Delinea

Identity Bridge

Documentation ⊗ 1.1.3

Delinea

Table of Contents

Delinea

Thycotic's **Identity Bridge** (ID Bridge) is a utility that allows the setting of values to be used in the Thycotic panels under Active Directory User and Computers, User and Group Properties. These values are used to enable the ID Bridge to manage the user authentication from Linux\Unix hosts to Active directory.

The ID Bridge Configuration Utility allows to globally set all values and selected values at an organizational unit (OU) level.

Installation and Upgrades

The agent should have a resolvable hostname set before installing the Thycotic Identity Bridge. If the agent has a default hostname of localhost.localdomain, the pmagent service will not function as expected.

Note: Updating the agent hostname post installation will require a reinitialization of the agent configuration.

*

CentOS 7.x, 8.x	100Mb - 2mb in each of /lib64 /etc/pam.d /usr/lib64/security and /etc	2Gb	For the Identity Bridge component to function correctly **SELinux** currently needs to be disabled on the host.
RedHat Linux 7.x, 8.x	100Mb - 2mb in each of /lib64 /etc/pam.d /usr/lib64/security and /etc	2Gb	For the Identity Bridge component to function correctly **SELinux** currently needs to be disabled on the host.
Oracle Linux, 7.x, 8.x	100Mb - 2mb in each of /lib64 /etc/pam.d /usr/lib64/security and /etc	2Gb	For the Identity Bridge component to function correctly **SELinux** currently needs to be disabled on the host.
Ubuntu 18.04, 20.04	100Mb - 2mb in each of /lib/x86_64-linux-gnu/security, /lib/x86_64-linux-gnu/ /etc/pam.d and /etc	2 Gb	

Windows & Active Directory Requirements

- Active Directory Forest Functional Level: Greater than or equal to 2012 R2 or newer
- Windows OS: Greater than or equal to Windows 2012 R2/Windows 7 (x64 only across all versions of Windows)
- Client Prerequisites:
  - Visual Studio C++ Redistributable 2019 x64 (https://aka.ms/vs/16/release/vc_redist.x64.exe)
  - Visual Studio C++ Redistributable 2019 x86 (https://aka.ms/vs/16/release/vc_redist.x86.exe)
  - ASP.NET Core 3.1 Runtime (v3.1.5) - Windows Hosting Bundle (https://download.visualstudio.microsoft.com/download/pr/7c30d3a1-f519-4167-b850-b9c49bf2aa0e/dbfa957a76a41a1e1795f59d400d4ccd/dotnet-hosting-3.1.5-win.exe)
  - .NET 4.5.2 (https://download.microsoft.com/download/E/2/1/E21644B5-2DF2-47C2-91BD-63C560427900/NDP452-KB2901907-x86-x64-AllOS-ENU.exe)

Note:

- If installing from the bundled installer/bootstrapper (ThycoticIdentityBridge_x64_.exe), the client prerequisites will automatically be installed.
- If installing the raw msi (ADBridge.Installer_x64_.msi), the user will have to manually download and install the client prerequisites.

Windows 7

If you install the Identity Bridge on a Windows 7 system, please refer to the following Microsoft KB: https://support.microsoft.com/en-us/help/2533623/microsoft-security-advisory-insecure-library-loading-could-allow-remot

Software Downloads

This page provides links to Thycotic Identity Bridge product software downloads.

Note:

- Only general availability releases are fully supported for usage with Thycotic's Identity Bridge.
- The Identity Bridge Configuration Utility software and Agent software versions need to match to work correctly.

Windows Management Tools		refer to System Requirements	Thycotic Identity Bridge for Windows Package V1.1.2
			Thycotic Identity Bridge Installer Only (No Dependencies) V1.1.2

Linux	Redhat	6.x	coming soon
		7.x	Thycotic Identity Bridge Linux Agent V1.1.3
		8.x	Thycotic Identity Bridge Linux Agent V1.1.3
	CentOS	6.x	coming soon
		7.x	Thycotic Identity Bridge Linux Agent V1.1.3
		8.x	Thycotic Identity Bridge Linux Agent V1.1.3
	Ubuntu LTS	14.x	coming soon
		22.x	coming soon
		18.04	Thycotic Identity Bridge Linux Agent V1.1.3
		20.04	Thycotic Identity Bridge Linux Agent V1.1.3
	SuSE Enterprise	12.x	coming soon
		15.x	coming soon
	Oracle	6.x	coming soon
		7.x	Thycotic Identity Bridge Linux Agent V1.1.3
		8.x	Thycotic Identity Bridge Linux Agent V1.1.3

Unix	AIX	6.x	coming soon
		7.x	coming soon
	HP-UX	11i v3	coming soon
	Solaris	10.x	coming soon
		11.3	coming soon
		11.4	coming soon

The following information will guide you through the process on how to install your Identity Bridge agent on CentOS.

Once you have downloaded the latest version of Thycotic's **pmagent** installer you will need to securely copy it onto you host. You will need to perform the installation as root or a user with root sudo permissions.

Installations Covered

- CentOS, RedHat, Oracle Linux
- Ubuntu

Thycotic File Locations

Core installation location: /opt/thycotic

Other Thycotic file locations: /lib64, /usr/lib64/security, /var/log, /etc

Other locations Thycotic agent will modify system files: /etc, /etc/pam.d, /etc/ssh, /etc/authselect/

Disable Security-Enhanced Linux (SELinux)

Currently for the Thycotic Identity Bridge agent to correctly authenticate against Active Directory Thycotic requires that the SELinux functionality of the host machine is disabled.

The agent installer will detect if SELinux is set to Enforcing or Permissive and provide the following message at the end of the installation.

```
======================================================================
Please disable SELinux to allow the Identity Bridge to function properly
======================================================================
```

To disable the SELinux functionality you will need to perform the following:

1. Edit the /etc/selinux/config file
2. Set the SELINUX line to: disabled
    - Example: SELINUX=disabled
3. Reboot your host

If SElinux is disabled the message will not be displayed.

For CentOS, RedHat, and Oracle there are 2 methods for installing packages, rpm and yum, both methods are outlined below.

RPM

For upgrades to version 1.1.3 only, as mentioned in the Release Notes under Known Issues, run this upgrade command:

```
rpm -U --force ./pmagent_x86_64_vn.n.n.nn_<platform>.rpm
```

For new installations only, performed as non root user with sudo permissions:

```
>> sudo rpm -i /root/Thycotic/pmagent_x86_64_vn.n.n.nn.rpm
```

Where, pmagent_x86_64_vn.n.n.nn.rpm is replaced with the actual software package and version that is being installed.

Below is the expected output of a successful installation

```
Created symlink from /etc/systemd/system/multi-user.target.wants/pmagent.service to /etc/systemd/system/pmagent.service.

Please start the pmagent service by running:

/bin/systemctl start pmagent.service

You need to join an Active Directory domain to start authenticating users using the command:

/opt/thycotic/sbin/pmagent --join

Please disable SELinux to allow the Identity Bridge to function properly
```

YUM

For upgrades to version 1.1.3 only, as mentioned in the Release Notes under Known Issues, run this downgrade command:

```
yum downgrade ./pmagent_x86_64_vn.n.n.nn_<platform>.rpm
```

For new installations only, performed as non root user with sudo permissions:

```
>> sudo yum install /root/Thycotic/pmagent_x86_64_vn.n.n.nn.rpm
```

Where, pmagent_x86_64_vn.n.n.nn.rpm is replaced with the actual software package and version that is being installed.

```
Below is the expected output of a successful installation
Loaded plugins: fastestmirror, langpacks
Examining pmagent_x86_64_v1.1.3.81.rpm:  pmagent_x86_64_1.1.3.81
Marking pmagent_x86_64_v1.1.3.81.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package pmagent.x86_64 0:1.1.3.81 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================

Package         Arch         Version         Repository                Size

================================================================================
Installing:

pmagent         x86_64       1.1.3.816       /pmagent_x86_64_v1.1.3.81       50 M

Transaction Summary
================================================================================
Install 1 Package
Total size: 50 M
Installed size: 50 M
Is this ok [y/d/N]: y
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : pmagent_x86_64_1.1.3.81 1/1
Created symlink from /etc/systemd/system/multi-user.target.wants/pmagent.service to /etc/systemd/system/pmagent.service.

Please start the pmagent service by running:
  /bin/systemctl start pmagent.service

You need to join an Active Directory domain to start authenticating users using the command:
  /opt/thycotic/sbin/pmagent --join

Verifying : pmagent_x86_64_1.1.3.81 1/1

Installed:
pmagent_x86_64_1.1.3.81
Complete!
```

Post Installation

By default CentOS, RedHat, and Oracle do not start a newly installed package, therefore you will need to manually start the Thycotic Agent.

Performed as non root user with sudo permissions:

```
>> sudo systemctl start pmagent.service
```

The pmagent service will be started automatically following a reboot of the host system.

Prerequisites

If the Ubuntu operating system is installed from either

- ubuntu-18.04-live-server-amd64.iso or
- ubuntu-20.04.1-live-server-amd64.iso

you will be required to update the operating system base files with the following command before installing the Identity Bridge agent.

```
sudo apt-get update
```

It is recommended that your base operating system is always running the latest vendor recommended patches.

Thycotic File Locations

Core installation location: /opt/thycotic

Other Thycotic file locations: /lib/x86_64-linux-gnu/security, /lib/x86_64-linux-gnu/, /var/log, /etc

Other locations Thycotic agent will modify system files: /etc, /etc/pam.d, /etc/ssh

There are 2 methods for installing packages, DPKG and APT, both methods are outlined below.

DPKG

Performed as non root user with sudo permissions

```
>> sudo dpkg -i pmagent-1.1.3.81-Linux.deb
```

Below is the expected output of a successful installation

```
Selecting previously unselected package pmagent.
(Reading database ... 184828 files and directories currently installed.)
Preparing to unpack pmagent-1.1.3.81-Linux.deb ...
Unpacking pmagent (1.1.3.81) ...
Setting up pmagent (1.1.3.81) ...
Created symlink /etc/systemd/system/multi-user.target.wants/pmagent.service  /etc/systemd/system/pmagent.service.

Please start the pmagent service by running:
    /bin/systemctl start pmagent.service

You need to join an Active Directory domain to start authenticating users
using the command:
    /opt/thycotic/sbin/pmagent --join
```

APT

Performed as non root user with sudo permissions

```
>> sudo apt install /root/Thycotic/pmagent-1.1.3.81-Linux.deb
```

Below is the expected output of a successful installation

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'pmagent' instead of '/home/installer/pmagent-1.1.3.81-Linux.deb'
The following packages were automatically installed and are no longer required:
  linux-hwe-5.4-headers-5.4.0-42 tcpd
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed
```

```
  pmagent
0 to upgrade, 1 to newly install, 0 to remove and 92 not to upgrade.
Need to get 0 B/8,669 kB of archives.
After this operation, 28.5 MB of additional disk space will be used.
Get:1 /home/installer/pmagent-1.1.3.81-Linux.deb pmagent amd64 1.1.3.81 [8,669 kB]
Selecting previously unselected package pmagent.
(Reading database ... 184828 files and directories currently installed.)
Preparing to unpack .../pmagent-1.1.3.81-Linux.deb ...
Unpacking pmagent (1.1.3.81) ...
Setting up pmagent (1.1.3.81) ...
Created symlink /etc/systemd/system/multi-user.target.wants/pmagent.service  /etc/systemd/system/pmagent.service.

Please start the pmagent service by running:
    /bin/systemctl start pmagent.service

You need to join an Active Directory domain to start authenticating users
using the command:
    /opt/thycotic/sbin/pmagent --join
```

Post Installation

By default Ubuntu does not start a newly installed package, therefore you will need to manually start the Thycotic Agent

Performed as non root user with sudo permissions

```
>> sudo systemctl start pmagent.service
```

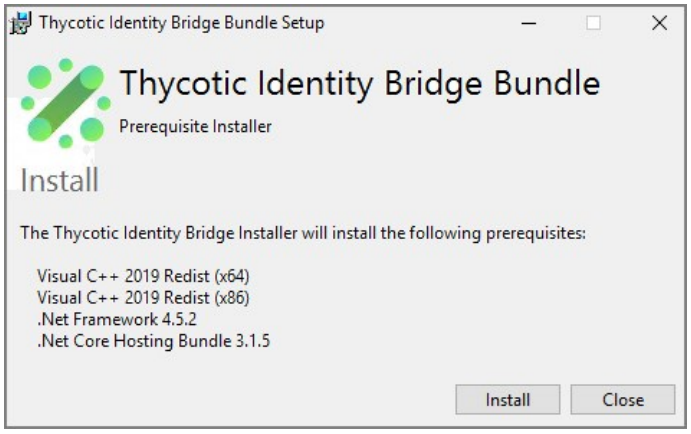
The pmagent service will be started automatically following a reboot of the host system.

The Identity Bridge for Active Directory Configuration application can be installed on Windows servers based on the specifications outlined on in the System Requirements section.

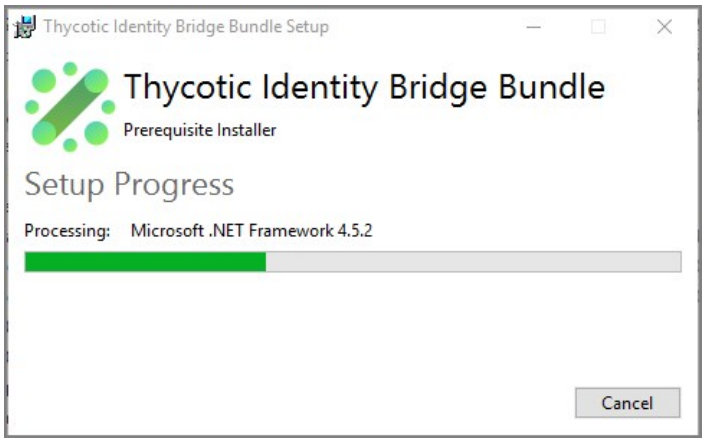
If you are co-hosting Thycotic products like Privilege Manager and installing the Identity Bridge Configuration application on an existing server already running Internet Information Services, the application pool identity might need to be reset to the correct account permissions, if the Active Directory Domain Server is added or created after the application pools for Privilege Manager have been established.

The executable for the Identity Bride installation on Windows systems, checks for prerequisites and installed those before entering the actual product installation.

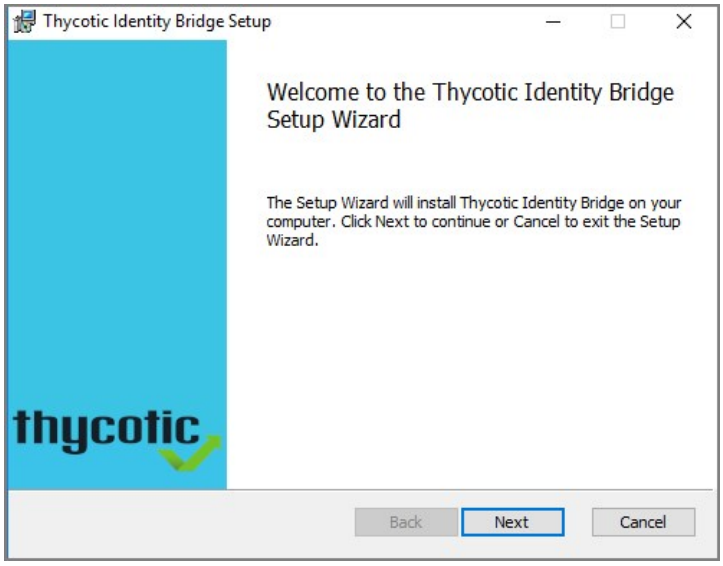
1. Double-click the downloaded Identity Bridge for Windows install executable.
2. The Thycotic Identity Bridge Bundle installer opens, click **Install**.



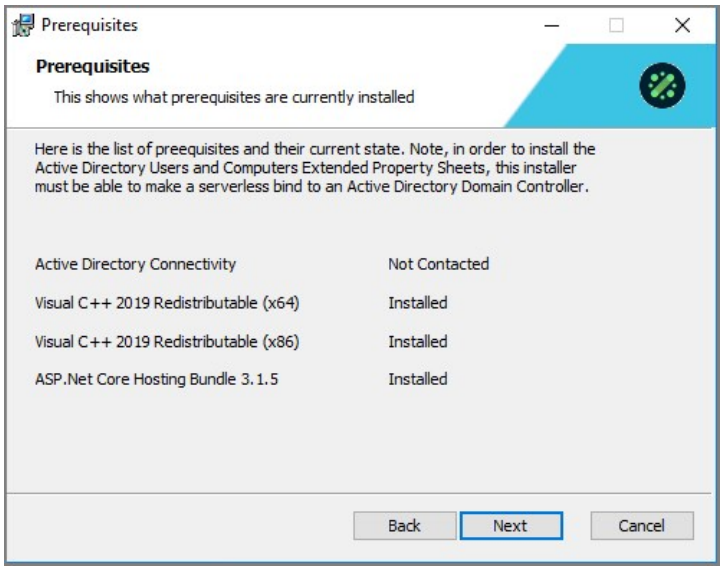
3. The installer shows the progress of the prerequisites verification and installation.



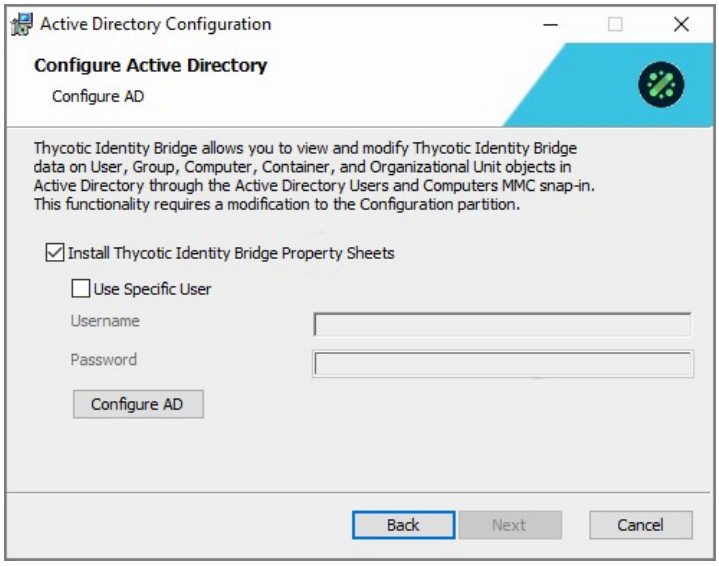
Once the prerequisites are applied the Installation wizard opens, click **Next**.



4. The install wizard shows the installed Prerequisites, click **Next**.

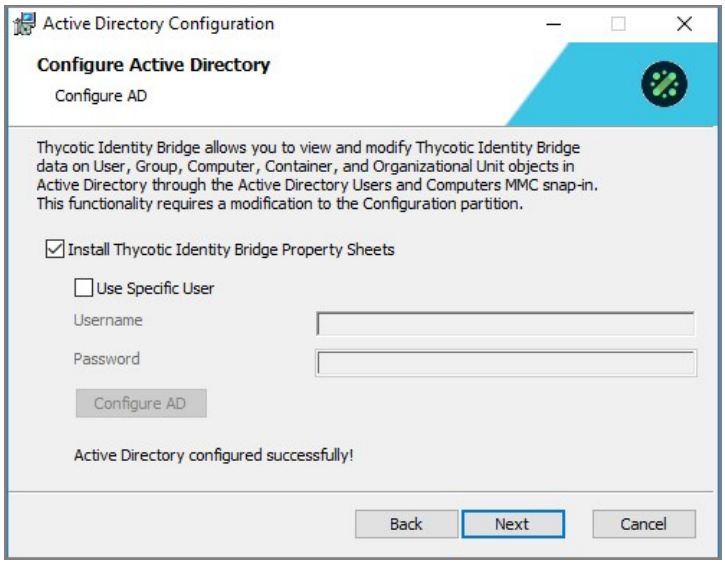


5. When Active Directory is detected, the Configure Active Directory dialog opens to the following:



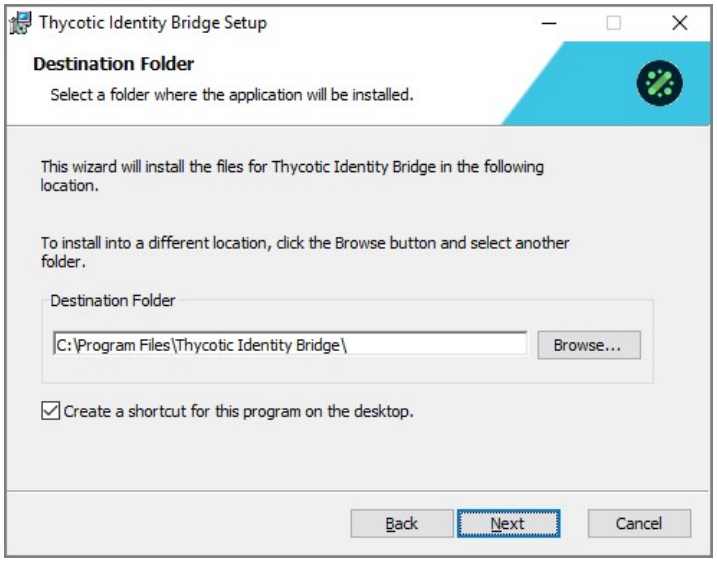
- Check the Install Thycotic Identity Bridge Property Sheets checkbox.
- If you are logged in as the default user (Administrator), ignore the specific user detail setup.
- Click **Configure AD**.

6. A successful AD Configuration is confirmed:



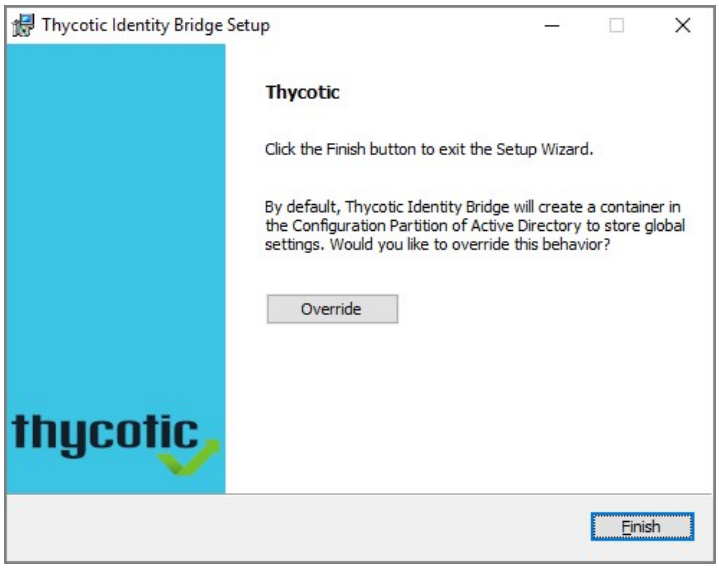
Click **Next**.

7. Confirm or change the default Destination Folder path:

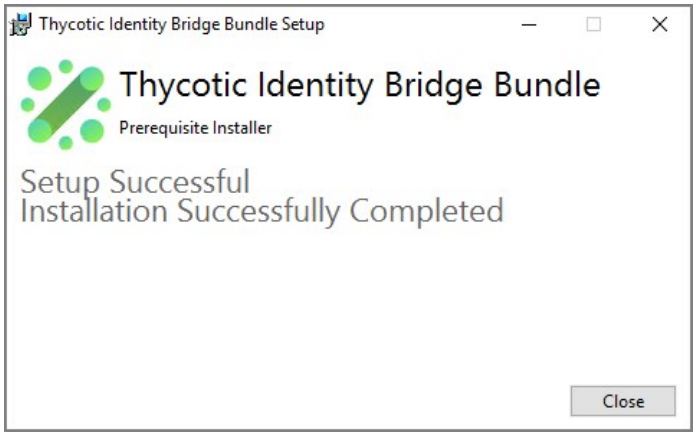


Click **Next**.

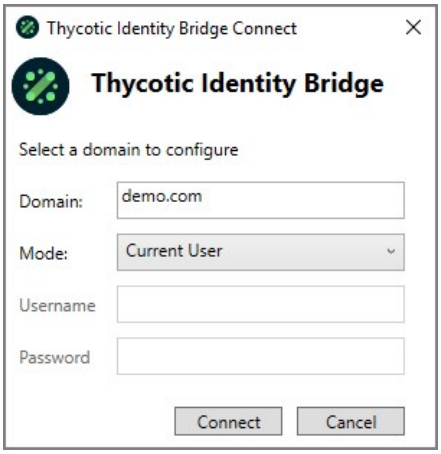
8. Click **Finish** once the setup completes.



9. On the Setup Successful dialog, click **Close**.



You are now ready to open the Identity Bridge application, it will open to the Thycotic Identity Bridge Connect dialog.



If you are the default user, you only need to click **Connect**. The Domain should have been automatically entered and the Mode drop-down is on the Current User option.

Refer to Identity Bridge Configuration Utility for details about the features of the configuration utility.

Linux/Unix Agents

After a successful installation of the Thycotic agent on your *nix host typing pmagent as a privileged user or sudo pmagent from a non privileged user will return all the usage options that can be used in conjunction with the pmagent command.

```
usage: pmagent [options]

Global options (specify --global)
  options:
  (-h|--help)                           display help
  (-V|--verbose)                        display verbose data
  (-v|--version)                        display version
  (-N|--init)                           (re)initialize the agent install
  (-H|--hostid)                         get the unique hostid
  (-s|--setcfg) <var=val>               set agent configuration value
  (-g|--getcfg) <var>                   get agent configuration value
  (-e|--exportcfg) [path]               export agent configuration
  (-i|--importcfg) [path]               import agent configuration
  (-l|--listsvcs)                       list agent services


Join Identity Bridge to Active Directory (specify --join)
  options:
  (-d|--domain) <domain>                domain to join
  (-a|--admin) <adminuser>              admin user for join
  (-p|--passwd) <adminpwd>              admin password for join
  (-D|--dc) <domaincontroller>          the domain controller for join
  (-n|--name) <computername>            override computer name for join
  --ou <ou>                             optional OU for computer account
  --disp "<display name>"               computer display name for join
  --force                               force join for existing computer
  --nosyscfg                            do not configure system files

Identity Bridge commands (specify --bridge)
  options:
  --syscfg <config|uninstall|unconfig|path>
                                        (un)configure or revert system files
  --stats                               retrieve bridge statistics
  --testuser <username>                 test user access to host
  --acl [--verbose]                     view Active Directory ACL information
  --leave [<domain>]                    leave an Active Directory domain
  --delete [<domain>]                   leave and delete Computer in Active Directory
      ... [(-a|--admin) <adminuser>]    admin user for delete
      ... [(-p|--passwd) <adminpwd>]    admin password for delete
      ... [--nosysuncfg]                do not unconfigure system files
  --purge [--user...][--group...]       purge cache data
  --cache [--user...][--group...][--agent]
                                        view cache data
      ... [--user|--user="<wildcard>"]  specify user cache data
      ... [--group|--group="<wildcard>"]   specify group cache data
      ... [--agent]                     select agent cache data
```

Joining

```
Join Identity Bridge to Active Directory (specify --join)
  options:
  (-d|--domain) <domain>              domain to join
  (-a|--admin) <adminuser>            admin user for join
  (-p|--passwd) <adminpwd>            admin password for join
  (-D|--dc) <domaincontroller>        the domain controller for join
  (-n|--name) <computername>          override computer name for join
  --ou <ou>                           optional OU for computer account
  --desc "<description>"              computer description for join
  --force                             force join for existing computer
  --nosyscfg                          do not configure system files
```

This page describes the process and options for joining your *nix agent to an Active Directory domain using Thycotic's Identity Bridge solution.

Before being able to join you *nix host to a domain the following requirements will need to be met

- For the Linux\Unix agents to be able to communicate with Active Directory the Domain Controllers will require LDAPS to be enabled.
- DNS and routing must be correct
  - DNS record for agent
  - Agent must be able to resolve the domain and domain controller
- Thycotic Agent installed on the *nix host
- Access to an Active Directory Account with permissions to add computer objects
- SELinux to be disabled on the *nix host otherwise the authentication to Active directory will be impacted.
  - The Thycotic Agent installer will post a message if detected
  - The Join command will also abort and provide a message if SElinux is detected:

    Please disable SELinux to allow the Identity Bridge to function properly
- Root access or a user with root sudo permissions

In order for your *nix agent to Join an available Active directory domain you will need to run the pmagent --join command. This will contact an available dc within you domain and add your *nix host as a computer object to that domain.

You can perform the join solely from using command line arguments or through an interactive method where you will be prompted to provide the required details.

As the Join process completes and the agent is registered, the join process will also configure the Thycotic agents system file configuration to allow authentication to pass through to Active Directory. This option can be skipped if required.

The command line also allows additional optional configuration options to be included in the Join, these will be details below.

As the join completes the system authentication files will also be configured to allow authentication of Active Directory users

If a computer object of the same name already exists within the AD the Join will overwrite the record with a new one for that host, as long as that computer object has no password (has never been actively used).

There is a force option to allow the overwrite of any computer object (however, this must be used with extreme caution)

Future: if an alternative host was registered with the now overwritten computer record it will cease to function and indicated within the logging. The host will then need to be joined back into the domain.

Command line options for joining your *nix hosts to the Active directory domain

--join	Base argument to Join an Active Directory domain must be present before any other argument listed below	The domain you wish to join can be added after Only argument required
-d | --domain	Specify the Domain you wish to join	Short and Long domain can be used, Demo or Demo.com
-a | --admin	Specify an Active Directory admin user with privileges for join the domain	**Accepted Input formats of**
		Username:
		Administrator **LDAP:**
		"CN=Administrator,CN=Users,DC=Domain,DC=com" **User Principal Name (must be configured in AD):**
		Administrator@Domain.com **Down-Level Logon Name:**
		Domain\\Administrator (Requires \\ as \ in *nix is an escape character)
-p | --passwd	Specify password for admin user	
-D | --dc	Specify a domain controller for join to be executed against	Optional - Provides a defined DC for performing the Join Effective when multiple DC available for a Domain
-n | --name	Specify the computer name for join	Optional - Uses the hostname of the *nix host by default
--desc *<"description">*	Specify the computer description for join	Optional - Uses the FQDN of the *nix host by default
--ou	Specify an alternative OU for the computer object to be placed in	Optional - Uses the Active Directories default of Computers to locate the computer object
		Example usage:

		--ou OU=CentOS,OU=Non-Windows,DC=Demo,DC=com
--nosyscfg	Will not configure the agents systems configuration files for AD authentication	Optional - By default the Join process will run the --bridge --syscfg config at the end of the process to allow AD users to authenticate to the agent.
		This optional will stop the --bridge --syscfg config from being run
--force	Allows the join to overwrite an existing computer record within the AD regardless of the existing computer objects status	**Caution!!** Optional - Using the force option could stop other previously registered hosts from working or a computer of higher importance could be overwritten by mistake

Note: When using the command line method to join Active directory is the pmagent service is not running before the join, you will need to manually start it after. If the service was already running, it will be automatically restarted

Following the completion of either CLI or Interactive join to AD you should expect to see the following type of output:

```
Successfully Joined domain: DEMO.COM
Domain Controller: DC01.Demo.com
With User: Administrator
Computer name: Agent01
In OU: CN=Computers,DC=Demo,DC=com
Description: [Agent01.Demo.com](http://DC01.Demo.com)

(Re)starting Identity Bridge Service
```

```
pmagent --join *Domain*
```

- User will be prompted for Admin user and Password

```
pmagent --join *Domain.com* -a "*CN=Administrator,CN=Users,DC=Domain,DC=com"*
```

- User will be prompted for Administrator Password

```
pmagent --join *Domain.com* -p *Password*
```

- User will be prompted for Admin user

```
pmagent --join *Domain.com* -a *Administrator\@Domain.com* -p *Password* -D *DC01*
```

- DC01 will be contacted to perform the join command

```
pmagent --join *Domain.com* -a *Domain\\\\Administrator* -p *Password* -n *Linux_Agent*
```

- Will create a computer object with a name of LINUX_AGENT1

```
pmagent --join -a *Administrator\@Domain.com* -p *Password* -desc “This is a Thycotic IB Agent”
```

- Will be prompted to provide a Domain to join
- Will create a computer object with a description of This is a Thycotic IB Agent

```
pmagent --join -d *Domain.com* -a *Administrator* -p *Password* -D *DC01* -n *Linux_Agent* -desc “This is a Thycotic IB Agent” --ou OU=CentOS,OU=Non-Windows,DC=Demo,DC=com --nosyscfg
```

- Example with all options defined
- Computer object will be created in the Non-Windows CentOS folder

```
pmagent --join
```

- User will be prompted to provide Domain, Admin User and Password
  - Enter domain:
    - Enter Active Directory username:
    - Enter *AD User@Domain.com*'s password:

Any required command line option not included, the user will be prompted to provide interactively

```
Identity Bridge commands (specify --bridge)
  options:
  --syscfg <config|uninstall|unconfig|path>
                                    (un)configure or revert system files
  --stats                           retrieve bridge statistics
  --testuser <username>             test user access to host
  --acl [--verbose]                 view Active Directory ACL information
  --leave [<domain>]                leave an Active Directory domain
  --delete [<domain>]               leave and delete Computer in Active Directory
      ... [(-a|--admin) <adminuser>]    admin user for delete
      ... [(-p|--passwd) <adminpwd>]    admin password for delete
      ... [--nosysuncfg]            do not unconfigure system files
  --purge [--user...][--group...]   purge cache data
  --cache [--user...][--group...][--agent]
                                    view cache data
      ... [--user|--user="<wildcard>"]  specify user cache data
      ... [--group|--group="<wildcard>"]   specify group cache data
      ... [--agent]                 select agent cache data
```

Prerequisites

Root access or a user with root sudo permissions.

--bridge Command Line Options

Once your Thycotic Identity bridge agent has been joined to Active Directory there are a number of other commands that you can utilise in conjunction with the **--bridge** option and these are identified below

--syscfg

Allows you to configure/unconfigure the hosts native authentication files for the Thycotic system configuration files to authenticate against your Active Directory Domain.

Thycotic uses json scripts to modify the hosts original authentication files. Before any **--syscfg** configuration any files to be modified are backed up. The Path option allows you to define an alternative json script to be used for the configuration of the hosts authentication files. This would be used when customers have specific alterations already defined on their hosts.

The default Thycotic scripts can be found in:

- /opt/thycotic/scripts

Files currently modified by **--syscfg**:

- /etc/pam.d/password-auth
- /etc/pam.d/passwd
- /etc/nsswitch.conf
- /etc/ssh/ssh_config
- /etc/ssh/sshd_config

If password-auth, passwd or nsswitch.conf are found to be missing during a --syscfg config the process will be aborted and the user informed that a required system file is missing. ssh_config and sshd_config are not required files. If missing during a --syscfg unconfig\uninstall the process will continue and modify\replace any files still available.

The uninstall option will instead of modifying the existing system file simply use the .thyorig backups created when create was run and reset

the system files to how they were originally.

The unconfig will modify the existing files creating a .thybak backup first.

In the event the .thyorig files are missing the agent will fallback to performing a modifying the existing files.

--stats

Provides on screen feedback of the status of the agent, including Process Id and currently active AD instance.

Useful commands to check under which OU the agent is defined and running.

--testuser

Performs and Active Directory check of the user status against the agent.

The following statuses can be returned:

- Access Allowed
- Account Disabled
- Account Expired
- Account Locked
- Thycotic ACL denied access and User doesn't exist

--acl

Displays the Access Control List for the Agent. Displays a list of Active Directory user that are able to access the Agent in accordance with the Thycotic ACL policy defined in the Configuration Utility.

Optional: --verbose will display the users assigned to a Group in the ACL list.

--leave

Leaves the Active Directory domain, although leaving the computer object in Active Directory. As the leave process completes the --syscfg uncfg will be run, reverting the host back to its original authentication configuration and removing the Thycotic system configuration files.

Leave will clear all Active Directory setting on the host, it will clear all cached information. Defining the Domain is not required, if not defined the agent will use it's stored details for the Domain.

Optional: --nosysuncfg stops the removal of the Thycotic system configuration files.

Do not unconfigure system files.

--delete

Leaves the Active Directory domain, also deleting the computer object in Active Directory. Although to complete the Delete command you will be required to provide the Domain, Admin username and Password. As the Delete process completes the --syscfg uncfg will be run, reverting the host back to it's original authentication configuration and removing the Thycotic system configuration files.

- [(-al--admin) <adminuser>] admin user for delete
- [(-pl--passwd) <adminpwd>] admin password for delete
- [--nosysuncfg] do not unconfigure system files

Delete can be completed solely through command line input or interactively. Interactively will default to showing the Domain the agent is currently joined to.

Optional: --nosysuncfg stops the removal of the Thycotic system configuration files.

--purge

- --purge [--user...][--group...] view cahce data
- .. [--userl--user="<wildcard>"] specify user cache data
- .. [--groupl--group="<wildcard>"] specify group cache data

Purge allows the deletion of the locally cached data stored on the agent. The purge can remove all user and group cached information or be filtered to down to individual user and group level.

The purge will only remove the locally cached information regarding users and groups on that Agent. The cached information is used to reduce user/group look up times in Active Directory and provide authentication in the event the Domain is unavailable.

The default of --purge will delete all information. You may use * wildcard matching and/or [Aa] for case matching.

--cache

- --cache [--user...][--group...][--agent] view cache data
- ... [--userl--user="<wildcard>"] specify user cache data
- ... [--groupl--group="<wildcard>"] specify group cache data
- ... [--agent] select agent cache data

Displays the cached information for the agent, users and groups. The cache can be displayed for all 3 categories or filtered to down to individual user and group level.

The cached information is used to reduce user/group look up times in Active Directory and provide authentication in the event the Domain is unavailable.

The default of --cache will display all information. You may use * wildcard matching and/or [Aa] for case matching.

> **Note**: The format of the cache output is subject to change and is of no particular format.

--bridge Examples

Syscfg

```
pmagent --bridge --syscfg /root/thycotic/corp-config.json
```

Rather than using the default /opt/thycotic/scripts/ to configure or unconfigure the authentication system files, the agent will call /root/thycotic/corp-config.json

Stats

```
pmagent --bridge --stats
```

Example output:

```
Process ID: 3770
Threads: 15
Started: Wed Jun 17 10:49:22 2020
Last Accessed: Wed Jun 17 11:16:21 2020
Status: running,connected,joined
Current Client Processes: 0
NSS Requests: 130
PAM Requests: 4
Current Joined Domain: DEMO
Computer name: AGENT1
OU: CN=Computers,DC=Demo,DC=com
```

Testuser

pmagent --bridge --testuser user1

Example output if account expired:

User user1 denied access to AGENT1
Reason: User account user1 has expired in Active Directory

ACL

pmagent --bridge --acl

The following Active Directory users / groups are allowed to login to this host

USERS
=====

[Username]	[Unix Username]	[User Principal Name]	[Display Name]
user10	user10	user10@Demo.com	user^10
user11	aduser11	user11@Demo.com	user^11

GROUPS
======

[Group Name]	[Alt Group Name]	[Description]
Linux^Admins	Linux^Admins	

ACL - Verbose

pmagent --bridge --acl --verbose

The following Active Directory users / groups are allowed to login to this host

USERS
=====

[Username]	[Unix Username]	[User Principal Name]	[Display Name]
user10	user10	user10@Demo.com	user^10
user11	aduser11	user11@Demo.com	user^11

GROUPS
======

[Group Name]	[Username]	[Unix Username]	[User Principal Name]	[Display Name]
Linux^Admins				
	user11	aduser11	user11@Demo.com	user^11
	user12	linux12	user12@Demo.com	user^12
	user14	aduser14	user14@Demo.com	user^14
	USer15	USer15	USer15@Demo.com	USer^15

Leave

pmagent --bridge --leave --nosysuncfg

This will leave the current Active Directory domain.

The --nosysuncfg mean that the Thycotic authentication system files will remain in place.

- The --bridge --syscfg unconfig will not be run at the end of the leave.

Delete

pmagent --bridge --delete

You will be prompted interactively to complete the deletion process.

1. Enter domain (default: DEMO):
2. Enter Active Directory username: *Administrator*
3. Enter *Administrator*@Demo's password:
4. Successful.

Cache - Default

```
pmagent --bridge --cache --user [Uu]ser\*
```

- Using both Character casing and wildcard matching
- Following the successful authentication of an AD user to your *nix host you can recall the cached information for that user.

Example output:

```
{
"Users:
   Names: user1, user1, DEMO/user1, user1@DEMO.COM
   SID: S-1-5-21-4211583412-2907095826-1833522802-3465
   uid: 446501, gid: 513
   groups: Domain^Users
```

Cache - Full

Using both Character casing and wildcard matching.

Following the successful authentication of an AD user to your *nix host you can recall the cached information for that user.


```
{
  "users": [
    {
     "usid": "S-1-5-21-4211583412-2907095826-1833522802-3465",
     "name": "user1",
     "adname": "user1",
     "sam": "DEMO/user1",
     "principal": "user1@DEMO.COM",
     "linked": 0,
     "uid": 446501,
     "gid": 513,
     "gecos": "user 1",
     "home": "/home/DEMO/user1",
     "shell": "/bin/bash",
     "lastUp": 1594725372,
     "expires": -1,
     "data": {
       "userName": "user1",
       "userPrincipalName": "user1@Demo.com",
       "KerberosName": "user1@Demo.com",
       "unixLoginName": "user1",
       "unixLoginShell": "/bin/bash",
       "unixHomeDirectory": "/home/DEMO/user1",
       "uidNumber": 446501,
       "gidNumber": 513,
       "sid": "S-1-5-21-4211583412-2907095826-1833522802-3465",
       "gecos": "user 1",
       "description": null,
       "displayName": "user 1",
       "groupDN": "CN=Domain Users,CN=Users,DC=Demo,DC=com",
       "groupDescription": "All domain users",
       "groupDisplayName": "Domain Users",
       "nETBIOSDomainName": "DEMO",
       "passThrough": false,
       "linkedUser": false,
       "accountExpires": 4294967295,
       "passwordExpired": false,
       "accountLocked": false,
       "accountDisabled": false,
       "accessDenied": false,
       "message": "Welcome user1 to the Thycotic Universal Bridge on AGENT1",
       "groups": [
```

```
        {
          "gidNumber": 513,
          "name": "Domain^Users",
          "altname": "Domain^Users",
          "description": "All^domain^users",
          "sid": "S-1-5-21-4211583412-2907095826-1833522802-513"
        }
      ]
    }
  }
 ]
}
```


Purge

pmagent --bridge --cache --user=[Uu]ser* pmagent --bridge --cache --user

- This will purge all cached user and group information from the agent
- Follow a purge this is the output you would see from checking the user cache


```
{
  "users": []
}
```

```
Global options (specify --global)
  options:
  (-h|--help)                          display help
  (-V|--verbose)                       display verbose data
  (-v|--version)                       display version
  (-N|--init)                          (re)initialize the agent install
  (-H|--hostid)                        get the unique hostid
  (-s|--setcfg) <var=val>              set agent configuration value
  (-g|--getcfg) <var>                  get agent configuration value
  (-e|--exportcfg) [path]              export agent configuration
  (-i|--importcfg) [path]              import agent configuration
  (-l|--listsvcs)                      list agent services
```

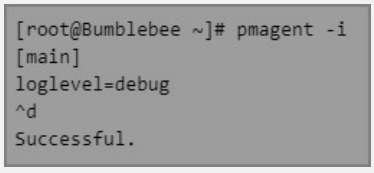
Prerequisites

Users need to have root access or root sudo permissions.

Agent Global Commands

Once your Thycotic Agent has been installed you have a number of Global options available which can be run directly after typing **pmagent** and are identified below.

-h | --help	Displays the pmagent options output	
-V | --verbose	Displays verbose data	Normally used in conjunction with options such as -v
-v | --version	Displays the installed version of the Thycotic agent	Example output: 1.0.0
-N | --init	Re-initializes the agent installation	The agents configuration settings are all stored in letc\pma.conf in the event this file is removed or you wish revert to a default configuration as per the installation then this option will regenerate the pma.conf
-H | --hostid	Displays the unique host ID	Displays the unique value created by the operating system that identifies the machine.
-s | --setcfg <var=val>	Updates an individual agent configuration setting	The variable component is in the format of section.field=new value
		Example of use: pmagent -s main.loglevel=debug

-g l --getcfg	Displays an individual agent configuration setting	The variable component is in the format of section.field=new value
		Example of use: pmagent -g main.loglevel
		The output will displayed as: main.loglevel=warning
-e l --exportcfg [path]	Exports the current agent configuration in ini format	Without the path defined will display all the current configuration settings of the agent to screen.
		Using the path option, all the current configuration settings of the agent will be exported to the file you define in a readable ini format
-i l --importcfg [path]	Imports an updated set of agent configuration settings from a specified file in ini format	Import files are required to be in the same format as the export If no file is defined in the command line the user is entered into an editor mode, where it you can define configuration settings.
		Once entered into the editor you define the settings by entering the settings as per the expected format. To complete the edit and exit the user will press the letter d along with holding down the CTRL key. A success message should be displayed to inform that the update was successful.
		
-l l --listsvcs	lists the agent services currently active on the agent	Detailed information regarding the different services the Thycotic agent is currently providing and monitoring.

Example of ___-l l --listsvcs___ global command following the install of pmagent:

```
task: pmagent_registration
key: register
when: 2020-06-22 08:00:56
reoccurs: 60s
maxretries: forever
backoff: yes
attempts: 0
expires: 2262-04-12 00:47:16
last tried: never
```

Identity Bridge Configuration Utility

The ID Bridge Configuration Utility allows the setting of values used in the Thycotic panels under Active Directory User and Computers and User and Group Properties.

These values are used to enable the ID Bridge to manage the user authentication from Linux/Unix hosts to Active directory.

The ID Bridge Configuration Utility will allow Global setting of all values and selected values at an OU level.Below are all panels that appear under the ID Bridge Configuration Utility, each page outlines the functionality of the Panel

Default settings of values for User, Group, and OU attributes, including starting Id's, default home and shell parameters.

Assign Active directory groups at a global level to allow or deny login access to your Linux/Unix hosts.

Defaults for setting agent specific values, including Cached Logins, time sync, home directory permissions, and character separators.

Allow Active directory values to be mapped to Thycotic ID Bridge fields. For example based on AD terms, Display Name is mapped to Unix Username.

Sets the amount of time the local Linux/Unix agent will store a copy of the users password within the agent's encrypted database. This is required in the event the Agent is unable to contact AD to verify the users credentials.

Allows the ID Bridge user to configure the custom attribute variables for use within the Default User & Group Settings.

Provide a list of local user accounts that will automatically bypass the Identity Bridge portion of the authentication stack.

Licensing panel to view, add, and remove Thycotic ID Bridge licenses.

Allows the Linux/Unix host to utilize SysLog functionality, either logging the agent information locally or to a defined remote SysLog server.

Allows custom messages to be defined. The messages are displayed to user when accessing the Linux/Unix hosts.

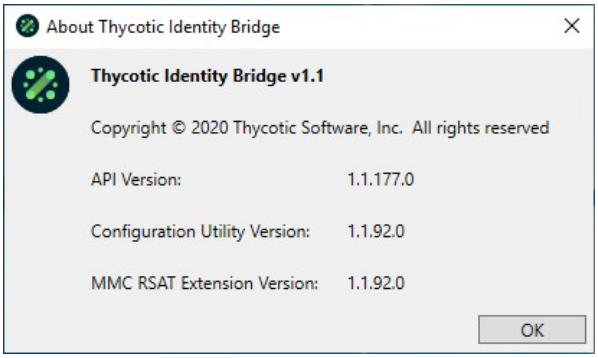
Shows an overview of where all Thycotic Identity Bridge configuration objects are stored in Active Directory.

Used to configure how Users and Groups are displayed.

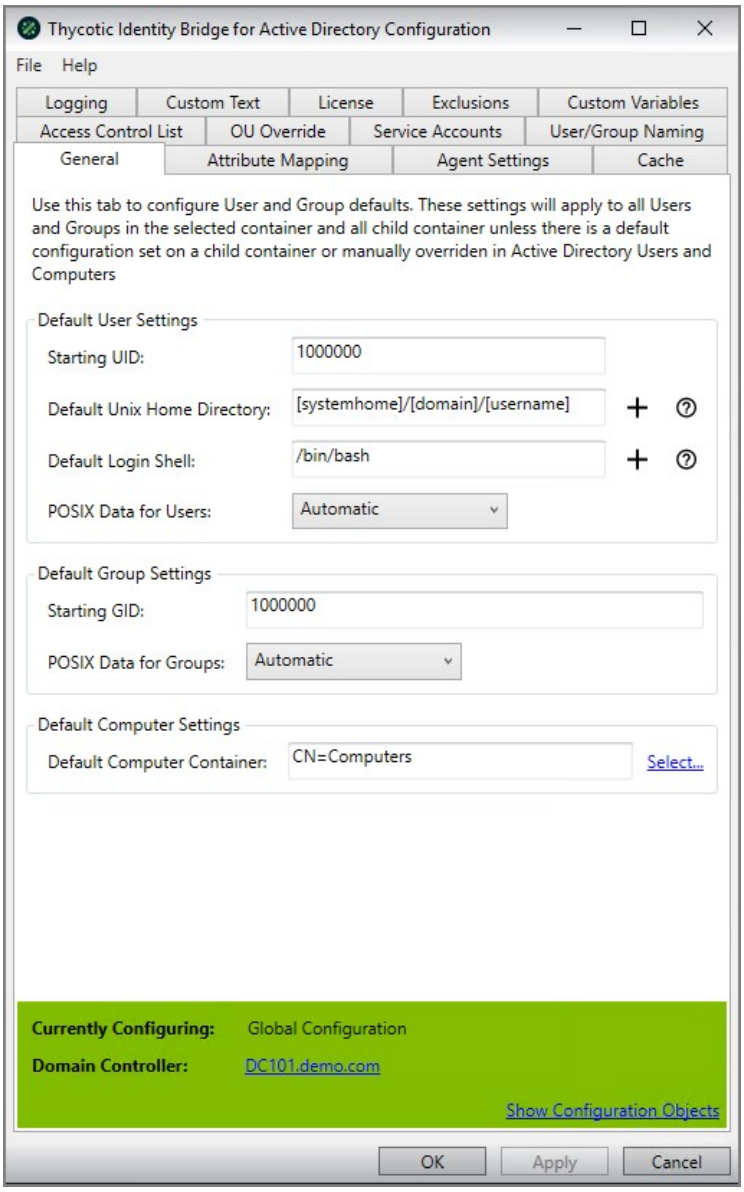
The File Menu of the configuration utility offers options like:

- Location: Opens the location selector.
- Refresh: Refreshes configuration utility data.
- Restore all Defaults: Restores the utilities data to default values.
- Export Changes to File: Audit feature, only exports the changed values in the application.
- Go to Global Configuration: If user is not already in the global configuration selecting this option navigates to it.
- Export Backup
- Import Backup

To view information about component versions of the Thycotic Identity Bridge, navigate to **Help** and select **About**.



Default settings of values for User and Group attributes, including starting ID's, default home and shell parameters.



Default User Settings

Starting UID

The starting UID that will be taken as starting point for all uid assignments.

- Default: value should be 1000000
- Only positive numeric characters can be set
- A maximum of 9 numeric characters can be used

Default Home Directory

The Home Directory Path that be used for users when logging into the Linux/Unix host.

- Default: [systemhome]/[domain]/[username]

Default Login Shell

The Shell that will be assigned to the user when logging into the Linux/Unix host.

- Default: /bin/bash

POSIX Data for Users

Defines if User POSIX data to be defined by Active Directory before Users are able to login into the Linux/Unix Hosts.

- Default: Automatic
- Automatic - If there is no POSIX data on the user in Active Directory (i.e. No UID/Shell/Home Dir), then generate POSIX data for the user during authentication.
- Manual - POSIX data will need to be specified for each User in ADUC before being able to authenticate to Linux/Unix Hosts
- Always - Always generate POSIX data during authentication, even if POSIX data has been set on user object

Default Group Settings

Starting GID

The starting GID that will be taken as starting point for all GID assignments.

- Initial Starting GID: value should be 1000000
- Only positive numeric characters can be set
- A maximum of 9 numeric characters can be used

POSIX Data for Groups

Defines if Group POSIX data to be defined by Active Directory before Users are able to login into the Linux/Unix Hosts.

- Default: Automatic
- Automatic - If there is no POSIX data on the group in Active Directory (i.e. No GID), then generate POSIX data for the group during authentication.
- Manual - POSIX data will need to be specified for each Group in ADUC before being able to authenticate to Linux/Unix Hosts.
- Primary Group Only - Generate GID for users primary group if Primary Group does not have an existing GID.
- Always - Always generate POSIX data during authentication, even if POSIX data has been set on group object.

Default Computer Settings

Default Computer Container

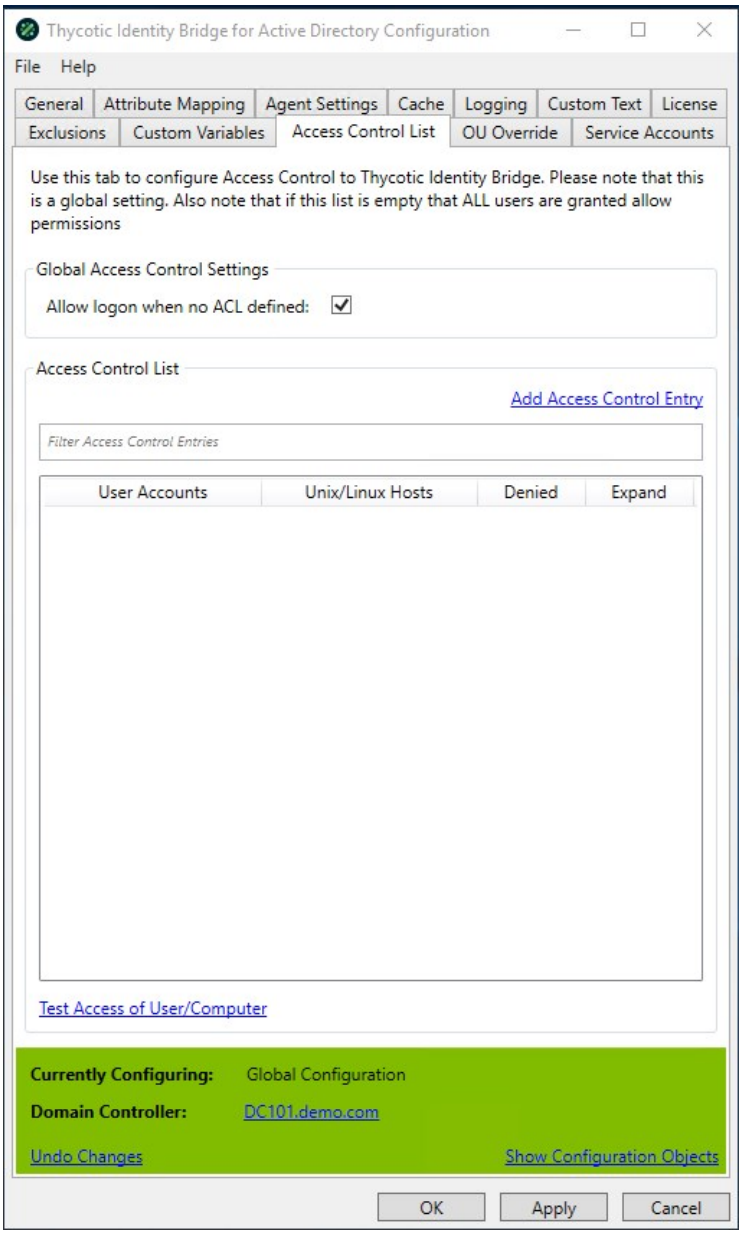
Defines the default OU container for Linux/Unix Hosts joining the Active Domain.

- Default: CN=Computers

Assign Active directory groups at a Global level to allow or deny login access to your Linux/Unix hosts.

If the Access Control List is empty All users are granted allow permissions.

For best practice a group should contain both user and computer objects, to create an effective Access Control List.



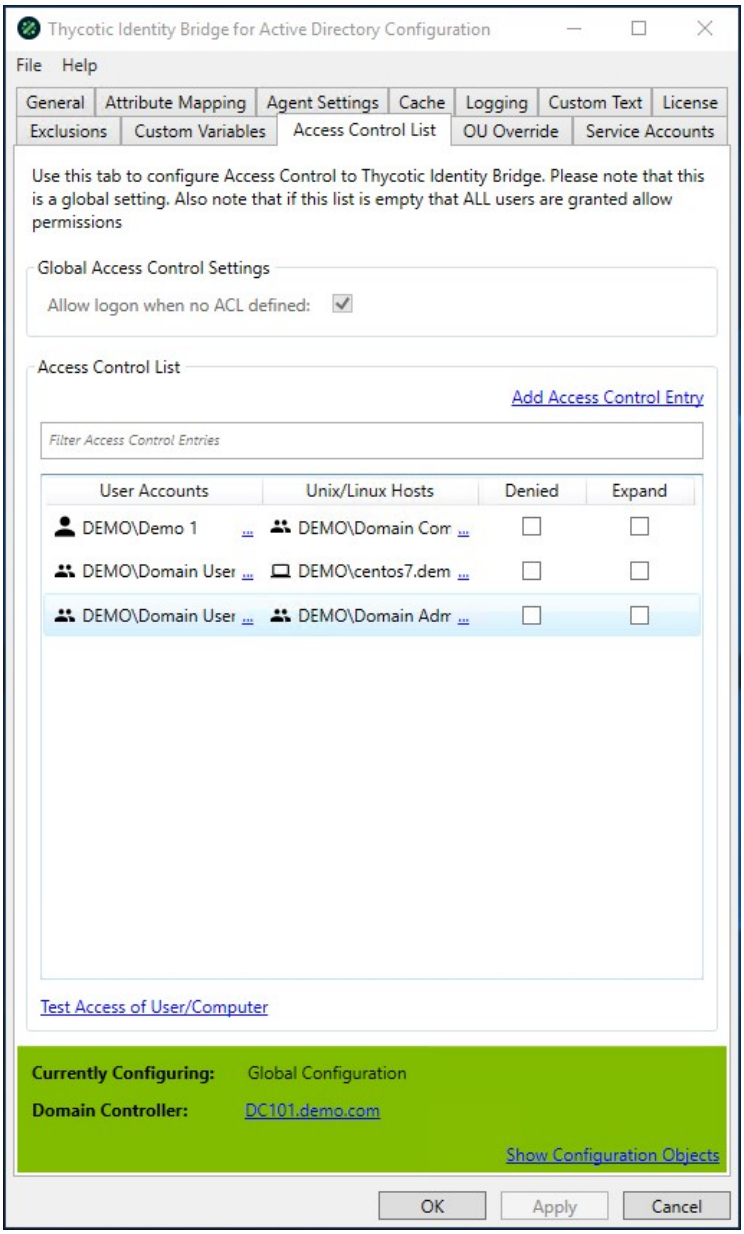
Global Access Control Settings

Allow logon when no ACL defined

Allows all Active Directory users logon permissions to all registered Linux/Unix hosts

- Default Allow logon when no ACL defined value: Enabled
- Once an ACL is defined, this option will become disabled and all access is controlled through the ACL definitions

Access Control List



Add Access Control Entry

Opens a modal to define User or User Group and Host or Host Group definitions for individual ACLs.

- An ACL must be unique combination

Filter

Allows filtering of exiting ACLs defined in the display panel

Panel

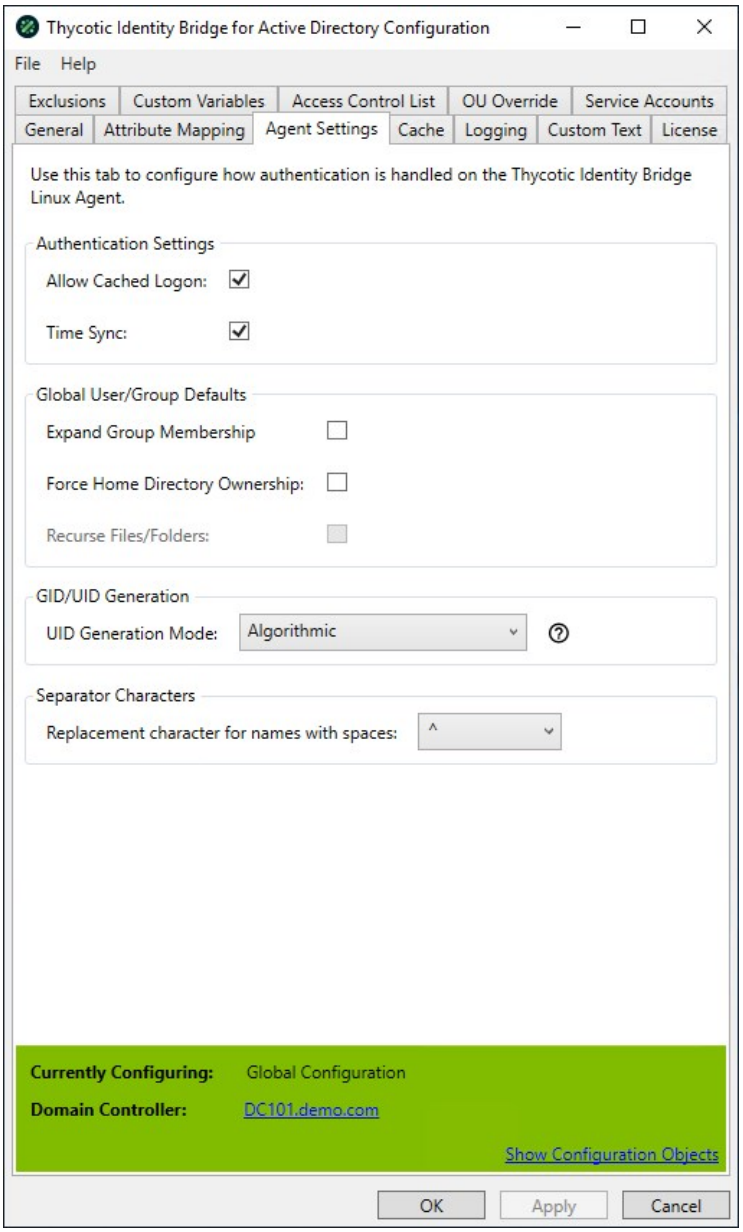
Displays that ACL combinations of Users and Hosts defined at a Global level.

- Once an ACL has been defined all access must abide by ACL rules.
- By default when an ACL is added permission for the ACL is enabled.
- Denied - When selected login access to the user host combination will be denied.
- Expand - When selected will display nested groups in the ACL report on the Unix/Linux Hosts.

Test Access of User/Computer

Test utility provided by Thycotic that reports access of users to computers against the defined ACLs.

Interface with Unix/Linux agents to manage settings that are passed to each agent.



Authentication Settings

Allow Cached Logon

Allows Active Directory Users to access Unix/Linux hosts using the encrypted cached information stored on the host

- A user must of logged onto the Unix/Linux Host previously for a cache entry to of been created.
- Default: Enabled.

Time Sync

Updates the Unix/Linux Hosts date & time to be the same as the Domain Controller of the Active Directory.

- Synchronises date and Time upon the host joining the Domain
- Enables a service on the host to keep the time within a minute of the Domain Controller
- Default value for Time Sync: Enabled

Global User/Group Defaults

Expanded Group Membership

Displays Active Directory Users extended group memberships when logged into the Unix/Linux hosts.

- When Disabled, the logged in Active Directory user will only see the groups the user is a member of directly.
- When Enabled, the logged in Active Directory user will also see any additional groups the users assigned groups are members of.
- Default: Disabled

Force Home Directory Ownership

When Active Directory users log into the Unix/Linux hosts the home directory ownership will be forcibly set to be owned by the user logging in.

- Default: Disabled

Recurse Files/Folders

Used in conjunction with Force Home Directory Ownership, when enabled all files and folders within the user's home directory will also have the ownership set to the Active Directory user logging into the Unix/Linux host.

- Can't be enabled unless Force Home Directory Ownership is enabled
- Default: Disabled## GID/UID Generation

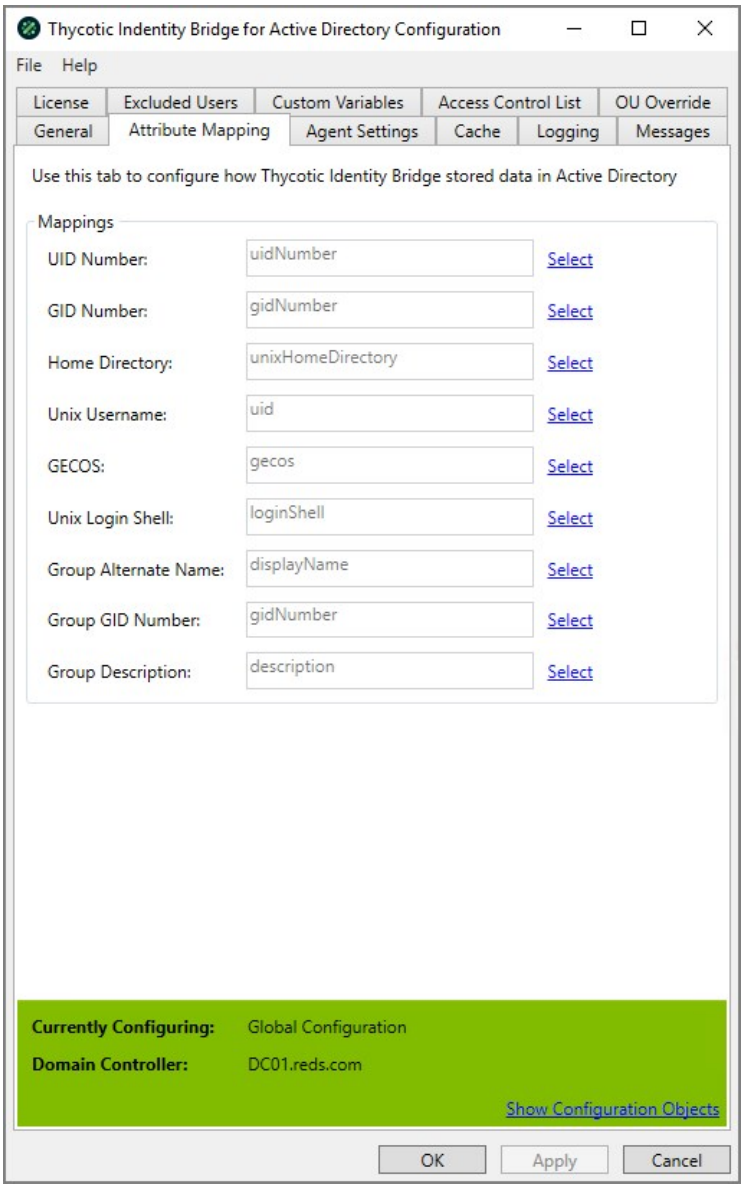
UID Generation Mode

Defines the format in which the UID and GID will be generate starting from the defined Starting ID values.

- Incremental – Will select the next ID available ID for user or group starting from the defined id
  - If a value has been previously assigned and removed it will not be added back to the available pool
- Default: Algorithmic

Provide the ability to directly map existing Active Directory fields to Thycotic ID Bridge fields.

We provide the ability to map attributes in the event a customer is leveraging a third party product in the AD environment that is already leveraging that value.



UID Number

The UID Number assigned to the Active Directory user

- Default value: uidNumber
- Thycotic value
- ADUC I User Properties I Thycotic I UID Number

GID Number

The GID Number assigned to the Active Directory Group

- Default value: gidNumber
- Thycotic value
- ADUC | Group Properties | Thycotic | GID Number

Home Directory

- Default value: unixHomeDirectory
- Thycotic value
- ADUC | User Properties | Thycotic | Home Directory

Unix Username

- Default value: uid
- AD value
- ADUC | User

GECOS

- Default value: gecos
- Thycotic value
- ADUC | User Properties | Thycotic | Comment (GECOS)

Unix Login Shell

- Default value: loginShell
- Thycotic value
- ADUC User Properties Thycotic Login Shell

Group Alternative Name

- Default value: groupAltName
- Thycotic value
- ADUC Group Properties Thycotic Alternative Group

Group GID Number

- Default value: gidNumber
- Thycotic value
- Querying

Group Description

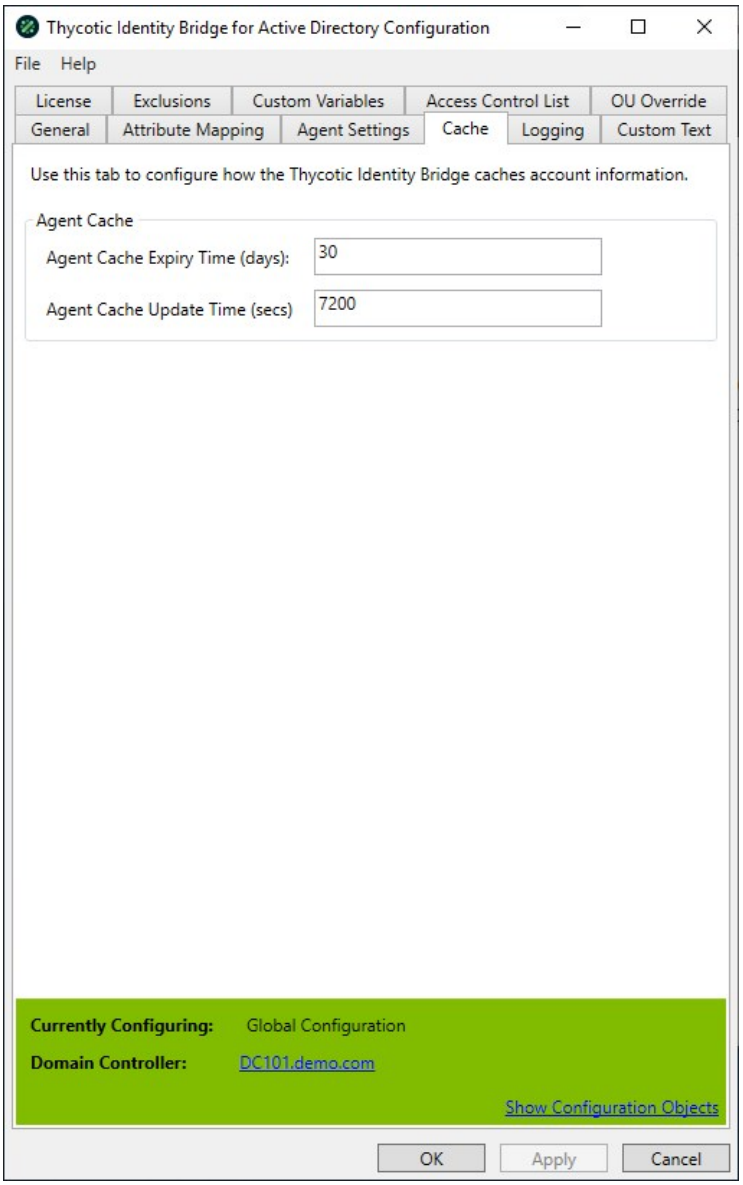
- Default value: description
- Thycotic value
- ADUC Group Properties Thycotic Description

Configures how the Thycotic Identity Bridge caches account information, values are sent down to the *nix Identity Bridge every 5 minutes or upon restart of the Agent.

The Cache tab contains two values:

- Agent Cache Expiry Time (days)
- Agent Cache Update Time (seconds)

These values are configurable.



Agent Cache Expiry Time (days)

Sets the amount of time until the Agent Cache expires on a local system.

Default: 30 days

Agent Cache Update Time

Sets the amount of time the local Linux/Unix agent will store a copy of the users password within the agent which can be used in the event the Agent is unable to contact AD to verify the users credentials. This value is user configurable, except when a trial license is in use. When licensed the Configuration Utility will enable the field and set the agents to use a default value of 7200 seconds. The field is disabled when the Identity Bridge is running with a Trial license and a hard coded value of 10 seconds on the *nix Agents, although the Configuration Utility will display the licensed default value.

- Default value: 7200 seconds with permanent key; 10 seconds with trial key

```
pmagent -s bridge.cachestale=7200
```

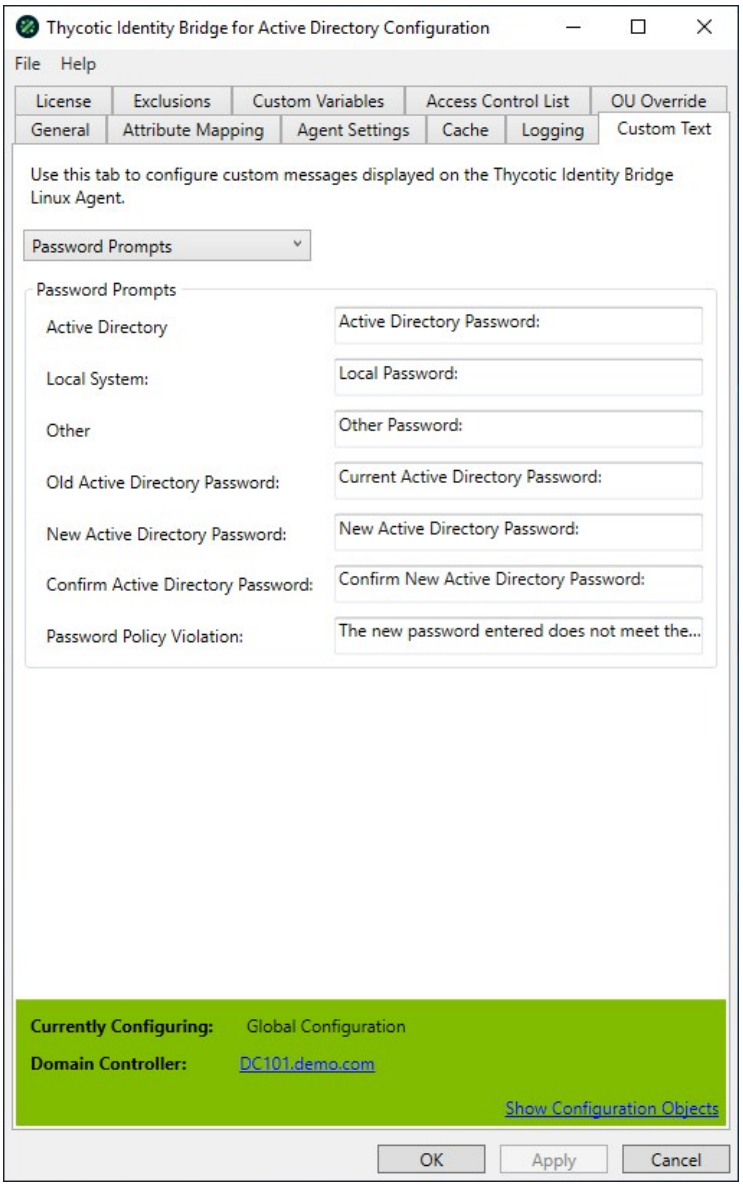
The Custom Text tab allows custom messages to be defined, that will be displayed to user when accessing the Linux/Unix hosts.

The following options are available:

- Password Prompts
- Friendly Messages
- Warning Messages
- Access Control Messages

Password message types can be customized via the Custom Text tab in the configuration utility.

Select Password Prompts from the drop-down options.



Note: Custom Variables cannot be used in the message fields.

Active Directory

Password prompt text displayed to Active Directory users when logging into Linux/Unix host

- Default Active Directory value: Active Directory Password

Local System

Password prompt text displayed to locally defined Linux/Unix users when logging into Linux/Unix host.

- Default Local System value: Local Password:

Other

Password prompt text displayed when user accessing Linux/Unix host via 3rd party remote user credential service.

- Default Other value: Other Password

Old Active Directory Password

Displayed when Active Directory users are changing their password on the Linux/Unix host.

- Request to define users existing password
- Default Old Active Directory Password value: Current Active Directory Password

New Active Directory Password

Displayed when Active Directory users are changing their password on the Linux/Unix host.

- Request to enter a new password
- Default New Active Directory Password value: New Active Directory Password:

Confirm New Active Directory Password

Displayed when Active Directory users are changing their password on the Linux/Unix host.

- Request to confirm new password
- Default Confirm New Active Directory Password value: Confirm New Active Directory Password

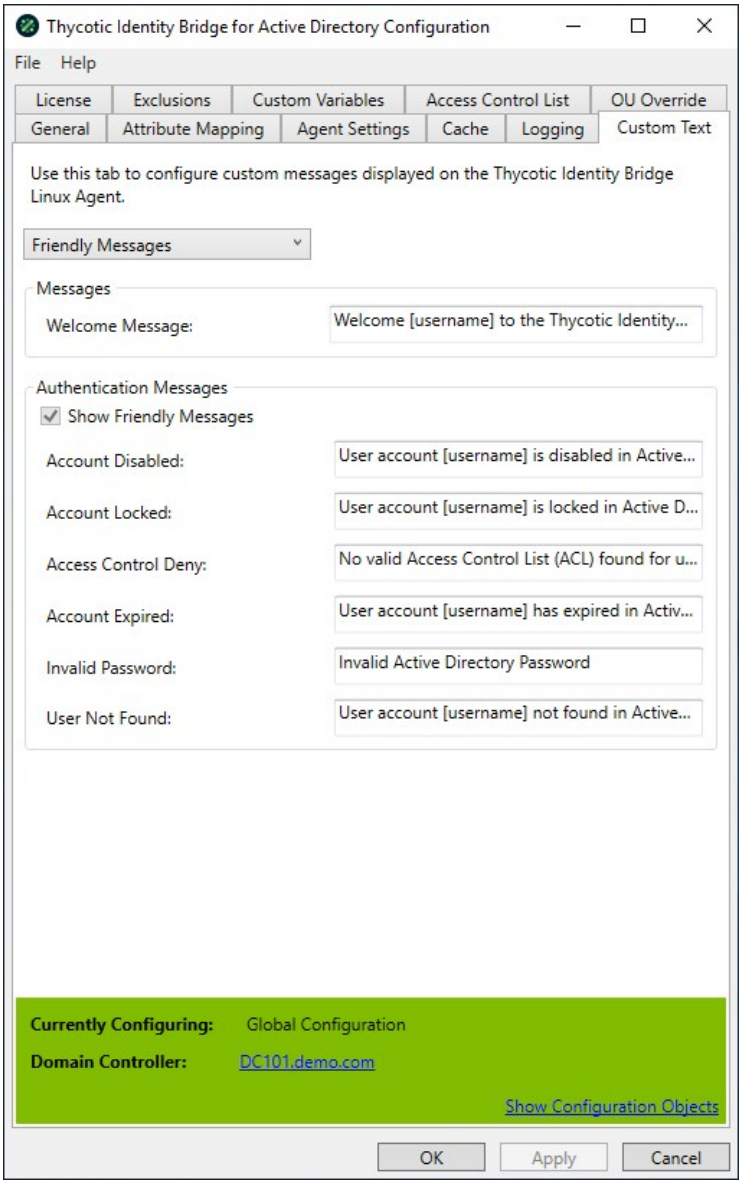
Password Policy Violation

Displayed when Active Directory users are changing their password and the new password does not meet the Active Directory policy requirements.

- Request to meet the AD password policy requirements
- Default: The new password entered does not meet the password policy defined in Active Directory.

Friendly Message message types can be customized via the Custom Text tab in the configuration utility.

Select Friendly Messages from the drop-down options.



Welcome Message

Message displayed to all Active Directory users as they login to the Linux/Unix Hosts

- Supports customer variables in the message field, such as [username] and [hostname]
- Default Welcome Message: Welcome [username] to the Thycotic Identity Bridge on [hostname]

Authentication Messages

Messages displayed to all Active Directory users when various Active Directory states are discovered upon logging into Linux/Unix hosts.

- Supports customer variables in the message field, such as [username] and [hostname]

Show Friendly Messages

Option to enable/disable all Authentication messages.

- With trial license in place, option will be defaulted to enabled.
- With a perpetual is license applied, option will be defaulted to disabled, but it can be enabled.

Account Disabled

Displayed when Active Directory user has been disabled within ADUC.

- Default Account Disabled value: User account [username] is disabled in Active Directory

Account Locked

Displayed when Active Directory user account has become locked through to many invalid password attempts.

- Default Account Locked value: User account [username] is locked in Active Directory

Access Control Deny

Displayed when the Active Directory user does not have a valid Access Control list entry within the Thycotic Configuration Utility.

- Default Access Control Deny value: No valid Access Control List (ACL) found for user [username] on [hostname]

Account Expired

Displayed when Active Directory user account has passed defined Account expiry value in ADUC.

- Default Account Expired value: User account [username] has expired in Active Directory.

Invalid Password

Displayed when Active Directory user enters an invalid password.

- Default Invalid Password value: Invalid Active Directory Password

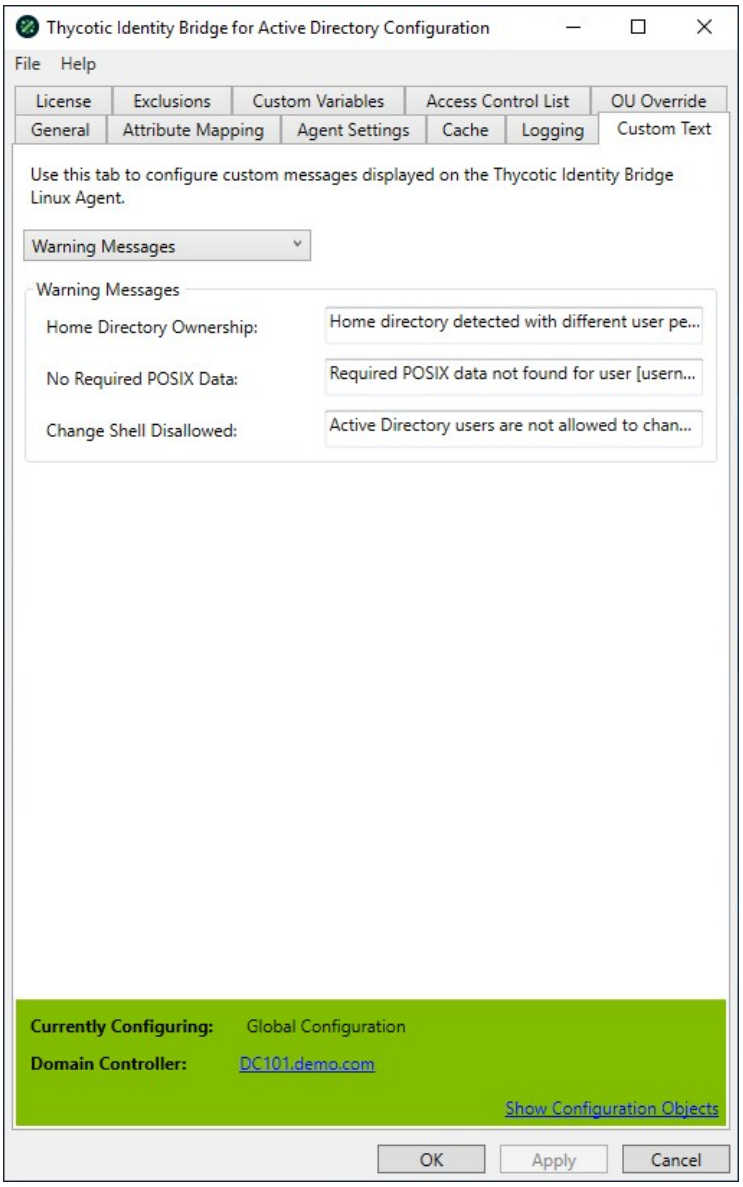
User Not Found

Displayed when username entered can not be found within Active Directory.

- Default User Not Found value: User account [username] not found in Active Directory

Warning Messages message types can be customized via the Custom Text tab in the configuration utility.

Select Warning Messages from the drop-down options.



Messages displayed to all Active Directory users when configuration discrepancies occur.

- Supports customer variables in the message field, such as [username] and [hostname]

Home Directory Ownership

Displayed when Active Directory user logs into Linux/Unix host and home directory location exists, but with different ownership rights.

- Default Home Directory Ownership value: Home directory detected with different user permissions

No Required POSIX Data

Displayed when Active Directory users require POSIX data to be defined in ADUC before being able to access Linux/Unix hosts.

- Default No Required POSIX Data value: Required POSIX data not found for user [username]

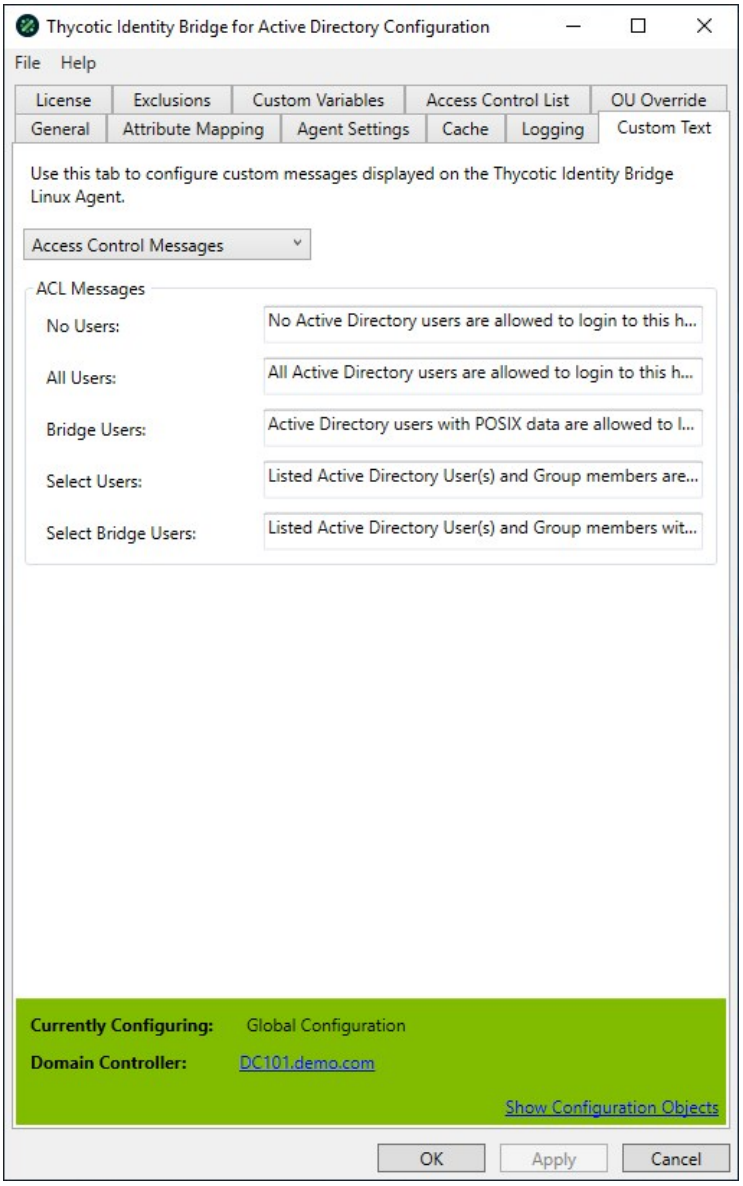
Change Shell Disallowed

Displayed when the Active Directory user attempts to change their Linux/Unix default shell type.

- Default: Active Directory users are not allowed to change their assigned shell.

Access Control Messages message types can be customized via the Custom Text tab in the configuration utility. These message can be displayed when running the ACL report command from the Linux/Unix agent.

Select Access Control Messages from the drop-down options.



The following message are displayed when the ACL report is run on the Linux/Unix agent by performing the following command: `pmagent --bridge --acl`

No Users

Message displayed when No Active Directory users have access to the Agent running the ACL report.

Default	No Active Directory users are allowed to login to this host.
Settings	Allow Logon when no ACL Defined: Disabled
	Access Control List: No ACL defined for user/host
General	POSIX Data for Users & Groups: Manual/Automatic

All Users

Message displayed when all Active Directory users have access to the Agent running the ACL report.

Default	All Active Directory users are allowed to login to this host.
Settings	Allow Logon when no ACL Defined: Enabled
	Access Control List: No ACL defined for user/host
General	POSIX Data for Users & Groups: Automatic

Bridge Users

Message displayed for Active Directory users with POSIX data defined and have access to the Agent running the ACL report.

Default	Active Directory users with POSIX data are allowed to login to this host.
Settings	Allow Logon when no ACL Defined: Enabled
	Access Control List: No ACL defined for user/host
General	POSIX Data for Users & Groups: Manual

Select Users

Message displayed when Active Directory users and group members defined within the configuration utility ACL panel have access to the Agent running the ACL report.

Default	Listed Active Directory User(s) and Group members are allowed to login to this host.
Settings	Allow Logon when no ACL Defined: Enabled (not changeable)
	Access Control List: No ACL defined for user/host

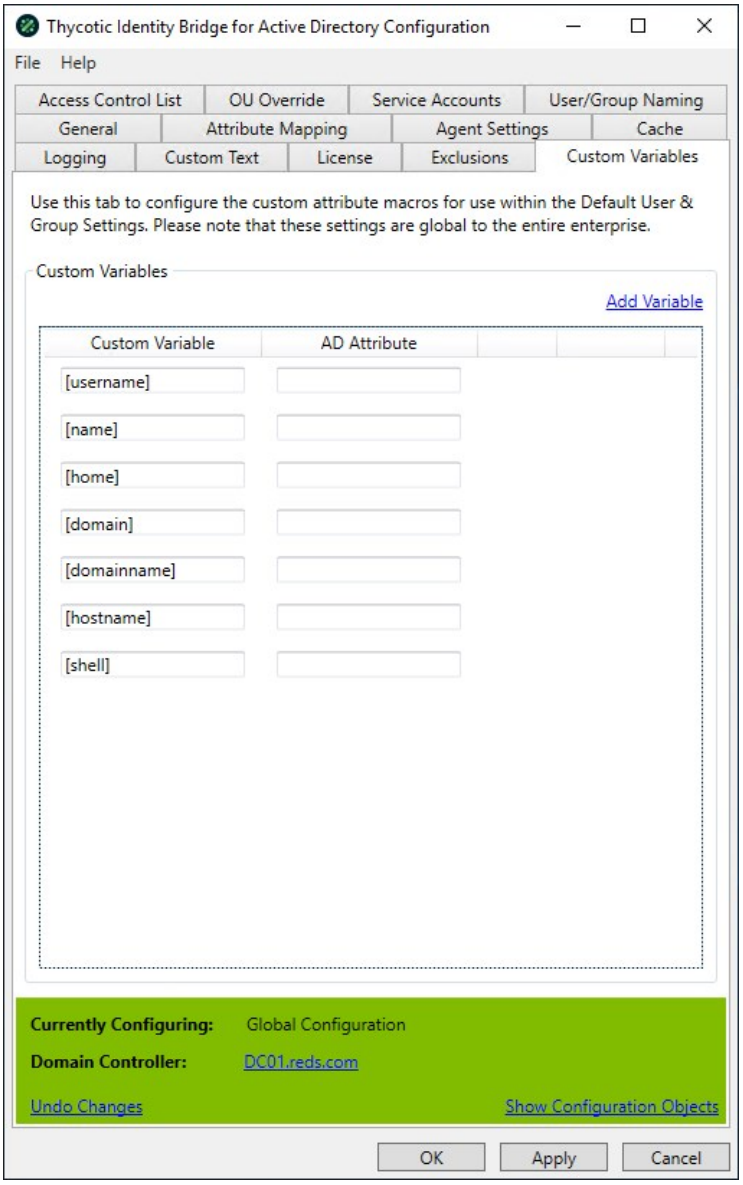
General	POSIX Data for Users & Groups: Automatic

Select Bridge Users

Message displayed for Active Directory users and group members defined within the configuration utility ACL panel with POSIX data defined to have access to the Agent running the ACL report.

Default	Listed Active Directory User(s) and Group members with POSIX data are allowed to login to this host.
Settings	Allow Logon when no ACL Defined: Enabled (not changeable)
	Access Control List: No ACL defined for user/host
General	POSIX Data for Users & Groups: Manual

Use this tab to configure the custom attribute variables for use within the Default User & Group Settings. Please note that these settings are global to the entire enterprise.



Add Variable

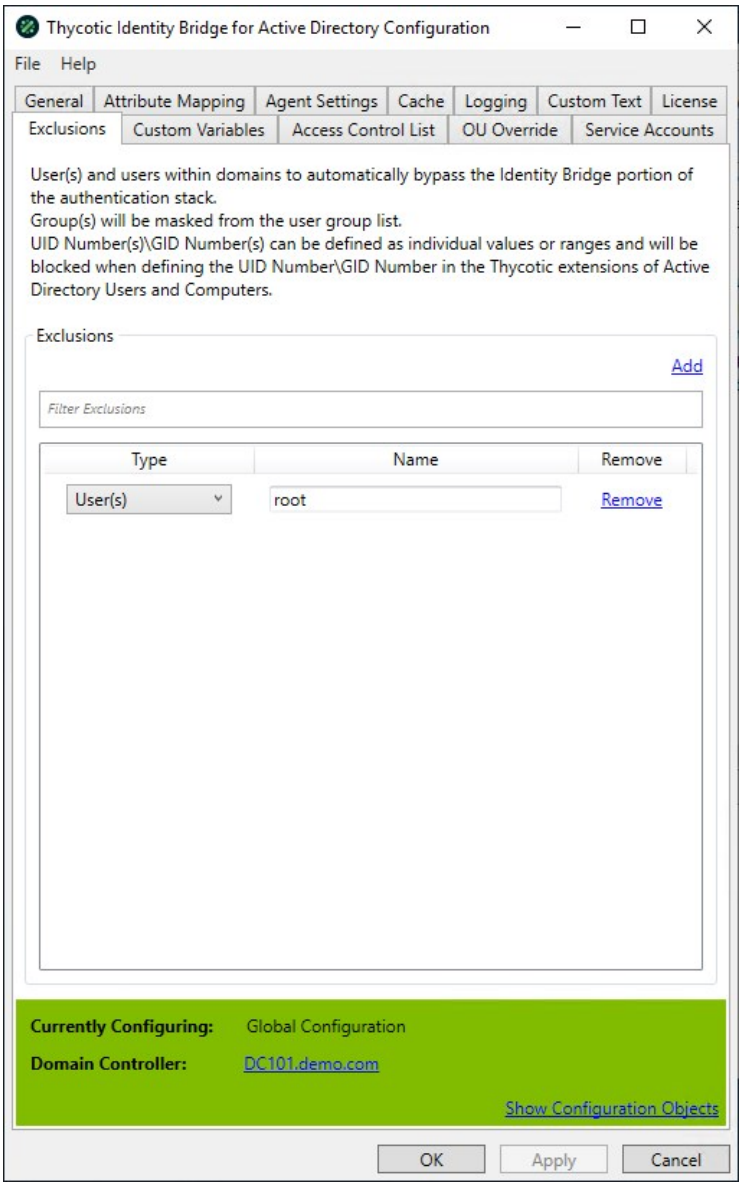
Adds a new line to the panel and allows you to define a variable name and then select from a list of Active Directory attributes and define a single attribute mapping per variable.

Defaults

A number of predefined default variables have been added by Thycotic, these are also used in the Messages panel.

Allows to provide a list of local and domain user accounts that will automatically bypass the Identity Bridge portion of the authentication stack. This excludes the domain the configuration utility is connected to.

Groups are masked from the list. It's possible to define individual or ranges of UIDs and GIDs to be excluded.



User and/or Group Exclusions

Add

Open a text based modal where the Linux/Unix username can be defined and added to the list of excluded user.

Filter

Allows the defined excluded user list to be filtered.

Exclusions Panel

The panel shows the applied exclusions types, the values assigned and an option to remove.

User(s)

Users will automatically bypass the Identity Bridge portion of the authentication stack on the *nix agents.

- Users can be defined singular or by a comma separated list
- Both Local and Active Directory users can be defined
- Default: root
    - By default the root user will always bypass the Identity Bridge portion of the authentication stack on the *nix agents.

UID(s) Number

UID value/range will be excluded as an applicable value as UID Number in the Thycotic User Data extension of ADUC.

- UID numbers can be defined as a single value, comma separated list or range of values.

GID(s) Number

GID value/range will be excluded as an applicable value as UID Number in the Thycotic User Data, Thycotic Group Data and Thycotic Overrides extensions of ADUC.

- GID numbers can be defined as a single value, comma separated list or range of values.

Domain

Users defined within the domain will automatically bypass the Identity Bridge portion of the authentication stack on the *nix agents.

- The domain is required to be defined in full FQDN format, for example: child.demo.com.
- Exclusion will not apply to the root domain the Configuration Utility is connected to.

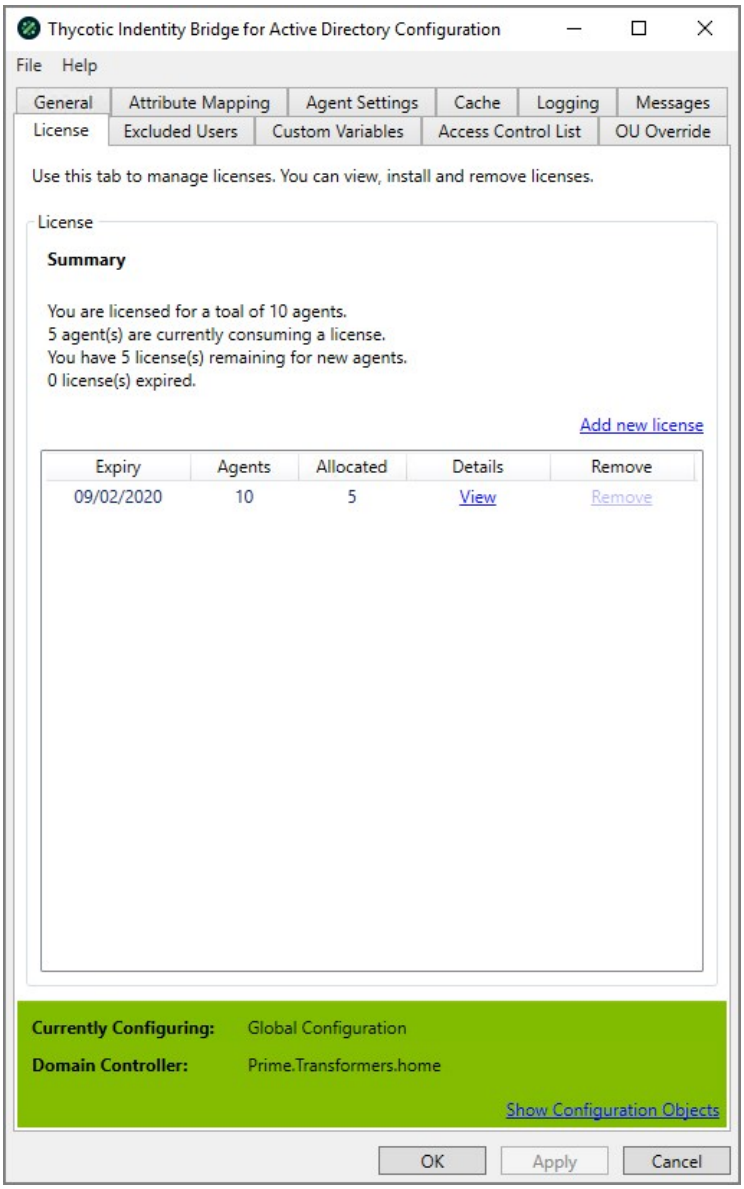
Group(s)

Defined Groups will be masked from the Active Directory users group list on the *nix agent.

- Groups can be defined singular or by a comma separated list.

Licensing Panel to view, add, and remove Thycotic Identity Bridge Licenses.

- Multiple licenses can be applied
- Licenses apart from the Trial license can be removed



Default Trial License

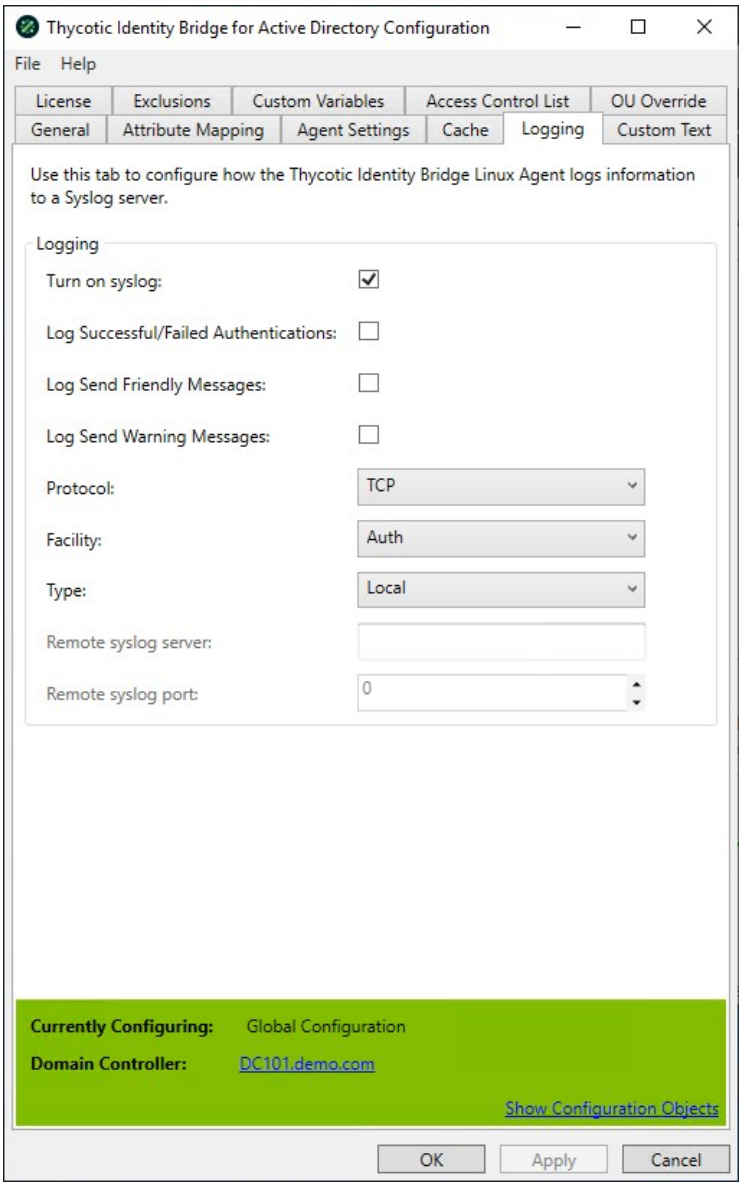
By default installing the Thycotic Identity Bridge a 10 agent Trial license is provided with a 30 day expiry.

Add new license

Provides a modal to allow addition of Thycotic allocated licenses.

Delinea

Allows the Linux/Unix host to utilize SysLog functionality, either logging the agent information locally or to a defined remote SysLog server.



Note: Making changes to the syslog settings in the Configuration Utility, will also require a restart of the *nix Agent for the updated settings to take effect.

Logging

Turn on SysLog

Defines if Agent logging also sent to SysLog as well as existing agent pmlog.

- Default: Disabled

Log Successful/Failed Authentications

Sends Active Directory Authentication outcomes to the syslog.

- Default: Disabled

Log Send Friendly Messages

Send Friendly Messages displayed to users to syslog.

- Default: Disabled

Log Send Warning Messages

Send Warning Messages displayed to users to syslog.

- Default: Disabled

Protocol

The communication protocol used to send Linux/Unix host information to SysLog.

- Default: TCP

Facility

Defines the Linux\Unix host process component that will be sent to the SysLog.

- Default: Auth

Type

Defines if Linux\Unix host will use a local or remote SysLog server.

- Default: Local
- If remote selected the Remote SysLog server and Remote SysLog port fields will become enabled.

Remote SysLog Server

Defines the address of the remote SysLog server to which the Linux/Unix hosts send their defined SysLog information.

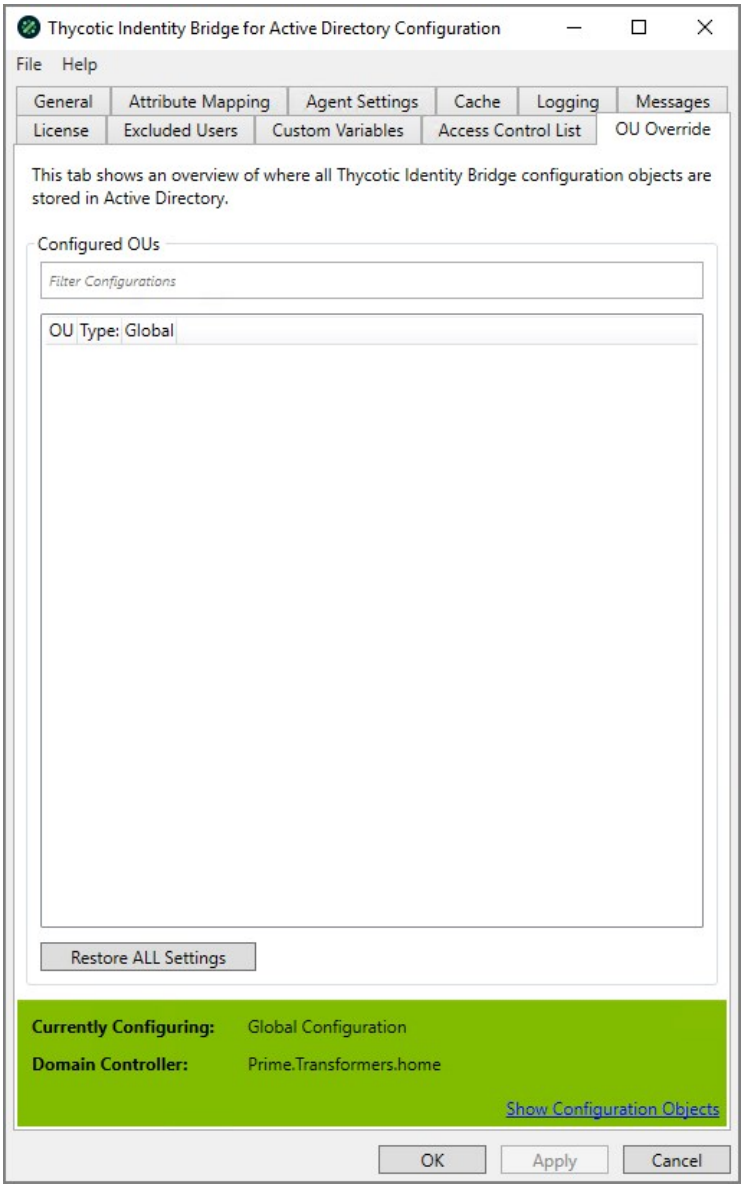
- Default: Blank
- When enabled defined by the resolvable host name or IP address.

Remote SysLog Port

Defines the port SysLog uses for communication.

- Default: 0

Shows an overview of where all Thycotic Identity Bridge configuration objects are stored in Active Directory.



Configured OUs

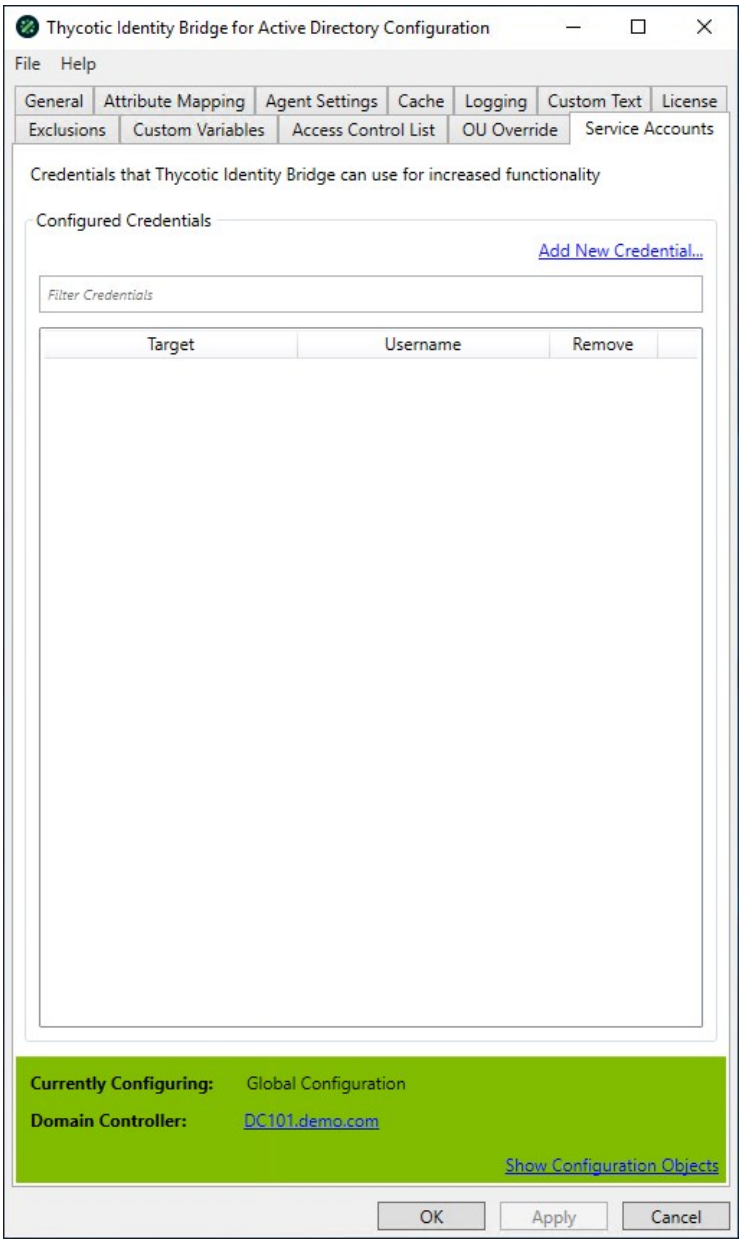
Filter

Allows filtering of Configured OU's defined in the display panel.

Restore ALL Settings

Will restore all configuration settings back to defaults, as if clean install has been performed.

Service Accounts allow to define Active Directory accounts across different domains that Identity Bridge can utilise to function effectively across multi-domain environments.



Configured Credentials

Add New Credentials

Opens a new modal that allows to define the domain, username and password of the credentials to access domains within the Active Directory environment.

Filter

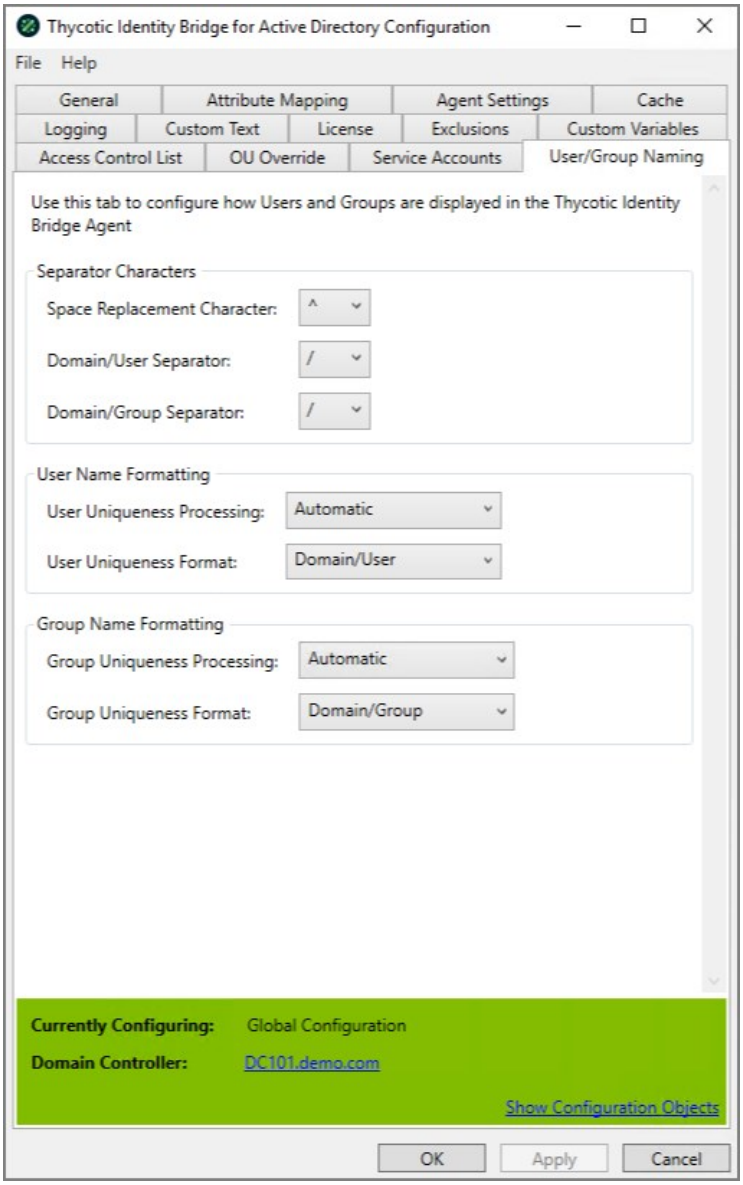
Allows filtering of existing Credentials defined in the display panel.

Panel

Displays the Target Domain and Username for the Configured Credentials. A remove option is available.

> **Note**: Defined Configured Credentials won't be included in Identity Bridge Configuration exports.

Used to configure how Users and Groups are displayed.



Separator Characters

Space Replacement Character

Defines how spaces in User and Group names will be displayed on the Unix/Linux hosts.

Default: **^**

Domain/User Separator

Defines how the separator between the Domain and User name is displayed.

Default: **/**

Domain/Group Separator

Defines how the separator between the Domain and Group name is displayed.

Default: **/**

User Name Formatting

User Uniqueness Processing

Defines how Identity Bridge will process Duplicate Active Directory usernames when user logs into the Unix/Linux Hosts

- Default: Automatic
- Never - Ignore Duplicate users
- Automatic - Generates a unique user name by adding or appending the domain information to the user for all domains except for the joined domain.
- Only Duplicates - Generates a unique user name by adding or appending the domain information to the user when a duplicate name is detected.
- Always - Generates a unique user name by adding or appending the domain information to the user for all domains.

User Uniqueness Format

Defines the order in which the Active Directory username will be displayed on the Unix/Linux Host when the Active Directory username is duplicated due to a Multi Active Domain environment

- Default: Domain/User
- The selection will reflect the defined Domain/User Separator.

Group Name Formatting

Group Uniqueness Processing

Defines how Identity Bridge will process Duplicate Active Directory groups with users logging into the Linux\Unix Hosts

- Default: Automatic
- Never - Ignore Duplicate groups
- Automatic - Generates a unique group name by adding or appending the domain information to the group for all domains except for the joined domain.
- Only Duplicates - Generates a unique group name by adding or appending the domain information to the group when a duplicate name is detected.
- Always - Generates a unique group name by adding or appending the domain information to the group for all domains.

Group Uniqueness Format

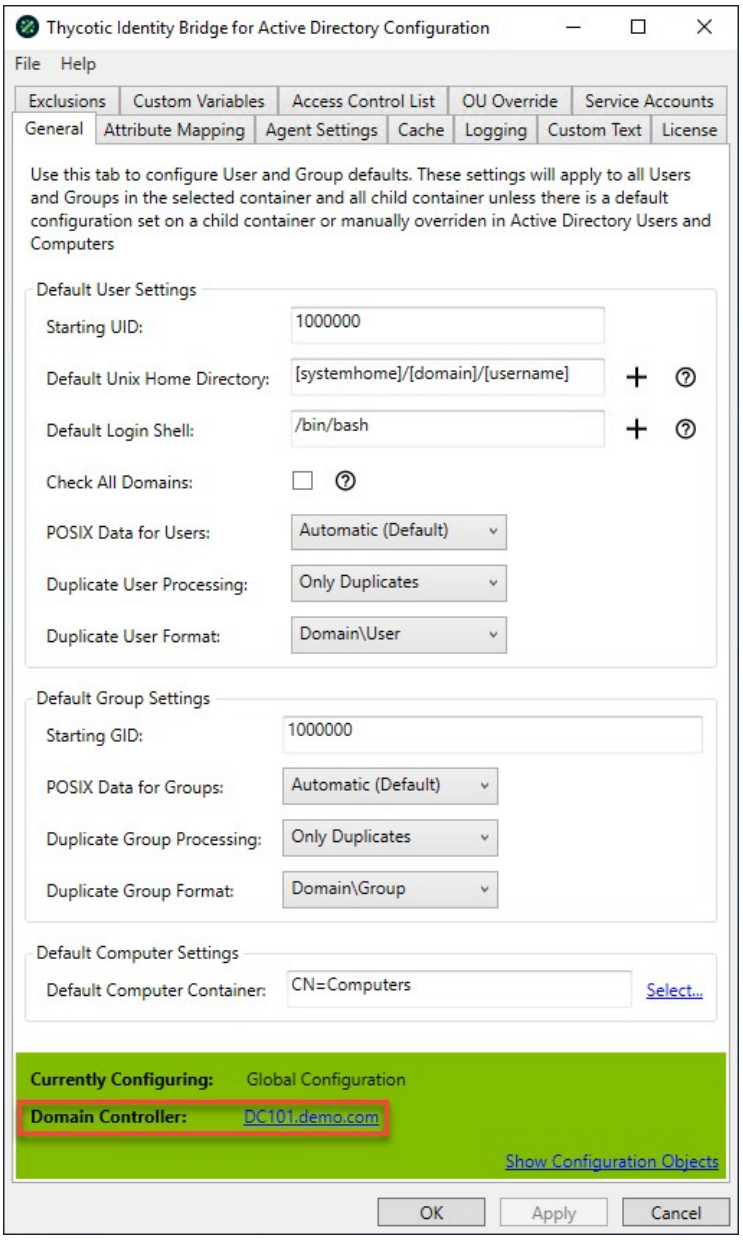
Defines the order in which the Active Directory group will be displayed on the Unix/Linux Host when the Active Directory username is duplicated due to a Multi Active Domain environment.

- Default: Domain/Group
- The selection will reflect the defined Domain/Group Separator.

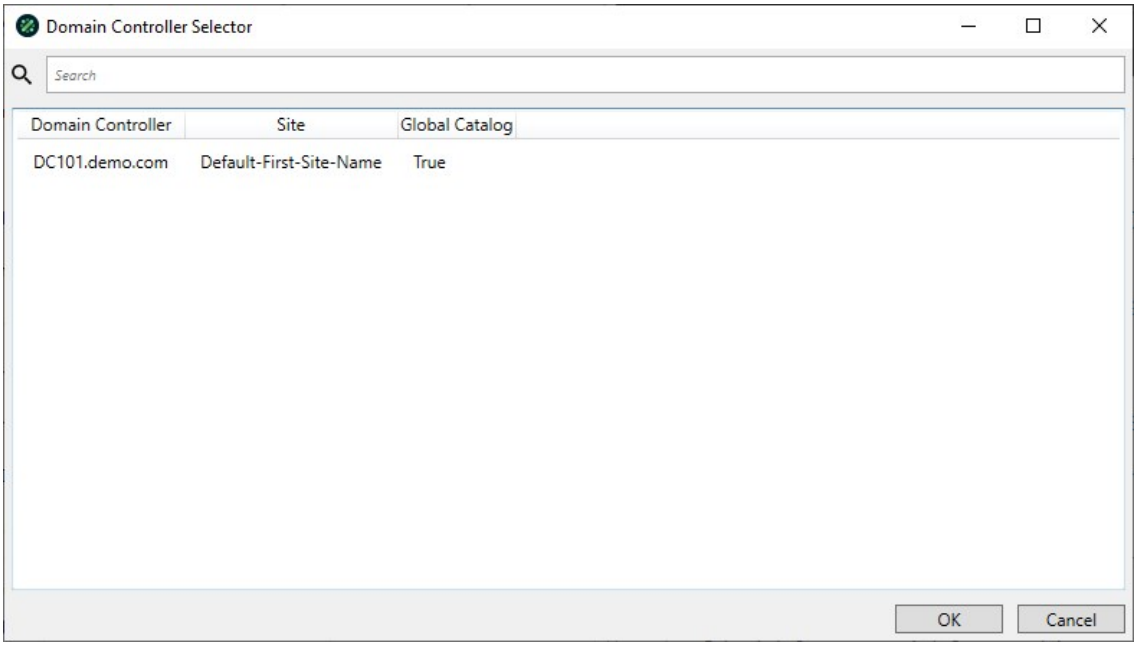
Domain Controller Selector

When the Configuration Utility is opened, it connects to the nearest Domain Controller according to the environmental setup in Active Directory Sites and Services.

Users can change the connected Domain Controller on their Configuration Utility pages. At the bottom of each utility tab is the Domain Controller information. Click on the link to select a different Domain Controller.

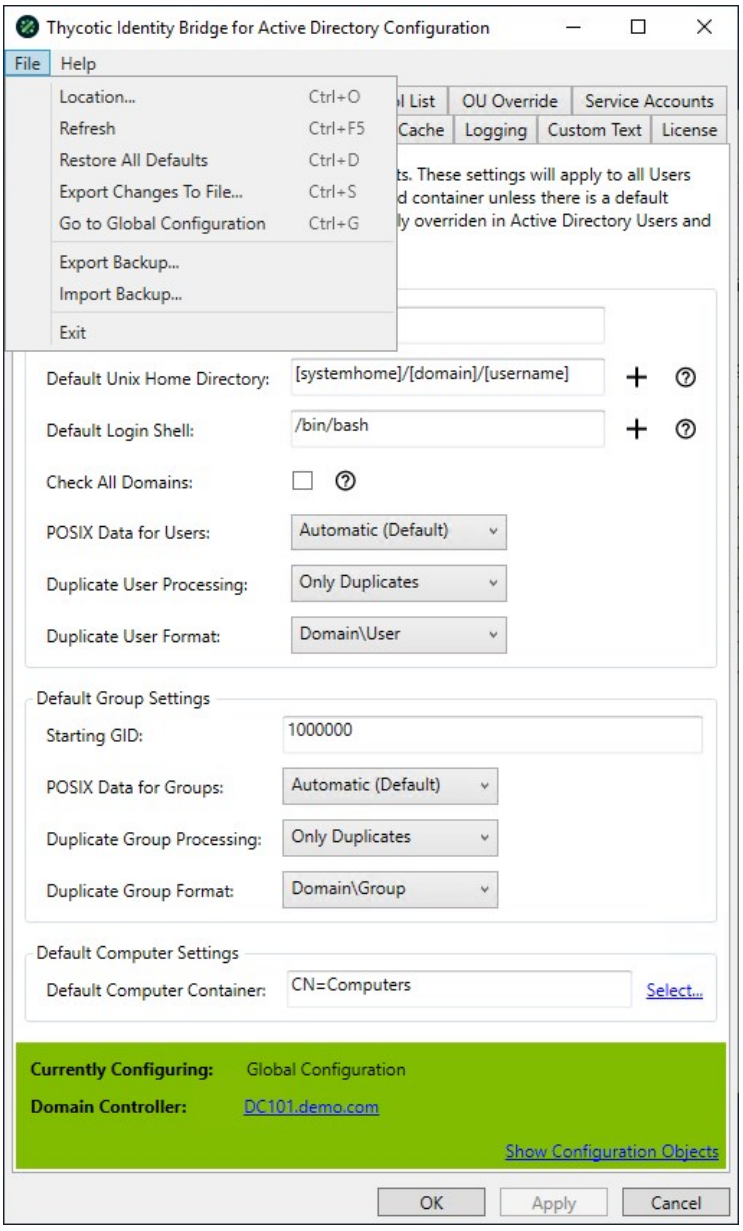


A modal opens, displaying available Domain Controllers for the users environment.


Domain Controller Selector
Search
Domain Controller
Site
Global Catalog
DC101.demo.com
Default-First-Site-Name
True
OK
Cancel

The Thycotic Identity Bridge Configuration Utility provides the ability to Export and Import all settings from the Configuration Utility via a backup file (.IBBAK).

The functionality can be accessed view the File Menu and the menu items are **Export Backup** and **Import Backup**.



Export Backup

Opens a modal to provide a location and name for the settings to be exported to.

- Any applied licenses will not be included in the export.
- Any accounts defined in the Service Accounts Panel will not be exported.

Import Backup

Provides a modal to select a previously created backup.

Backup Files

Backup files can be edited using a standard text editor. Exercise caution when modifying backup files as not to cause corruption.

> **Warning**: Exporting and and Importing backups across different domains connected to the Identity Bridge Configuration Utility may cause unexpected behavior. Backups contain settings that are domain specific based on the domain they were created in and not all domains contain the same structures or information.

ADUC Extension

The Thycotic Identity Bridge Extension provides Thycotic Panels in Active Directory Users and Computers (ADUC) MMC for a number of container types.

The Thycotic extension panel can accept settings from the ID Bridge Configuration Utility allowing certain fields to be pre-populated, although there is no dependency between the Utility and the Extension.

From the Thycotic panel you can manage fields independently as well as generate UID and GID values for users and groups respectively.

- Panel that allows you to manage the ID Bridge values on an individual user basis.
- This includes UID Number, primary group membership and additional Linux/Unix user attributes.

Panel that allows creation of an alternate username (logon alias) which can be used when accessing the Unix/Unix host.

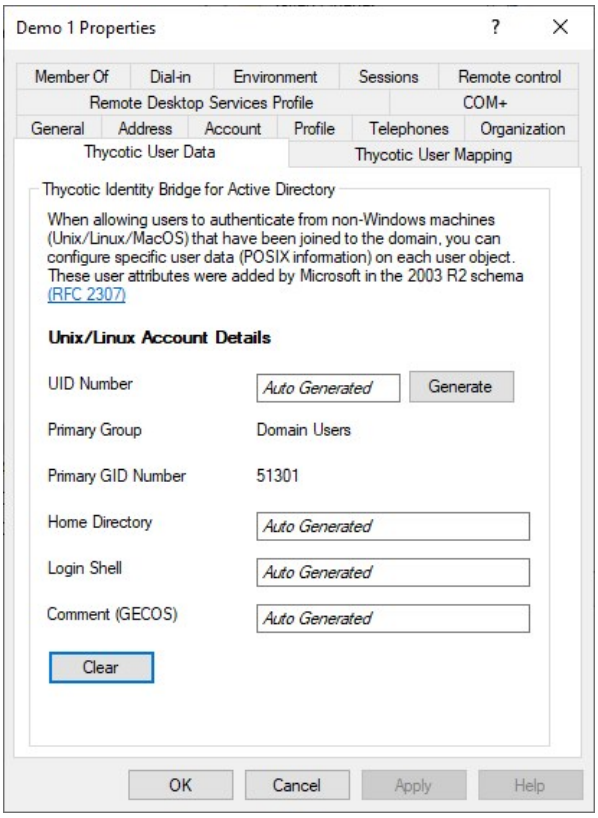
- Panel that allows you to manage the ID Bridge values on an individual group basis.
- This includes GID Number, Description and additional Linux\Unix group attributes.

Allows override of some global POSIX user fields at the OU level.

Displays a list of all the Active Directory users that can access this computer and their associated user mapping name (username alias).

Thycotic User Data

The Thycotic panels under user properties of ADUC allows you to manage the ID Bridge components related to Linux/Unix user attributes.



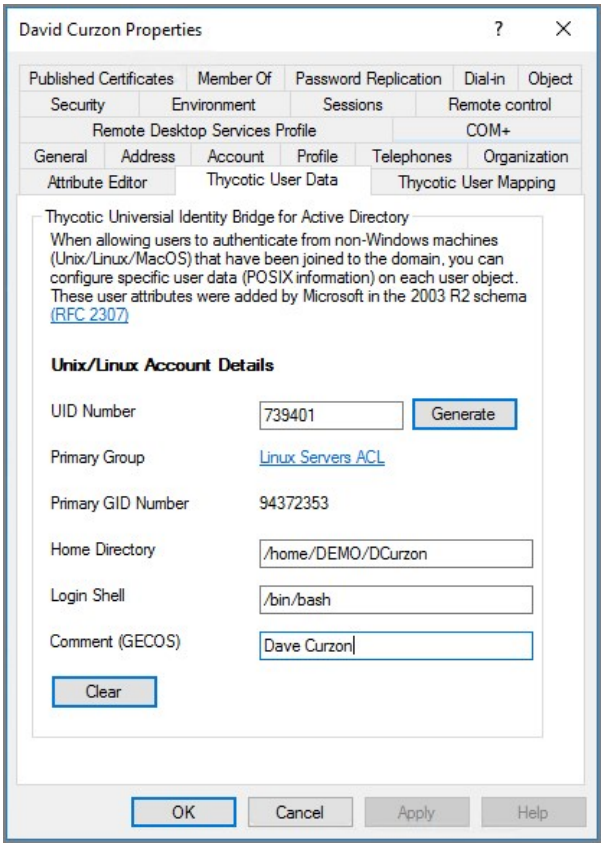
When the POSIX Data for the Users & Groups field in the Thycotic Configuration Utility is set to Automatic the user fields will be displayed with Auto Generated, meaning when the user accesses a Linux/Unix host the fields will automatically be generated.

Mousing over the fields will display the parameters that have been assigned to that field.

These fields can be manually overridden and will display as such once saved.

- This is the unique user id number to both the active directory forest and each AD user account for accessing Linux/Unix agents.

- The Generate button will create a unique UID Number in accordance to the chosen method for that user account.
- UID's will not be re-used
- The generated UID value will be greater than the Starting UID defined in the ID Bridge Configuration utility
- If the User has a UID Number the generate button will not create a new UID



The GID number of the Primary group assigned to the user under the Member of Panel of the User Properties.

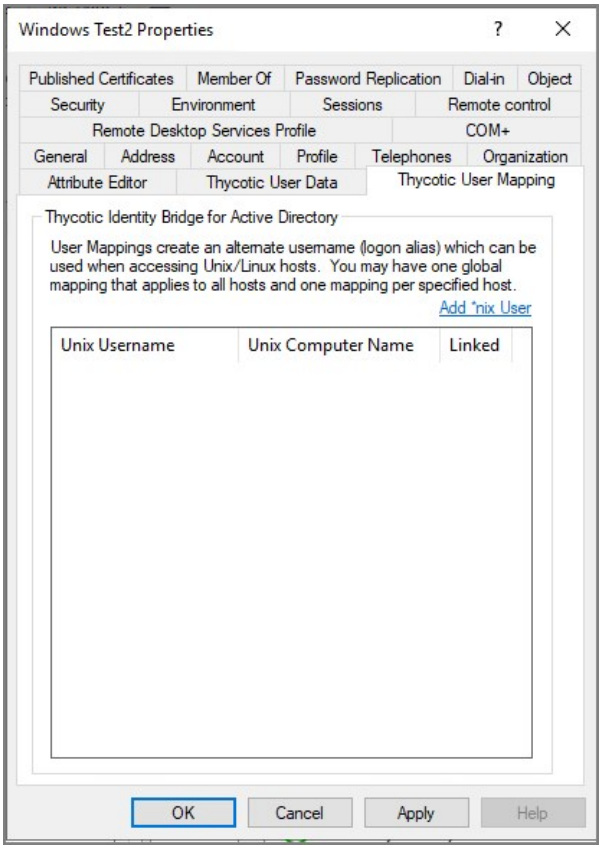
- Defines the home location of the user when they log into the Linux/Unix agent.
- This is normally their landing folder.

- Defines the Linux/Unix shell that will be assigned to that user on login.

- Gecos is are short text fields in /etc/passwd of the Linux/Unix Agent that keeps the users real name

Thycotic User Mapping

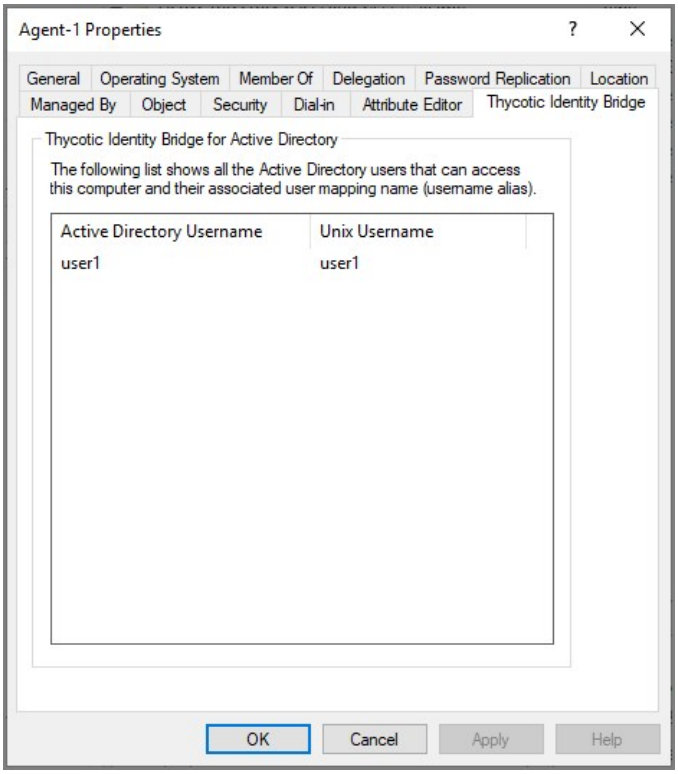
User Mappings create an alternate username (logon alias) which can be used when accessing Linux/Unix hosts. You may have one global mapping that applies to all hosts and one mapping per specified host.



Open a modal with a free text username field and optional hosts selection field.

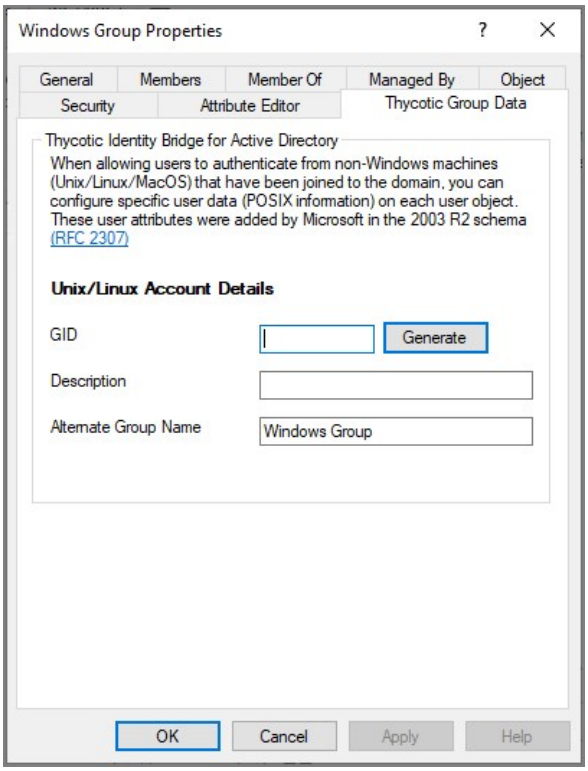
Thycotic ID Bride - Computers

The Thycotic Identity Bridge panel under group properties of ADUC, displays a list of all the Active Directory users that can access this computer and their associated user mapping name (username alias).



Thycotic Group Data

The Thycotic panels under group properties of ADUC allows you to manage the ID Bridge components related to Linux/Unix user attributes



- This is the unique group id number assigned to each AD group account, which is assigned to a user account for accessing Linux/Unix agents.

- The Generate button will create a unique GID Number in accordance to the chosen method for that group account.
- GID's will not be re-used.
- The generated GID value will be greater than the Starting GID defined in the ID Bridge Configuration utility.
- If the User has a GID Number the generate button will not create a new GID.

- Selects the method applied to creating the GID Number
- Algorithmic - algorithm based GID generation
- Incremental - Add ones to the last allocated GID

- Provides a Linux/Unix appropriate display name of the Active Directory group.
- Field limit is defined in AD schema. Thus no limit will be enforced in the GUI. If limit is exceeded, data will fail to save and a message will be shown to the user.

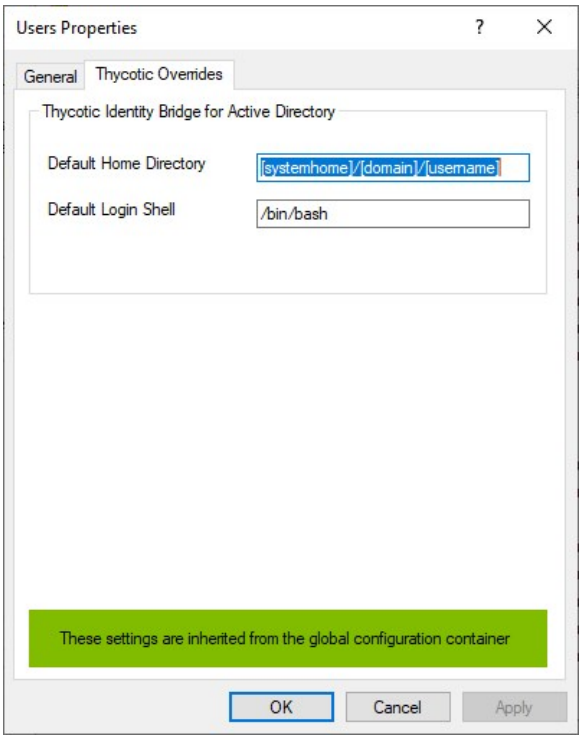
Delinea

Thycotic Overrides

The Thycotic Overrides panel under OU properties of ADUC allows you to override some of the POSIX user fields normally set Globally in the Thycotic Configuration Utility or Individually under ADUC User Properties.

These will then be used as the default values for any users created under that OU.

When using the global configuration a banner will be displayed.

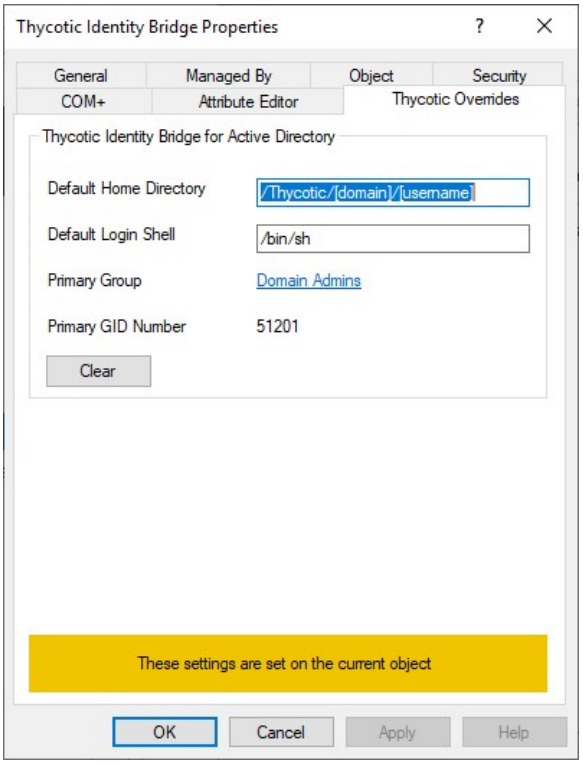


- Defines the home location of the user when they log into the Linux/Unix agent.
- This is normally their landing folder.

Defines the Linux/Unix shell that will be assigned to that user on login.

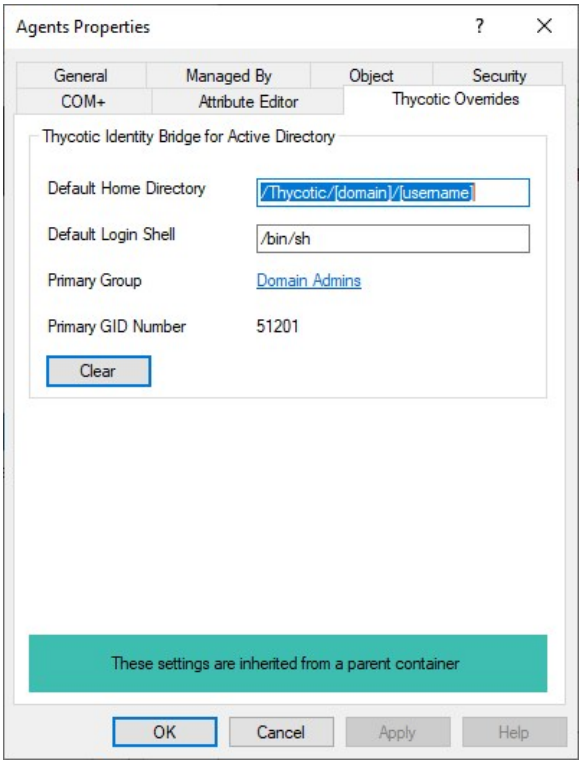
The GID number of the Primary group assigned to the user under the Member Of Panel of the User Properties.

A **Clear** button is available with an override implemented on an OU Container. When clicked, the OU overrides are cleared and default back to the Global values as defined in the Thycotic Configuration Utility.



When viewing any child OU properties with an override in place on an OU Container, a message is display that it's Thycotic Overrides are inherited from the parent container.

The Clear option is also available to default back to the Global values as defined in the Thycotic Configuration Utility.


Agents Properties
General
Managed By
Object
Security
COM+
Attribute Editor
Thycotic Overrides
Thycotic Identity Bridge for Active Directory
Default Home Directory
/Thycotic/[domain]/[username]
Default Login Shell
/bin/sh
Primary Group
Domain Admins
Primary GID Number
51201
Clear
These settings are inherited from a parent container
OK
Cancel
Apply
Help

Release Notes

This section includes the most recent Identity Bridge Release Notes.

1.1.3 Release Notes

February 24th, 2021:

- When using "User Name Formatting" configurations from the Thycotic Configuration Utility ensure that Active Directory Users are able to update their passwords regardless of the username format they are assigned.
- When Active Directory updates the Computer Object Password, this is now correctly updated on the Agent to ensure continued Kerberos Ticket renewal between Active Directory and the Agent.

- Updating the CentOS, Redhat Enterprise and Oracle Linux agents requires a change to the upgrade command and a pmagent service restart.
    - For RPM you will need to perform the following upgrade command:

      ```
      rpm -U --force ./pmagent_x86_64_v1.1.3.xx_<platform>.rpm
      ```

    - For YUM you will need to run the following downgrade command:

      ```
      yum downgrade ./pmagent_x86_64_v1.1.3.xx_<platform>.rpm
      ```

1.1.2 Release Notes

January 11th, 2021:

Enhancements available with the 1.1.2 release of Identity Bridge.

- Added an About modal to provide version details.

- Fix to improve local AD group caching in API.
- Group checking performance fix.
- Improvement to Group expansion for users defined in ACL.
- Clean Install of Configuration Utility/Removal of Thycotic Folder in ADSI Edit causes a Configuration Utility login error.

1.1.1 Release Notes

December 8th, 2020:

Enhancements available with the 1.1.1 release of Identity Bridge.

- Added Expand option to Access Control List Panel.
- Added Global User/Group Defaults on Agent Settings tab.
- Added User/Group Naming tab.

- Fix to ensure the ACL report on the *nix agents correctly reports users extend group memberships across multi-domain environments.
- Improvement to displaying Active Directory extended group memberships when using the id command.

1.1.0 Release Notes

November 24th, 2020:

Enhancements available with the 1.1.0 release of Identity Bridge.

- The Message Tab in the Configuration Utility was split to provide friendly message setup.
- Overhaul and renaming of the Excluded Users tab now called Exclusions.
- Full Configuration Utility backup support via ex- and imports options on the File Menu.
- Added DC Selector option to Configuration Utility.
- User/Group support for multi-domain environments.
- Added Service Accounts support to the Configuration Utility.
- The Primary Group configuration option was removed from the Configuration Utility and MMC extension.

- Added libjansson for pmagent to fullfil prerequisite regarding Ubuntu 18.04 and 20.04 live server issue mentioned as a known issue here and as a prerequisite here.
- Changes to the Thycotic Configuration Utility > Custom Text > Friendly Messages > Account Expired filed are now being correctly applied.
- User Properties - Thycotic User Data Panel - Auto population of fields corrected when using Automatic POSIX data generation.
- Reduced number of PreAuth calls made to Active Directory when users authenticating against locally cached information.
- When duplicate users exist across Parent/Child domain environments, entering the domain with the username now correctly accesses the correct user information.

1.0.1 Release Notes

October 8th, 2020:

- Improvements to the pmagent functionality in the event the Hosts UUID changes.
- The Agent Kerberos Ticket renewal in the event Active Directory Domain controller is unavailable at point of renewal. If the Agent is unable to contact the DC it moves to an unjoined status. With this fix it moves to a connecting status and continues to reattempt a renewal.
- Improvement to agent cache purging for users. Group cache will remain when associated with multiple users.
- Agent number reported on join is incorrect. *nix agent versions now display as short version number in ADUC, e.g. Thycotic Identity Bridge (1.0.1).
- Error resolved when loading Server Manager | Tools | Active Directory Administrative Center with Identity Bridge installed on Server.
- When creating an Active Directory user's home directory on the *nix agent, it will pull the files and folders from the `/etc/skel` directory or the skeleton directory defined under `/etc/default/useradd`.
- Authenticating AD users shouldn't pass through `/etc/login.defs`. These should be AD defined.
- Show success message following a license import instead of reporting an error.
- Improved license import functionality. Errors will be better captured.
- Improved feedback to user when running an invalid custom json script for `syscfg` command.
- AD User login appears to be defaulting as Failover login.
- *nix Agents are now able to join Active Directory Domains when BASE enabled within the hosts /etc/openldap/ldap.conf file

- For Ubuntu 18.04 and 20.04 Operating System installs from the Ubuntu-xx.xx-live-server.iso you will need to install the libjansson-dev package on the system before installing the Identity Bridge agent. This can be done using the following command:

  ```
  sudo apt-get install libjansson-dev
  ```

Delinea

1.0.0 Initial Release

August 12th, 2020:

With this release, Thycotic is rolling out the **Identity Bridge** (ID Bridge) for CentOS 7 Active Directory integration support.

Thycotic Identity Bridge provides centralized authentication and authorization for Unix and Linux systems. This enables organizations to validate that someone is who they say they are, so they can be granted access to the resources they need to perform their job. This software utilizes the organization's existing directory service (e.g. Active Directory) to achieve consistency in identities across the enterprise regardless of platform and operating system. The ID Bridge simplifies access as users have one username and one password to remember. It also streamlines identity management as administrators have a single place to manage users, groups, and the systems they have access to.

- Joins a non-windows host (CentOS 7) to Active Directory, creating a computer object in Active Directory and a Kerberos trust between the CentOS 7 and Active Directory.
- Allows User and Group POSIX data (UID/GID/Home Dir/Shell/GECOS) to be set directly in Active Directory without the need for any schema extension.
- Provides Kerberos Authentication against Active Directory.
- Allows User and Group POSIX data (UID/GID/Home Dir/Shell/GECOS) to be generated on the fly when a user logs on.
- Stores all agent data centrally without the need for an external database or schema extension.
- Honors password and account policies when authenticating from non-windows systems (CentOS 7).
- Allows for users to be locked and/or de-provisioned in the central directory and take immediate effect on all CentOS 7 endpoints.
- Allows for a user to authenticate using their Active Directory username and password on Unix & Linux systems that have been joined to Active Directory.
- Allows for a user to authenticate using their Active Directory username and password on Unix & Linux systems that have been joined to Active Directory even when disconnected from Active Directory, so long as they have authenticated within the last 30 days.
- Allows Access Control Lists (ACLs) (users and hosts) to be defined using native Active Directory groups. Provide selective access to target hosts based on group membership.
- Automatic Time Sync with Active Director.
- Identity Bridge Configuration Tool for Centralized Configuration Management.
- *Nix Command Line Tools:
  - Domain Join/Leave
  - System Configure/Unconfigure
  - ACL Reporting
  - User Testing
  - Cache Management
  - Agent Stats

- If you are running the Thycotic Identity Bridge Configuration Utility on a Domain Controller, while being logged in as an account that is not the primary administrator for the Domain Controller, you will have to perform one of the following actions so that the Thycotic Identity Bridge Configuration Utility has the appropriate permissions to write configuration settings to Active Directory:

  1. Use a specific user when attempting to connect to Active Directory in the Thycotic Identity Bridge Configuration Utility.
  2. Log into the Domain Controller with the primary administrator account.
  3. Run the Thycotic Identity Bridge Configuration Utility as Administrator.
  4. Grant the user you are attempting to connect with explicit read/write permissions to the Configuration Partition of your domain.

  This is due to a security feature implemented by Windows on Domain Controllers to enhance security."

- Root will always have SU access to user accounts.

- Standard ftp (vsftp) doesn't display the Windows Messages.
- Root will not have permission to change Active Directory users passwords via the `passwd` command.
- When AD Accounts disabled, telnet and su display an additional message stating "User account has expired". Unfortunately Thycotic is unable to control these additional messages.
- If a an Active Directory Username or Alias matches a Local Agent Username, the login will be blocked, with the exception of of root SU.
- If an Active Directory users UID Number matches a Local Agents users UID, the Active Directory user will be blocked. The Local Agents user will be granted access.
- If the agent has a default hostname of `localhost.localdomain`, the pmagent service will not function as expected and will return an error. Updating the agent hostname post installation will require a re-initialization of the agent configuration using the `pmagent --init` command.
- VNC and Remote Desktop will not be supported authentication methods for version 1 of Thycotic Identity Bridge. We recommend that these methods are disabled.

- A reboot will be required after the Agent joining the Domain to allow AD users to login via Gnome desktop.
- Logging into an Agent with cached credentials can only accept the case of the username as defined in Active Directory.
- SSH logins drop-back to a local login attempt following 3 failed Active Directory attempts.
- Chsh command is not currently supported for Active Directory users, if you are required to change the shell for an Active Directory user, please use the Thycotic User Data panel in ADUC.

Documentation Changelog

This topic provides a chronological list of documentation changes. Minor content alterations are not tracked.

- Added version 1.1.3 Release Notes, including a known issue pertaining to upgrades on CentOS, Redhat Enterprise and Oracle Linux endpoints only.

- Added version 1.1.2 Release Notes
- Added About

Added information to:

- Added version 1.1.1 Release Notes
- Access Control List tab.
- Agent Settings tab.

Changes in support of the Identity Bridge 1.1.0 feature release.

- The Message Tab split to provide friendly message setup.
- Excluded Users tab is now called Exclusions.
- Backup support via ex- and imports options on the File Menu.
- Added DC Selector.
- User/Group support for multi-domain environments.
- Service Accounts support.
- The Primary Group configuration option was removed from the Configuration Utility and MMC extension.

Changes in support of the Identity Bridge 1.0.1 bug fix release. Refer to the Release Notes for details. Expanded the list of verified and supported systems. Refer to theSoftware Downloads reference.