Quest® On Demand Migration – Active Directory 20.12.17

Release Notes

Feb 21, 2025

This release of Quest® On Demand Migration – Active Directory includes the following solutions:

- **Directory Sync**

  Directory Sync can set up and maintain an Active Directory sync, an Microsoft Entra ID sync, or even a sync between Active Directory and Microsoft Entra ID. Users in merging organizations can find each other in a unified Global Address List (GAL).

- **Active Directory**

  Active Directory enables you to migrate Active Directory to accelerate your enterprise M&A and modernization initiatives. Quest® On Demand Migration – Active Directory is a solution that integrates and migrates Active Directory, Microsoft Entra ID, and hybrid directory environments without requiring trusts, SQL, network connectivity, or installing servers.

- **Domain Move**

  Domain Move provides the "Domain Cutover" or move functionality. This powerful feature guides the migration operator through the entire domain move process and automates many of the steps.

- **Domain Rewrite**

  On Demand Migration provides the "Domain Rewrite" or Email Rewrite (ERS) functionality. This powerful feature allow end users to communicate from a common email domain from Day One—on both inbound and outbound mail—so you present as a unified, cohesive brand. And, you get all of this without downtime — so you won't have critical gaps in communication.

View the online Quest® On Demand Migration – Active Directory User Guide for more information:
https://support.quest.com/technical-documents/on-demand-migration/current/active-directory-user-guide

These release notes provide information about the Quest® On Demand Migration – Active Directory release.

Topics:

New features

New features in this deployment:

- Deployment of Self-Service endpoints.

See also:

- Enhancements
- Resolved issues

Enhancements

The following is a list of enhancements implemented in this deployment.

General enhancements

Enhancement	Issue ID
In Device Profiles, the Match Status value has been updated to display "Matched" or "Not Matched."	45670
A "Copy Diagnostic" button has been added to the Workflow Detail page. This button copies workflow diagnostic log details to the clipboard.	54510

Resolved issues

The following is a list of issues addressed in this deployment.

General resolved issues

Resolved Issue	Issue ID
The Directory Sync Agent does not get new changes to LDAP password filter.	525509
The Directory Sync agent defaults to the Legacy Password sync the first time it is installed.	52641
The Stage OU filter processes all objects in child domains when the root is the only one selected and the environment has the child domains in scope.	54137
Cannot reset the status for multiple Device File Shares.	54373
The Directory Sync client app is removed when the Directory Sync license expires but the Active Directory license is valid.	54408

Known issues

The following is a list of issues, including those attributed to third-party products, known to exist at the time of this deployment.

Directory Sync known issues

Known Issue	Issue ID
An attempt to install an older version of the agent software will fail if a newer version has already been successfully installed. If, for some reason, the older version is needed, first uninstall the newer version, then remove all registry references to the agent.	8060
The agent installer cannot accept a password with a first character of !.	8122
When discovery discovers an environment, it will read in the OU structure of all domains within the forest. The UI will show all domains and you can select them for use in all workflows. However, if a DC for that domain is not included, or the agent account does not have read access to the objects, they will not be read into the database.	8077
Cloud Only Security Groups are not read in when reading a cloud endpoint.	22453
User thumbnail photos do not sync to cloud environments.	8069
The PowerShell User Group should be added to the Tenant Group Filter as the Group Owner. A security group should not be used.	8070
An account with access to all domains within the forest is needed if you want to sync all domains within a single forest with a single agent. Using an enterprise admin account is the most efficient method for doing this.	8073
Mapping functions do not work with multivalued attributes. For example, (results (proxyaddresses,"x500:") will not return a true even if an X500 address is present.	8075
When a workflow for a cloud environment has been run once, but then has been idle for longer than 30 days, an error will be encountered when the job starts, and the job will fail and loop repeatedly until the retry count has been reached.	8079
In the German and Chinese Office365 tenants, Directory Sync will always do full synchronizations because the delta sync functionality is not available in these local tenants.	8095
An "Object with ID xyz was not found" error may occur when reading recently created Azure guest users due to the longer length of time for guest users to propagate.	8101
Remote Mailboxes from the source are incorrectly created in the target as Users instead of MailUsers.	8102
Delta syncs are limited to 30 days. To avoid full synchronization, a read in should be performed for all cloud environments every 29 days or less.	8108
Password sync does not support AES hashes.	21796
A template configured to sync a binary attribute to a non-binary attribute will not sync correctly. For example, if syncing Binary (ThumbnailPhoto) to String(ExtensionAttribute), the target attribute will be synced as "System.Byte[]" instead of the expected binary value converted into a string.	15683
A security group cannot be used as a filter group.	8057
When using filter groups for Cloud environments you need to ensure that a group containing any newly created objects is present in the environment filter. This can be accomplished by having a source and target filter group with the same name so they will match and synchronize between the environments. If these objects are not read in after creation, they will not have any additional	8076

Known Issue	Issue ID
updates synchronized and they will not be matched.	
When synchronizing local AD groups to Office 365 as Office 365 groups (Unified Groups) any contact in the source group will record an error in the logs and the contact will not appear in the target group.	8081
Office 365 Group settings are not copied to the target Office 365 Group.	8104
Likes for Office 365 Group conversations are not migrated.	8122
Custom schema attributes can be added to template mappings but are not visible in the drop-down selection list.	8072
All domains within an Active Directory Forest are visible within an environment when adding a single domain even though the agent account credentials may not have access to all domains.	8074
The DS-Core-Propagation-Data attribute is not synchronized by Directory Sync. The DS-Core-Propagation-Data attribute is a system attribute which is used by the Active Directory service and cannot and should not be modified by anything other than the directory itself.	34400
The mapping does not update the mailnickname attribute of Non mail-enabled security groups.	34481
Attribute filters cannot be applied to Security Groups.	14933
Cloud Environments that use Object Filter Exclusion options may see Unlicensed or Disabled Accounts read in when configured to Exclude Unlicensed or Disabled Accounts. This is because the AccountDisabled and SKUAssigned properties in Exchange Online Management are not always updated to reflect the true state of the object in Office365.	35957, 36574
Updates of non mail-enabled Security groups in Cloud to Local syncs fail due to an empty samAccountName value.	37254
Custom schema attributes can be added to template mappings, but are not visible in the drop-down selection list.	52326
Directory Sync will attempt to add Group Object as Owner to Teams/M365 and Distribution Group when the Group object shares similar name as the Group Owner. For M365 Groups and Teams, an error will be logged for these groups as they cannot be added as an owner.	41463
Password sync will fail for objects with non-English characters in the sAMAccountName.	41570
A directory operation error occurs when running a cloud to local workflow.	42444
The RC4 encryption (Rivest Cipher 4 or RC4-HMAC) is an element of Microsoft Kerberos authentication that Quest migration products require to sync Active Directory passwords between Source and Target environments. Disabling the use of the RC4 protocol enabled makes password syncing between environments impossible. Beginning on November 8, 2022 Microsoft recommended an out of band (OOB) patch be employed to set AES as the default encryption type. The enabling and disabling use of the RC4 encryption protocol has potential impact beyond the function of password syncing of Quest migration tooling and should be considered carefully.	N/A
Comment fields that exceed the maximum length of 4000 characters will cause an error.	44556
When mail contacts are deleted from Exchange Online, the deletion is not reflected in the product. Workflows with 'Delete Objects' steps will not process contact deletes.	45392

Active Directory known issues

Known Issue	Issue ID
The Server 2016 Rollback action may break a user's profile if the user is not a member of the BUILTIN\Administrators group on the target machine.	29544
The Cleanup job should not be used with bi-directional match/sync configurations as it may incorrectly remove target ACLs.	32588
On a Windows 10 or Windows 11 device, when performing the Entra Cutover action, the migrated user profiles may lose some of the installed Windows Store application or other Provisioned AppX Packages. These packages will need to be reinstalled by the user after they logon to their target profile.	36079
An Microsoft Entra ID device cannot be ReACLed if there is no matching group in mapping file.	36124
For Entra Device Cutover, Windows Hello for Business Setup cannot be completed when Source Account is a Direct Member of the Device BUILTIN\Administrators Group.	36627
The ODMAD Device Agent has not been designed to take special requirements of application servers, such as Exchange, SharePoint, Remote Desktop Services, IIS, etc. into consideration. Applications should be analyzed to determine if domain migration will be supported by each individual application and what remediation(s) may be required. Recreating/redeploying Application Servers in the target environment is recommended for best results.	43466
An group with the name of two or less characters cannot be assigned to a migration wave.	45514
Certificates are not migrated with Device Cutover.	46002
Rollback is not supported for Cloud to On-Prem and Cloud to Cloud Device Migration.	46422
When installing a provisioning package that has been renamed (filename is different from the package name in the package metadata), the cutover script will fail when trying to verify that installation was successful.	47517
ReACL will receive an Access Denied error if the share is an Azure Storage Account Share integrated with Azure Domain Directory Service.	54899

Domain Move known issues

Known Issue	Issue ID
Domain Move can not move the domain if it is being used for Active Directory Federation Service (ADFS) between on-prem Active Directory and Microsoft Entra ID.	35529

Domain Rewrite known issues

Known Issue	Issue ID
Signed and encrypted messages will not be rewritten by the email rewrite service (ERS).	8004
When ERS is disabled, external email addresses of MEU's are not removed.	40937
Cloud Rewrite workflows will not run when prepare jobs are queued for both hybrid and cloud-only target objects.	44319
Forwarding from mailbox cannot be removed if ERS was enabled using skip setting up forwarding.	47362

Release History

The following lists the new features and resolved issues by deployment.

20.12.16.4

Resolved issues

Resolved Issue	Issue ID
When configured for a low polling interval, the device agent will poll at that interval until registered. Situations where registration does not happen cause repeated queries to the endpoint resulting in extra processing.	54305
A custom file download to a particular location, sends the file to the Downloads folder of the agent.	54460

20.12.16.3

Resolved issues

Resolved Issue	Issue ID
In the Password Propagation Service UI, the Domain Alias credentials cannot be verified.	53293
The CustomAttribute filter, under Devices Filter, is not labeled to include Devices as it is under the Global tab.	53589

20.12.16.2

Enhancements

Enhancement	Issue ID
A new option "Clear Existing Migration Wave" to allow removal of selected users from the migration wave has been added.	35085
The ability to reset the delta timestamp and sequence number (USN) value for an environment has been added.	52519

Resolved issues

Resolved Issue	Issue ID
The action "Remove Device(s)" does not check for and remove associated Device Shares.	44309
The mapping zipped folder cannot be opened.	53609
Cloud Environment Discover, Settings, and Delete button are incorrectly enabled.	53710
ERS Cluster Deployment PowerShell does not look for the config file in the download folder.	53779

20.12.16.1

Enhancements

Enhancement	Issue ID
In the Quest DS Password Change Service installer, updated message on the Access Token dialog and changed "ODMAD" to "Directory Sync."	53316
Minor updates to the Password Filter and Password Propagation Service installer.	53415

Resolved issues

Resolved Issue	Issue ID
Intermittent issue creating the local access group 'DSPasswordChangeService' during installation on Server 2025.	52801

Incident response management

Quest Operations and Quest Support have procedures in place to monitor the health of the system and ensure any degradation of the service is promptly identified and resolved. On Demand relies on Azure and AWS infrastructure and as such, is subject to the possible disruption of these services. You can view the following status pages:

- Quest On Demand: https://status.quest-on-demand.com/

- Azure Services: https://azure.microsoft.com/en-ca/status/

- AWS Services: https://status.aws.amazon.com/

System requirements

The following web browsers are supported with On Demand:

- Chrome or Firefox is recommended for the best cloud-based platform experience.

Product licensing

Quest On Demand is a Software as a Service (SaaS) application where application software is hosted in the cloud and made available to users through quest-on-demand.com.

Use of this software is governed by the Software Transaction Agreement found at www.quest.com/legal/sta.aspx and the Data Processing Addendum at www.quest.com/legal/dpa.aspx. This software does not require an activation or license key to operate.

You can sign in to Quest On Demand as a Guest user and sample the solutions the product can offer. As a Guest user, you can add your Microsoft Entra tenant and look for problems that can be solved by Quest On Demand. To sign in as a Guest user, go to quest-on-demand.com and click **Continue as Guest**.

Trial licenses are available. To enable a trial license, you must use a Quest account to sign up for Quest On Demand. Use one of the following procedures:

- To enable a trial license with an existing Quest account
- To create a Quest account and enable a trial license

To enable a trial license with an existing Quest account

1. Go to https://www.quest.com/on-demand/

2. Scroll down to the module you are interested in and click **Try Online**.

3. On the Free Trial of <Module Name> page, click **Sign In for your Free Trial**.

4. Fill in your Quest account credentials and click **Sign In**.The Welcome to Quest On Demand page opens.

5. In the **Add organization name** field, enter a name for your Quest On Demand organization.

6. In the **Select Region** field, select the region where you want your data to reside.

7. Click **Create New Organization**.

You can now add your Microsoft Entra tenant and begin using the module. See the Global Settings User Guide for more information on working with Quest On Demand.

To create a Quest account and enable a trial license

1. Go to https://www.quest.com/on-demand/

2. Scroll down to the module you are interested in and click **Try Online**.

3. To try online, you must create a Quest account and then sign up for Quest On Demand.

4. Create a Quest account.

    a. Click **Create a Trial Account**.

    b. Fill in the fields on the Create Account page. Note that the email and password entered here will be the credentials you use to sign in to Quest On Demand.

    c. Click **Create Account**.The "We've sent you an email" page opens.

5. Sign in to Quest On Demand.

    a. Go to your email account and open the email from support.quest.com. Click on the verification link. The Welcome to Quest On Demand page opens.

    b. In the **Add organization** name field, enter a name for your Quest On Demand organization.

    c. In the **Select Region** field, select the region where you want your data to reside.

    d. Click **Create New Organization**.

You can now add your Microsoft Entra tenant and begin using the module. See the Global Settings User Guide for more information on working with Quest On Demand.

More resources

Additional information is available from the following:

- Online product documentation (Enter On Demand Active Directory in the Product search field.)
- Quest On Demand community on-demand

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

On Demand Migration – Active Directory Release Notes
Updated - Feb 21, 2025