Migration for Active Directory

Quick Start Guide

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

Quest Software Inc.

Attn: LEGAL Dept

20 Enterprise, Suite 100

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

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.

Migration for Active Directory – Quick Start Guide
Updated – October 2024

Contents

Introduction

This guide is designed to provide a quick reference for getting set up with a Active Directory project. At the end of this guide you will be familiar with supported setups, basic requirements, and deployment components. This guide assumes some familiarity with the Active Directory platform and in particular Directory Sync.

Assumptions

The word ‘Devices’ in a Active Directory context refers to workstations or servers. That is, the domain joined end-user computers on your network which you will be migrating.

This guide covers the setup of a one-way device migration scenario between one (1) source local Active Directory environment and one (1) target local Active Directory environment.

This guide does not specifically cover File Share and Network Storage migration, Group and other resource migration, or consolidation or divestiture scenarios. However, those operations can easily be performed following onto the information provided in this guide.

Getting Started

A typical device migration can be broken into 4 easy steps to get started quickly.

1. Set up Directory Sync
2. Install the Active Directory Agent
3. Set up Active Directory Profiles and Configurations
4. Perform migration activities ReACL and Cutover of Devices

Step One: Set up Directory Sync

The first step in a Active Directory Device migration is to set up one-way directory synchronization between the source and target local environments. Active Directory works on top of Directory Sync so we will set up this synchronization there.

Directory Sync Agents

Install Directory Sync agents in both the source and target using the standard configuration for directory synchronization as directed in the User Guide.

Environment and Workflow Configurations

You will need source and target Directory Sync Environments defined which have Device objects included in the OU and object filter scopes. You will also need a Directory Sync Workflow using those Environments with at minimum a Read step and a Match step in order for those Devices to become visible in Active Directory.

Note: In order to successfully perform a migration and ReACL activities, User objects will also need to be read in from the source and target and matched. Those User operations can be performed in a separate Directory Sync Workflow, there is no need to include them in the Devices Workflow.

Should you choose to include User objects in the same Workflow with your Device objects you will need to include the Stage Data and Write out steps. If you go this route see also the Help Center for more information on the Device Migration Profile setting 'Join to Existing Devices'.

Run the Workflow at least twice in order to verify that any object creations or matches which have been done in the target have been added to the Directory Sync database.

At this point Device Objects which have been Read In from the source Environment should appear in the Active Directory Devices + Servers page on the Not Ready Devices tab. If this has not happened troubleshoot the Directory Sync Environments and Workflow. Then proceed to Step Two when Not Ready Devices are showing up as expected.

Step Two: Install the Active Directory Agent

If you are following along in this guide, after performing Step One the Devices from your source Environment should now be visible in the Not Ready Devices tab on the Active Directory Devices + Servers page. The way Devices move from the Not Ready Devices tab to the Ready Devices tab is by having a Active Directory agent installed on them and communicating with the Active Directory server.

The Active Directory agent will need to be installed on each Device which is to be migrated.

The Agent installer msi file can be downloaded from the Downloads section of the Active Directory Configurations page. Installing the agent will also require the values of the Service URL and Auth Key which are listed in the same page in Active Directory below the download button.

An example PowerShell command to install the agent would be:

msiexec.exe /I 'C:\workspace\AD.Agent-20.3.1.1401.msi' SERVICEURL=https://us.odmad.quest-on-demand.com /api/ADM AUTHKEY=##

Run this command to invoke the installer UI. Walk through the screens filling out the needed information and click finish when completed. The settings for using a customer web proxy for communications are optional and can be left blank for the purposes of this guide.

As needed the installer can also be invoked in quiet mode with the /QN switch (requires running PS as admin). The fields which can be populated when included as command line arguments to the installer are SERVICEURL and AUTHKEY. Additionally, it is possible to configure the agent to use a web proxy using command line arguments as well. They are beyond the scope of this guide but listed here for info: WEBPROXYENABLE (optional), WEBPROXYURL (optional), WEBPROXYPORT (optional), WEBPROXYUSER (optional), and WEBPROXYPASS (optional).

The agent communicates with the Active Directory server over three outbound ports: TCP 443/80 and UDP 3030. When in web proxy mode the agent will communicate to the proxy on the defined port and outbound to the internet on TCP 443/80 only, UDP over port 3030 is not used when using a web proxy

The agent uses .Net framework 4.5.2 and will download it on install if it is not present and an internet connection is available.

Agent communications – To avoid overload, each workstation agent will communicate with our server at specific random and uniformly distributed intervals. On startup an agent will first register with the server within four hours. Thereafter a running agent will check for work by calling our job availability cache once every two minutes over UDP port 3030. Note that in the product UI the 'Agent Last Contact' column relates to the TCP communications not to the UDP communications, so do not expect it to update every 2 minutes. There is a per client limit of 600 agent jobs which will be available to agents per two-minute interval. If an agent has a job queued it will then connect over https to retrieve the job. As a fallback for this the agent will also connect by https once every four hours even if a job has not been available in the job availability cache.

Wait up to four hours for initial registration. While you are waiting for this initial communication can be a good time to read ahead and get a head start on Step Three: Set up Active Directory Profiles and Configurations.

Now that you have installed the Active Directory agent on a Device you wish to migrate and waited up to the initial four hours for it to register, you should see that Device move from the Not Ready Devices tab over to the Ready Devices tab in Active Directory. If you do not see this transition take place troubleshoot the network connectivity for agent communications and check the logs from the agent locally on the device.

Step Three: Set up Active Directory Profiles and Configurations

Now that Directory Sync is configured and the Active Directory agent is installed on the device to migrate you can proceed with configuring the profiles and configurations.

Profiles: Profiles are groups of related settings and options related to the device migration. There are six kinds of profiles in Active Directory: Migration, Network, Device ReACL, File Share ReACL, Credentials, and Credential Cache.

For the minimum purposes of this guide we will not need to set up a File Share ReACL profile, Credentials profile, or a Credential Cache profile.

Migration Profile - Migration Profiles contain common device cutover settings used to manage the domain join process.

Network Profile - Network Profiles contain common network adapter settings that need to be updated during the device's migration to the new domain.

Device ReACL Profile - Device ReACL Profiles contain common settings to manage updating permissions of Windows workstations and servers prior to migration.

The Migration, Network, and Device ReACL profiles have a default profile available. Review the settings on the default profiles and determine if you need to create your own new profiles which have different settings.

Configurations: New in Active Directory are the Configurations page and sections.

Downloads: You should already have seen the Downloads page when downloading the agent. This is the only Configuration section which will apply to this simple guide. Also, on the Downloads page is the setting for the agent auto-upgrade feature for your whole project. This is one of the best new features which will ensure that if a new version of the agent is released, your agents will be updated automatically. If necessary, you can also disable this setting.

The Repositories page defines storage locations for certain migration jobs which require local storage of files. These job types are 'Upload Logs', 'Download File', and 'Offline Domain Join'. For the purposes of this guide none of these locations will need to be defined, but they will be very important should you proceed to using their related jobs.

Custom migration Actions and their constituent Tasks are organized in a similar system to the Active Directory Pro product. Click 'Show System' to view the standard Actions which come with the product and then copy them if you want to edit them or create your own. For this guide we are only using the system actions, but here is where you would customize your own as needed.

Variables is a section for defining global variables to be made available to scripts running as part of Custom Tasks and Actions.

If you have proceeded this far in setting up Profiles and Configurations while waiting for initial agent registration, you will need to pause here until that step is completed. Otherwise you are ready to proceed to performing migration activities.

Step Four: Perform migration activities ReACL and Cutover of Devices

Once Profiles and Configuration have been set up you can proceed to migration activities.

Before or while performing migration activities it may be helpful to organize and partition the list of devices to be migrated by using the Migration Waves feature. To assign devices to a migration wave for grouping select devices in the Ready Devices tab and then select the 'Add to Migration Wave' action from the drop down and click the Apply Action button. You can also manage Migration Waves by going directly to the Waves page from the left menu. A powerful tool for tracking devices and statuses throughout the migration is combining the defined migration waves with the Ready Devices table filters.

The simplest migration activities flow consists of applying a ReACL action followed by a Cutover action. This is the flow we will follow in this guide.

Before working with the devices, ensure that the users related to the device you are going to migrate have already been matched in the target in Directory Sync. This will allow the ACLs to be updated correctly for use in the target by the ReACL process. Remember that if those users were created by your Workflow you will need to run the workflow a second time in order to read them back into the database and finish the matching.

From the Active Directory Devices + Servers page on the Ready Devices tab select a device on which to perform a migration action. There are several useful actions in the Select Action dropdown which you can apply to that device. For this guide the first action we need to use is ReACL. Device ReACL is non-destructive and can be performed multiple times prior to the cutover event. After clicking to apply the action the ReACL Job Options dialog is displayed and you can enable 'Do Not Start Before' and choose a time in the future to start the job. Otherwise, it will be queued when you click Apply. Do not enable the option for now and click Apply.

Wait for the ReACL job to be picked up by the agent and for the job to complete. You can track the status as it updates in the Ready Devices table or from the product dashboard.

If you want to see what jobs are currently queued for a device or review the outcome of previous jobs for that device select the device from the Ready Devices table and then select and apply the 'View Jobs' action. For planning which User objects need to be migrated to the target prior to migrating the devices they are using, the 'Show Profiles' action is a helpful one to see which user profiles have logged into the device in question.

After the ReACL process has been completed successfully it is time to queue a Cutover action.

From the Ready Devices table select the device you just ReACLed on which to perform a cutover action. Select the Cutover action from the dropdown and click the Apply Action button. After clicking to apply the action the Cutover Job Options dialog is shown. You can select here to ignore the ReACL status of that device. The cutover action will error out and fail to queue it if the ReACL status of the device is not 'Completed' or chosen to be ignored. On this dialog you can also enable 'Do Not Start Before' and choose a time in the future to start the job. Otherwise, it will be queued when you click Apply. Choose that option for now.

Wait for the Cutover job to be picked up by the agent and for the job to complete. You can track the status as it updates in the Ready Devices table or from the main Product dashboard.

When the Cutover is completed inspect the workstation or server and ensure that things went as expected. When the entire project is completed the Cleanup action can also be run. Congratulations on

For more information about other topics visit the online help center.

What's Next?

Now that the first device(s) have been configured and migrated in Active Directory you are ready to progress to more planning and more involved migration scenarios. For instance, further information is available on Offline Domain Join and the related Credential Cache jobs should they meet the needs of your project scenario.

Learn more by visiting the On Demand Migration Active Directory User Guide.

FAQs

1. What ports does the agent use to connect?

   The Active Directory Agent uses three outbound ports

   - TCP 443/80
   - UDP 3030

2. I've installed the agent and the device isn't ready, what do I do?

   On startup the Active Directory agent will phone home sometime in the first four hours. This communication offset time is an agent specific random and evenly distributed offset so the initial communications of a large number of devices set up at once will be spaced out and not overload the servers. If your device has the agent installed but you haven't waited up to four hours yet, wait up to four hours and then re-check the Ready Devices list to see if your device shows up before proceeding to other network troubleshooting operations.

3. How do I adjust the agent polling interval?

   In Active Directory, unlike in Active Directory Pro, the agent polling interval is not end user adjustable. The polling interval is every two minutes over UDP and every four hours over TCP. Should this amount of network traffic be an issue contact Support to investigate reducing the polling interval. Note that reducing the polling interval will cause queued migration actions to take longer to be picked up by the agents.

4. How many migration actions can I queue at once?

   In Active Directory you can queue as many migration actions at once as you would like. There is a hard limit of 600 agents per each two minutes who will be notified by the job availability cache that they have a job waiting for them. Therefore, the minimum amount of time which could be required for those queued migration actions to be picked up will be the number of queued migration actions divided by 600 and multiplied by two minutes.

5. Agent last contact time isn't updating every two minutes, is something wrong?

   In Active Directory the Agent last contact time is updated based on the TCP connection with the back end. This will occur if a job is retrieved or every 4 hours as a fall back. It is not expected that the agent last contact time will update every two minutes even if the UDP requests to the job availability cache are functioning correctly.

6. The machine name was changed during the migration project, will it keep working?

Changing the machine name during a migration project may have unexpected implications. We recommend that you avoid doing so if possible. If not, you will need to delete the device from Active Directory and reinstall the agent. Use the Status Resets action to reset the registration status of the device, then set the Directory Sync Workflow to reconcile on next run and run it. This will delete the old device from the database. Finally, reinstall the Active Directory Agent on that device and run the Workflow again to read it in.

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.