:       593495196
Gid:       593494529
Gecos:     <null>Shell:    /bin/bash
Home dir:  /home/EXAMPLE/hab
TotalNumUsersFound:      1
[root@rhel5d bin]#
```

To view the command's syntax and arguments, execute the following command:

```
/opt/pbis/bin/ad-cache --help
```

## Clear a Corrupted SQLite Cache

To clear the cache when AD Bridge is caching credentials in its SQLite database and the entries in the cache are corrupted, use the following procedure for your type of operating system.

## Clear the SQLite cache:

1. Stop the AD Bridge authentication service by executing the following command as root: `/opt/pbis/bin/lwsm stop lsass`.
2. Clear the AD-provider cache and the local-provider cache by removing the following two files, substituting a fully-qualified domain name for **FQDN**:
  - `rm -f /var/lib/pbis/db/lsass-adcache.filedb.FQDN`  
`rm -f /var/lib/pbis/db/lsass-local.db`



### IMPORTANT!

*Do not delete the other .db files in the /var/lib/pbis/db directory.*

3. Start the AD Bridge authentication service: `/opt/pbis/bin/lwsm start lsass`.

## Pluggable Authentication Modules (PAM)



*For instructions on how to generate a PAM debug log, see ["Generate a PAM Debug Log for AD Bridge" on page 20](#).*

### PAM Configuration Changes on an Upgrade

The following configuration changes occur automatically during an AD Bridge upgrade.

At the start of the AD Bridge upgrade, if the machine is joined to a domain, both the PAM and nsswitch modules are unconfigured. This allows for a safe upgrade in the event the upgrade fails. Access to the machine is still possible.

Commands to unconfigure modules:

```
/opt/pbis/bin/domainjoin-cli configure --disable pam
```

```
/opt/pbis/bin/domainjoin-cli configure --disable nsswitch
```

Toward the end of the AD Bridge upgrade, if the machine is joined to a domain, both the PAM and nsswitch modules are configured again to restore functionality.

Commands to configure modules:

```
/opt/pbis/bin/domainjoin-cli configure --enable pam
```

```
/opt/pbis/bin/domainjoin-cli configure --enable nsswitch
```

## Troubleshoot PAM Error

### Warning: Unknown PAM configuration

The PAM module cannot be configured for the <MODULE> service. Either this service is unprotected (does not require a valid password for access), or it is using a PAM module that this program is unfamiliar with. Please email technical support and include a copy of `/etc/pam.conf` or `/etc/pam.d`.

#### Cause

During the PAM configuration phase of the domainjoin process there is an unknown PAM module that AD Bridge does not recognize. If this is a resumable error then this is not in a critical area and the lsass module is not added to that file. This can still cause issues on later upgrades.

#### Resolution

There are a few ways to address this issue:

- Remove the unknown module and re-add the module after the domainjoin. This can still present itself as an issue on later upgrades.
- Use `--ignore-pam` and manually add lsass into your PAM files. We do not recommend this unless you have a strong understanding of PAM.
- Remove the need for the unknown module from PAM entirely.
- Submit a request for the module to be supported by AD Bridge.

## Dismiss the Network Credentials Required Message

After leaving the screen saver on a Gnome desktop that is running the Gnome Display Manager, or GDM, you might see a pop-up notification saying that network authentication is required or that network credentials are required. You can ignore the notification. The GDM process that tracks the expiration time of a Kerberos TGT might not recognize the updated expiration time of a Kerberos TGT after it is refreshed by AD Bridge.

## Perform OS-Specific Troubleshooting

The following topics provide AD Bridge agent troubleshooting guidance that is unique to individual operating systems.

### Red Hat and CentOS

The following procedures may help resolve issues with the AD Bridge agent on computers running the Red Hat or CentOS operating systems.

#### Modify PAM to Handle UIDs Less than 500

By default, the configuration file for PAM system authentication, `/etc/pam.d/system-auth`, on Red Hat Enterprise Linux 5 and CentOS 5 contains the following line, which blocks a user with a UID value less than or equal to 500 from logging on to a computer running the AD

Bridge agent. The symptom is a login failure with a never-ending password prompt.

```
auth requisite pam_succeed_if.so uid >= 500 quiet
```

Solution: Either delete the line from **/etc/pam.d/system-auth** or modify it to allow users with UIDs lower than 500:

```
auth requisite pam_succeed_if.so uid >= 50 quiet
```

## Ensure That the Correct Version of the coreutils RPM Is Installed

Some patch levels of the **coreutils** RPM on Red Hat Enterprise Linux 3 have a version of the **id** command that does not return complete group membership information when the command is run with the **id username** syntax. The command returns only the UID and primary GID for a user. Secondary groups may be omitted.

On Linux, there are four commands to get group memberships:

- Call **getgroups**. It returns the primary and secondary GIDs of the current process. The **id** command calls this when a username is not passed.
- Call **initgroups** followed by **getgroups**. The **initgroups** call will query **nsswitch** for the users primary and secondary groups. The result is stored in the process, which is then returned by **getgroups**. You need root access to call **initgroups**, so **id** sometimes does this when you run the command as root.
- Call **getgrouplist**. This function calls **nsswitch** to return the group list of a user, and it does not require root access. Unfortunately this function was added in glibc 2.2.4, and the **id** command started using it after that.
- Call **getrent** to enumerate all the groups on the system, and search for the user in the **gr\_mem** field.

On RHEL 3, **id** from **coreutils** version 4.5.3-28.4 can use the **getgrouplist** function, but that code was removed in 4.5.3-28.7. To check your **coreutils** version for **glibc**:

```
rpm -q coreutils glibc coreutils-4.5.3-28.7 glibc-2.3.2-95.50
```

Without the **getgrouplist** function, the **id** command falls back on using **getrent** to get the groups. By default, AD Bridge returns abbreviated results when enumerating all groups, so **id** does not find the user in the member's field. You could turn on full group enumeration, but then the **id** command would download the group membership of everyone in Active Directory just to obtain the results for one user.



### Example:

1. Check the user.

```
[root@example-03293b root]# su - corpqa\\user0001
[CORPQA\user0001@example-03293b user0001]$ id CORPQA\\user0002
uid=105559(CORPQA\user0002) gid=1661993473(CORPQA\domain^users) groups=1661993473
(CORPQA\domain^users)
[CORPQA\user0001@example-03293b user0001]$ logout
```

2. Turn on full group enumeration locally by using **config**.



```
[root@example-03293b root]# /opt/pbis/bin/config NSSGroupMembersQueryCacheOnly  
false  
[root@example-03293b root]# /opt/pbis/bin/config NSSEnumerationEnabled true
```

### 3. Check the user again:

```
[root@example-03293b root]# su - corpqa\user0001  
[CORPQA\user0001@example-03293b user0001]$ id CORPQA\user0002  
uid=105559(CORPQA\user0002) gid=1661993473(CORPQA\domain^users)  
groups=1661993473(CORPQA\domain^users),1662020290(CORPQA\enabled),  
1662020291(CORPQA\enabledparent),100395(CORPQA\innergroup1),  
100401(CORPQA\loopgroup),100394(CORPQA\outergroup),  
100381(CORPQA\usergroup0001),100382(CORPQA\usergroup0002),  
1662002383(CORPQA\usergroup0009),1662002420(CORPQA\usergroup0047),  
1662003573(CORPQA\usergroup0200)
```

Even with NSS settings enabled, the **id** command does a case-sensitive search even though AD Bridge does not treat the usernames as case sensitive. Therefore, if you use the non-canonical case, the groups are not displayed.

To fix the output of the **id** command on RHEL 3 computers where this problem occurs, ensure that the correct version of the **coreutils** RPM is installed.

## Ubuntu

Try the following to resolve issues with the AD Bridge agent on computers running Ubuntu.

```
su segfaults
```

## SUSE Linux Enterprise Desktop (SLED)

Review the following sections to fix SUSE issues.

### Home Directory on SLED 11

When a user gains access to SLED 11 through Nomad, a remote desktop using RDP protocol with session management, the default home directory specified in **/lib/security/pam\_lsass.so** is ignored.

To correct the issue, change **/etc/pam.d/xrdp-sesman** to include the following line:

```
session sufficient /lib/security/pam_lsass.so
```

### Update PAM on SLED 11

Novell has issued a PAM update (**pam-config-0.68-1.22**) for SLED 11 that modifies the **common-session-pc** file to include the following entry:

```
session optional pam_gnome_keyring.so auto_start_if=gdm
```

Because the PAM update makes a backup of the file and replaces it with the modified version, the changes that AD Bridge had made to the file are no longer present, which blocks new AD users from logging on. The similar error message may appear:

```
Could not update ICEauthority file /home/john/.ICEauthority  
There is a problem with the configuration server.  
(/user/lib/gconf/2/gconf-sanity-check-2 exited with status 256)
```

Solution: After you update PAM, run the following command as root:

```
/opt/pbis/bin/domainjoin-cli configure --enable pam
```

Or, you can make the changes manually. Open the backed up version of the **common-session-pc** file, add the following line to it, and then use it to overwrite the new version of the **common-session-pc** file:

```
session optional      pam_gnome_keyring.so      auto_start_if=gdm
```

## AIX

Try the following to resolve issues with the AD Bridge agent on computers running AIX.

### Increase Max Username Length on AIX

By default, AIX is not configured to support long user and group names, which might present a conflict when you try to log on with a long Active Directory username. On AIX 5.3 and AIX 6.1, the symptom is that group names, when enumerated through the **groups** command, are truncated.

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

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



**Example:**

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

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

The safest value to which you can set **max\_logname** is **255**.

You must reboot for the changes to take effect:

```
# shutdown -Fr
```



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

## Updating AIX

When you update AIX, the authentication of users, groups, and computers might fail because the AIX upgrade process overwrites changes that AD Bridge makes to system files. Specifically, upgrading AIX to version 6.1tl3 overwrites **/lib/security/methods.cfg**, so you must manually add the following code to the last lines of the file after you finish upgrading:

```
LSASS:  
program = /usr/lib/security/LSASS
```

## Not Supported on AIX

The following features are not supported on AIX platforms: **user-ignore**, **user-override**, **group-ignore**, and **group-override**.

## FreeBSD

Try the following to resolve issues with the AD Bridge agent on computers running FreeBSD.

### Keep Usernames to 16 Characters or Less

On FreeBSD, user names that are longer than 16 characters, including the domain name, exceed the FreeBSD username length limit. Attempts to connect by **ssh**, for example, to a FreeBSD computer with a user name that exceeds the limit can result in the following notification:

```
bvt-fbs72-64# ssh testuser1@localhost  
Password:  
Connection to localhost closed by remote host.  
Connection to localhost closed.
```

The log for **sshd**, meanwhile, might show an error that looks something like this:

```
Oct  7 18:22:57 vermont02 sshd[66387]: setlogin(EXAMPLE\adm.kathy):  
Invalid argument  
Oct  7 18:25:02 vermont02 sshd[66521]: setlogin(EXAMPLE\adm.kathy):  
Invalid argument
```

Although **testuser1** is less than 16 characters, when you use the **id** command to check the account, something longer than 16 characters is returned:

```
[root@bvt-fbs72-64 /home/testuser]# id testuser1  
uid=1100(BVT-FBS72-64\testuser1) gid=1801(BVT-FBS72-64\testgrp)  
groups=1801(BVT-FBS72-64\testgrp)
```

The result of the **id** command exceeds the FreeBSD username length limit.

There are several solutions: set the default domain, change the user name to 16 characters or less, or with AD Bridge use aliases. Keep in mind, though, that aliases will not solve the problem in relation to the AD Bridge local provider.

## Solaris

Try the following to resolve issues with the AD Bridge agent on computers running Solaris.

### Turn On Core Dumps on Solaris 10

If you are investigating a process that is crashing on Solaris 10 or Solaris Sparc 10, but a core dump is not being generated, it's probably because per-process core dumps are turned off. You can use the **coreadm** command to manage the core dumps. The settings are saved in the **/etc/coreadm.conf** file.

A configuration for core dumps with the per-process option turned off looks like this:

```
# coreadm
  global core file pattern:
  global core file content: default
    init core file pattern: core
    init core file content: default
      global core dumps: disabled
      per-process core dumps: disabled
      global setid core dumps: disabled
    per-process setid core dumps: disabled
      global core dump logging: disabled
```

You need per-process core dumps to troubleshoot a process that is terminating unexpectedly. To turn on core dumps for a process, execute the following command as root:

```
coreadm -e process
```



For more information, see [Core Dump Management on the Solaris OS](https://www.oracle.com/solaris/technologies/core-dump-management.html) at <https://www.oracle.com/solaris/technologies/core-dump-management.html> and the man page for **coreadm**.

## Troubleshoot Logon Issues with Systems

### Solve Logon Problems from Windows

To troubleshoot a problem with a user who cannot log on a to Linux or Unix computer, perform the following series of diagnostic tests sequentially.

- On a Windows computer, log off and then log on again with the problem user's AD credentials to verify that the password is correct and that the account is not locked or disabled.
- Try to SSH to the target Linux or Unix computer again with the user's full NT4-style credentials and password, not just the user's alias. In your SSH command, make sure to use a slash character to escape the slash.
- If you are using AD Bridge, make sure that the user's computer is in the correct AD Bridge Cell.
- Make sure that the user is enabled to log on the computer, either by being enabled in the cell (with AD Bridge) or by being in a group allowed to access the computer. Then try to log on the target computer again.
- Ensure that the AD Bridge client can communicate with the Active Directory domain controller.
- Make sure that the shell specified for the user account in Active Directory is available on the target computer. Specifying a shell that is unavailable will block the user account from logging on.
- Verify that the home directory is set and can be created. A home directory that cannot be created because the path is incorrect or the permissions are insufficient can block an attempt to log on.
- Make sure there are no logon restrictions in place, for example, the Group Policy setting that restricts logon to certain users or groups, that prevents the user account from logging on the computer.
- Log on the computer with a different user account, and that is enabled for access to the computer.

### Solve Logon Problems on Linux or Unix

To troubleshoot problems logging on a Linux computer with Active Directory credentials after you joined the computer to a domain, perform the following series of diagnostic tests sequentially with a root account.

The tests can also be used to troubleshoot logon problems on a Unix computer. However, the syntax of the commands on Unix might be slightly different.

#### Make Sure You Are Joined to the Domain

Execute the following command:

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

#### Check Whether You Are Using a Valid Logon Form

When troubleshooting a logon problem, use your full domain credentials: **DOMAIN\username**.

Example: **example.com\hoenstiv**

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

Example: **example.com\\hoenstiv**

## Clear the Cache

You may need to clear the cache to ensure that the client computer recognizes the user's ID.



For more information, see the *AD Bridge Installation Guide*.

## Destroy the Kerberos Cache

Clear the *AD Bridge* Kerberos cache to make sure there is not an issue with a user's Kerberos tickets. Execute the following command with the user account that you are troubleshooting:

```
/opt/pbis/bin/kdestroy
```

## Check the Status of the AD Bridge Authentication Service

Check the status of the authentication service on a Unix or Linux computer running the *AD Bridge* Agent by executing the following command as the root user:

```
/opt/pbis/bin/lwsm status lsass
```

If the result looks like this...	Do This
lsass is stopped	Restart the service.
lsass (pid 1783) is running...	Proceed to the next test.

## Check Communication between the AD Bridge Service and AD

Verify that the *AD Bridge* service can exchange data with AD by executing this command:

```
/opt/pbis/bin/get-dc-name FullDomainName
```



**Example:**

```
/opt/pbis/bin/get-dc-name example.com
```

If the result does not show the name and IP address of your domain controller:

1. Make sure the domain controller is online and operational.
2. Check network connectivity between the client and the domain controller.
3. Join the domain again.
4. View log files.

If the result shows the correct domain controller name and IP address, proceed to the next test.

## Verify that AD Bridge Can Find a User in Active Directory

Verify that the *AD Bridge* agent can find your user by executing the following command, substituting the name of a valid AD domain for **domainName** and a valid user for **ADUserName**:

```
/opt/pbis/bin/find-user-by-name domainName \\ ADUserName
```



**Example:**

```
/opt/pbis/bin/find-user-by-name example\\hab
```

If the command fails to find the user:

1. Check whether the computer is joined to the domain by executing the following command as root:

```
domainjoin-cli query
```

This displays the hostname, current domain, and distinguished name, which includes the OU to which the computer belongs. Make sure the OU is correct. If the computer is not joined to a domain, it displays only the hostname.

2. Check Active Directory to make sure the user has an account. If you are using *AD Bridge*, also ensure that the user is associated with the correct cell.
3. Check whether the same user is in the **/etc/passwd** file. If necessary, migrate the user to Active Directory.
4. Make sure the AD authentication provider is running by proceeding to the next test.

If the user is found, proceed to the PAM test later in this topic.

## Make Sure the AD Authentication Provider Is Running

*AD Bridge* includes two authentication providers:

- the local provider
- the Active Directory provider

If the AD provider is not online, users are unable to log on with their AD credentials. To check the status of the authentication providers, execute the following command as root:

```
/opt/pbis/bin/get-status
```

A healthy result should look like this:

```
LSA Server Status:  
  
Compiled daemon version: 10.1.561.63589  
Packaged product version: 10.1.725.63590  
Uptime: 6 days 23 hours 36 minutes 29 seconds
```

```
[Authentication provider: lsa-activedirectory-provider]
```

```
Status:          Online
Mode:           Default Cell
Domain:         EXAMPLE.COM
Domain SID:     S-1-5-21-1234567890-1234567890-1234567890
Forest:         example.com
Site:          Default-First-Site-Name
```

An unhealthy result will not include the AD authentication provider or will indicate that it is offline. If the AD authentication provider is not listed in the results, restart the authentication service.

 For more information, see "[Restart the Authentication Service](#)" on page 15.

If the result looks like the line below, check the status of the *AD Bridge* services to make sure they are running.

```
Failed to query status from LSA service.
The LSASS server is not responding.
```

 For more information, see "[AD Bridge Services and Status](#)" on page 12.

## Run the id Command to Check the User

Run the following **id** command to check whether **nsswitch** is properly configured to handle AD user account information:

```
id DOMAIN\\username
```

 Example:

```
id example\\kathy
```

If the command does not show information for the user, check whether the **/etc/nsswitch.conf** file is properly configured for passwd and group: Both entries should include the **lsass** parameter.

If **/etc/nsswitch.conf** is properly configured, the *AD Bridge* name service libraries might be missing or misplaced. It is also possible that the **LD\_PRELOAD** or **LD\_LIBRARY\_PATH** variables are defined without including the *AD Bridge* libraries.

## Switch User to Check PAM

Verify that a user's password can be validated through PAM by using the switch user service. Either switch from a non-root user to a domain user or from root to a domain user. If you switch from root to a domain user, run the command below twice so that you are prompted for the domain user's password:

```
su DOMAIN\\username
```

**Example:**

```
su example\\hoenstiv
```

If the switch user command fails to validate the user:

- Generate a PAM debug log.



For more information, see ["Generate a PAM Debug Log for AD Bridge" on page 20.](#)

- Also, check the following log files for error messages (the location of the log files varies by operating system):
  - /var/log/messages
  - /var/log/secure

## Test SSH

Check whether you can log on with SSH by executing the following command:

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

**Example:**

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



If you believe the issue might be specific to SSH, see ["Troubleshoot SSH SSO Login Problems" on page 46.](#)

## Run the Authentication Service in Debug Mode

To troubleshoot the lookup of a user or group ID, you can set the *AD Bridge* authentication service to run in debug mode and show the log in the console by executing this command:

```
/opt/pbis/bin/lwsm set-log-level lsass - debug
```

## Check Nsswitch.Conf

Make sure **/etc/nsswitch.conf** is configured correctly to work with *AD Bridge*.



For more information, see [Configuring Clients Before Agent Installation in the AD Bridge Installation Guide.](#)

## Additional Diagnostic Tools

There are additional command-line utilities that you can use to troubleshoot logon problems in the `/opt/pbis/bin` directory:

 For more information, see ["Resolve an AD Alias Conflict with a Local Account" on page 27.](#)

## Red Hat Enterprise Linux 9 Fips Systems

If AD authentication fails, run the following command and then reboot the machine.

```
update-crypto-policies --set FIPS:AD-SUPPORT
```

This will allow AD authentication through the encryption types required by Active Directory.

## Troubleshoot SSH SSO Login Problems

Solve problems logging on with SSH to Linux and Unix computers running AD Bridge.



*Tip: Make sure you are joined to the domain by executing the following command as root:*

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



*If you are not joined, see Join Active Directory with the Command Line in the [AD Bridge Installation Guide](#) at [www.beyondtrust.com/docs/ad-bridge/getting-started/installation](http://www.beyondtrust.com/docs/ad-bridge/getting-started/installation).*

You can use the following steps to troubleshoot problems logging on to Linux and Unix computers with **ssh**. It is assumed that the computer is connected to Microsoft Active Directory with AD Bridge and that you are trying to log on with an Active Directory account.

## Use NT4-style Credentials and Escape the Slash Character

Try to SSH to the target Linux or Unix computer again with the user's full NT4-style credentials, not the user's alias. In your **ssh** command, make sure to use a slash character to escape the slash.



*Example:*

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

## Perform General Logon Troubleshooting



**Note:** If you cannot logon after you escape the slash character in your full NT4-style credentials and use your password, execute the general logon troubleshooting steps in "Troubleshoot Logon Issues with Systems" on page 41 and "Solve Logon Problems on Linux or Unix" on page 41. If those steps do not help solve the problem, return to this page and perform the following AD Bridge-specific **ssh** troubleshooting steps in the order listed.



**Note:** This document contains little general SSH troubleshooting information. If you believe your issue is not specific to AD Bridge or if the information here does not solve your problem, see *SSH: The Secure Shell: The Definitive Guide*, published by O'Reilly. See especially the following sections:

- [Troubleshooting and FAQ](https://docstore.mik.ua/orelly/networking_2ndEd/ssh/ch12_01.htm) at [https://docstore.mik.ua/orelly/networking\\_2ndEd/ssh/ch12\\_01.htm](https://docstore.mik.ua/orelly/networking_2ndEd/ssh/ch12_01.htm)
- [Logging and Debugging](https://docstore.mik.ua/orelly/networking_2ndEd/ssh/ch07_04.htm#ch07-20984) at [https://docstore.mik.ua/orelly/networking\\_2ndEd/ssh/ch07\\_04.htm#ch07-20984](https://docstore.mik.ua/orelly/networking_2ndEd/ssh/ch07_04.htm#ch07-20984)
- [Password Authentication](https://docstore.mik.ua/orelly/networking_2ndEd/ssh/ch12_02.htm#ch12-48295) at [https://docstore.mik.ua/orelly/networking\\_2ndEd/ssh/ch12\\_02.htm#ch12-48295](https://docstore.mik.ua/orelly/networking_2ndEd/ssh/ch12_02.htm#ch12-48295)

## Get an SSH Log

You should obtain debug logs for the AD Bridge authentication service (**lsass**), PAM, and **sshd**.



For more information, see the following:

- ["Generate Debug Logs for AD Bridge Services" on page 17](#)
- ["Generate a PAM Debug Log for AD Bridge" on page 20](#)

To get an **ssh** log, locate **sshd** and then start it in a separate terminal window with the following options:

```
`which sshd` -vvv -p 9999 >/tmp/sshd.log 2>&1
```

The command starts an instance of **sshd** listening on Port 9999 and routes logging information to a log file in **/tmp/sshd.log**.

Now try to **ssh** to the localhost at that port:

```
ssh -ddd -p 9999 yourADUserName@localhost
```

When the logon fails, kill **ssh**; the **sshd** session will stop as well.

Finally, check the log file at **/tmp/sshd.log** for information that might help you resolve the issue. In addition, check the log files for **lsass** and PAM.



For more information on how to generate a log for SSH, see ["Logging and Debugging" at https://docstore.mik.ua/orelly/networking\\_2ndEd/ssh/ch07\\_04.htm#ch07-20984](#), or the man page for **ssh**.

## After an Upgrade, Reconfigure SSH for AD Bridge

If **ssh** was recently upgraded, run the following command as root to make sure that the **sshd\_config** file is set up properly to work with AD Bridge:

```
domainjoin-cli configure --enable ssh
```

## Verify that Port 22 Is Open

A common problem is that a firewall is blocking the port used by SSH. Take a moment to verify that Port 22, which SSH typically connects to, is available by telneting to it. Failure looks like this:

```
root@example:~# telnet 10.0.0.17 22
Trying 10.0.0.17...
telnet: Unable to connect to remote host: Connection refused
```

Success looks like this:

```
root@example:~# telnet 10.0.0.17 22
Trying 10.0.0.17...
Connected to 10.0.0.17.
Escape character is '^].
SSH-2.0-OpenSSH_5.1p1 Debian-5
```

## Make Sure PAM Is Enabled for SSH

If your Active Directory account is not working with SSH, make sure that **UsePAM** is enabled in **sshd\_config** and make sure that your **sshd** application is linked to the PAM libraries.

1. Determine which **sshd** is running by executing the following command:

```
bash-3.2# ps -ef | grep sshd
root 8199 1 0 Feb 6 ? 0:00 /opt/ssh/sbin/sshd
root 2987 8199 0 Mar 3 ? 0:04 sshd: root@notty
root 24864 8199 0 12:16:25 ? 0:00 sshd: root@pts/0
root 2998 8199 0 Mar 3 ? 0:05 sshd: root@notty
root 24882 24880 0 12:16:54 pts/0 0:00 grep sshd
```

2. Either use **lsof** to find out which configuration file it is reading or start it up with debugging to figure out the default path.



### Example:

```
username@computer:~$ /usr/sbin/sshd -d -t
debug2: load_server_config: filename /etc/ssh/sshd_config
debug2: load_server_config: done config len = 664
```



```
debug2: parse_server_config: config /etc/ssh/sshd_config len 664
debug1: sshd version OpenSSH_5.1p1 Debian-3ubuntu1
Could not load host key: /etc/ssh/ssh_host_rsa_key
Could not load host key: /etc/ssh/ssh_host_dsa_key
```

3. Verify that **UsePAM** is enabled in the config file. As a best practice, make a backup copy of the configuration file before you change it.
4. Run **ldd** on **sshd** to make sure it links with **libpam**.

## Make Sure GSSAPI Is Configured for SSH

Logging onto a system with keys does not provide that system with the means of getting a PAC from the domain controller. Without a PAC there is no group membership information for the user. Automated Kerberos ticket renewal will also be unavailable. So, when the ssh login hits the login restrictions in the account phase as it tests for the group memberships, it will not find the user's group information, causing an ssh error like this:

Not in an Allowed Group!

A workaround is to have each user log in once with a password. Subsequent logins with keys should work until the AD cache is flushed, after which the user will have to log in again.

## Check the Configuration of SSH for SSO

Although AD Bridge automatically configures OpenSSH to support SSO through Kerberos using GSSAPI, it is worthwhile to review how AD Bridge does. Since you might need to configure or troubleshoot other applications for SSO, understanding the process will make it easier to apply the technique to other applications.



*Note: Not all versions of OpenSSH support Kerberos. Versions older than 4.2p1 might not work or might work improperly.*

### SSH Service Principal Name

The first thing that needs to be considered is the Kerberos service principal name (SPN) used by **ssh** and **sshd**. The SPN is a string that identifies the service for which an authentication ticket is to be generated. In the case of **ssh**, the SPN has the form:

```
host/<server name>@<REALMNAME>
```

For example, when a user uses **ssh** to connect to a computer named **fozzie.mycorp.com**, the **ssh** program requests a service ticket for the SPN:

```
host/fozzie.example.com@EXAMPLE.COM
```

The Kerberos realm is the computer's domain name in uppercase letters.

## System Keytab Generation

In order for Microsoft Active Directory to generate a Kerberos ticket for this SPN, a service account must exist for it. Additionally, a keytab must be created for the service account and placed on the sshd server. AD Bridge completely automates this operation. When a Linux or Unix computer is joined to AD, a machine account is created for the computer. If the computer is called **fozzie**, a machine account called **fozzie\$** is created in AD. AD Bridge then automatically creates a keytab for the SPN and places it in the standard system location (typically, **/etc/krb5.keytab**).

## User Keytab Generation

When the user runs the **ssh** program and OpenSSH determines that it will use Kerberos authentication, it will need to access a keytab for the user so that it can obtain a service ticket for the service or computer to which it is trying to connect. This keytab must be created using the user's account name and password. Manually, this can be performed by using the **kinit** utility. AD Bridge, however, does it automatically when the user logs on the computer. On most systems, the user keytab is placed in the **/tmp** directory and named **krb5cc\_UID** where **UID** is the numeric user ID assigned by the system.

## Configure OpenSSH

AD Bridge automatically configures OpenSSH at both the client and server computer. On the client, the **ssh\_config** file (typically in **/etc/ssh/ssh\_config**) is modified. On the server, **ssh\_config** (typically in **/etc/ssh/ssh\_config**) is modified. AD Bridge adds the following lines of code to the right files if they are not already present and if they are required by the system's version of sshd:

In the server, the following lines must be present in **sshd\_config**. If you are troubleshooting, make sure these lines are there:

```
GSSAPIAuthentication yes  
GSSAPICleanupCredentials yes
```

On the client, the following line must be present in **ssh\_config**:

```
GSSAPIAuthentication yes
```

On the client, **GSSAPIDelegateCredentials yes** is an optional setting that instructs the ssh client to delegate the krb5 TGT to the destination machine when SSH single sign-on is used.

In addition, if any of the following options are valid for the system's version of sshd, they are required and configured by AD Bridge:

```
ChallengeResponseAuthentication yes  
UsePAM yes  
PAMAuthenticationViaKBDInt yes  
KbdInteractiveAuthentication yes
```

Setting these options to **yes** instructs **ssh** to use the **kbdinteractive** ssh authentication mechanism and allows that mechanism to use PAM, settings that are required for AD Bridge to function properly.

 For more information, see the man pages for **ssh**, **sshd**, and the comments in the **ssh** and **sshd** configuration files.

## Test SSO

With OpenSSH properly configured, demonstrating SSO support is simple: Log on a Linux or Unix machine running AD Bridge by using your Active Directory credentials and then use **ssh** to connect to another machine that is also running AD Bridge. OpenSSH should establish a connection without prompting for a username or password.

## Platform-Specific Issues

If you are using Red Hat, CentOS, Fedora, FreeBSD, or AIX operating systems, review any of the following sections that are relevant for your operating system.

### Red Hat and CentOS: Solve the SSO Problem

There is a known bug with some versions of Red Hat and CentOS that prevents SSO from working with SSH, SSHD, and PuTTY. The following versions are known to be affected:

- CentOS 5
- Red Hat Enterprise Linux 5

The system incorrectly concatenates the Kerberos ticket's service principal name on the target Linux computer. For example, in the final entry of the results of the **klist** command below, the full name of the service principal is cut off after the @ symbol:

```
[EXAMPLE\fanthony@centos52 ~]$ /opt/pbis/bin/klist
Ticket cache: FILE:/tmp/krb5cc_1689257039
Default principal: fanthony@EXAMPLE.COM
Valid starting     Expires            Service principal
07/31/08 09:25:13  07/31/08 19:25:31  krbtgt/EXAMPLE.COM@EXAMPLE.COM
    renew until 08/07/08 09:25:13
07/31/08 09:25:31  07/31/08 19:25:31  CENTOS52$@EXAMPLE.COM
    renew until 08/07/08 09:25:13
07/31/08 09:30:04  07/31/08 19:25:31  host/centos52.example.com@
    renew until 08/07/08 09:25:13
```

To determine whether you need to implement the solution below on your Red Hat or CentOS computer, execute the following series of tests:

1. Connect to your target machine with SSH by using PuTTY and a valid Active Directory user. Be sure to use the FQDN of the host.
2. Execute the following command:

```
/opt/pbis/bin/klist
```

The results should look like this:

```
EXAMPLE\fanthony@centos52 ~]$ klist
Ticket cache: FILE:/tmp/krb5cc_1689257039
Default principal: fanthony@EXAMPLE.COM
Valid starting     Expires            Service principal
07/31/08 09:25:13  07/31/08 19:25:31  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

```
renew until 08/07/08 09:25:13
07/31/08 09:25:31 07/31/08 19:25:31  CENTOS52$@EXAMPLE.COM
renew until 08/07/08 09:25:13
```

3. SSH again to the same host and when prompted for the password, type **CTRL+C**.
4. Execute the **klist** command again:

```
/opt/pbis/bin/klist
```

5. Check the results to determine whether there is an incorrectly concatenated service principal, as there is in the following output:

```
[EXAMPLE\fanthony@centos52 ~]$ klist
Ticket cache: FILE:/tmp/krb5cc_1689257039
Default principal: fanthony@EXAMPLE.COM
Valid starting     Expires            Service principal
07/31/08 09:25:13  07/31/08 19:25:31  krbtgt/EXAMPLE.COM@EXAMPLE.COM
                  renew until 08/07/08 09:25:13
07/31/08 09:25:31  07/31/08 19:25:31  CENTOS52$@EXAMPLE.COM
                  renew until 08/07/08 09:25:13
07/31/08 09:30:04  07/31/08 19:25:31  host/centos52.example.com@
                  renew until 08/07/08 09:25:13
```

If the tests confirm that the problem exists, implement the following solution:

1. On Red Hat Enterprise Linux 5, make sure that the reverse PTR host definitions are defined in DNS.
2. On the target Linux computer, add the following line to **/etc/krb5.conf** under the **[domain\_realm]** entry of the file:

```
.yourdomainname.com = YOURDOMAINNAME.COM
```



**Example:**

```
[domain_realm]
.example.com = EXAMPLE.COM
```

3. Restart SSHD by running the following command at the shell prompt:

```
/sbin/service sshd restart
```

## Red Hat and Fedora: Solve SSH Config Problem

On Fedora 14 and Red Hat 5, there is an issue with the configuration of the platform that blocks SSH SSO. You must either use a workaround to connect to the client or modify the **sshd\_config** file on the server side. This section illustrates the problem and shows you how to connect to the client or fix the server.

After you join a domain with AD Bridge, Network Manager restarts and leaves the **/etc/hosts** file looking like this:

```
[root@nile-fedora14 etc]# cat /etc/hosts
10.100.0.26 nile-fedora14.nile-domain.example.com nile-fedora14 # Added by NetworkManager
127.0.0.1 localhost.localdomain localhost localhost4
::1 nile-fedora14.nile-domain.example.com nile-fedora14 localhost6 nile-fedora14.ramp.example.com
```

It should, however, look like this, but Network Manager keeps resetting it:

```
10.100.0.26 nile-fedora14.nile-domain.example.com nile-fedora14 # Added by NetworkManager
127.0.0.1 nile-fedora14.nile-domain.example.com nile-fedora14 localhost.localdomain localhost
localhost4
::1 nile-fedora14.nile-domain.example.com nile-fedora14 localhost6.localdomain6 localhost6
```

The configuration set by Network Manager blocks SSO because it ends up restricting reverse name lookups to ipv4 only.

When using the client, you can work around the problem by connecting by the external IP address. In other words, instead of using **ssh -l user nile-fedora14.nile-domain.example.com** to connect, use the following form:

```
ssh -l user 10.100.0.26
```

Alternatively, to fix the problem, you can turn off **GSSAPIStrictAcceptorCheck** in **sshd\_config** on the server, but such a resolution might be unavailable when you do not have administrative access to the server or when doing so might cause intractable side effects or security holes.

Another way to fix the problem is to turn off reverse DNS lookups in Kerberos. However, such a solution might result in side effects that block other applications or operations.

## FreeBSD: Invalid Argument with SSHD

On FreeBSD, user names that are longer than 16 characters, including the domain name, exceed the FreeBSD username length limit. Attempts to connect by ssh with a user name that exceeds the limit can result in the following notification:

```
bvt-fbs72-64# ssh testuser1@localhost
Password:
Connection to localhost closed by remote host.
Connection to localhost closed.
```

The log for sshd, meanwhile, might show an error that looks something like this:

```
Oct  7 18:22:57 vermont02 sshd[66387]: setlogin(EXAMPLE\adm.kathy):
Invalid argument
Oct  7 18:25:02 vermont02 sshd[66521]: setlogin(EXAMPLE\adm.kathy):
Invalid argument
```

Although **testuser1** is less than 16 characters, when you use the **id** command to check the account, something longer than 16 characters is returned:

```
[root@bvt-fbs72-64 /home/testuser]# id testuser1
uid=1100(BVT-FBS72-64\testuser1) gid=1801(BVT-FBS72-64\testgrp)
groups=1801(BVT-FBS72-64\testgrp)
```

The result of the **id** command exceeds the FreeBSD username length limit. There are several solutions:

- Set the default domain.
- Change the user name to 16 characters or less.
- With AD Bridge use aliases.

Keep in mind, however, that aliases will not solve the problem in relation to the AD Bridge local provider.

## AIX and Red Hat: Set Reverse PTR Host Definitions for SSO

For single sign-on with SSH to work on Red Hat Enterprise Linux 5 and AIX, reverse PTR host definitions must be set in DNS.

### AIX: Configure for Outbound Single Sign-On

On AIX 5.3, client-side SSH is not set up by default. Here is how to configure it so that it will work with AD Bridge:

1. On your AIX 5.3 computer, make sure the network authentication service, version 1.4.0.8, is installed.



#### Example:

```
-bash-3.00$ lslpp -l | grep krb
krb5.client.rte 1.4.0.8 COMMITTED Network Authentication Service
```

2. After joining an Active Directory domain with AD Bridge, append the following lines to the end of **/etc/krb5/krb5.conf**:

```
[domain_realm]
.demo.example.com = DEMO.EXAMPLE.COM
demo.example.com = DEMO.EXAMPLE.COM
```

3. Make sure that **/etc/krb5/krb5.conf** links to **/etc/krb5.conf**.

4. Also make sure that **/etc/krb5/krb5.keytab** links to **/etc/krb5.keytab**.

5. Make a backup of the credentials directory by executing the following command as root:

```
mv /var/krb5/security/creds /var/krb5/security/creds_old
```

6. As root, make a symbolic link to the **/tmp** directory so that the AIX Kerberos libraries can access the directory in which AD Bridge stores its credential caches:

```
ln -s /tmp /var/krb5/security/creds
```

7. Open **/etc/environment**, which contains the list of environmental variables that are set when a user logs on, and add the following line to the end of it:

```
KRB5_CONFIG=/var/lib/pbis/krb5-affinity.conf:/etc/krb5.conf
```

8. If you are logged on the machine whose environmental variable you changed, you must log off and log on again for the change to take effect.

## Troubleshoot Issues with Kerberos



The following resources can help you troubleshoot time synchronization and other Kerberos issues:

- *Kerberos Authentication Tools and Settings:* [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc738673\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc738673(v=ws.10))
- *Authentication Errors Caused by Unsynchronized Clocks:* [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc780011\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc780011(v=ws.10))
- *Kerberos Technical Supplement for Windows:* [https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649429\(v=pandp.10\)](https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649429(v=pandp.10))
- *Troubleshooting Windows Server Issues (including Kerberos errors):* <https://docs.microsoft.com/en-us/windows/deployment/deploy-whats-new>

The following topics can help you address common issues related to Kerberos and AD Bridge.

### Fix a Key Table Entry-Ticket Mismatch

When an AD computer account password changes two or more times during the lifetime of a domain user's credentials, the computer's entry that matches the Kerberos service ticket is dropped from the Kerberos key table. Even though the service ticket has not expired, an action that depends on the entry, such as reading the event log or using single sign-on, will fail.

To avoid issues with Kerberos key tables, keytabs, and single sign-on, the computer password expiration time must be at least twice the maximum lifetime for user tickets, plus a little more time to account for the permitted clock skew.

The expiration time for a user ticket is set by using an Active Directory Group Policy setting called Maximum lifetime for user ticket. The default user ticket lifetime is 10 hours; the default AD Bridge computer password lifetime is 30 days.

### Causes

The computer account password can change more frequently than the user's AD credentials under the following conditions:

- Joining a domain two or more times.
- Setting the expiration time of the computer account password Group Policy setting to be less than twice the maximum lifetime of user tickets.



For more information, see the [AD Bridge Group Policy Administration Guide](#) at [www.beyondtrust.com/docs/ad-bridge/how-to/group-policy](http://www.beyondtrust.com/docs/ad-bridge/how-to/group-policy).

- Setting the local **machine-password-lifespan** for the lsass service in the AD Bridge registry to be less than twice the maximum lifetime for user tickets.

### Solution

If a computer's entry is dropped from the Kerberos key table, you must remove the unexpired service tickets from the user's credentials cache by reinitializing the cache. Here is how:

On Linux and Unix, reinitialize the credentials cache by executing the following command with the account of the user who is having the problem:

```
/opt/pbis/bin/kinit
```

## Resolve a KRB Error During SSO in a Disjoint Namespace

When you are working in a network with a disjoint namespace in which the Active Directory domain name is different from the DNS domain suffix for computers, you may need to modify the domain\_realm section of **/etc/krb5.conf** on your target computer even though your DNS A and PTR records are correct for both DNS domains and can be found both ways.

The following error, in particular, indicates that you might have to modify your **krb5.conf** file before single sign-on (with SSH, for example) will work:

```
KRB ERROR BAD OPTION
```

Assume your computer's Active Directory domain is **bluesky.example.com** and your computer's FQDN is **somehostname.green.example.com** and you have already created the following entries in DNS:

```
_kerberos._tcp.green.example.com 0 100 389 ad2.bluesky.example.com  
_kerberos._udp.green.example.com 0 100 389 ad2.bluesky.example.com
```

On the target computer, the **[domain\_realm]** entry of your **/etc/krb5.conf** file looks like this:

```
[domain_realm]  
.bluesky.example.com = BLUESKY.EXAMPLE.COM  
bluesky.example.com = BLUESKY.EXAMPLE.COM
```

To resolve the error, add the following two lines to the **[domain\_realm]** entry of your **/etc/krb5.conf** file:

```
.green.example.com = BLUESKY.EXAMPLE.COM  
green.example.com = BLUESKY.EXAMPLE.COM
```

After adding the two lines above, the complete **[domain\_realm]** entry now looks like this:

```
[domain_realm]  
.bluesky.example.com = BLUESKY.EXAMPLE.COM  
bluesky.example.com = BLUESKY.EXAMPLE.COM  
.green.example.com = BLUESKY.EXAMPLE.COM  
green.example.com = BLUESKY.EXAMPLE.COM
```

Finally, make sure that you have a correct **k5login** file and then try to log on again.



For more information, see [Disjoint Namespace](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc731125(v=ws.10)), at [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc731125\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc731125(v=ws.10)).

## Eliminate Logon Delays When DNS Connectivity Is Poor

If connectivity to your DNS servers is tenuous or becomes unavailable, name resolution can time out, delaying the logon process. Because Active Directory is heavily dependent on a well-functioning DNS system, you should work to resolve your DNS issues.

If you cannot fix your DNS system, however, you can as a last resort set up a caching-forwarding name server on the AD Bridge client to eliminate the logon delay. For instance, you can set up a BIND server on each Linux or Unix computer on which you are running AD Bridge. Then you can configure BIND as a local caching resolver and add your nameserver addresses to the forwarder list, leaving `/etc/resolv.conf` with only the local loopback address:

```
search example.com
nameserver 127.0.0.1
```

 For instructions on how to set up BIND, see the *BIND documentation*.

## Eliminate Kerberos Ticket Renewal Dialog Box

There is an applet called **krb5-auth-dialog** that by default is active on many Linux distributions. It is intended to assist you with renewing your Kerberos tickets before they expire. Because AD Bridge renews your tickets for you, the dialog box is superfluous and can be a nuisance.

To disable the dialog box:

1. In the menu, click **System > Preferences > More Preferences > Session**.
2. Click the **Startup Programs** tab and disable the **krb5-auth-dialog** program. This change prevents it from restarting next time you log on.
3. Close the **Sessions** window and then run this command from the shell:

```
pkill krb5-auth-dialog
```

## Troubleshoot the AD Bridge Database

If the information in your reports or the events displayed in the Operations Dashboard seem incomplete, perform the following series of diagnostic tests sequentially:

- ["Check the Endpoints" on page 58](#)
- ["Check the AD Bridge BTCollector" on page 61](#)
- ["Check Events in the AD Bridge Database" on page 63](#)
- ["Troubleshoot Checklists for Reporting Components" on page 60](#)
- ["Switch Between Databases in AD Bridge" on page 63](#)

### Check the Endpoints

To troubleshoot potential endpoint problems:

1. Log on to a computer that you suspect might have a problematic endpoint and confirm that events are logged in the local event database. Run the following command as root or as an AD user with administrator privileges:

```
/opt/pbis/bin/eventlog-cli -s - localhost
```

2. Note the ID of the last event. If you run the following command, the last ID in this database should match the ID if the events are getting to the collector properly. If the IDs do not match, there is a configuration issue with one of the endpoints.

```
cat /var/lib/pbis/db/eventfwd-next-record.db
```

3. If no recent events are displayed or if the command returns errors, make sure that the **eventlog** service is running:

```
/opt/pbis/bin/lwsm status eventlog
```

4. If it is not running, check **/var/log/messages** to find out why and report the information to BeyondTrust Technical Support. Then, restart the service:

```
/opt/pbis/bin/lwsm start eventlog
```

5. If recent events are present but are not being forwarded, make sure that the event forwarding service is running:

```
/opt/pbis/bin/lwsm status eventfwd
```

6. If it is not running, check **/var/log/messages** to try to identify the cause and report the information to BeyondTrust Technical Support. Then, restart the service:

```
/opt/pbis/bin/lwsm start eventfwd
```

7. Check the event forwarding service's configuration in the AD Bridge registry to make sure that it properly identifies a collector server and, if the collector server is identified by its IP address, its **collector-principal**. If you modify the settings of the **eventfwd** service, you must restart the service for the changes to take effect.

Example of a configuration that uses the host name of its collector:

```
[HKEY_THIS_MACHINE\Services\eventfwd\Parameters]
"Collector"="w2k3-r2.example.com"
```

8. Make sure the collector can be resolved:

```
[root@rhel5d bin]# nslookup w2k3-r2.example.com
Server:      192.168.1.20
Address:     192.168.1.20#53
Name:       w2k3-r2.example.com
Address:    192.168.1.20
```

9. Make sure the collector server can be reached:

```
[root@rhel5d bin]# ping w2k3-r2.example.com
PING w2k3-r2.example.com (192.168.1.20) 56(84) bytes of data.
64 bytes from 192.168.1.20: icmp_seq=1 ttl=128 time=1.40 ms
```

10. If the collector is identified by IP address, make sure the **collector-principal** is properly set. For example, if the collector server is at IP address 192.168.1.255 and has a Kerberos machine name of **EventCollector** in the AD domain **example.com**, the **collector-principal** parameter would be:

```
collector-principal = host/EventCollector@EXAMPLE.COM
```

11. Check **/var/log/messages** for errors.

12. Stop the **eventfwd** service and then run it from the command line to display error information about the event forwarder's communication with the collector server:

```
/opt/pbis/bin/lwsm stop eventfwd
/opt/pbis/sbin/eventfwd --loglevel debug
```

After you run **eventfwd** from the command line, stop it with **CTRL-C** and then restart it:

```
/opt/pbis/bin/lwsm start eventfwd
```

After you verify that the endpoint is properly receiving events and forwarding them to a collector server, check the collector. If there are recent events, make a note of the last event's time stamp, event category, and event description.



To check whether the collector received the event, see ["Check the AD Bridge BTCollector" on page 61](#).

## Troubleshoot Checklists for Reporting Components

The checklists in this section can help you troubleshoot problems with the reporting components.

### Endpoints

To check for endpoint problems, confirm the following:

- **eventlog** service running
- **eventfwd** service running
- **reapsysl** service running
- **eventfwd** service properly configured



#### Example:

```
/opt/pbis/bin/regshell  
HKEY_THIS_MACHINE\> ls Policy\Services\eventfwd\parameters\  
  
[HKEY_THIS_MACHINE\Policy\Services\eventfwd\parameters]  
+ "Collector" REG_SZ           "services.umon.com"
```

- Collector name resolvable and address reachable



#### Example:

```
ping services.umon.com  
PING services.umon.com (10.100.1.1) 56(84) bytes of data.  
64 bytes from services.umon.com (10.100.1.1): icmp_seq=1 ttl=128 time=0.867 ms
```



For more information about the services, see ["AD Bridge Services and Status" on page 12](#).

- Collector principal properly set



#### Example:

```
/opt/pbis/bin/regshell  
HKEY_THIS_MACHINE\> ls Policy\Services\eventfwd\parameters\  
  
[HKEY_THIS_MACHINE\Policy\Services\eventfwd\parameters]  
+ "CollectorPrincipal" REG_SZ           "10.100.1.1"
```

- **/etc/syslog.conf** properly configured
- events present in local event log (test with **eventlog-cli**)

- **eventfwd** service seems to forward messages properly (run from command-line to test)
- firewall not blocking RPC access of collector server

## Collector Servers

To check for problems with the collector servers, confirm the following:

- **BTCollector** service running
- **BTEventDBReaper** service running
- events present in local collector database (test with **BTCollector-cli**)
- **BTEventDBReaper** properly configured (test with **BTEventDBReaper /s**)
- database provider and connection string properly set
- collector ACL allows endpoints to write to it (set with **Event Management Console**)
- collector machine account has sufficient privileges to write to database
- no unusual errors in Windows event log (run **eventvwr.exe**)
- firewall not blocking incoming RPC connections or outgoing database connections

## Database

To check for problems with the database, confirm the following:

- can connect to it with SQL Server Management Studio
- **Events** table contains events
- **EventsWithOUName** view contains events
- database security set to allow writing by **collector servers**, by **lDbupdate** user, and by **administrators**
- **lDbupdate** utility recently run to account for new endpoints joined to AD
- named-pipe client access enabled in SQL Server
- firewall not blocking incoming database connection

## Windows Reporting Components

To check for problems with the Windows reporting components, confirm the following:

- database connection strings set properly
- user has sufficient privileges to access database
- firewall not blocking database connections

## Check the AD Bridge BTCollector

1. Make sure **BTCollector** is running by executing the following command at the shell prompt of the Windows computer running the collector:

```
C:\Program Files\BeyondTrust\PBIS\Enterprise\DBUtilities>sc query BTCollector  
  
SERVICE_NAME: BTCollector  
    TYPE               : 10  WIN32_OWN_PROCESS  
    STATE              : 4   RUNNING
```

2. If the process is stopped, use **eventvwr.exe** to check the Windows event log for information about why the service failed.



**Note:** The collector server must be running Windows 2003 or Windows 2008.

3. If the process is not running, start it by executing the following command:

```
C:\Program Files\BeyondTrust\Enterprise\DBUtilities>sc start BTCollector
```

4. Verify that the service is receiving forwarded events by viewing the contents of the collector's local SQLite database. To execute the following command, the **BTCollector** process must be running and you must have read privileges in the access control list:

```
C:\Program Files\BeyondTrust\Enterprise\DBUtilities>BTCollector-cli -s - localhost
```



**Note:** The command should return a list of the events collected from the endpoints. If there is no data, it is likely that your endpoints are improperly configured (see the previous section). If the event that you noted when you checked the event forwarder in the previous section is among the results, make sure the **BTEventDBReaper** service is functioning properly.

5. Verify that **BTEventDBReaper** is running:

```
C:>sc query BTEventDBReaper
```

6. If the process is stopped, use **eventvwr.exe** to check the Windows event log for information about why the service failed. Restart the service with:

```
C:>sc start BTEventDBReaper
```

7. Check the database connection string and the service's other execution parameters:

```
C:\Program Files\BeyondTrust\Enterprise\DBUtilities>BTEventDBReaper /s
```

The results should look something like this:

```
Database provider:      System.Data.SqlClient  
Connection string:     Data Source=SomeCollector;Initial  
Catalog=LikewiseEnterprise;Integrated Security=yes
```

```
Record id last copied: 487
Records per period:    120
Seconds in a period:   10000
```

If the database server (**Data Source**= for SQL Server) is identified by name (as in the example), verify that the name can be resolved to an address by using **nslookup** and verify that the address is reachable from the collector server by using **ping**.

8. Use **eventvwr.exe** to check the Windows event log for messages. If **BTEventDBReaper** is failing to write to the central AD Bridge database and if you are using SQL Server with integrated security, make sure that the collector server's machine account has sufficient privileges to write to the AD Bridge database.

## Check Events in the AD Bridge Database

1. Check the AD Bridge database on the database server to check whether the table containing events is complete. If necessary, write a manual query to view recent events or to look for an event. For example, with SQL you can use the SQL command-line utility to open the LikewiseEnterprise database and run the following command to display all the events in the table named **Events**:

```
select * from Events;
```

2. If you cannot open or read the database, you might not have sufficient privileges to access it, which can result in problems when you run reports in the management console or use the **Operations Dashboard**.
3. If you use SQL Server and the **Events** table is empty, use the **SQL Server Configuration Manager** to make sure that the name-pipe client protocol is enabled. If it is not and you have to enable it, you must restart the **SQL Server** service for the changes to take effect.
4. If you find events in the **Events** table, check whether the events are also present in the **EventsViewWithOUName** view. If an event appears in the **Events** table but not in the **EventsWithOUName** view, it is because the database cannot associate your event with a computer in Active Directory. Run the **Idbupdate.exe** script and then check whether the event now appears in both views.

## Collector is not Displayed in the Management Console

1. Right-click the **Enterprise Database Management** node to check the **Reporting** database connection.
2. Run a test connection to ensure that it can connect.
3. Close the BeyondTrust management console.
4. On the services server, open the **Reporting Database Connection**.
5. Configure the reporting connection for the **Reaper** service.
6. Restart the **Collector** and **Reaper** services.
7. Open the management console and the collector is displayed under the **Database Management** node.

## Switch Between Databases in AD Bridge

To send events to a different database, you must change the database connection string in at least two places:

- The reaper service for the database (**BTEventDBReaper**)
- The **Enterprise Database Management** page in the BeyondTrust Management Console.



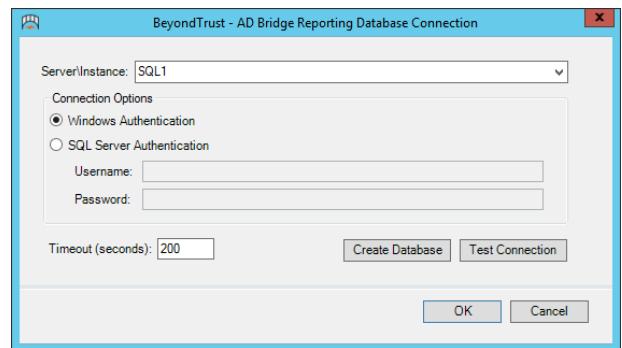
**Note:** Changing the setting on the **Enterprise Database Management** page automatically changes the same setting on the console's **Audit and Access Reporting** page and the **Operations Dashboard**.

However, if you installed different plug-ins of the BeyondTrust Management Console on different computers - to run the **Operations Dashboard** on a separate computer, for example, then you must change the database connection string on each computer. You may also have to change it in the following additional locations, especially if the computer's AD Bridge Console does not include the Enterprise Database Management plug-in: the **Audit and Access Reporting** page and the **Operations Dashboard** page.

After making the changes, you must reset the reaper service so it begins sending events to the new database.

1. In the AD Bridge Console tree on your Windows administrative workstation, right-click the **Enterprise Database Management** node and then click **Connect to database**.

- Click **Change**. Under **Database Type**, select **Microsoft SQL Server**, and then enter the name of the database server instance in the **Server/Instance** box.
- Enter the credentials of the database definer account if required for the authentication type that you selected, and then click **OK**.



2. In the console tree, right-click the **Operations Dashboard** node and then click **Connect to**.
  - Click **Change**.
  - Change the database settings as needed, and then click **OK**.
3. In the console tree, right-click the **Audit and Access Reporting** node, and then click **Advanced**.
  - Click **Change**.
  - Change the database settings as needed, and then click **OK**.
4. Open a command prompt window as an administrator and then change directories to **C:\Program Files\BeyondTrust\PBIS\Enterprise\DBUtilities**, and then run the following command:

```
BTEventDBReaper /gui
```

Make the changes that you want, and then click **OK**.

5. Reset the **BTEventDBReaper** to **0** and then refresh its settings to prompt it to send the events to the new database. To do so, from the **C:\Program Files\BeyondTrust\PBIS\Enterprise\DBUtilities** folder, run the following commands as an administrator:

```
BTEventDBReaper /f 0
BTEventDBReaper /r
```

## Troubleshoot Windows Setup for AD Bridge

### RID Pool Error

**Issue:** If you have more than  $2^{19}$  (524,288) users, groups, or computers created in your domain, you cannot use the **Suggest** button to suggest UID numbers for users, as the UID can no longer be guaranteed unique.

You may run into this problem with having too many RIDs in the domain if running a version of AD Bridge earlier than 10.0 and you are:

- a large university that onboard students in AD, and who, so far, has used StudentID or *human resource management software-assigned unique ID numbers*
- a large companies who uses Employee IDs
- a customer who has broken scripts exhausting the RID pool, and who has moved to Employee IDs.

**Details:** The SID in AD is a 96-bit number of form *Domain SID – Relative ID*. Each user in the domain has the same domain SID, but an incrementing RID. This SID is unique worldwide, and therefore the correct value to translate into a Unix UID. The problem is that the Unix UID or GID Number can only be 32 bits. At first glance, the answer would seem to be just use the RID directly, but that runs into problems in multi-domain environments, where it is absolutely guaranteed that RIDs between 2 domains will collide. For example, the **Domain Users** group always has RID 513.

Therefore, the UID/GID needs to be generated from a combination of a hash of the domain SID and the RID. To allow a larger forest that may have 20-30 domains in the trust list, the part of the hash for the Domain SID needs to be large enough to not collide at that range. We determined this by using 12 bits for the domain SID hash, and 19 bits for the RID, giving us a protection against collision up to 30 AD domains in the trust list, and 512,000 RIDs (the **uidNumber** in AD is a signed int, so we can only use 31 bits).

**Summary:** The only effect is that you can not use the **Suggest** button to generate UID numbers or GID numbers that are certain to be unique. Just type your own number in. Use something like Student ID, Employee ID, PeopleSoft unique ID, or some other previously-generated unique number, or keep a single-source *last used* value and simply increment it with each user add.

## Troubleshoot Entra ID Authentication Issues

Here is a list of known issues with Entra ID Authentication and how to resolve them.

### Tenant Join Issues

#### The Join Was Successful but Authentication Is Not Working

Check the permissions on the application in Azure, because there are issues with the permissions. These can be:

- There are missing permissions.
- Permissions are issued but not granted. Confirm they have a green checkmark by them.
- The **Allow public client flows** setting has not been enabled.

#### Authenticating Users Are Not Prompted With the Device Code

If the **tenant name** used during the join does not match the **tenant id**, users attempting to authenticate will be prompted for a password, not the device code and URL.



##### Example:

```
sudo /opt/pbis/bin/tenantjoin-cli join --tenant-id #####-###-###-###-##### -  
-tenant-name bananas --app-id #####-###-###-###-##### --app-secret-file  
secret-file
```

Rejoin the tenant with the correct tenant name.

# Troubleshoot Performance Issues

## Configure Max Buffer Size

By default OpenLDAP tries to allocate 16 MB of contiguous memory when **malloc()** is invoked. This is known to cause issues on AIX. After several iterations the heap becomes so fragmented that it cannot allocate 16 MB even though there is enough contiguous memory. Changing the buffer size to 1 MB resolves the fragmentation but will impact performance.

You can use the AD Bridge **config** tool to configure the max buffer size.

Configuring buffer size was added to the **config** tool in AD Bridge version 8.3.0.

## Display the Details of the Max Buffer Size

```
/opt/pbis/bin/config --details SaslMaxBufSize
```

## Set the Max Buffer Size

```
/opt/pbis/bin/config SaslMaxBufSize 1048576
```



*Note: The default value on most platforms is 16 MB. The default value on AIX is 1048575 MB.*

## Solaris

### Set AD Bridge File Descriptors on Solaris

On busy Solaris systems it may be necessary to tune the number of file descriptors (FD) to achieve optimum performance:

```
/opt/pbis/bin/regshell set_value '[HKEY_THIS_MACHINE\Services\lsass]' FdLimit 1024
```

The command sets the **lsass** FD limit higher. This is read by **lwsmd** when **lwsmd** starts, and controls what **ulimit** is set by **lwsmd** for **lsass** (or other daemons, as appropriate in the registry). The value of 1024 may be increased as needed or set to **65535** or **unlimited**.

To use an alternative FILE handler for **fopen()** and other calls:

```
svccfg -s lwsmd setenv -s -m start LD_PRELOAD_32 /usr/lib/extendedFILE.so.1
```



*Note: This is only available on Solaris 10u5 and later.*

To apply the changes run the following commands. The Solaris service manager reads in the configuration set by **svccfg**, and then restarts **lwsmd**:

```
svcadm refresh lwsmd  
svcadm restart lwsmd
```

## Troubleshoot AD Bridge Group Policy

This appendix provides information on how to troubleshoot the AD Bridge Group Policy Objects and the Group Policy agent.

### Autoenrollment GPO

First set the log level of **autoenrollment** to **debug**:

```
/opt/pbis/bin/lwsm set-log-level -p autoenroll - debug
```

Then check the system logs for autoenroll errors. This will also generate additional logs in **/tmp/pbis-curl.log**

Errors with sending a request to the Certificate Enrollment Service (CES) are stored in the **/tmp/pbis-crl.log** log file.

Common Issues	Potential Resolution
SSL: Certificate subject name <b>test-DC1-CA</b> does not match target host name <b>dc1.test.com</b>	Correct the IIS certificate to match the URL of the hosting machine.

### Wifi GPO

Common Issues	Potential Resolution
Wifi GPO certificate not downloading	The certificate template field is case sensitive. Verify the template name is correct. Best practice is to copy the certificate name into the certificate template field.

### Force AD Bridge Group Policy Objects to Update

The AD Bridge Group Policy agent, a component of AD Bridge, connects to Active Directory, retrieves changes to Group Policy Objects (GPOs), and applies the changes once every 30 minutes, when a computer boots or restarts, or when requested by the AD Bridge GPO update tool.

You can run the AD Bridge GPO update tool at any time on a Linux or Unix computer joined to a domain with the AD Bridge agent.

Run the following command at the shell prompt:

```
/opt/pbis/bin/gpupdate --verbose
```

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

```
GPO Update succeeded
```

```
GPO Update was unsuccessful, error code <code> (<error message>)
```

On target computers, AD Bridge stores its GPOs in **/var/lib/pbis/grouppolicy**.

## Check the Status of the AD Bridge Group Policy Daemon

You can check the status of the AD Bridge Group Policy daemon on a AD Bridge client computer that is running Unix or Linux by running the following command as the root user:

```
/opt/pbis/bin/lwsm status gpagent
```

## Restart the AD Bridge Group Policy Daemon

You can restart the AD Bridge Group Policy daemon on a computer that is running Unix or Linux by executing the following command as root:

```
/opt/pbis/bin/lwsm restart gpagent
```

## Generate an AD Bridge Group Policy Agent Debug Log

You can generate an AD Bridge Group Policy agent debug log on a Unix or Linux computer running the AD Bridge agent.

1. Log on as root user.
2. Stop the Group Policy daemon by executing the following command at the shell prompt:

```
/opt/pbis/bin/lwsm stop gpagent
```

3. Start the Group Policy daemon in command-line debug mode and capture the output in a file with these two commands:

```
/opt/pbis/sbin/lwsmd --loglevel debug --logfile /var/log/gpagentd.log --container gpagent &
```

```
/opt/pbis/bin/lwsm start gpagent
```

4. When you are done logging the information and debugging the service, use the **kill** command to stop the service, which returns the log level to its default setting.
5. Start the Group Policy daemon with the AD Bridge service manager:

```
/opt/pbis/bin/lwsm start gpagent
```

## Modify or Inspect GPOs from the gp-admin Command

The **gp-admin** command-line utility lets you modify the settings in a Group Policy Object (GPO) in Active Directory from a Linux or Unix computer. For example, you can use the tool to specify a GPO, download a policy setting in the GPO from Active Directory to a Unix folder, modify it, and then upload it to Active Directory.

You run the tool as root. It is located at **/opt/pbis/bin/gp-admin**.

To view the tool's arguments, run the following command:

```
/opt/pbis/bin/gp-admin --help
```

Here's what the help looks like:

```
Usage: gp-admin --list --gpolicy <Group Policy setting>
  --help      |   -h     Show help
  --listgpcses |   -lgp   List all the Group Policy extensions
  --listall    |   -la    List all the enabled policy settings in all the GPOS
  --list       |   -l     List the GPOS where the specified policy setting is configured
  --download   |   -d     Download the specified Group Policy setting to the specified
                        path
  --upload     |   -u     Upload the specified Group Policy setting from the specified
                        path
  --gpolicy    |   -gp    Specify the desired Group Policy setting
                        This should be set with the option '-l' '-d' or '-u'
  --gpobject   |   -gpo   Specify the desired Group Policy Object from which policy
                        setting
                        to be downloaded or uploaded. This should be set only with
                        the option '-d' or '-u'
  --path       |   -p     Specify the desired path to download or upload policy settings
                        from or to AD. This should be set only with the option '-d' or
                        '-u'.
                        Please provide the directory path where GPT.INI is present
```



### Example:

```
gp-admin -lgp
```

```
gp-admin -la
```

```
gp-admin -l -gp <ID>
```

```
gp-admin -d -gp <ID> -gpo <gpo name> -p <path>
```

Here's an example of how you can use **gp-admin** as root to inspect and modify a GPO:

1. List all the GPOs applied to the computer by name and policy identifier:

```
/opt/pbis/bin/gp-admin -la
```

Here is an example of an abbreviated list:

```
[root@rhel5d bin]# ./gp-admin -la
AD Bridge Syslog GP Extension is enabled in the GPO's
GPO name:AD Bridge settings for test  PolicyIdentifier: {46c77e22-bb04-4dec-a788-
8cf3a30ebcb7}
GPO name:AD Bridge settings for apps  PolicyIdentifier: {c2152211-e134-4eb1-a53a-
```

```
b90378d7f056}
AD Bridge Settings GP Extension is enabled in the GPO's
GPO name:Default Domain Policy PolicyIdentifier: {31B2F340-016D-11D2-945F-00C04FB984F9}
GPO name:Engineering ACL Policy 1.0 PolicyIdentifier: {33E3DE4C-02DF-4CEE-8785-
1F43FB750AFB}
...
AD Bridge Automount GP Extension is enabled in the GPO's
GPO name:LinuxServers AutoFS 1.0 PolicyIdentifier: {2A84EEE7-47E9-4C80-9FC9-0F6CBFB36654}
...
```

- Check the GPO extension's ID, which should be the same across different platforms:

```
/opt/pbis/bin/gp-admin --lgp
```

```
[root@rhel5d bin]# /opt/pbis/bin/gp-admin -lgp
Computer Policy Settings
ID = 1 AD Bridge SELinux GP Extension {0BCE95E2-5332-49dc-9878-D3F8B678734B}
ID = 2 AD Bridge Syslog GP Extension {0D18828D-E7DA-434c-A537-8AF8122E2602}
ID = 3 AD Bridge Settings GP Extension {0EED766B-2404-46A6-A6B6-F8971164A920}
ID = 4 AD Bridge Sudo GP Extension {20D139DE-D892-419f-96E5-0C3A997CB9C4}
ID = 5 AD Bridge Fstab GP Extension {36C20771-2724-4ee3-B1B0-36A396CDA5E3}
ID = 6 AD Bridge AppArmor GP Extension {5554B0EB-ABE5-4654-A123-3B7818B2A48A}
ID = 7 AD Bridge Computer Network Settings {5FB45FF0-A68C-430b-8C6E-347B14AEB975}
ID = 9 AD Bridge Login Prompt GP Extension {9020E541-F49C-4ab8-88F3-55BE2D95B440}
ID = 10 AD Bridge Automount GP Extension {9994B0EB-ABE5-4654-A123-3B7818B2A999}
ID = 11 AD Bridge Message of the Day GP Extension {9A9F29C0-B1B1-467d-A255-
0BD3D7AAAE59}
ID = 12 AD Bridge Files GP Extension {AE472D6F-0615-4d12-BC70-8A381CA67D53}
ID = 13 AD Bridge Computer Gconf GP Extension {B078EE20-01A1-4FEE-8DCC-032B758FA1F8}
ID = 14 AD Bridge LogRotate GP Extension {B1BBA22A-08FF-4826-9B4B-151C8A0BC1CA}
ID = 15 AD Bridge Cron GP Extension {B9CA8919-71D7-4aaa-9567-7225965F4A0E}
ID = 16 AD Bridge Script GP Extension {DDFF8E72-5C29-4987-8FB3-DF7EB7CE8FC2}
User Policy Settings
ID = 8 AD Bridge User Gconf GP Extension {74533AFA-5A94-4fa5-9F88-B78667C1C0B5}
ID = 17 AD Bridge User Files GP Extension {E62C4C67-D187-4b89-8EEC-A8A2570390BF}
```

- You can then use the ID to locate the GPOs that apply a setting. The following example uses the ID for the automount policy setting (10) to list the GPOs that are applying the automount extension:

```
[root@rhel5d bin]# ./gp-admin --list -gp 10
AD Bridge Automount GP Extension enabled in the below mentioned GPO's
GPO name:LinuxServers AutoFS 1.0 PolicyIdentifier: {2A84EEE7-47E9-4C80-9FC9-0F6CBFB36654}
```

- You can use the ID and the GPO name to download the latest version of a GPO that contains the automount setting:

```
./gp-admin -d -gp 10 -GPO "LinuxServers AutoFS 1.0" -p /var/lib/pbis/grouppolicy
```

The result of the command is as follows:

```
[root@rhel5d bin]# ./gp-admin -d -gp 10 -GPO "LinuxServers AutoFS 1.0" -p /var/lib/pbis/grouppolicy  
Downloading policy data for setting:  
(AD Bridge Automount GP Extension) in GPO: (LinuxServers AutoFS 1.0)  
to path: (/var/lib/pbis/grouppolicy)  
Copying policy data from location:  
\demo.com\SysVol\demo.com\Policies\{2A84EEE7-47E9-4C80-9FC9-0F6CBFB36654}  
Downloaded AD Bridge Automount GP Extension to /var/lib/pbis/grouppolicy/  
\{2A84EEE7-47E9-4C80-9FC9-0F6CBFB36654} folder
```

5. You can now change directories to the folder that contains the GPO and view it:

```
[root@rhel5d bin]# ls /var/lib/pbis/grouppolicy/  
\{2A84EEE7-47E9-4C80-9FC9-0F6CBFB36654} GPT.INI krb5cc_gpagentd systemfiles  
[root@rhel5d bin]# ls /var/lib/pbis/grouppolicy/\{2A84EEE7-47E9-4C80-9FC9-0F6CBFB36654\}/  
\9994B0EB-ABE5-4654-A123-3B7818B2A999  
[root@rhel5d bin]# cd /var/lib/pbis/grouppolicy/\{2A84EEE7-47E9-4C80-9FC9-0F6CBFB36654\}/  
[root@rhel5d \{2A84EEE7-47E9-4C80-9FC9-0F6CBFB36654}\]# cd \{9994B0EB-ABE5-4654-A123-  
3B7818B2A999\}/  
[root@rhel5d \{9994B0EB-ABE5-4654-A123-3B7818B2A999}\]# ls  
auto.home auto_master lwisettings.xml  
[root@rhel5d \{9994B0EB-ABE5-4654-A123-3B7818B2A999}\]# cat lwisettings.xml  
<LWIMachinePolicy> <GPItem clientGUID="{9994B0EB-ABE5-4654-A123-3B7818B2A999}"  
itemGUID="{12587328-5C0D-46bd-BE9B-BF264F6CA720}" name="AutoMount settings" Version="2.0">  
<autoMount>
```

6. You can also view the files referenced by the automount policy setting.
7. In the preceding example, the value of the Executable attribute for the auto\_master file should be set to no, not yes. You can open the file in an editor, make the change, and then upload the modified file to Active Directory:

```
/opt/pbis/bin/gp-admin -u -gp 10 -GPO "LinuxServers AutoFS 1.0" -p  
/var/lib/pbis/grouppolicy/  
\{2A84EEE7-47E9-4C80-9FC9-0F6CBFB36654\}/  
\{9994B0EB-ABE5-4654-A123-3B7818B2A999\}/lwisettings.xml
```



For more information, see, ["Troubleshoot User Rights with Ldp.exe and Group Policy Modeling" on page 30.](#)

## Log a Support Case 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](http://www.beyondtrust.com/support).

## Before Contacting BeyondTrust Technical Support

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

- AD Bridge version: available in the AD Bridge Console by clicking **Help > About** on the menu bar
- AD Bridge 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 issues, 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, see [Generate Debug Logs in the AD Bridge Troubleshooting Guide](#), at [www.beyondtrust.com/docs/ad-bridge/how-to/troubleshoot](http://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, see the [AD Bridge Linux Administration Guide](#), at [www.beyondtrust.com/docs/ad-bridge/getting-started/linux-admin](http://www.beyondtrust.com/docs/ad-bridge/getting-started/linux-admin).

- tcpdump

## Generate a Support Pack

The AD Bridge support script copies 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`