Offline Domain Join Credential Cache

Quick Start Guide

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal .

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Offline Domain Join Credential Cache – Quick Start Guide
Updated – October 2022

Contents

Offline Domain Join -Trust Requirements

In order to successfully facilitate the new Cached Credentials job (which supports the Offline Domain Join feature) a one-way external trust must be configured from the source domain to the target domain (source trusts target).

Cached Credentials will validate and cache the login of a target user account prior to a workstation cutover so that they may successfully login to the target forest after cutover without the need to be on the network for the first login which for remote users is typically a challenge. In order to facilitate the caching of target user accounts the workstations being migrated must be allowed to use the target user accounts for authentication which is why the dependency of a one-way trust is required.

With the addition of the one-way trust we can establish a selective authentication model to limit and restrict the access of target objects to explicitly chosen target accounts and source resources by source forest administrators.

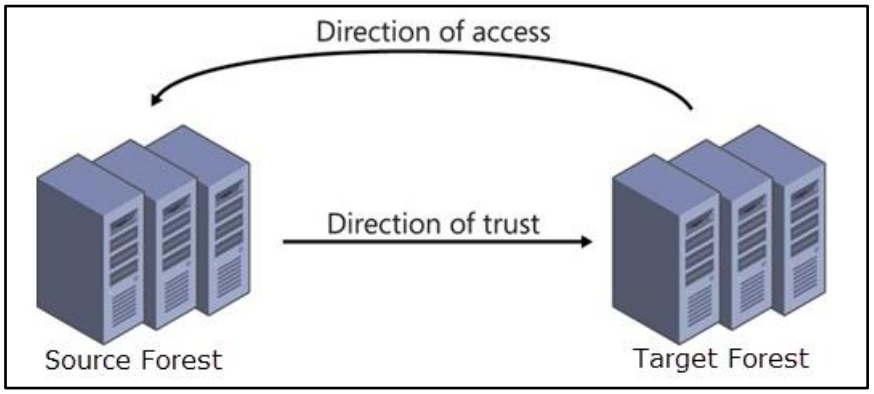


Figure 1 – Source Forest with a 1-way trust to the Target AD Forest

Offline Domain Join - Trust Options

When setting up a forest trust you have the options of limiting the direction of the trust (incoming vs outgoing), 1-way or 2-way as well the scope of authentication. With an Active Directory Trust, you can perform Forest-wide authentication or Selective Authentication.

Forest-wide Authentication

With Forest-wide authentication users from the trusted forest can automatically authenticate for all resources in the local forest.

Selective Authentication (Recommended Method)

When using the Selective Authentication model, users from the trusted forest are not automatically granted the permission to authenticate to resources in the local forest and must be explicitly giving the permission to authenticate. This is the preferred method for handling trust relationships between two different organizations or where you want to limit the access you grant the trusted forest.

For Offline Domain Join purposes we can use selective authentication to limit the access of the target accounts that have the ability to perform the cache credential steps as well as limit the computer objects where these accounts have the ability to authenticate from which greatly limits the security implications of establishing a trust during an ongoing Active Directory Migration since the source domain is in complete control of where target authentication is allowed to be performed in the local forest.

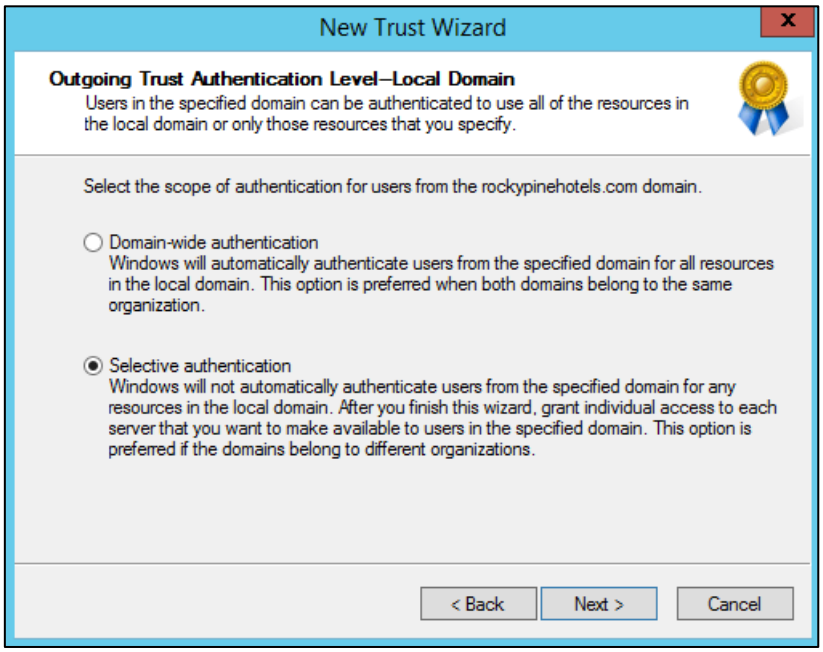


Figure 2 – Authentication Models for Outgoing Trust Relationships

Configuring an Active Directory Trust

Before we can start setting up selective authentication permissions, we first need to get a one-way trust established so target domain accounts can be cached on source workstations prior to cutover via Offline Domain Join. Below is a guide process to establishing a one-way trust between two organizations with selective authentication being used to limit target forest access.

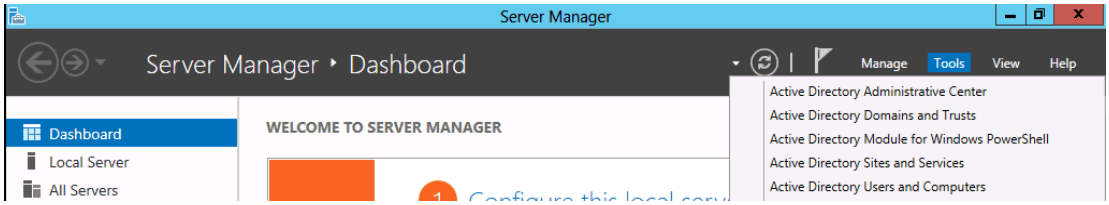
DNS and Firewall Port Requirements

This guide assumes you have already met all required DNS, Firewall and Network Connectivity Requirements for establishing a trust as most of these would already be in place in order to perform a successful Active Directory Migration:

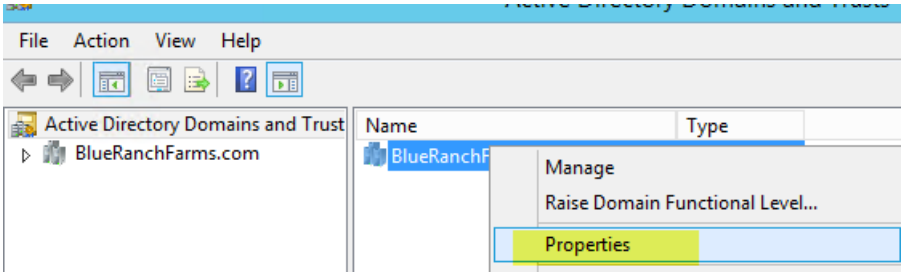
Item	Description
Network Connectivity	**Ensure there is network connectivity established between Forest A and Forest B**
Firewall Ports	**Ensure these ports are unblocked between two forests, at network level :** 53 TCP/UDP DNS 88 TCP/UDP Kerberos 389 TCP/UDP LDAP 636 TCP LDAP (SSL) 445 TCP SMB 135 TCP RPC Endpoint Mapper 1024-65535/TCP RPC for LSA, SAM, Netlogon (*)
Name Resolution	**Name Resolution should work between Forest A and Forest B**. For that use conditional forwarder or stub zone.
Access	**Membership of Enterprise Admin group is required. Alternatively, the Domain Admin of Forest Root Domain (or equivalent access through delegation) can create Forest Trust.**

Trust Creation

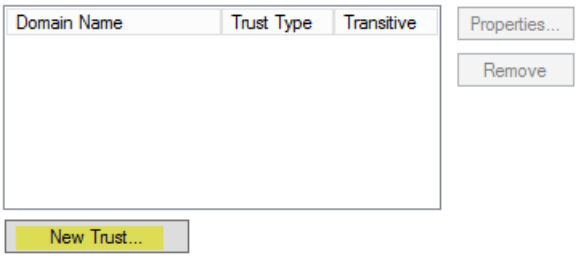
1. From a Source Forest Domain Controller, launch **Server Manager**, using the Tools drop down menu select **Active Directory Domain and Trusts**.



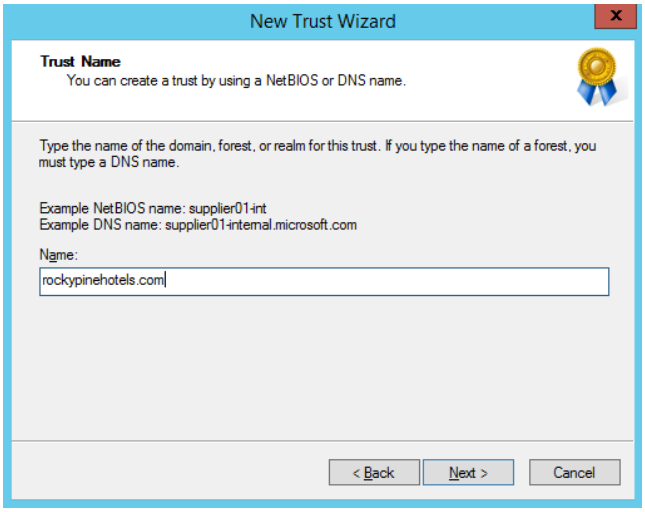
2. In Active Directory Domain and Trusts, right click and choose **Properties**.



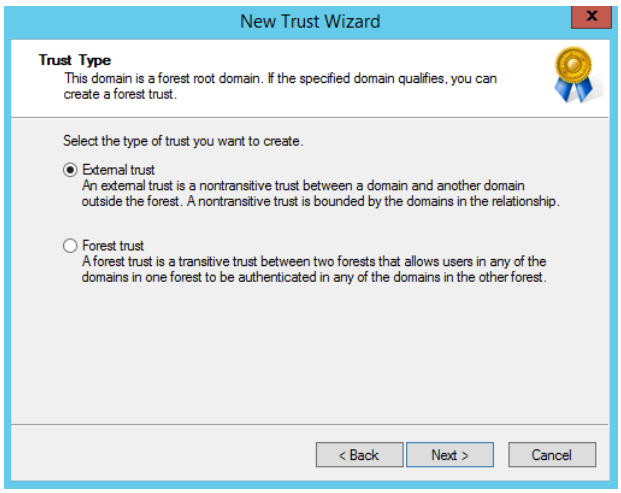
3. On the domain properties sheet, click on the **Trusts** tab.
4. Click on **New Trust**, on the Welcome to the Trust Wizard click **Next**.



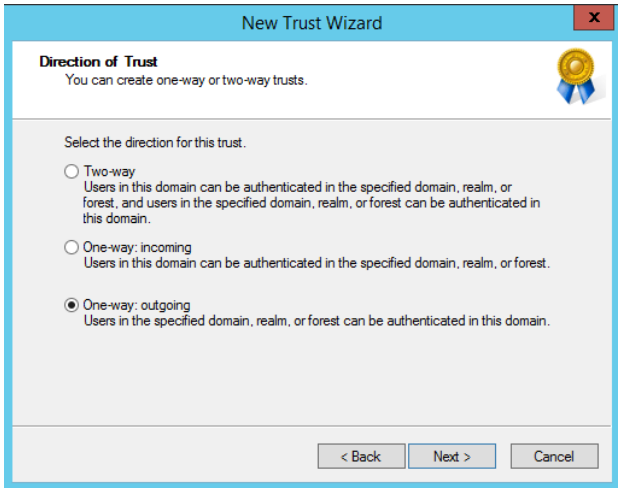
5. On the Trust Name page, enter the name of the forest you want to establish the trust with, click **Next**.



6. On the Trust Type page click on **External trust**, click **Next**.

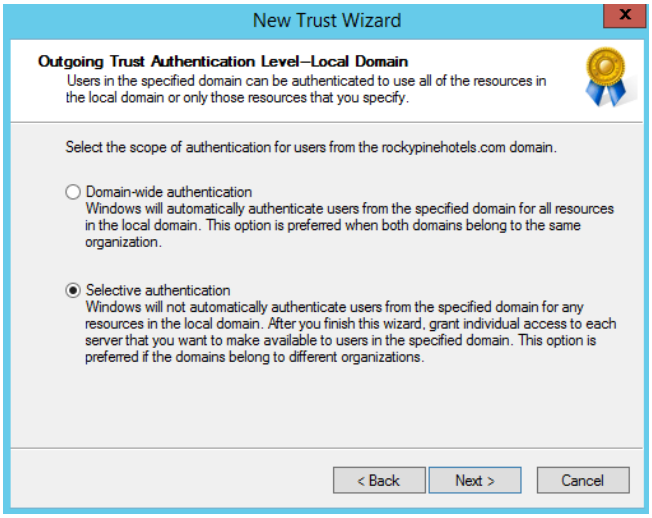


7. On the Direction of Trust page choose **One-way: outgoing**, click **Next**.

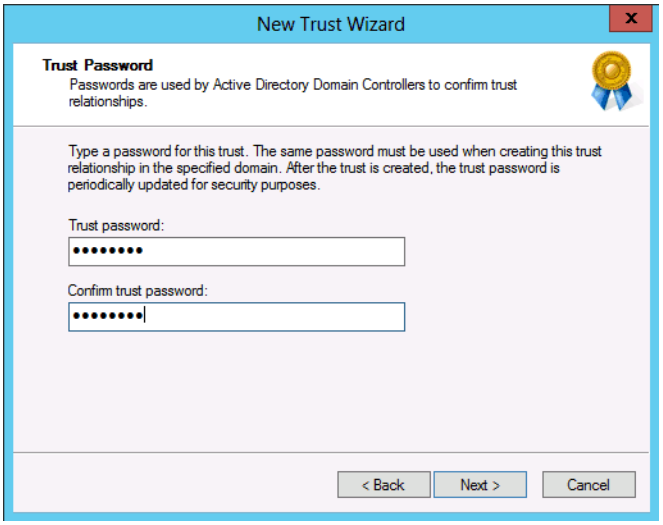


8. On the Sides of Trust page, in order to set the trust up for both domains you will need the administrative privileges or know the administrator account and password for both domains. In this example I will choose **This Domain Only**, click **Next**.

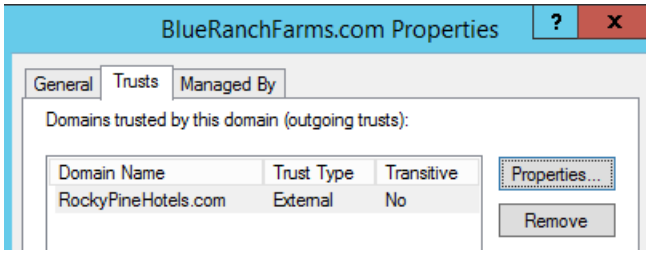
9. On the Outgoing Trust Authentication Level page, choose **Selective authentication**, click **Next**.



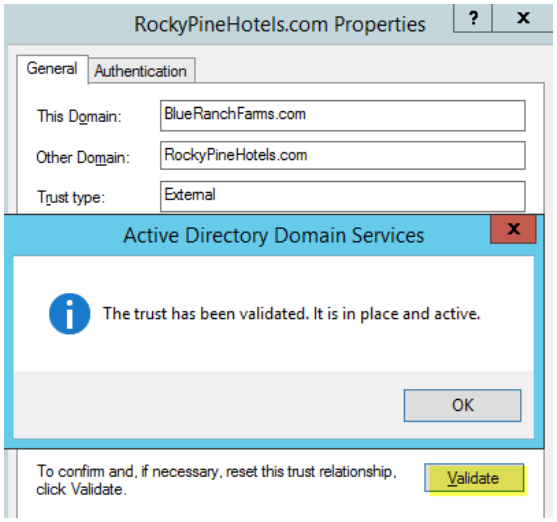
10. On the Trust Password page, enter a password that the administrators from both forests have agreed upon as the trust password, click **Next**.



11. On the Trust Selections Complete page click **Next**.
12. On the Trust Creation Complete page click **Next**.
13. On the Confirm Outgoing Trust page and the Confirm Incoming Trust page click **Next**. You will not be able to confirm the trust until the target side has been completed or if you are creating both relationships at the same time.
14. On the Completing the New Trust Wizard page click **Finish**.
15. On the Domain Properties page, click **Apply**.



16. Once the Forest Trust has been created you must have an administrator for the Target Forest complete the same process but for a **one-way: incoming** trust using the Password agreed upon when setting up the source side trust relationship.
17. Once both sides have been setup you can then **Validate** the relationship from the Source Forest Active Directory Domain and Trusts **Properties** view for the outgoing trust.



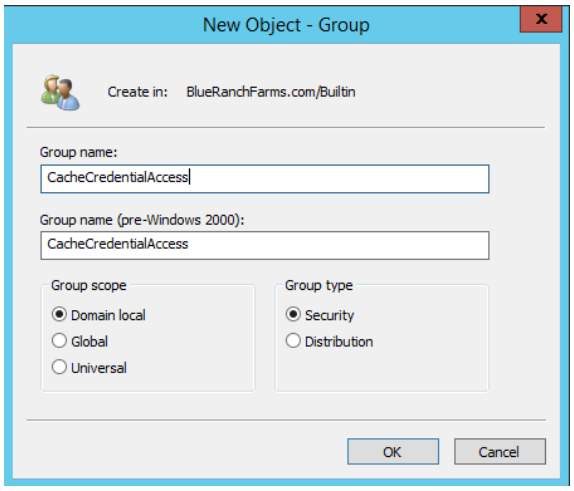
Configuring Authentication Permissions

With our Active Directory Trust configured and validated we can now move to setting up selective permissions for Cache Credentials to work with Offline Domain Join.

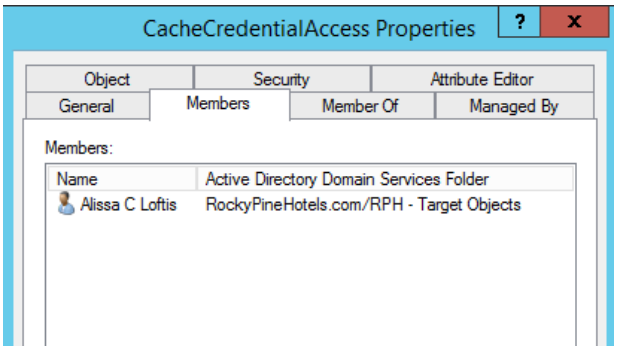
Configure Access Group

In order to limit the target accounts that have access to use cached credentials we will use a Domain Local group in the Source Environment to add in the target account members to control which target users accounts will have the ability to authenticate to source workstations.

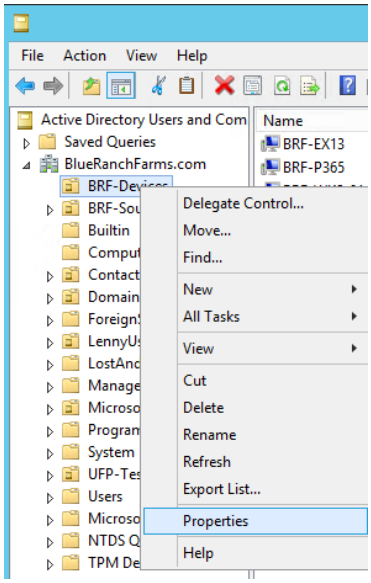
1. In Active Directory Users and Computers Create a Domain Local Group.



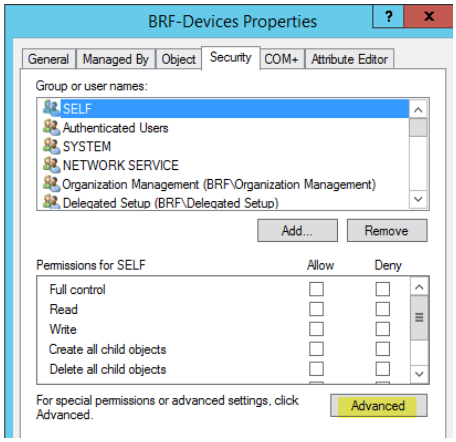
2. Open the group and add in the target user accounts for all migrating source users. In the below example I am adding the target account for Alissa Loftis who is a migrating user from the Source Forest.



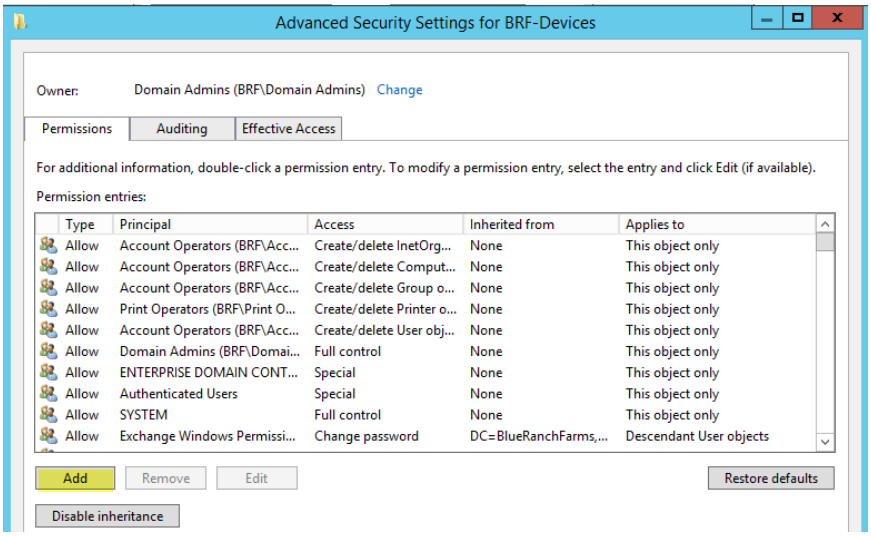
3. Once everyone's Target user accounts have been added to the source local group, we will then want to assign the right to authenticate for that domain local group on any OU containing workstations being migrated.
4. Once you find the OUs you need to assign the permissions to you want to right click the OU and choose **Properties**.



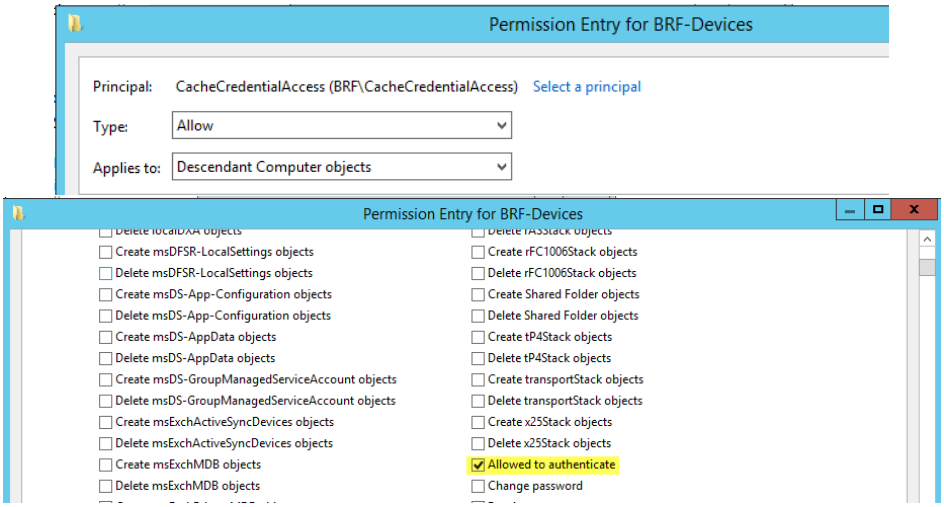
5. Click on the **Security** tab and choose **Advanced.**



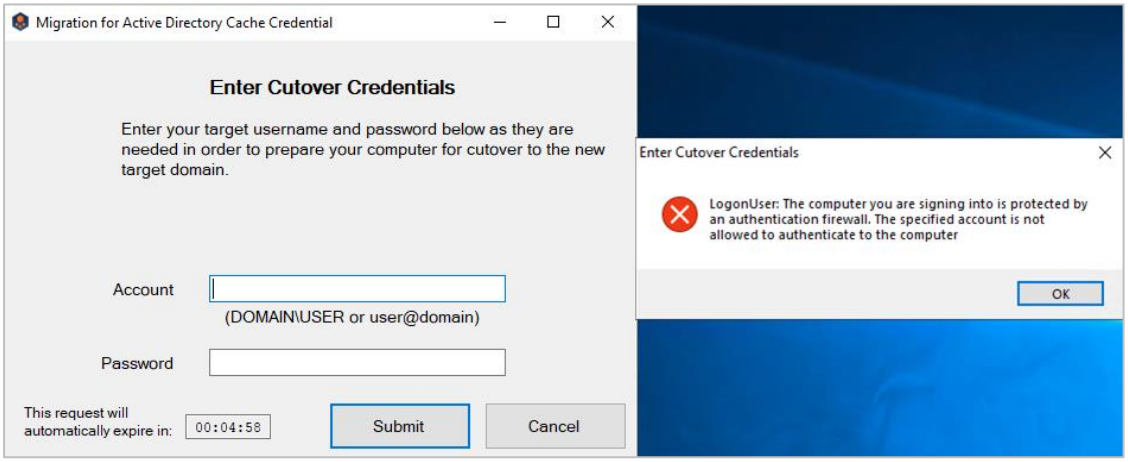
6. On the Advanced Security Setting screen click on **Add.**



7. Click **Select a Principal** and find the domain local group you created previously, ensure the type is set to **Allow** and the Applies to is set to **Descendant Computer Objects.** Once the permissions have loaded you want to find and check off the permission **Allowed to authenticate**. You may have to screen down the list of available permissions to find it. Click **Ok**, once completed.



8. Back on the Advanced Security Settings screen, click **Apply** and close both menus.
9. Repeat this process for any OU that you have migrating workstations to ensure each workstation is allowing the domain local group the ability to authenticate so we can pre cache their credentials prior to cutover.
10. Once all the steps have been completed you should be able to successfully run the Cache Credentials action without error. If you are getting the below error for a workstation, ensure that the domain local group has been assigned the permission to authenticate to it.



Post Migration Cleanup

Once migrations have completed you can safely tear down the trust relationship and remove any assigned permissions for the domain local group.

About us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product.