Connection Errors

To describe the errors you need to understand that Privileged Identity don't attempt a connection to your machines. Rather, we tell the system that you are running our software to connect to those machines and do something. As we do not use agents, we do not perform networking. This means those errors that you sometimes see in the status columns is what Windows believes to be the reason it cannot connect.

For further description of what these errors are, from a command prompt you can type *net helpmsg ##* where *##* is the error message you received. Here you will see the definition of the error.

> ***Note:*** *Privileged Identity may return these errors in hex format such as* ***0x00000035****, which should be converted to decimal (error 53) to find the correct information.*

Typical errors you will see include:

Error 5 - "Access is denied". As we do not use agents do connect or authenticate we require administrative privileges on the system you are attempting to connect to.

To resolve an error 5, you should ensure that you (and your deferred processor account) are seen as admins on the boxes you are intending to manage. This can be a direct membership of the administrators group or by virtue of domain group membership.

In Windows XP, an error 5 can also be encountered in workgroup (untrusted domain) scenarios because of a default policy that limits you to guest access. This policy can be found by running **gpedit.msc** and navigating to **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network Access: Sharing and security model for local accounts**. Change the value to **Classic: local users authenticate as themselves**.

In Windows Vista\Server 2008, this can occur in a workgroup (untrusted domain) scenario as a result of UAC and other enhanced security policies. While BeyondTrust is not advocating turning off User Access Control (UAC), that is certainly one of your options. The other option without turning off UAC is to force network connections to behave a little more like they did in XP. This will require a change to the Vista/2008 system's registry and a reboot.

IMPORTANT!

Modifying the registry improperly can cause damage if you do not know what you are doing. BeyondTrustassumes no liability if you choose to implement the changes described here.

Open regedit and navigate to the following key: **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Pol icies\system**. Add a new **DWORD** value called **LocalAccountTokenFilterPolicy** and set its data to *1*. Then reboot your system.

Error 53 - "The network path was not found". This is the result of bad information in DNS, WINS, HOSTS file, or LMHOSTS file. This error can also be generated when there is a firewall or similar item blocking communication.

HOSTS and LMHOSTS files are always tried first before DNS and WINS. Meaning if you or someone edited this file to include static information for a system, then the information changed but the file did not get updated, you may end up with misinformation and an inability to connect to the desired system. These files can be found in **%systemroot%\system32\drivers\etc** and can be edited with any text editor.

In the case of DNS and WINS the error has a little more meaning but also requires a preface. When a machine shuts down properly, it releases its DNS and WINS records (provided those records were not added statically to the DNS/WINS server). This allows the record to be purged from DNS/WINS and another system to register the same name/IP (useful when using DHCP). This means, if the record is

correctly purged from DNS/WINS you should be receiving errors 64 or 1203 (more on that later). if the record is not successfully purged, because the machine did not properly shutdown and release its records then you will see error 53 when attempting to contact your system. In other words, error 53 means there is information in WINS/DNS and it is bad.

To fix this error, assuming the machine is still online and not experiencing other problems, you can typically run the following commands to update DNS and WINS respectively:

1. *ipconfig /registerdns*
2. *nbtstat -RR* (the RR must be uppercase)

You may also need to purge your negative cache on your system before you will be able to resolve these names. Do the following:

1. wait a couple of minutes
2. run *ipconfig /flushdns*, *nbtstat -R*, and *arp -d **

Finally, Windows firewall can cause this problem as well because the machine is online and it has registered correctly, but you cannot connect to the system because the firewall is blocking your access.

To resolve this, you can disable the firewall locally, via group policy, or you can create remote management exceptions locally or via group policy. To manage the firewall via group policy (or local policy) navigate to **Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\[Domain,Standard] Profile**. For machines that are part of a domain, use the Domain key. For standalone systems, use the Local key. for laptops that are on and off the network, modify both.

To turn off the firewall, modify the policy *Protect all network connections* and set it to *Disabled*.

Error 64 - "The network name has been deleted". This builds on the premise of error 53 in a good way. It means that the target machine did shutdown properly and has initiated deletion of its name record from DNS/WINS.

Error 1203 - "No network provider accepted the given network path". This error builds on the concept of error 64, but indicates more. Specifically, error 64 said the name was marked for deletion (or tombstoned) while error 1203 indicates one of two things:

1. The name record has been deleted form all possible servers
2. The name you are requesting does not exist on the network anywhere and cannot be resolved by HOSTS, DNS, LMHOSTS, WINS, or even broadcast.

In the case of error 64 and 1203 (reason 1), there is not much you can do as it is indicative that everything is working properly. In the case of 1203 (reason 2), you need to validate that you are not having trouble talking to your DNS and WINS servers.

Error 1069 - "The service did not start due to a logon failure". This is one of the more descriptive error messages but has a few potential reasons:

1. Bad username
2. Good username, bad password
3. The logon as a service right is not held by the account

Error 1326 - "Logon failure: unknown username or bad password". This is one of the more descriptive error messages but can be misleading.

Typically this error is found in scenarios where you specified the correct username but the password is bad. For example in workgroup scenarios where pass-through authentication is utilized. You logon to XP1 as administrator with a password of pass and attempt to access XP2. XP1 says you are logged in as administrator and that your password is pass. XP2 says, while administrator is a valid account for me, that is not his password. This exchange will result in a 1326 error.

To resolve this error you may take two possible actions:

1. Make use of the way Windows performs networking and first establish a connection to the machine using the credentials you wish to use. This can be done at a command prompt or run menu by using the following command: *net use \\server_name\ipc$ /user:*

[domain_name\]user_name [password]. The password field is optional but should be used to provide the correct password and avoid error 1326 again. As shown below a domain user would connect as follows:

net use \\server_name\ipc$ /user:domain_name\user_name password

A local user would connect as follows:

net use \\server_name\ipc$ /user:user_name password

After you authenticate, Windows will continue to use this authentication for the remainder of your Windows session when connecting to the specified machine.

2. In Privileged Identityuse the **Alternate Administrators** option available form the **Settings** menu. This effectively performs the same operation as mentioned in item 1 above but it does it automatically for you when you enable the feature.

Error 1396 - "Logon Failure: The target account name is incorrect". There are multiple potential causes for this error, which involve naming issues.

1. This error message can occur if two computers have the same computer name. One computer is located in the child domain; the other computer is located in the parent domain.

   To resolve this issue rename one of the computers, or delete the machine account on the parent domain.

   Bad DNS information.

2. Validate that the machine has the correct DNS information and that DNS server does not have incorrect information pertaining to this system. This error will appear when DNS refers you to one system but you are actually targeting a different system.

Error 1722 - "The RPC server is not available". This error is a bit more difficult to troubleshoot that the others as there are many reasons it can happen. Typically a reboot of the remote system fixes these issues.

Error 2245 - "The password is shorter than required". This is a generic message that Windows returns when the password does not meet your password requirements. When using the admin interface to change passwords as we are, causes are generally related to length and characters used. For example, if you have turned on password complexity then If this policy is enabled, passwords must meet the following minimum requirements:

- Not contain all or part of the user's account name
- Be at least six characters in length
- Contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Nonalphanumeric characters (e.g., !, $, #, %)

Additionally, setting a minimum length on the password greater than six characters will also affect this.

To resolve this error for Privileged Identity, consider your domain policy. If you have configured the RPG settings to not contain any of the above items, or your domain’s password policy requires a longer password, that is the most likely cause of your issues.

For example, in the password job, set the *compatibility level* to be *Windows 2000 and later* and be sure to include all of the options in the *password may contain* area.

Further, in the constraints area (constraints button) in the center right region, you can identify minimum requirements for characters. By default these items are set to 0 which means if you do have complexity turned on in your environment and these values set to 0, there is a potential for some passwords to not contain characters required by your policy; it is not likely if you use long passwords, but possible.

To resolve this problem for Account Reset Console, be sure to instruct users to create passwords which comply to your domain policy. You may also create a banner on the password change page as well as on the credential provider (CTRL+ALT+DEL) that can identify what the policy currently is. For further instructions, please see the tool's help manual.