



Quest® Identity Recovery for Active Directory

User Guide



© 2026 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

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

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.

Contents

About Identity Recovery for Active Directory	1
Overview of Identity Recovery for Active Directory	3
Before You Start	4
Backup Considerations and Best Practices	4
Recovery Considerations and Best Practices	5
Recovery Strategies Overview	6
Forest Recovery Overview	6
Forest Recovery Strategies	7
Recovery Methods	8
Hybrid Agents and Domain Controller Agents	10
Compatibility with Recovery Manager for Active Directory (RMAD) FE/DRE	12
Server Access Credentials	14
DNS Configuration	14
Security	15
Sign up for Quest Security Management Platform	20
Configuring Identity Recovery for Active Directory	21
Organizations and Regions	21
Access Control	21
Roles and Permissions in Security Management Platform	22
Email Notifications	25
Configuring Notification Templates	26
Working with Identity Recovery for Active Directory	27
Forests	28
Adding and Configuring Forests	29
Creating and Installing Hybrid Agents	29
Adding Forests into Identity Recovery for Active Directory	30
Topology	32
Topology Discovery	34
Installing Domain Controller Agents	34
Backup Plans and Backups	36
Backup Plans	36
Creating and Editing Backup Plans	37

Backups	38
Recovery	39
Creating Recovery Plans	40
Recovery Page Tiles	41
Configuring Recovery Plans	42
Configuring Settings	43
Recovery Using Latest Backups	43
Recovery Using Specific Date	44
Configuring Domains	44
Configuring Domain Controllers	47
Handling Errors and Warnings	51
Working with Recovery Plans	51
Verifying Recovery Plans	52
Performing Recovery	53
Recovery Plan Progress	53
Domain Controller Operations	55
Events Management	57
Task Management	58
About us	59
Technical support resources	59

About Identity Recovery for Active Directory

Quest® Identity Recovery for Active Directory offers off-network abilities to manage on-premises domain controllers, including Active Directory® backups and restore operations, in the case of a disaster. It is essential for any modern business to have uninterrupted network and computer systems, which are essential for business continuity. Unforeseen outages, like directory service failures, can significantly disrupt operations. To mitigate such risks, critical infrastructure must be designed for swift recovery from failures.

Identity Recovery for Active Directory leverages advanced technologies to minimize downtime resulting from Active Directory corruption or accidental modifications. This solution automates backups and enables rapid, remote recovery of data stores in Active Directory, and dramatically reduces the time required to restore Active Directory.

Identity Recovery for Active Directory allows you to perform the following operations:

- Configure and manage backups using Backup Plans.
- Store Active Directory backups in Quest Azure tenant.
- Configure and manage recovery of an Active Directory Forest.
- Restore Active Directory using Restore to Clean OS method, allowing you to restore the entire forest or any of its parts on a freshly installed Windows machine.
- Set recovery method for individual domain controllers to Install Active Directory.
- Schedule backup of domain controllers based on business needs.
- Verify recovery configurations to validate your disaster Recovery Plan.

The solution simplifies and automates the process of preparing for and responding to disasters, such as the corruption of directory object data. These disasters can stem from hardware or software failures, or accidental human errors. Some examples of forest-wide failures include:

- None of the domain controllers can replicate with its replication partner.
- Changes cannot be made to Active Directory at any domain controller.
- New domain controllers cannot be installed in any domain.

- All domain controllers have been logically corrupted or physically damaged to a point that business continuity is impossible (for instance, all business applications that depend on Active Directory are non-functional).
- A rogue administrator has compromised the Active Directory environment.
- An adversary intentionally or an administrator accidentally runs a script that spreads data corruption across the Active Directory Forest.
- An adversary intentionally or an administrator accidentally extends the Active Directory schema with malicious or conflicting changes.

Identity Recovery for Active Directory can be started from [Quest Security Management Platform](#) single SaaS command point. For more information about the platform, see the *Security Management Platform Global Settings* documentation.

To access Security Management Platform, you need to provide Security Management Platform credentials or use your existing [Quest Software](#) account. For more information, see [Signing up for Quest Security Management Platform](#) in the *Security Management Platform Global Settings User Guide*.

The following sections describe how to configure and work with Identity Recovery for Active Directory:

- [Overview of Identity Recovery for Active Directory](#)
- [Before You Start](#)
- [Sign up for Quest Security Management Platform](#)
- [Configuring Identity Recovery for Active Directory](#)
- [Working with Identity Recovery for Active Directory](#)
- [Forests](#)
- [Topology](#)
- [Backup Plans and Backups](#)
- [Recovery](#)
- [Events Management](#)
- [Task Management](#)

Overview of Identity Recovery for Active Directory

The user interface of Identity Recovery for Active Directory consists of six main tabs. The main page, **Forests**, is displayed after you select **Recover** in the left hand navigation panel, and then **Active Directory**.

- **Forests**

On the **Forests** page, you can view a summary of all forests available in Identity Recovery for Active Directory. From this page, you can add your Active Directory forests into the product.

- **Topology**

The **Topology** page shows a summary of your Active Directory forest, including a list of domains and domain controllers within the forest. On this page, you can run forest discovery, perform actions related to the domain controller agent, and create Backup Plans.

- **Backup**

The **Backup** page allows you to create and run Backup Plans. You can view a list of Backup Plans created in the product and a list of backups created from the Backup Plans.

- **Recovery**

The **Recovery** page allows you to create new Recovery Plans and view a summary of the Recovery Plans created in the product. You can open a Recovery Plan to view and edit the details of the plan and perform Recovery Plan verification or forest recovery. When verification or recovery operations are running, the progress of the operation can be viewed by opening the progress view from the Recovery Plan configuration.

- **Events**

The **Events** page provides you with detailed information about errors and warnings that occur during discovery, backup, recovery and verification operations.

- **Tasks**

The **Tasks** page allows you to view task statuses and manage them.

Before You Start

This section provides an overview of some of key information that should be considered when using Identity Recovery for Active Directory. Understanding this information is essential for effectively using the product and troubleshooting any issues that may arise.

Backup Considerations and Best Practices

In this topic:

- [How many domain controllers to backup?](#)
- [Backup frequency](#)
- [Active Directory backups vs Windows System State backups](#)
- [Backup storage and encryption](#)

How many domain controllers to backup?

This depends on the recovery strategy you choose for your environment (see [Recovery Strategies Overview](#) in *Recovery Considerations and Best Practices*).

It is recommended to back up at least two domain controllers from each domain in the forest that are DNS servers and FSMO role holders. However, a maximum of ten domain controllers per domain can be backed up within each forest in Identity Recovery for Active Directory. If a domain controller is added to multiple Backup Plans, each instance counts towards the maximum.

Backup frequency

When deciding on how often to create backups, it is important to note that in case of a disaster, you will need recent and reliable backups. These backups should be created around the same time (within 24 hours) to minimize potential discrepancies after the forest recovery process. The product allows you to restore a domain in the forest to its prior state at the time of the last trusted backup. Consequently, the restore operation will result in the loss of at least the following Active Directory data:

- All objects (such as users and computers) that were added after the last trusted backup.
- All updates made to existing objects since the last trusted backup.
- All changes made to either the configuration partition or the schema partition in Active Directory since the last trusted backup (such as schema changes).

Quest recommends daily backups for each domain controller you want to be able to restore.

Active Directory backups vs Windows System State backups

The Active Directory and Windows System State backups are very similar. The key components that the product backs up as part of the Active Directory system state are the Registry, the NTDS.dit file, and SYSVOL.

What differences do they have?

- Windows System State backup is a full backup of the Windows operating system; Active Directory backup contains only pieces of Active Directory that allow you to restore the domain controller on a clean operating system.
- Windows System State backups contain more components - not all of these components are necessary for Active Directory recovery, e.g. IIS Metabase, Cluster Services, etc.
- Windows System State backup may contain viruses in the components of the operating system.
- Windows System State backups are larger than Active Directory backups.

For the list of Windows System State backup components, see [Microsoft documentation](#).

Identity Recovery for Active Directory enables the backup and restoration of the following Active Directory components on domain controllers:

- DIT Database
- SYSVOL
- Registry, including all registry hives and the file NTUSER.DAT

Backup storage and encryption

Identity Recovery for Active Directory encrypts backups with a password for added security. The passwords used for accessing backups are encrypted using organization specific keys stored in Microsoft Azure Key Vault and are protected using AES-256 algorithm. These passwords are unique, randomly generated and are each 16-characters long. The encrypted passwords are then stored as part of the backup metadata in the Azure SQL database. For details about encryption within Azure Key Vault, see [Privacy and Protection of Customer Data](#) in the *Security Management Platform Global Settings Security Guide*.

At rest, on-premises domain controller backups are stored in Azure Blob Storage and encrypted using AES-256 with the encryption key protected using PBKDF2 and SHA-2.

Recovery Considerations and Best Practices

In this topic:

- [Recovery Strategies Overview](#)
- [Recovery Methods](#)
- [Hybrid Agents and Domain Controller Agents](#)
- [Compatibility with Recovery Manager for Active Directory \(RMAD\) FE/DRE](#)
- [Server Access Credentials](#)
- [DNS Configuration](#)

Recovery Strategies Overview

When planning for Active Directory® forest recovery, ensure that you maintain a detailed topology map of your forest. The map should include all necessary information about each domain controller, such as its name, FSMO roles, DNS configurations, backup status, and the trust relationships between domains.

Identity Recovery for Active Directory allows you to restore selected domains or an entire forest to its prior state at the time of the last trusted backup. When creating a Recovery Plan, use the information from the topology map to verify that all essential components are set to be recovered and are configured properly.

In general, full forest recovery is necessary when none of the domain controllers in the forest can function normally or when corrupted domain controllers can spread dangerous data to other domain controllers.

Before you choose one of the recovery strategies described in this section, it is strongly recommended that you read Microsoft's [Active Directory Forest Recovery Guide](#). When choosing a recovery strategy, note that every recovery is unique, and the strategy might need adjustments to suit your needs.

i **IMPORTANT:** It is highly recommended that:

- You periodically test your chosen strategy to ensure that you are familiar with the process, and that the strategy can be run during a disaster.
- You have Recovery Plans created in Identity Recovery for Active Directory using the most up to date Active Directory forest topology before a disaster occurs. For more information, see [Topology Discovery](#) and [Configuring Recovery Plans](#).

Forest Recovery Overview

At a high level, the recovery of the entire forest or any of its parts using Identity Recovery for Active Directory involves the following steps:

1. Ensure that the hybrid agent used for the Identity Recovery for Active Directory forest has access to the environment where the restore will be performed.
2. Using a new or existing Recovery Plan, set up domain and domain controller configurations according to the Active Directory forest topology map and the combination of the recovery methods available in the product. For more information, see [Configuring Recovery Plans](#) and [Recovery Methods](#).

i **NOTES:**

- Ensure you have specified an appropriate DNS server selection method for each domain. For more information, see [DNS Configuration](#).
- Ensure you are using backups that were created before the forest failure occurred.

3. Start the recovery using the Recovery Plan, which performs the following actions:
 - a. Restores domain controllers within each domain from backups using the **Restore to Clean OS** recovery method, utilizing the most reliable backups.

i **NOTE:** The greater the number of domain controllers restored from backups, the more rapid the recovery process will be. For more information on how many domain controllers to restore, see [Forest Recovery Strategies](#).
 - b. Installs Active Directory on the domain controllers that do not have backups using the **Install Active Directory** recovery method or manually.

i **NOTE:** To reduce replication traffic, you can use the **Enable Install from Media** option.
 - c. Updates DNS settings in any ignored domains that were not recovered or deletes information about any domains or domain controllers that were not recovered.
4. Wait for the domain controllers with installed Active Directory to replicate Active Directory data from domain controllers restored from reliable backups.

After recovery, the Active Directory forest will lose any data that was created or modified after the date of the backup used for recovery. As a result, required changes will need to be performed manually. This includes:

- Objects (such as users and computers) that were added or removed
- Updates to existing objects
- Changes to either the configuration partition or the schema partition in Active Directory (such as schema changes)

Additionally, any software applications that were running on the domain controllers will need to be reinstalled after recovery.

Forest Recovery Strategies

Recovery strategy 1: Restore all critical domain controllers from backups

This strategy is recommended by Quest.

Advantages

- Rapid recovery of the most critical infrastructure allowing to get to business as usual faster.
- Enhanced stability of the recovery process compared to restoring only one domain controller per domain. The use of multiple backups ensures that the entire forest can be recovered, even if the restoration of some domain controllers is unsuccessful.
- The more domain controllers restored from backup, the closer recovered forest resembles its pre-failure state.

Limitations

- The risk of reintroducing corrupted or unwanted data due to the use of multiple backups, there is no guarantee that corrupted or unwanted data from the backups will not be introduced into the recovered forest.

Recovery strategy 2: Restore one domain controller per domain from backups

Advantages

- Recommended by Microsoft - this recovery approach is aligned with Microsoft's best practices as outlined in the [Planning for Active Directory Forest Recovery Guide](#).
- The limited number of backups allows for thorough inspection to ensure they are free of corruption or unwanted data.

Limitations

- Successful recovery of an entire domain relies on the successful restoration of a single domain controller. Active Directory can only be reinstalled on other domain controllers within the domain after the initial domain controller is successfully restored from backup.
- The full forest recovery process may be time-consuming.
- The original forest infrastructure is not preserved - as Active Directory is reinstalled on most domain controllers within the forest, the recovered forest will not be an exact replica of its pre-failure state.

Recovery strategy 3: Restore at least 2 domain controllers per domain from backups

Advantages

- Enhanced stability of the recovery process compared to restoring only one domain controller per domain. The use of multiple backups ensures that the entire forest can be recovered, even if the restoration of some domain controllers is unsuccessful.

Limitations

- The forest recovery process may be time-consuming.
- The original forest infrastructure is not preserved - as Active Directory is reinstalled on most domain controllers within the forest, the recovered forest will not be an exact replica of its pre-failure state.

Recovery Methods

This section describes the recovery methods for domains and domain controllers that you can use to restore the forest or specific domains in Identity Recovery for Active Directory. Depending on your recovery strategy, a different combination of recovery methods may be needed to perform recovery.

The following recovery methods are available for domains:

Recover Domain

The **Recover Domain** recovery method enables the restoration of the entire forest or specific domains within the forest. This is the default recovery method assigned to all domains when a new Recovery Plan is created. At least one domain in the Recovery Plan must be recovered, and at least one domain controller in the domain must be restored from a backup (using the **Restore to Clean OS** recovery method).

i **NOTE:** If the recovery method for the domain is set to **Recover Domain**, the **Restore to Clean OS** recovery method is set by default for all domain controllers in the domain.

i **NOTE:** For information on setting a correct DNS configuration for domains, see [DNS Configuration](#).

Ignore Healthy Domain

Use the **Ignore Healthy Domain** recovery method to exclude the domain from recovery while keeping it intact in the forest. This option performs configuration changes on domain controllers within the domain to ensure connectivity to the recovered domains.

i **NOTE:** If the recovery method for the domain is set to **Ignore Healthy Domain**, the **Adjust to Active Directory Changes** recovery method is set for all domain controllers and cannot be modified.

Delete Domain

The **Delete Domain** recovery method removes the domain from the forest by cleaning up its metadata from all restored and existing domains. This option cannot be used on the forest root domain.

i **NOTE:** If the recovery method for the domain is set to **Delete Domain**, the **Remove DC** recovery method is set for all domain controllers and cannot be modified.

The following recovery methods are available for domain controllers:

Restore to Clean OS

The **Restore to Clean OS** method recovers a domain controller from a backup onto a freshly installed Windows machine. At least one domain controller must be restored with this method in order to recover a domain. This method can be used with servers hosted on-premises or virtual machines hosted by a cloud service provider of your choice.

i **NOTE:** If the recovery method for the domain is set to **Recover Domain**, the **Restore to Clean OS** recovery method is set by default for all domain controllers in the domain.

The target server should comply with the following requirements:

- The operating system version of the target machine must match the version of the failed domain controller.
- The target machine must have sufficient free disk space to accommodate Active Directory and SYSVOL data.
- The account specified to access the target machine must possess local Administrator privileges on that machine.

i **IMPORTANT:** It is crucial that the Windows operating system version matches the deployed version. The verify operation will issue a warning if a mismatch is detected between the target and backup Windows versions. The specific versions will be reported in the status information. If the Major and Minor versions do not match, indicating that at least one of the operating system versions is prior to 2016, an error message will be displayed.

The **Restore to Clean OS** recovery method involves installing the DNS Server role on a domain controller.

- If a domain used AD-integrated DNS infrastructure and is configured in the Recovery Plan to select the DNS server automatically, then during recovery, all domain controllers within the domain will synchronize DNS partitions and continue to function as DNS servers.
- If a domain used external DNS and is configured in the Recovery Plan to use preferred DNS servers, then after recovery, all domain controllers will operate as non-functional DNS servers, which can be uninstalled manually.

For more information on DNS server settings, see [DNS Configuration](#).

Install Active Directory

The **Install Active Directory** recovery method installs Active Directory Domain Services (AD DS) on the computer and promotes it as a domain controller using the domain and forest name of the original domain controller. After the recovery, the domain controller replicates Active Directory data from domain controllers restored from backups. To reduce replication traffic, you can use the **Enable Install from Media** option.

The target server should comply with the following requirements:

- Operating system version should be equal to the original DC operating system.
- Operating system should follow organization security best practices (e.g. have latest updates, security software) since this operating system will be used to run the Active Directory Domain services after

the restore.

- The physical disks should have enough free space to host the Active Directory® data after recovery.

The **Install Active Directory** recovery method includes the option to install the DNS server on the domain controller, which is enabled by default. For more information on DNS server settings, see and [DNS Configuration](#).

Remove DC

The **Remove DC** recovery method isolates the domain controller from other domain controllers and completely removes it from the domain; no actions are performed on the domain controller itself. This method should be used if the domain controller is inaccessible or you do not want to recover the domain controller due to failures. Identity Recovery for Active Directory removes all metadata of domain controllers that are set for removal.

i | **NOTE:** If the recovery method for the domain is set to **Delete Domain**, the **Remove DC** recovery method is set by default for all domain controllers.

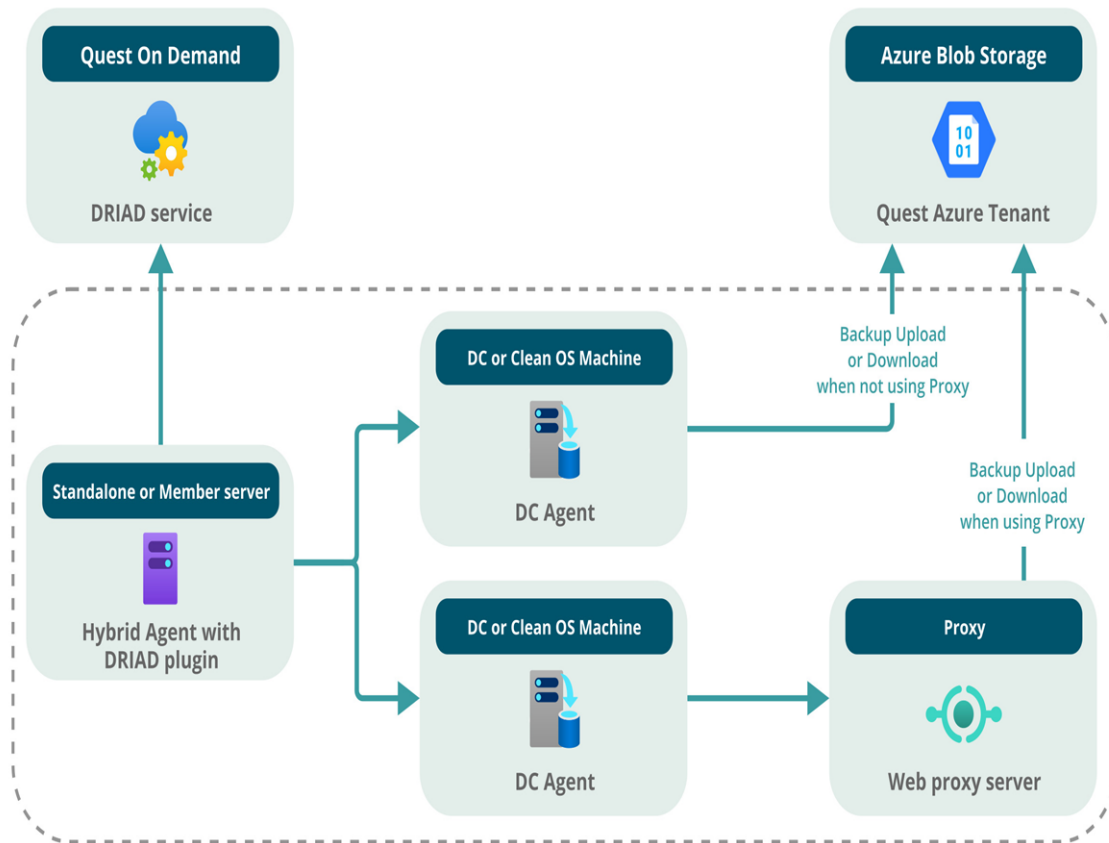
Adjust to Active Directory Changes

The **Adjust to Active Directory Changes** recovery method adjusts the DNS and IP configuration of the existing domain controller to ensure connectivity to the recovered domains. For example, in domains with AD-integrated DNS infrastructure, this recovery method automatically updates the DNS configuration of domains that were not restored if the IP address of the primary DNS server in the restored domain has changed, or if the IP addresses of non-restored domain controllers are removed from the DNS configuration.

i | **NOTE:** If the recovery method for the domain is set to **Ignore Healthy Domain**, the **Adjust to Active Directory Changes** recovery method is set for all domain controllers in the domain and cannot be modified.

Hybrid Agents and Domain Controller Agents

Identity Recovery for Active Directory uses two types of agents: hybrid agents and domain controller (DC) agents. This section explains their roles, installation requirements, and best practices to ensure secure communication and reliable backup and recovery operations in your Active Directory environment.



Hybrid agents

A hybrid agent is used to securely communicate with any installed on-premises DC agents. To facilitate communication with your environment, a hybrid agent must be manually installed on-premises.

Ensure that the hybrid agent has a stable internet connection during the recovery operation and uses a DNS server that is not affected by the forest failure.

Where should the hybrid agent be installed?

The hybrid agent needs to be installed on a server that can access the Active Directory forest on which backup and restore operations intend to be performed. You can install the agent on either a standalone or domain-joined server; however, the use of a standalone server is recommended to avoid disruptions caused by potential forest malfunctioning.

When setting up a hybrid agent server, ensure it can access Identity Recovery for Active Directory even in the case of a disaster. For example, if the server uses an AD-integrated DNS server on a domain controller, and that domain controller becomes unavailable, the hybrid agent will lose access to product and backup or recovery will not be possible. Therefore, it is important to ensure that an alternate DNS is specified to mitigate this risk.

To download the hybrid agent installer, go to **Tenants | Hybrid Agents**, select the **Add agent** button, and follow the instructions to install the agent. The account used for installing a hybrid agent must be a member of the local administrator's group. Only a single hybrid agent per forest is currently supported.

What if the hybrid agent is not available to the new environment?

When restoring a forest into a new environment, the existing hybrid agent might not be available because it was destroyed during the disaster or lacks access to the environment. In this case, you need to deploy a new hybrid agent in the environment. Before starting the recovery, update the forest to use the new hybrid agent. To do so, on the **Forests** tab, select **Edit** on the relevant tile, navigate to **Connection Settings**, and select the new hybrid agent.

Troubleshooting hybrid agent connectivity issues

The hybrid agent may become unavailable and prevent recovery from starting or proceeding if the machine hosting the hybrid agent loses internet connectivity due to a DNS server failure caused by a forest failure or outage. In this case, assign an operational DNS server to the hybrid agent machine.

Domain Controller Agents

A DC agent perform actions such as backup or restore on a single domain controller within your Active directory forest.

Where should the DC agent be installed?

The DC Agent should be installed on each domain controller on which you may need to perform certain operations such as restoring from a backup during recovery.

Before you can install the DC agent on domain controllers, you must first add a forest and run topology discovery. You can install the DC agent from the **Topology** tab by either:

- a. Selecting the checkboxes for the relevant domain controllers and then selecting **DC Agent | Install Agent**, or
- b. Downloading the DC agent installer by selecting **DC Agent | Download Agent** and manually installing the agent on the desired machine.

The account used for installing a DC agent must be a member of the local administrator's group.

For more information about the permissions required for the hybrid agent and DC agent, see *Required permissions* in the [Security](#) section.

Compatibility with Recovery Manager for Active Directory (RMAD) FE/DRE

When using Identity Recovery for Active Directory (Identity Recovery for AD) and Recovery Manager for Active Directory Forest Edition (RMAD FE) or Recovery Manager for Active Directory Disaster Recovery Edition (RMAD DRE) in the same Active Directory environment:

- RMAD FE/DRE 10.3.2.46178 or later is required.
- It is recommended to install the Identity Recovery for AD hybrid agent on the same machine as the RMAD Forest Recovery Console.

Forest Recovery Agent vs Domain Controller Agent

Identity Recovery for AD uses the RMAD FE/DRE Forest Recovery Agent as a domain controller agent (DC agent). Identity Recovery for AD can connect and use an existing Forest Recovery Agent deployed in the environment when a hybrid agent is installed on the machine hosting the Forest Recovery Console.

Supported Versions for the DC Agent

The DC agent uses separate minimum supported versions for backup and recovery tasks:

- For backup tasks, agent versions on the current and previous RMAD FE/DRE releases, including hotfixes, are supported. Agents running an older but supported version will show an **Outdated** status on the **Topology** page and need to be updated soon to avoid backup interruptions. Older versions that are no longer supported will show a **Not Supported** status and require an update for backup tasks to run.

- For verification and recovery tasks, agent versions on the latest available RMAD FE/DRE release or hotfix are supported. Agents running an older but supported version will show an **Outdated** status on the **Domain Controllers** tab of the Recovery Plan configuration; verification and recovery will run, but updating the agent to the latest version is strongly recommended. Agents running older versions will show a **Not Supported** status and will be automatically updated when you run verification against the target server or recovery.

Communication Keys Synchronization

It is possible to install the Identity Recovery for AD hybrid agent and the Forest Recovery Console on different machines or add RMAD DRE/FE into an environment that already has Identity Recovery for AD. In this case, manual key synchronization may be required to allow both products to use the same Forest Recovery Agent.

1. If the Identity Recovery for AD hybrid agent and Forest Recovery Console are installed on different machines:
 - a. If RMAD FE/DRE was installed first, it is recommended that you copy the RMAD keys after installing the hybrid agent:
 - In the Forest Recovery Console, open the **Tools | Fault Tolerance | Export communication keys...** dialog. Select the file to which you want to export the keys and enter a secret password of your choice. After exporting, copy the file to the hybrid agent machine.
 - On the hybrid agent machine, open an elevated ("Run as Administrator") command prompt and run the following command (assuming that the keys were copied to the C:\Temp\exported_keys.pfx file):


```
C:\ProgramData\Quest\OnDemandAgent\Service\OdradPlugin\

This command imports keys from the exported_keys.pfx file and stores them in the ConsoleCommunicationKeys.rmad and AgentCommunicationKeys.rmad files in the C:\ProgramData\Quest\OnDemandAgent\Service\OdradPlugin\


```
 - Finally, copy the ConsoleCommunicationKeys.rmad and AgentCommunicationKeys.rmad files from C:\ProgramData\Quest\OnDemandAgent\Service\OdradPlugin\
 - b. If the Identity Recovery for AD hybrid agent was installed first, it is recommended that you copy the hybrid agent keys to RMAD:
 - On the hybrid agent machine, open an elevated ("Run as Administrator") command prompt and run the following command (the exported_keys.pfx file name and path may be different, use a secret password of your choice):


```
C:\ProgramData\Quest\OnDemandAgent\Service\OdradPlugin\

This command exports the keys to the file exported_keys.pfx. After the export, copy the file to any folder on the RMAD machine. Then, in the Forest Recovery Console, open the Tools | Fault Tolerance | Import communication keys... dialog. Select the copied file and enter a password.


```
2. If the Identity Recovery for AD hybrid agent and Forest Recovery Console are on the same machine and the hybrid agent was installed first, reinstall the agents either from Identity Recovery for AD or the Forest Recovery Console.

Server Access Credentials

The following are definitions for each credential when configuring domains or domain controllers:

Domain User

This account must be a domain administrator in the domain that is being restored. After the domain is restored, the password for this account is reset to the specified value, regardless of the value restored from the backup. Supported format is domain\username or username. If only the username is specified, then the local domain name is automatically added.

Local User

Specifies the account that will be used to access the target computer to install the agent before the target computer is promoted to a domain controller. This account must be a local administrator on the target computer. Supported format is machine\username or username. If only the username is specified, then the target machine name is automatically added.

DSRM Administrator

Specifies the account used to promote the target computer to a domain controller in the Restore to Clean OS recovery method. After the domain is restored, the password for the DSRM Administrator account is reset to the specified value, regardless of the value restored from the backup.

DNS Configuration

When using the **Recover Domain** recovery method, you need to specify the DNS configuration for domain controllers within that domain. This section helps you select the correct option for your environment.

In the domain configuration, you can choose one of the following options for DNS server selection:

- **Select DNS server automatically** – Automatically selects and assigns a DNS server for each domain controller in the domain. This option is selected by default.
- **Use preferred DNS server(s)** – Assigns DNS servers from a user-specified list of one or more IP addresses, each separated by a semicolon (;).

Select DNS server automatically

The **Select DNS server automatically** option is recommended in the following cases:

- Your DNS is Active Directory-integrated (AD-integrated DNS service).
- Your DNS is not Active Directory-integrated (external DNS service), and the original DNS servers are available to the restored domain controllers.

For Active Directory-integrated DNS, ensure that at least one DNS server for each DNS zone is restored from backup. The best practice is to restore as many DNS servers as possible from backup.

When the original DNS servers are available, automatic DNS selection uses an ordered list of the original DNS servers as follows. First, it includes IP addresses configured in the DNS client settings of the domain controller. Next, it includes the preferred DNS addresses of other domain controllers within the same domain and their DNS client settings. This approach is then used for domain controllers in the parent domain hierarchy, followed by those in child and direct child domains. During recovery, Identity Recovery for Active Directory automatically selects a functioning DNS server from the resulting list and assigns that DNS server to the domain controller.

Use preferred DNS servers

The **Use preferred DNS server(s)** option is recommended when using a new external DNS server during recovery. When this option is specified, ensure the DNS servers:

- Are properly configured to work with the domain controllers being recovered;
- Support dynamic updates;
- Have DNS zones configured for each domain within the forest you intend to recover.

During recovery, Identity Recovery for Active Directory checks whether the specified DNS server is accessible. If the DNS server is unavailable or not functioning properly, one or more of the original DNS servers will be selected.

Security

In this topic:

- [Required permissions](#)
- [Endpoint requirements](#)
- [Windows Firewall](#)

Required permissions

This section describes specific permission requirements needed for agents and credentials in Identity Recovery for Active Directory. For permissions needed to operate the solution, see [Roles and Permissions in Security Management Platform](#).

Method	Service	Permissions
Restore to Clean OS	Hybrid agent	A service account used to run the hybrid agent service must be a local administrator account on the computer where the hybrid agent is installed. The domain FQDN\username should at least have forest-wide read permissions.
	Domain controller agent	A service account used to run the domain controller agent is always a Local System account. An account used to install the domain controller agent remotely a member of the Local Administrators group.
	Domain User	When configuring a domain or domain controller, this account must be a domain administrator in the domain that is being restored.
	Local User	When configuring a domain or domain controller, this account must be a local administrator on the target computer.
Install Active Directory	Hybrid agent	A service account used to run the hybrid agent service must be a local administrator account on the computer where the hybrid agent is installed. The domain FQDN\username should at least have forest-wide read permissions.
	Domain controller agent	A service account used to run the domain controller agent is always a Local System account. An account used to install the domain controller agent remotely a member of the Local Administrators group.

Method	Service	Permissions
	Domain User	When configuring a domain or domain controller, this account must be a domain administrator in the domain that is being restored.
	Local User	When configuring a domain or domain controller, this account must be a local administrator on the target computer.

Endpoint requirements

Hybrid agent requirements

TCP Port	Direction	Endpoints	Description
389	Outbound	Domain Controllers	LDAP port to domain controllers to discover forest topology.
445	Outbound	Domain Controllers	SMB port to domain controllers to install domain controller agents.
443	Outbound	<p>AU odjrs-auprod-au-iothub.azure-devices.net https://odjrсаuproduаgrssto.blob.core.windows.net https://odrjsаuprodausto.blob.core.windows.net</p> <p>CA odjrs-caprod-ca-iothub.azure-devices.net https://odjrscaprodcagrsto.blob.core.windows.net https://odrjscaprodcasto.blob.core.windows.net</p> <p>EU odjrs-euprod-eu-iothub.azure-devices.net https://odjrseuprodeugrsto.blob.core.windows.net https://odjrseuprodeusto.blob.core.windows.net</p> <p>UK odjrs-ukprod-uk-iothub.azure-devices.net https://odjrѕukprodukgrsto.blob.core.windows.net https://odjrѕukproduksto.blob.core.windows.net</p> <p>US odjrs-usprod-us-iothub.azure-devices.net https://odjrѕusproduѕgrsto.blob.core.windows.net https://odjrѕusproduѕsto.blob.core.windows.net</p>	Agent connection to Identity Recovery for Active Directory backend services (see Security Management Platform Global Settings User Guide for more)

TCP Port	Direction	Endpoints	Description
80	Outbound	<p>AU odjrсаuprodauiotinst- odjrсаuprodauiotacct.b.nlu.dl.adu.microsoft.com</p> <p>CA odjrscaprodcaiotinst- odjrscaprodcaiotacct.b.nlu.dl.adu.microsoft.com</p> <p>EU odjrseuprodeuiotinst-- odjrseuprodeuiotacct.b.nlu.dl.adu.microsoft.com</p> <p>UK odjrѕukprodukiotinst-- odjrѕukprodukiotacct.b.nlu.dl.adu.microsoft.com</p> <p>US odjrѕusprodusiotinst-- odjrѕusprodusiotacct.b.nlu.dl.adu.microsoft.com</p>	Agent connection to Identity Recovery for Active Directory backend services (see Security Management Platform Global Settings User Guide for more)

Domain Controller Agent requirements

TCP Port	Direction	Endpoints	Description
445	Inbound		SMB port to allow automatic agent installation.
135	Inbound		RPC Endpoint Mapper port used by the RPC runtime.
49152-65535	Inbound		RPC dynamic port range to accept RPC connection from hybrid agent.
443 or proxy server port	Outbound	<p>AU https://odradprodausa.blob.core.windows.net</p> <p>CA https://odradprodcasa.blob.core.windows.net</p> <p>EU https://odradprodeusa.blob.core.windows.net</p> <p>UK https://odradproduksa.blob.core.windows.net</p>	Download and upload backups from Azure Blob Storage accounts.

TCP Port	Direction	Endpoints	Description
		US https://odradprodussa.blob.core.windows.net	

Windows Firewall

A firewall in your environment may block network traffic on ports used by Identity Recovery for Active Directory, potentially hindering backup and restore operations. Before using the product, ensure your firewall does not restrict traffic on the necessary ports.

You can configure built-in Windows Firewall on domain controllers to be backed up either automatically or manually. For firewall rules for the hybrid agent, see [On-premises agent requirements](#) in the *Security Management Platform Global Settings User Guide*.

Automatic

This is enabled by default and will not configure any outbound firewall rules. Depending on your environment, you may need to configure outbound rules manually (allow outbound 443 or proxy port).

Manual

This is used if the automatic method fails for any reason, or if the automatic method has been disabled. Depending on your environment, you may also need to configure outbound rules manually (allow outbound 443 or proxy port).

The following list describes the settings for each firewall rule. Any setting not described in this list can be left as the default value:

Rule 1

- Rule Type: Custom
- Program Path: System
- Service settings: Apply to all programs and services
- Protocol: TCP
- Local ports: 445
- Remote ports: Any
- Local IP addresses: Any
- Remote IP addresses: Any
- Action: Allow the connection
- Rule profile: Domain, Private, and Public
- Allowed users: Any
- Allowed computers: Any

PowerShell for the Rule 1 settings: *New-NetFirewallRule -DisplayName "Rule 1" -Group DRIAD -Enabled True -Profile Any -Direction Inbound -LocalPort 445 -Protocol TCP -Program System*

Rule 2

- Rule Type: Custom
- Program Path: %SystemRoot%\System32\Svchost.exe
- Service settings: Remote Procedure Call (RpcSs)
- Protocol: TCP

- Local ports: RPC Endpoint Mapper
- Remote ports: Any
- Local IP addresses: Any
- Remote IP addresses: Any
- Action: Allow the connection
- Rule profile: Domain, Private, and Public
- Allowed users: Any
- Allowed computers: Any

PowerShell for the Rule 2 settings: *New-NetFirewallRule -DisplayName "Rule 2" -Group DRIAD -Enabled True Profile Any -Direction Inbound -LocalPort RPCEPMap -Protocol TCP -Program "%SystemRoot%\System32\Svchost.exe" -Service RpcSs*

Rule 3

Rule Type: Custom

Program Path: C:\Program Files\Quest\Recovery Manager for Active Directory Forest Edition\FRRRestoreService64.exe

Service settings: Apply to all programs and services

Protocol: TCP

Local ports: RPC dynamic port range

Remote ports: Any

Local IP addresses: Any

Remote IP addresses: Any

Action: Allow the connection

Rule profile: Domain, Private, and Public

Allowed users: Any

Allowed computers: Any

PowerShell for the Rule 3 mn nmsettings: *New-NetFirewallRule -DisplayName "Rule 7" -Group DRIAD -Enabled True Profile Any -Direction Inbound -LocalPort RPC -Protocol TCP -Program "C:\Program Files\Quest\Recovery Manager for Active Directory Forest Edition\FRRRestoreService64.exe"*

Sign up for Quest Security Management Platform

To access Identity Recovery for Active Directory, you need to sign up for the Security Management Platform service and create an organization. Go to quest-on-demand.com and use one of the following options:

- Sign up using the existing Quest account.
- Create a new Quest account and sign up for Quest Security Management Platform.
- Join an existing Security Management Platform organization.

For details, see [Signing up for Quest Security Management Platform](#) in the *Security Management Platform Global Settings User Guide*.

Configuring Identity Recovery for Active Directory

- [Organizations and Regions](#)
- [Access Control](#)
- [Roles and Permissions in Security Management Platform](#)
- [Email Notifications](#)

Organizations and Regions

When you sign up for Security Management Platform for the first time, you create an organization and you are granted the Platform Administrator role. You can add additional organizations and administrators.

When selecting a region for an organization, this indicates where all Identity Recovery for Active Directory services are running as well as the region for backup storage.

For more information about managing your organization, see [Managing organizations and regions](#) in the *Security Management Platform Global Settings User Guide*.

Access Control

Quest Security Management Platform uses the Role-based Access Control (RBAC) security policy that restricts information system access to authorized users. Your Security Management Platform organization comes configured with a number of default roles. The default role permissions settings cannot be changed, but you can create custom roles with specific permission settings to align with your company policies.

If you are the Platform Administrator or the owner of the subscription, you can add users to an existing organization and assign the required roles. If you are not the subscription owner or administrator, contact your Platform administrator for access.

For more information on assigning roles, see [Adding users to an organization](#) in the *Security Management Platform Global Settings User Guide*.

Roles and Permissions in Security Management Platform

This section lists the minimum user account permissions required to perform specific tasks in Identity Recovery for Active Directory. The role definitions and their associated permissions for Identity Recovery for Active Directory are listed below. For more information on roles in Security Management Platform, see [Access Control: Roles](#) in the *Security Management Platform Global Settings User Guide*.

Identity Recovery for Active Directory role permissions

- **Identity Recovery for AD Viewer:** The Identity Recovery for AD Viewer role allows read only access to all areas of Identity Recovery for Active Directory.
 - Identity Recovery for AD:
 - Can View All
- **Identity Recovery for AD Backup Operator:** The Identity Recovery for AD Backup Operator role allows to set up and manage backups and backup-related operations.
 - Identity Recovery for AD:
 - Can Manage Backups
 - Can View All
- **Identity Recovery for AD Restore Operator:** The Identity Recovery for AD Restore Operator role allows to manage all backup and recovery operations.
 - Identity Recovery for AD:
 - Can Manage and Verify Recovery Plans
 - Can Manage Backups
 - Can Run Recovery
 - Can View All

- **Identity Recovery for AD Administrator:** The Identity Recovery for AD Administrator role allows full access to Identity Recovery for Active Directory.
 - Security Management Platform organization:
 - Can Configure Agents
 - Can Export Data: Identity Recovery
 - Can Read Access Control Roles
 - Can Read Activity Trail: Identity Recovery
 - Identity Recovery for AD:
 - Can Manage and Verify Recovery Plans
 - Can Manage Backups
 - Can Manage Domain Controller Agents
 - Can Manage Forests
 - Can Run Forest Topology Discovery
 - Can Run Recovery
 - Can View All

- **Identity Recovery Administrator:** The Identity Recovery Administrator role allows full access to Identity Recovery (Identity Recovery for Active Directory and Identity Recovery for Microsoft Entra ID).
 - Security Management Platform organization:
 - Can Configure Agents
 - Can Export Data: Identity Recovery
 - Can Read Access Control Roles
 - Can Read Activity Trail: Identity Recovery
 - Identity Recovery for AD:
 - Can Manage and Verify Recovery Plans
 - Can Manage Backups
 - Can Manage Domain Controller Agents
 - Can Manage Forests
 - Can Run Forest Topology Discovery
 - Can Run Recovery
 - Can View All
 - Identity Recovery for Entra ID:
 - Can Download Hybrid Credentials
 - Can Manage Backup Settings
 - Can Manage Events
 - Can Manage Project Settings
 - Can Read Backup History
 - Can Read Differences
 - Can Read Events
 - Can Read Restore Attributes
 - Can Read Task History
 - Can Read UI Projects
 - Can Read Unpacked Objects
 - Can Restore from Differences
 - Can Restore from Objects
 - Can Run Backup Manually
 - Can Run Difference Report
 - Can Unpack Backups

Permission definitions

The following table describes each permission used in Identity Recovery for Active Directory.

Permission	Description
Can View All	View all areas of Identity Recovery for Active Directory, including email notifications in Settings Notifications .
Can Manage Backups	Manage Backup Plans and backups, including starting, pausing, and canceling backup tasks.
Can Manage and Verify Recovery Plans	Manage Recovery Plans and run plan verification. Perform actions during verifications including starting, pausing, and canceling verification tasks.
Can Run Recovery	Ability to start, pause, and cancel recovery tasks.
Can Run Forest Topology Discovery	Ability to run, pause, and cancel topology discovery.
Can Manage Domain Controller Agents	Ability to download, install and upgrade domain controller (DC) agents, as well as starting, pausing, and canceling agent tasks.
Can Manage Forests	Ability to add a new or modify an existing forest. Can configure email notifications for Identity Recovery for Active Directory in Settings Notifications .

Email Notifications

Email notifications in Security Management Platform alert designated recipients when specific events occur. For example, if a Backup Plan fails, the configured recipients receive an email notification. Identity Recovery for Active Directory includes built-in notification templates to ensure that you are kept up to date on critical activity within your organization. For information on how to configure who will receive the notification, see [Configuring Notification Templates](#).

The following built-in notification templates are currently available:

- Agent Upgrade Needed

i **NOTE:** This email notification is enabled by default. If a DC agent version is detected as **Outdated** or **Not Supported** when a Backup Plan runs, a notification is sent to the Recovery Administrator and Recovery for AD Administrator once every 24 hours. This notification is not sent when you manually refresh the agent status. If you receive this notification, go to the **Topology** page to identify the affected domain controllers and update the DC agents.

- Backup of Domain Controller Failed
- Backup Plan Completed
- Backup Plan Created
- Backup Plan Failed
- Backup Plan Removed
- Backup Plan Updated
- Forest Added
- Forest Removed
- Forest Updated
- Recovery Completed

- Recovery Failed
- Recovery Plan Created
- Recovery Plan Removed
- Recovery Plan Updated
- Recovery Plan Verification Completed
- Recovery Plan Verification Failed

Configuring Notification Templates

Notification templates allow you to configure who will receive notifications so that they can take the appropriate action to address the outlined risks to your environment. Notification templates are managed through Security Management Platform Global Settings. For information about required permissions, see [Roles and Permissions in Security Management Platform](#).

To edit a notification template

1. In the side navigation panel of Security Management Platform, select **Settings**.
2. In the main panel, select **Notification | Email Notifications** in the menu bar.
3. Expand **Identity Recovery for Active Directory**.
4. Select the notification template name of the template you want to edit.
5. To enable sending email notifications, turn the **Email Notifications** toggle on. To disable notifications, turn the toggle off.
6. To add recipients by role or email address:
 - Under **Role Recipients**, select the required roles, then select **Add Role Recipients**.
 - Under **Email Recipients**, enter the required email addresses, then select **Add Recipients**.
7. To remove recipients, under **Recipient Role** or **Recipient Email**, select the checkboxes for the relevant recipients and select **Remove**.
8. Optionally, send a test email by selecting the checkboxes for one or more recipients and selecting **Send Test Email**.
9. Select **Save**.

The next time an event associated with this notification template occurs, the listed recipients receive a notification email.

Working with Identity Recovery for Active Directory

This section provides step-by-step instructions on how to start using Identity Recovery for Active Directory.

1. Go to quest-on-demand.com and sign up for Quest Security Management Platform. For more information, see [Sign up for Quest Security Management Platform](#).
2. To launch Identity Recovery for Active Directory, select **Recover** in the left pane, then select **Active Directory**.

Below is a general overview of the steps required to successfully use Identity Recovery for Active Directory:

1. Deploy hybrid agents on the standalone or domain-joined server connected to the forest you wish to backup and restore.

i **NOTE:** When using Recovery Manager for Active Directory Forest Edition (RMAD FE) or Disaster Recovery Edition (RMAD DRE), it is highly recommended to install the hybrid agent on the Forest Recovery Console machine.

2. Add the forest into Identity Recovery for Active Directory by selecting the hybrid agent deployed in the Active Directory forest.
3. Discover forest topology and install domain controller agents on the domain controllers you want to back up.
4. Create Backup Plans and schedule regular backups of the domain controllers.
5. Create a Recovery Plan to be used in case of disaster.
6. Verify the Recovery Plan on a regular basis to identify any potential issues with the plan.

! **CAUTION:** Microsoft Entra is a dynamic and rapidly evolving platform, which means its APIs may be updated or changed with limited notice. These ongoing changes may occasionally impact features in Identity Recovery for Active Directory. When possible, Quest aims to provide timely notification to customers in cases of such impact. For the latest updates on Entra ID APIs, refer to the [Microsoft Entra ID](#) documentation and [Microsoft Graph Changelog](#).

Forests

Once you start adding forests in Identity Recovery for Active Directory, a tile will appear on the **Forests** tab representing each forest. Each tile displays the status of the forest, a summary of its scope, and actions links.

Status

This section displays information on the status of a current or latest discovery, backup, verification, and recovery. For a newly added forest, you can run a discovery by selecting **Run Discovery**. For more information on verification and recovery statuses, see [Recovery Page Tiles](#).

Forest Summary

This section shows the number of domains and domain controllers (DCs) in the forest discovered during the last topology discovery run. Select **View Topology** to see more details.

Hybrid Agent

This section displays the name and FQDN of the hybrid agent and indicates if the hybrid agent is both connected and online. If the plugin version is outdated, the latest available version is displayed along with a prompt to restart the hybrid agent to update the plugin.

If Secure LDAP (LDAPS) is enabled on the hybrid agent for the forest, a badge labeled **Secure LDAP** is displayed above the hybrid agent name. If Secure LDAP is not enabled, the badge displays **LDAP**.

For more information on hybrid agents, including how to add a hybrid agent, see [Managing your Microsoft Entra tenants and on-premises domains](#) section in the *Security Management Platform Global Settings User Guide*. You can configure the agent by selecting **Manage Agent**.

Toolbar

You can perform the following actions using the toolbar at the top of the page:

- **Add Forest** – Add an Active Directory forest into Identity Recovery for Active Directory. For more information, see [Adding and Configuring Forests](#).
- **Manage Notifications** – Opens the Security Management Platform Global Settings where you can configure notification templates. For more information, see [Email Notifications](#).

- **RMAD Compatibility** – View information on how Identity Recovery for Active Directory and Recovery Manager for Active Directory (RMAD) work in the same environment. For more information, see [Compatibility with Recovery Manager for Active Directory \(RMAD\) FE/DRE](#).
- **About Agents** - View an information panel to learn more about hybrid agents and domain controller agents.

Action Links

You can use the links on the bottom of the card to perform the following actions:

- **View** – See details about the forest configuration in Identity Recovery for Active Directory, including the name, associated hybrid agent, account used to perform topology discovery, and agent proxy settings.
- **Edit** – Change the forest configuration in Identity Recovery for Active Directory, including the name, associated hybrid agent, credentials used to perform topology discovery, and agent proxy settings.
- **Remove** – Delete the forest from Identity Recovery for Active Directory.

i | **NOTE:** If you delete the forest, all backups created by the solution will no longer be available.

i | **NOTE:** While topology discovery, backup, or Recovery Plans are in progress, you cannot edit or remove the forest.

Adding and Configuring Forests

To start using Identity Recovery for Active Directory, you will need to add your Active Directory forest into the product.

Each Active Directory forest you plan to back up and restore needs to be added into the solution. Forests in Identity Recovery for Active Directory are isolated from each other; each forest has its own topology, agent management, Backup Plans, and Recovery Plans.

Each forest also needs to have its own hybrid agent to facilitate communication between the product and on-premises domain controller agents.

In this section:

- [Creating and Installing Hybrid Agents](#)
- [Adding Forests into Identity Recovery for Active Directory](#)

Creating and Installing Hybrid Agents

Before you add a forest into Identity Recovery for Active Directory, a hybrid agent will need to be installed on-premises. A hybrid agent is used to securely communicate with any installed on-premises domain controller (DC) agents. To facilitate communication with your environment, a hybrid agent must be manually installed on-premises. To do this:

1. Log in to Security Management Platform using the credentials you used to sign up for the platform.
2. In the navigation panel on the left, select **Tenants**.
3. Select **Hybrid Agents**.
4. Select **Add agent**.

5. Go to the [Adding an on-premises agent](#) section in the *Security Management Platform Global Settings User Guide* and follow the instructions to download and install the hybrid agent.

i **NOTE:** If you enable Secure LDAP (LDAPS) during installation of the hybrid agent by entering `Y` when prompted to enable SSL/TLS encryption on LDAP queries, Secure LDAP queries are used when running topology discovery. Topology discovery will fail if Secure LDAP queries are unsuccessful. For more information, see the section *Using Secure LDAP (LDAPS) for Hybrid Agent Queries* in [Topology Discovery](#).

6. When the hybrid agent is selected for a forest in Identity Recovery for Active Directory, the agent configuration is automatically set to include the action **Identity Recovery for Active Directory**. For more information, see [Adding Forests into Identity Recovery for Active Directory](#).

Adding Forests into Identity Recovery for Active Directory

To add a forest

1. On the **Forests** tab, select **Add Forest**.
2. Enter a unique name to identify the forest.
3. Select the hybrid agent you created from the drop down menu.

i **NOTES:**

- Agents already assigned to a forest are not displayed in the drop down menu.
 - Only a single hybrid agent per forest is currently supported.
4. To use Secure LDAP (LDAPS) for the hybrid agent when performing topology discovery queries, turn on the **Use Secure LDAP (LDAPS) for Hybrid Agent Queries** toggle. By default, this toggle is enabled if Secure LDAP is set during hybrid agent installation. For more information, see the section *Using Secure LDAP (LDAPS) for Hybrid Agent Queries* in [Topology Discovery](#).

i **NOTE:** After saving the forest, the **Use Secure LDAP (LDAPS) for Hybrid Agent Queries** setting is preserved for the forest and overrides any changes made to the hybrid agent, even if the hybrid agent is reinstalled or updated with a different LDAPS setting.

5. Enter the Active Directory domain username and password that will be used to discover Active Directory domains and domain controllers.

i **NOTES:**

- The entered domain\username should have at least forest-wide read permissions.
 - When using a standalone agent, provide the domain FQDN\username.
5. Select the internet access configuration to be used by domain controller agents to upload and download backups by choosing a proxy configuration. You can use one of the following options:
 - a. **System proxy configuration** – Selected by default, this option uses the proxy settings configured on the machine to access the Internet.
 - b. **Manually configured proxy** – Manually specify the server address and port in the relevant boxes.

6. Select **Save**. After the forest is added, run a discovery of your Active Directory forest by selecting **Run Discovery** either on the tile for the newly created forest or on the **Topology** page.

i | **NOTE:** To prevent unexpected behavior, add an Active Directory forest into Security Management Platform only once.

Topology

On the **Topology** tab, you can see the latest discovered topology of your Active Directory forest.

Forest Summary

The header in **Forest Summary** shows the following:

- The number of domains and domain controllers in the forest.
- How long ago the last topology discovery was run.
- The date and time of the latest discovered topology changes to the forest.

In the **Forest Summary** table, you can view the following:

- **Domain Controller** – The FQDN of the domain controller within the Active Directory forest.
- **Type** – The domain controller type, which can be one of the following:
 - GC – Global catalog server
 - DC – Writable domain controller
 - RODC – Read-only domain controller
- **Domain** – The FQDN of the domain within the Active Directory forest.
- **FSMO Role** – The FSMO (Flexible Single Master Operation) roles assigned to the domain controller, displayed as a badge for each role. The FSMO roles are as follows:
 - PDC emulator
 - RID master
 - Infrastructure master
 - Schema master
 - Domain naming master
- **Site** – The name of the site in which the domain controller is located.

- **DC Agent Status** – The status of the domain controller agent. This status displays the agent’s connectivity and indicates whether its version is supported for backup tasks. By hovering over the status icon, you can see the currently installed agent version and, if applicable, the minimum supported version and the latest available version.
 - **Online** – The domain controller agent is online and the latest version is installed.
 - **Outdated** – The domain controller agent is online and running a supported but older version. Backup tasks will run, but an agent update to the latest version is strongly recommended.
 - **Not Supported** – The domain controller agent is installed and online, but the version is no longer supported and requires an update. Backup tasks cannot be performed until the agent is updated.
 - **Offline** – The domain controller agent cannot be reached or is not installed.
 - **Installing** – The domain controller agent is being installed.
 - **Refreshing** – The status of the domain controller agent is being updated.
 - **Unknown** – The status of the domain controller agent has not been checked yet. To get the latest status, select the checkboxes for one or more domain controllers, then select **DC Agent | Refresh Agent Status**.

i **NOTE:** If an agent is detected as **Outdated** or **Not Supported** when a Backup Plan is run, an email notification is sent by default to the Identity Recovery Administrator and Identity Recovery for AD Administrator once every 24 hours. For more information, see [Email Notifications](#).

- **In Backup Plans** – The Backup Plans which include the associated domain controller. If the domain controller is associated with multiple Backup Plans, hover over the icon to view the Backup Plans which include the domain controller. A maximum of ten domain controllers per domain can be backed up within the forest. If a domain controller is added to multiple Backup Plans, each instance counts towards the maximum.
- **Last Backup Status** – The status of the most recent backup task and how long ago it was run. By hovering over the status, you can see the exact date and time of the backup task.

Toolbar

You can perform the following actions using the toolbar in the top panel of the **Topology** page:

- **Filters** – Filter the list of domain controllers by one or more domains, DC agent statuses, or Backup Plans.
- **Run Discovery** – Run topology discovery in the Active Directory forest. This action updates the domain controllers listed in the table.
- **DC Agent** – Select this button to access agent-related actions:
 - **Refresh Agent Status** – Refresh the domain controller agent status.

i **NOTE:**

- You can select a single or multiple domain controllers to refresh their status only.
- The agent status is automatically refreshed each time a backup is performed.

- **Install Agent** – Deploy or upgrade a domain controller agent on one or multiple domain controllers. For more information, see [Installing Domain Controller Agents](#).
- **Download Agent** – Download the domain controller agent package. A task is generated to download the agent, and once the task is complete, a download link will be available on the **Tasks** page. The download package will expire in 30 minutes. For more information on domain controller agents, either select **About Agents** on the **Forests** page or see [Hybrid Agents and Domain Controller Agents](#) in the *Recovery Considerations and Best Practices* section.

- **Create Backup Plan** – Create a Backup Plan for the selected domain controllers from the **Topology** page. For more information, see [Backup Plans and Backups](#).

Topology Discovery

After adding a forest, select **Run Discovery** to run a discovery for domains and domain controllers for the selected forest. To run a discovery, the user must have the *Identity Recovery for AD: Can Run Forest Topology* permission. For more information, see [Roles and Permissions in Security Management Platform](#).

Recovery Plans should be created based on the latest topology to ensure full preparedness in case of a disaster. We recommend that you manually rediscover topology when any domain controller or domain configuration is changed on-premises. However, if the last topology discovery finished more than 24 hours before a Backup Plan runs, an automatic discovery is performed.

If a domain controller is demoted or removed and a topology discovery has run, you need to remove that domain controller from any Backup Plans in which it is included; otherwise, the Backup Plan will fail.

i **NOTE:** IP addresses of domain controllers are collected during topology discovery and persistently stored in the database. For recovery methods that do not require an explicit Target Server IP, these pre-resolved IP addresses are used by the hybrid agent during recovery if DNS resolution by FQDN fails. We recommend regularly performing topology discovery to keep cached IP addresses up-to-date.

Using Secure LDAP (LDAPS) for Hybrid Agent Queries

When adding a forest, you can enable the **Use Secure LDAP (LDAPS) for Hybrid Agent Queries** toggle in the forest configuration to use Secure LDAP (LDAPS) queries when running topology discovery. If you already enabled Secure LDAP during installation of the hybrid agent (by entering \checkmark when prompted to enable SSL/TLS encryption for LDAP queries), the toggle is enabled by default.

After saving the forest, the **Use Secure LDAP (LDAPS) for Hybrid Agent Queries** setting is preserved for the forest and overrides any changes made to the hybrid agent, even if the hybrid agent is reinstalled or updated with a different LDAPS setting.

i **NOTE:** Topology discovery will fail if Secure LDAP queries are unsuccessful.

Installing Domain Controller Agents

You can deploy or upgrade a domain controller agent (DC agent) on one or more DCs within a forest using the Identity Recovery for Active Directory interface. Alternatively, you can manually install or upgrade the DC agent.

If an agent version 10.3.1.43711 or earlier is detected, it is considered to be installed by Recovery Manager for Active Directory Forest Edition/Disaster Recovery Edition (RMAD FE/DRE), and you cannot automatically install or update the agent from Identity Recovery for Active Directory. Upgrade RMAD to 10.3.2.46178 or later before proceeding to use Identity Recovery for Active Directory and RMAD in the same Active Directory environment.

For more information on DC agents, see [Hybrid Agents and Domain Controller Agents](#) in the *Recovery Considerations and Best Practices* section.

To install the domain controller agent

1. On the **Topology** page, select one or more DCs, and then select **DC Agent | Install Agent**.
2. In the **Install Agent** flyout, use either the credentials saved for the forest, or deselect the **Use credentials saved for the forest** checkbox and enter alternate credentials. These credentials must have domain administrator permissions.
3. Select **Install Agent**.

i | **NOTE:** If the installation fails, the **DC Agent Status** is set to **Offline**. Go to the **Tasks** page to view the reason for failure.

After successful installation or upgrade, the **DC Agent Status** displays **Online**. You can hover over the status icon to see the installed agent version.

Manual installation

To download the latest available version of the DC agent, first prepare or download an agent installer package.

1. On the **Topology** page, select **DC Agent | Download Agent**. If the agent package is expired or does not exist, a task is generated to prepare the installer package. When the task is complete, a download link is available in the details of the Prepare Agent Installer task on the **Tasks** page. The download link is valid for 30 minutes after it is generated. Alternatively, after the package is prepared, you can select **DC Agent | Download Agent** again to download the package directly from the **Topology** page.
2. Copy the package to the machine and run RecoveryAgent64.exe to install or upgrade the DC agent.

After the DC agent installation successfully completes, the Quest Forest Recovery Service is installed on the DC and runs as Local System.

Once the agents have been installed on all relevant DCs, you can now create a Backup Plan for the forest.

Backup Plans and Backups

Identity Recovery for Active Directory is designed to scale efficiently in large, multi-domain environments. This solution provides excellent performance, creates backups for multiple computers in parallel, and is easily scalable to service additional domain controllers. Administrators can logically group domain controllers based on roles, location, or other criteria for easier management by creating different Backup Plans.

This product also uses domain controller agents to streamline backup creation and application processes. This agent-based approach enhances scalability and reduces network overhead by compressing data before transmission and performing parallel backups for multiple domain controllers.

The **Backup** tab is where you can create and view Backup Plans and backups for each forest.

NOTE: It is highly recommended that you visit the [Backup Considerations and Best Practices](#) section in the *Before You Start* chapter before you begin to create Backup Plans.

In this topic:

- [Backup Plans](#)
- [Backups](#)

Backup Plans

Identity Recovery for Active Directory enables you to create backups of Active Directory components, including the database, on domain controllers. You can back up any domain controller on your network, and the backup process can be scheduled to run regularly without disrupting normal operations.

On the **Backup** tab, the **Backup Plans** table allows you to create and configure a Backup Plan to back up one or more domain controllers within the Active Directory forest.

In this section:

- [Creating and Editing Backup Plans](#)

Backup Plans shows a list of all Backup Plans within a forest. For each Backup Plan, you can view:

- The unique name for each Backup Plan.
- If a schedule for the Backup Plan is enabled or disabled.
- The date and time of the next scheduled backup of the Backup Plan (if enabled).

- The date and time the backup was last run.
- The most recent status of a backup session run for a Backup Plan:
 - **Completed** - all domain controllers within the Backup Plan are successfully backed up.
 - **In Progress** - the backup is currently running.
 - **Failed** - one or more domain controllers failed to backup. Go to the **Tasks** tab for more details.
 - An empty status indicates that a backup has not been run yet.

You can perform the following actions on Backup Plans:

- View, create, and edit Backup Plans.
- Use the **Back Up Now** button to initiate an immediate backup of a selected Backup Plan.
- Remove a Backup Plan.

Creating and Editing Backup Plans

Identity Recovery for Active Directory allows users to automate backup creation, reducing network load and saving time. Once Backup Plans are created and scheduled, the product automates the backup process, requiring no further manual intervention.

To create or edit a Backup Plan

1. On the **Backup** tab, select **Backup Plans**.
2. To create a Backup Plan, select **Create**. To edit a Backup Plan, select the checkbox next to the Backup Plan you want to edit, then select **Edit**. Alternatively, select the Backup Plan name to open the plan, then select **Edit**.
3. Enter a unique name for the Backup Plan, or use the default name.
4. If you want to schedule to run backups at regular intervals, turn on the **Enable Schedule** toggle, then set the recurrence by choosing the frequency (daily, weekly, or monthly) and the day and time.

i NOTE: The time shown is in the UTC (Coordinated Universal Time) time zone. The corresponding local time is displayed below the UTC time.

- a. For daily scheduling, select **Day** from the **Every** dropdown menu. Set the time in the 12-hour format using the dropdown menus.
 - b. For weekly scheduling, select **Week** from the **Every** dropdown menu. Select one or more days of the week from the **On Days** dropdown menu, then set the time in the 12-hour format using the dropdown menus.
 - c. For monthly scheduling, select **Month** from the **Every** dropdown menu. Select one or more days of the month from the **On Days** dropdown menu, then set the time in the 12-hour format using the dropdown menus.
5. Click **Select Domain Controllers**.
 6. In the **Select Domain Controllers** full-page flyout, select the domain controllers you want to back up. To apply your changes, click **Save**.

i TIP: Use the **Filters** button to filter the list of domain controllers by one or more domains, sites, DC agent statuses, or Backup Plans.

i NOTES:

- The domain controller agent must be installed on the domain controller in order to run backups. If you wish to backup a domain controller that has an Offline or Not Supported status, install or upgrade the agent on that machine before running a backup.
- Consider [recovery strategies](#) before selecting which domain controllers to backup.
- If you see missing or additional domain controllers, or an incorrect domain controller type, run a discovery on the **Topology** page to refresh the topology, and then update the Backup Plan.
- A maximum of ten domain controllers per domain can be backed up within the forest. If a domain controller is added to multiple Backup Plans, each instance counts towards the maximum.

7. Save the Backup Plan.

Backups

On the **Backup** tab, the **Backups** table allows you to view the backups generated from your Backup Plans.

i **NOTE:** Backups are stored for 180 days. After this period, the backups are automatically deleted.

For each backup, you can view:

- The name of the Backup Plan from which the backup was created.

i **NOTE:** If you delete a Backup Plan, the backups are still visible in the Backups table and display *Backup plan has been deleted* in the Backup Plan name.

- The domain from which the backup was created.
- The domain controller from which the backup was created.
- The date and time when the backup was created.
- The schedule type:
 - **Manual** – The Backup Plan was run by selecting **Back Up Now** on the **Backup Plans** page.
 - **Scheduled** – The Backup Plan was run according to a configured schedule.
- The size of the backup.

i **NOTE: Using Filters**

You can select to filter the list of backups by Backup Plan, domain, domain controller, schedule type, or the date created.

Once backups have been created, you can then create a Recovery Plan for your forest.

Recovery

The **Recovery** tab allows you to create, manage, and run a Recovery Plan for the restore of an Active Directory forest on-premises, including all domains and domain controllers. Identity Recovery for Active Directory provides centralized remote management for domain controller recovery within your Active Directory forest. This product also allows you to centrally restore multiple domain controllers within a forest simultaneously, streamlining the recovery process and saving time compared to manual restoration of individual domain controllers. It is recommended to create and verify Recovery Plans prior to a disaster to ensure they are configured correctly. You can create multiple Recovery Plans to support multiple configurations. We recommend that you review the [Recovery Strategies Overview](#) section in *Recovery Considerations and Best Practices*.

A Recovery Plan allows you to manage the process for recovering the entire Active Directory forest. Each Recovery Plan includes a list of domain controllers to be restored, along with their associated configurations. Recovery Plans enable you to prepare and run targeted recoveries for your Active Directory forest using either the latest available backups or a selected date to recover from. By creating and reviewing the plan, you can gain a comprehensive understanding of the recovery configurations for each domain controller, enabling you to fine-tune the process as needed.

i **IMPORTANT:** After recovery, the Active Directory forest will lose any data that was created or modified after the date of the backup used for recovery. As a result, required changes will need to be performed manually. This includes:

- Objects (such as users and computers) that were added or removed
- Updates to existing objects
- Changes to either the configuration partition or the schema partition in Active Directory (such as schema changes)

Additionally, any software applications that were running on the domain controllers will need to be reinstalled after recovery.

The product also enables selective recovery of specific domains within an Active Directory forest. This allows you to restore individual domains, rather than the entire forest, which can be useful when dealing with compromised or unwanted data.

i **NOTE:** It is highly recommended you make sure that the dangerous or unwanted data is not replicated to other domains in the forest.

In this chapter:

- [Creating Recovery Plans](#)
- [Recovery Page Tiles](#)
- [Configuring Recovery Plans](#)
- [Working with Recovery Plans](#)

Creating Recovery Plans

To create a Recovery Plan

1. On the **Recovery** tab, select **Create Recovery Plan**.
2. Enter a unique name for the Recovery Plan or use the default name.
3. Select one of the following options, depending on your recovery scenario. This selection determines the initial configuration of the Recovery Plan. You can change your selection later on the **Settings** tab of the Recovery Plan configuration.
 - **Prepare for a future recovery** – Select this option if you intend to run the Recovery Plan in the future. This option configures the plan to use the latest discovered topology at the time the plan was created and the latest available backups.

i **NOTE:** If the Active Directory forest topology in your environment changes after the plan is created, the product automatically discovers the new topology when a Backup Plan runs. In the Recovery Plan configuration, **Recover From** in the summary panel displays a badge labeled **Latest Backups with Outdated Topology**. You can then update the Recovery Plan to the latest topology on the **Settings** tab. For more information, see [Recovery Using Latest Backups](#).
 - **Run recovery using a specific date** – Select this option if you want to run a recovery based on a specific date and time. This option configures the plan to use the most recent forest topology and backups on or before the selected date and time.

i **NOTE:** This option uses the latest backup for each domain controller within a 14-day age range on or before the target date. You can modify the selected date and the backup age range later in the Recovery Plan configuration if needed. For more information, see [Recovery Using Specific Date](#).
4. If you selected the **Run recovery using a specific date** option, pick a date and time from the calendar. Dates highlighted in green indicate that a topology change was discovered on that day. After making your selection, select **Apply**.
5. Review the summary in the **Recovery Plan Overview** table.
 - **Forest Topology Discovery Date** – The date of the forest topology that will be used in the plan. If you selected a specific date in the calendar, this matches the green-highlighted date closest to and before the selected date.
 - **Backup Selection Criteria** – Displays the backup selection that will be used in the plan (**Latest available backups** for future recovery or **Latest backups on or before the selected date** for a specific date).
6. Select **Create**.

A new tile is displayed for the Recovery Plan as the first tile on the top left of the **Recovery** page. For more information, see [Recovery Page Tiles](#).

Recovery Page Tiles

On the **Recovery** tab, the **Recovery** page provides a visual summary of all Recovery Plans created in the forest. When you create Recovery Plans, a tile for each plan is displayed on the **Recovery** page. The tiles provide an at-a-glance overview of the current state of each Recovery Plan and allows you to manage them from one place.

After you create a Recovery Plan, on the **Recovery** page, a new tile is displayed showing the default plan name, status (in this case, **New**), a summary of its scope, and links that allows you to take quick actions. After you configure the Recovery Plan (see [Configuring Recovery Plans](#)), you can verify the plan (see [Verifying Recovery Plans](#)) and then start recovery (see [Performing Recovery](#)). The tile then updates to reflect the progress or completed actions of verification and recovery tasks, including any errors.

Status

This section displays recent activity and the current state of your Recovery Plan. Selecting a status entry on the tile opens the **Tasks** page filtered by the specific Task ID. The possible status entries are as follows:

- **New** – The Recovery Plan has been created but not yet run.
- Verification
 - **Verify Recovery Plan in Progress** – The verification of the Recovery Plan is in progress.
 - **Last Successful Verify Recovery Plan** – The time of the last successful verification of the Recovery Plan.
 - **Verify Recovery Plan Canceling** – The verification of the Recovery Plan is in the process of being canceled.
 - **Verify Recovery Plan Canceled** – The verification of the Recovery Plan has been canceled.
 - **Verify Recovery Plan Failed** – The time of the last failed verification of the Recovery Plan.
- Recovery
 - **Recovery in Progress** – The Recovery Plan is in the process of recovery.
 - **Last Successful Recovery** – The time of the last successful recovery.
 - **Recovery Canceling** – The recovery process is being canceled.
 - **Recovery Canceled** – The recovery process has been successfully canceled.
 - **Recovery Failed** – The time of the last failed recovery.

Summary

This section displays an overview of the scope of your Recovery Plan.

- **Recover from** – Indicates which forest topology and backups the Recovery Plan uses, based on the recovery scenario you chose when creating the plan.

- If you chose **Prepare for a future recovery**, this displays **Latest**, indicating that the latest discovered topology at the time the plan was created and the latest backups are used.

i | **NOTE:** If a newer topology is available, this displays **Latest Backups with Outdated Topology**.

- If you chose **Run recovery using a specific date**, this displays the selected date and time. The forest topology and backups closest to and before your selected date are used.

i | **NOTE:** You can change the selected option on the **Settings** tab of the Recovery Plan configuration.

- **Domains to recover** – The number of domains set to be recovered out of the total number of domains in the forest.
- **Domain controllers to recover** – The number of domain controllers in the domain set to be recovered out of the total number of domain controllers.

Action Links

You can use the links on the bottom of the card to perform the following actions:

- **Open** – View or edit the Recovery Plan configuration and perform verification and recovery tasks. For more information, see [Configuring Recovery Plans](#) and [Working with Recovery Plans](#).
- **View Progress** – View the progress of ongoing or the last completed verification or recovery task. For more information, see [Recovery Plan Progress](#).
- **Remove** – Delete the Recovery Plan.

Configuring Recovery Plans

This section guides you through the process of configuring a Recovery Plan.

- **Configuring Settings.** On the **Settings** tab, enter a name for the plan, enable simulation mode (optional), and select how backups and the forest topology are chosen for recovery.
- **Configuring Domains.** On the **Domains** tab, configure the domains in the forest by selecting a recovery method for each domain. Depending on the chosen recovery method, you may need to specify credentials and DNS configurations.
- **Configuring Domain Controllers.** On the **Domain Controllers** tab, configure the domain controllers in the forest by selecting a recovery method for each domain controller. Depending on the chosen recovery method, you may need to specify credentials, target server, backup selection, and other options.

i | **NOTE:** If you edit any details in the Recovery Plan configuration (on the **Settings**, **Domains**, or **Domain Controllers** tab), the verification or recovery progress view will no longer be available until a new task is started. For more information, see [Recovery Plan Progress](#).

Configuring Settings

After creating a Recovery Plan (see [Creating Recovery Plans](#)), on the **Settings** tab, you can view and change the basic plan details, such as the name and whether or not to use simulation mode, and select how the forest topology and backups are chosen for recovery.

To configure settings

i **NOTE:** If you edit the settings, this clears the **Status** column in the progress view and removes access to the list of operations performed during the last verification or recovery. For more information, see [Recovery Plan Progress](#).

1. From the **Recovery** tab, on the tile for the Recovery Plan you want to edit, select **Open**.
2. On the **Settings** tab, enter a unique name for the Recovery Plan or use the default name.
3. To enable simulation mode, turn on the **Enable Simulation Mode** toggle. This mode allows you to run simulated verification or recovery operations using topology information from the connected Active Directory forest and its backups. It completes verification and recovery without using target machines, allowing you to test the workflow of Recovery Plans and identify issues without risk to the data or forest.
4. If needed, modify the recovery option you selected when creating the Recovery Plan. This option determines the topology used for the Recovery Plan and backups used during verification and recovery.
 - **Keep the plan up to date by using the latest backups** – Selected if you chose **Prepare for a future recovery** when you created the Recovery Plan. This option uses the forest topology from the time the plan was created or last updated, and automatically selects the latest available backups for domain controllers set to automatic backup selection. For detailed steps, see [Recovery Using Latest Backups](#).
 - **Use a specific date to recover from** – Selected if you chose **Run recovery using a specific date** when you created the Recovery Plan. This option uses the forest topology closest to and before the date and time you specify, and selects the latest backups before that date and time for domain controllers set to automatic backup selection. For detailed steps, see [Recovery Using Specific Date](#).

Recovery Using Latest Backups

To configure the Recovery Plan for latest backups

1. On the **Settings** tab of the Recovery Plan configuration, select **Keep the plan up to date by using the latest backups**.

i **NOTE:** If the Recovery Plan was previously configured to use a specific date, switching to this option updates the plan to use the latest available forest topology and the latest backups for domain controllers that use automatic backup selection.

2. From the dropdown, select the maximum age range of backups allowed in the Recovery Plan (the default is 14 days). This automatically selects the most recent backup within that range for each domain controller that is set to use automatic backup selection.

i **NOTES:**

- This selection applies only to domain controllers configured to be recovered.
 - Domain controllers with manually selected backups are not switched to automatic backup selection.
 - If there is no backup for a domain controller that meets the criteria, a backup must be manually selected; otherwise, the restore will fail.
3. If a newer forest topology is available, a summary table is displayed that allows you to compare the current topology date to the date of the latest available topology. To update the Recovery Plan with the latest available topology, select **Update Topology to Latest**. The changes apply after you select **Save**.
 4. Select **Save**.

Recovery Using Specific Date

To configure the Recovery Plan for a specific target date

1. On the **Settings** tab of the Recovery Plan configuration, select **Use a specific date to recover from**.
2. From the dropdown, select the maximum age range of backups allowed in the Recovery Plan (the default is 14 days). This automatically selects the latest backup within that range on or before the target date for each domain controller that is set to use automatic backup selection.

i **NOTES:**

- This selection applies only to domain controllers configured to be recovered.
 - Domain controllers with manually selected backups are not switched to automatic backup selection.
 - If there is no backup for a domain controller that meets the criteria, a backup must be manually selected; otherwise, the restore will fail.
3. To specify the date to recover from, select **Select Date** and pick a date and time from the calendar. Dates highlighted in green indicate that a topology change was discovered on that day. After making your selection, select **Apply**.
 4. In the summary table, review the values based on your selected date:
 - **Recover From or Before** – The date and time you selected in the calendar.
 - **Forest Discovery Date** – The discovery date of the forest topology used in the plan. This is the topology date closest to and before the selected date.
 - **Latest Backup within Range** – The date of the latest backup used in the plan. This is the most recent backup within the specified age range before the selected date.
 5. Select **Save**.

Configuring Domains

After specifying details on the **Settings** tab, you need to configure the domains within the forest. The table on the **Domains** tab allows you to view and edit the configurations for each domain, including the recovery method, the credentials, and DNS configurations (if applicable).

The following information is displayed for each domain:

- **Domain** – The fully qualified domain name (FQDN) of the domain.
- **Domain Recovery Method** – The recovery method selected for the domain. To change the recovery method, double-click the cell, select a new value from the dropdown, and select **Save**.
- **DC Backup Coverage** – The number of domain controllers (DCs) that have backups matching the selected backup criteria out of the total number of DCs in the domain. If needed, adjust your backup selection or create additional backups.
- **Credentials** – Indicates whether or not credentials are provided (or not required).
- **DNS Configuration** – Indicates the method for selecting a DNS server (**Automatically Selected** or **Manually Selected**). If the recovery method does not require DNS configuration, **Not Applicable** is displayed.

i **NOTE: Using Filters**

- You can select to filter the list of domains by domain recovery method, credentials (whether provided or not), or DNS configuration (selection method).
- Use the **Domains with Issues** filter option to display only domains that have warnings or errors.

To configure domains

On the **Domains** tab, select the name of the domain you want to configure. The **Domain Configuration** page is displayed.

i **NOTE:** If you edit the domain configurations, this clears the **Status** column in the progress view and removes access to the list of operations performed during the last run verification or recovery. For more information, see [Recovery Plan Progress](#).

For each domain, you need to specify a recovery method. When you create a Recovery Plan, the default recovery method **Recover Domain** is set for the domain. You can change the recovery method for the domain to one of the other available methods. In some cases, the recovery method you select for the domain affects the recovery method that is available for the domain controller. Click the link below to go to the recovery method you want to select or configure and follow the steps in that section.

- [Recover Domain](#)
- [Ignore Healthy Domain](#)
- [Delete Domain](#)

i **NOTES:**

- Before selecting a recovery method, it is highly recommended that you read [Recovery Methods](#) in the *Recovery Considerations and Best Practices* section.
- The **Ignore Healthy Domain** and **Delete Domain** options are not supported at the same time; you cannot include both options in a Recovery Plan.

Recover Domain

This method enables the restoration of the entire forest or specific domains within the forest by recovering one or more domain controllers from a backup. This is the default recovery method assigned to all domains when a new Recovery Plan is created. At least one domain in the Recovery Plan needs to be set to be recovered, and at least one domain controller in the domain must be restored from a backup (using the **Restore to Clean OS** recovery method).

i **NOTE:** If the recovery method for the domain is set to **Recover Domain**, the **Restore to Clean OS** recovery method is set by default for all domain controllers in the domain.

If the **Recover Domain** method is selected, perform the following steps:

1. Specify or change the server access credentials. To learn more about each credential type, see [Server Access Credentials](#) in the *Recovery Considerations and Best Practices* section. When credentials are specified at the domain level, they are applied to all domain controllers within that domain. If needed, you can change the credentials for individual domain controllers from the **Domain Controllers** tab.
 - **Domain Username** – An Active Directory Domain Admin account that existed when the backup was created.
 - **Domain User Password** – The password for the domain.
 - **Local Username** – The username for the local account that has Local Administrator rights on the target.
 - **Local User Password** – The password for the local account.
 - **DSRM Administrator** – The username for the DSRM administrator.
 - **DSRM Administrator Password** – The password that the DSRM password will be set to when the target machine is promoted to the domain controller.
 - **Confirm DSRM Administrator Password** – Confirm the DSRM administrator password.
2. You can change the DNS server configuration. It is highly recommended that you read [DNS Configuration](#) in the *Recovery Considerations and Best Practices* section.
 - **Select DNS server automatically** – Automatically selects and assigns a DNS server for each domain controller in the domain. This option is selected by default.
 - **Use preferred DNS server(s)** – Specify the DNS servers manually by entering one or more IP addresses, each separated by a semicolon.
3. Select **Save**.

i **NOTE:** For the **Recover Domain** method, you need to specify all credentials here or in the domain controller configuration.

Ignore Healthy Domain

This method excludes the healthy domain from recovery while keeping it intact in the forest. This option performs configuration changes on domain controllers within the domain to ensure connectivity to the recovered domains.

i **NOTE:** If the recovery method for the domain is set to **Ignore Healthy Domain**, the **Adjust to Active Directory Changes** recovery method is set for all domain controllers and cannot be modified.

If the **Ignore Healthy Domain** method is selected, perform the following steps:

1. You can change the domain credentials. When credentials are specified at the domain level, they are applied to all domain controllers within that domain. If needed, you can change the credentials for individual domain controllers from the **Domain Controllers** tab.
 - **Domain Username** – An Active Directory Domain Admin account that existed when the backup was created.
 - **Domain User Password** – The password for the domain.

i **NOTE:** For the **Ignore Healthy Domain** method, you need to specify domain credentials here or in the domain controller configuration.

2. Select **Save**.

Delete Domain

This method removes the domain from the forest by cleaning up its metadata from all restored and existing domains. This option cannot be used on the forest root domain.

i | **NOTE:** If the recovery method for the domain is set to **Delete Domain**, the **Remove DC** recovery method is set for all domain controllers and cannot be modified.

After selecting the **Delete Domain** recovery method, select **Save**.

Configuring Domain Controllers

After configuring the domains in your Recovery Plan, you need to configure the domain controllers within the forest. The table on the **Domain Controllers** tab allows you to view and edit the configurations for each domain controller, such as the recovery method, target server, backup selection, and credentials (if applicable).

The following information is displayed for each domain controller:

- **Domain Controller** – The FQDN of the domain controller.
- **Domain** – The fully qualified domain name (FQDN) of the domain.
- **Type** – The domain controller can be of the following type:
 - **GC** - Global Catalog
 - **RODC** - Read-only domain controller
 - **DC** - Domain controller
- **FSMO Role** – The FSMO (Flexible Single Master Operation) roles assigned to the domain controller, displayed as a badge for each role. The FSMO roles are as follows:
 - PDC emulator
 - RID master
 - Infrastructure master
 - Schema master
 - Domain naming master
- **DC Recovery Method** – The recovery method selected for the domain controller. To change the recovery method, double-click a cell, select a new value from the dropdown, and select **Save**.

i | **NOTE:** You can only change the recovery method for domain controllers in domains where the **Recover Domain** method is selected.
- **Target** – The target server IP address. To change the IP address, double-click a cell, enter a valid IP address, and select **Save**.
- **Target Agent Status** – The status of the domain controller agent installed on the target machine. This status displays the agent's connectivity and indicates whether its version is supported for verification and recovery tasks. By hovering over the status icon, you can see the currently installed agent version and, if applicable, the minimum supported version and the latest available version. The agent statuses are as follows:
 - **Online** – The domain controller agent is online and the latest version is installed.
 - **Outdated** – The domain controller agent is online and running a supported but older version. Verification and recovery tasks will run, but an agent update to the latest version is strongly recommended.

- **Not Supported** – The domain controller agent is installed and online, but the version is no longer supported and requires an update. The agent will be automatically updated to the latest version when you run verification or recovery.
- **Offline** – The domain controller agent cannot be reached or is not installed.
- **Installing** – The domain controller agent is being installed.
- **Refreshing** – The status of the domain controller agent is being updated.
- **Unknown** – The status of the domain controller agent has not yet been checked, or the target server IP has been changed. To get the latest domain controller agent status, select the checkboxes for one or more domain controllers, then select **Refresh Agent Status**.

i | **NOTE:** After verification or recovery, you need to manually refresh the agent status.

- (Empty) – Indicates that the recovery method selected for the domain controller does not require an agent to be installed on the target, or that the Target Server IP has not been provided for recovery methods that require it.
- **Selected Backup** – The date and time that the selected backup was created.

i | **NOTE:** If there is no backup for the domain controller that meets the backup criteria, **No Backup Available** is displayed in this column.

i | **NOTE: Using Filters**

- You can select to filter the list of domain controllers by domain, type, FSMO role, domain controller recovery method, or target agent status.
- Use the **DCs with Issues** filter option to display only domain controllers that have warnings or errors.

To configure domain controllers

On the **Domain Controllers** tab, select the name of the domain controller you want to configure. The **DC Configuration** page is displayed.

i | **NOTE:** If you edit the domain controller configurations, this clears the **Status** column and removes access to the list of operations performed during the last run verification or recovery. For more information, see [Recovery Plan Progress](#).

For each domain controller, you need to specify a recovery method. In some cases, the recovery method for the domain controller is set by default depending on the recovery method selected for the domain. You can change the recovery method of the domain controller to one of the following options. Click the link below to go to the recovery method you want to select or configure and follow the steps in that section.

- [Restore to Clean OS](#)
- [Install Active Directory](#)
- [Remove DC](#)
- [Adjust to Active Directory Changes](#)

i | **NOTE:** Before selecting a recovery method, it is highly recommended that you read [Recovery Methods](#) in the *Recovery Considerations and Best Practices* section.

Restore to Clean OS

This recovery method restores the domain controller from a backup onto a freshly installed Windows machine.

i **NOTE:** If the recovery method for the domain is set to **Recover Domain**, the **Restore to Clean OS** recovery method is set by default for the domain controller.

If the **Restore to Clean OS** recovery method is selected, perform the following steps:

1. The **Target Server** field is empty by default. You must specify a valid Target Server IP for a successful recovery with the **Restore to Clean OS** method.
2. Under **Backup Selection**, specify whether you want backups to be automatically selected or manually selected.
 - **Automatic** – By default, a backup is selected automatically according to the backup selection criteria configured for the Recovery Plan.

i **NOTE:** If a backup that meets the backup selection criteria does not exist, you can proceed to save the domain controller configuration. However, verification and recovery will not start if a backup is not available for the domain controller. Once a valid backup is available, it will be automatically selected.

- **Manual** – To manually select a backup for the domain controller, click **Select Backup**. In the **Select Backup** flyout, select a backup to be used for recovery. You can use the **Filters** button to filter the list of domain controllers by Backup Plans, the schedule type, or the date created.

i **NOTE:** If no backups are available for the domain controller, you cannot use the **Manual** option.

3. Specify or change the server access credentials. By default, if server access credentials are specified in the domain configuration, domain-level credentials are used for all domain controllers within the domain and are marked with a badge labeled **Inherited credentials**. If the domain controller requires different credentials to those specified in the domain configuration, you can specify one or more credentials for that domain controller to replace the inherited credentials. For descriptions of each credential type, see [Server Access Credentials](#) in the *Recovery Considerations and Best Practices* section.

i **NOTE:** For the **Restore to Clean OS** recovery method, you need to specify all credentials here or in the domain configuration.

4. Select **Save**.

Install Active Directory

This recovery method installs Active Directory Domain Services on the computer and promotes it to a domain controller. After the recovery, the domain controller replicates Active Directory data from domain controllers restored from backups.

To reduce replication traffic, you can use the **Enable Install from Media** (IFM) option. The IFM option pre-populates Active Directory and Sysvol on the target domain controller with data from a backup for another domain controller in the same domain. This option is selected by default if there are backups available for the domain.

If the **Install Active Directory** recovery method is selected, perform the following steps:

1. The **Target Server** field is empty by default. You must specify a valid Target Server IP for a successful recovery with the **Install Active Directory** method.
2. Under **Backup Selection**, use the **Enable Install From Media** checkbox to turn on or off the option.

3. If the **Enable Install From Media** option is selected, specify whether you want backups to be automatically selected or manually selected.
 - **Automatic** – Selected by default if IFM is enabled. This option automatically selects the most recent backup for a domain controller in the same domain that meets the backup selection criteria configured for the Recovery Plan.

i | **NOTE:** If a backup that meets the backup selection criteria does not exist, you can proceed to save the domain controller configuration. However, verification and recovery will not start if a backup is not available for the domain controller. Once a valid backup is available, it will be automatically selected.

 - **Manual** – To manually select a backup, click **Select Backup**. In the **Select Backup** flyout, select a backup for the domain to use for recovery. You can use the **Filters** button to filter the list of domain controllers by Backup Plans, domain controllers, the schedule type, or the date created.

i | **NOTE:** If no backups are available for the domain controller, you cannot use the **Manual** option.

 - 4. Under **Domain Controller Options**, select one or more server roles for the domain controller:
 - **Configure as a global catalog server** – Use this option if you need to configure the global catalog on the domain controller during Active Directory Domain Services® installation. This option will be selected by default if the original domain controller was a global catalog. Microsoft recommends that all domain controllers provide DNS and global catalog services for high availability in distributed environments. For more information, click [here](#).
 - **Install DNS server on the domain controller** – Use this option to install the DNS server during the **Install Windows features** step. This option is enabled by default. - 5. Specify or change the server access credentials. By default, if server access credentials are specified in the domain configuration, domain-level credentials are used for all domain controllers within the domain and are marked with a badge labeled **Inherited credentials**. If the domain controller requires different credentials to those specified in the domain configuration, you can specify one or more credentials for that domain controller to replace the inherited credentials. For descriptions of each credential type, see [Server Access Credentials](#) in the *Recovery Considerations and Best Practices* section.
- i** | **NOTE:** For the **Install from Active Directory** recovery method, you need to specify all credentials here or in the domain configuration.
6. Select **Save**.

Remove DC

This recovery method isolates the domain controller from other domain controllers and removes it from the domain. Use this method if the domain controller is inaccessible or you do not want to recover the domain controller due to failures.

i | **NOTE:** If the recovery method for the domain is set to **Delete Domain**, the **Remove DC** recovery method is set for the domain controller and cannot be modified.

After selecting the **Remove DC** recovery method, select **Save**.

Adjust to Active Directory Changes

This recovery method adjusts the DNS and IP configuration of the existing domain controller to ensure connectivity to the recovered domains.

i **NOTE:** If the recovery method for the domain is set to **Ignore Healthy Domain**, the **Adjust to Active Directory Changes** recovery method is set for the domain controller and cannot be modified.

If the **Adjust to Active Directory** recovery method is set, perform the following steps:

1. Specify valid domain credentials. By default, if domain credentials are specified in the domain configuration, domain-level credentials are used for all domain controllers within the domain and are marked with a badge labeled **Inherited credentials**. If the domain controller requires different credentials to those specified in the domain configuration, you can specify one or more credentials for that domain controller to replace the inherited credentials.
2. Select **Save**.

Handling Errors and Warnings

When you open a Recovery Plan and a single error or warning exists, a notification banner is displayed at the top of the page. If multiple errors or warnings exist, the banner indicates the number of issues that need to be resolved.

To handle multiple Recovery Plan errors

1. On the notification banner, select the **View Details** link.
2. In the **Recovery Plan Validation** flyout, check the errors and warnings related to domain or domain controller configurations. Use the navigation link under each warning or error to open the relevant tab.

i **NOTE:** If the error or warning is on the **Domain Controllers** tab, you can hover over the warning icon next to the domain controller name in the **Domain Controller** column to view details of the warnings or errors.

3. Select the link for the relevant domain or domain controller and resolve the configuration issues.

Working with Recovery Plans

When working with Recovery Plans, the panel at the top of the configuration page allows you to perform specific actions related to recovery and provides you with relevant information at a glance.

You can perform the following actions using the toolbar in the top panel:

- **Verify Plan** – Checks that the configurations for the domain controllers within the Recovery are valid and can be used for forest or domain recovery. Verification details will be displayed in the Verification Progress view of the Recovery Plan configuration, while the progress of individual domain controllers will be displayed on the Operations page. For more information, see [Verifying Recovery Plans](#) and [Domain Controller Operations](#).
- **Start Recovery** – Begin running the recovery. Recovery details will be displayed in the Recovery Progress view of the Recovery Plan configuration, while the progress of individual domain controllers will be displayed on the Operations page. For more information, see [Performing Recovery](#) and [Domain Controller Operations](#).
- **Cancel** – Stops the verification or recovery task.

i **NOTE:** Individual domain controllers cannot be canceled from this page.

CAUTION: Canceling a recovery operation may result in a corrupt forest.

- **View Progress** – Opens the progress view, where you can monitor the progress of verification and recovery tasks running for the Recovery Plan. For more information, see [Recovery Plan Progress](#).

NOTE: While verification or recovery tasks are running, you can view the Recovery Plan configuration, but you cannot make changes.

Below the toolbar, you can see a summary of the current or latest completed verification or recovery task performed on the forest, including:

- The overall latest status of the Recovery Plan, displayed underneath the forest FQDN. This indicates the status of an ongoing or completed task, including any warnings, errors, or user actions. If configuration errors exist in the Recovery Plan, the status will show **Not Ready**.
- **Recover From** – Corresponds to your selected option on the **Settings** tab:
 - If you selected to use the latest backups, this shows **Latest**.
 - If you selected to use the latest backups but a newer topology is available, this shows **Latest Backups with Outdated Topology**. To update the Recovery Plan to the latest available topology, on the **Settings** tab, select **Update Topology to Latest**.
 - If you selected to recover based on a specific date, this shows the date and time you selected to recover from.
- **Overall Time** – The elapsed time for the running or completed task.
- The number of domain controllers that have the following statuses:
 - **Failed**
 - **Completed with Warnings**
 - **Completed**
 - **Canceled**
 - **In Progress**

Verifying Recovery Plans

To minimize downtime during Active Directory forest recovery, it is recommended to regularly verify your Recovery Plan configurations. The following is performed during Recovery Plan verification:

NOTE: If the target machine is not provided, the following steps will be completed against the source domain controller.

- Check connectivity to the hybrid agent and domain controller agents.
- Install or upgrade the domain controller agent on a target machine when the Target Server IP has been provided.
- Check that a backup is available that meets the backup selection criteria for each domain controller with a specified recovery method.
- Ensure that the target server has correct OS, drive letters and enough disk space.
- Verify access to the backup from the domain controller agents.

If you do not verify a Recovery Plan, the above steps will take place during recovery (with the exception that the Target Server IP is required for a successful recovery).

To verify a Recovery Plan

1. From the **Recovery** page, open the Recovery Plan you want to verify.
2. Select **Verify Plan**.

All domain controllers that are set to be recovered in the Recovery Plan will be verified. To view the current status of the verification of each domain controller, select **View Progress**. For more information, see [Recovery Plan Progress](#).

Performing Recovery

Once verification of a Recovery Plan is completed successfully, you can proceed with the recovery of your Active Directory forest or selected domains. For more information about verification, see [Verifying Recovery Plans](#).

NOTE: It is highly recommended that you visit the [Recovery Considerations and Best Practices](#) section in the *Before You Start* chapter before you recover the forest or selected domains.

To begin recovery

1. From the **Recovery** page, open the Recovery Plan you want to use for recovery.
2. Select **Start Recovery**. Select the corresponding checkboxes to confirm that the hybrid machine is configured with a DNS server, and that you want to begin recovery immediately. Then select **Start Recovery**.

All domain controllers in the Recovery Plan that are set to be recovered will be recovered. To view the current status of the recovery of each domain controller, select **View Progress** in the toolbar, then navigate to the **Status** column. For more information, see [Recovery Plan Progress](#).

Recovery Plan Progress

You can monitor the progress of verification and recovery tasks running for a Recovery Plan using the progress view. Progress information is displayed when a verification and recovery task is in progress or has recently been completed.

i **NOTE:** If you edit any details in the Recovery Plan configuration (on the **General**, **Domains**, or **Domain Controllers** tab), the verification or recovery progress will no longer be available until a new task is started.

To access the progress view of a Recovery Plan

- a. From the **Recovery** page, navigate to the tile for the Recovery Plan and select **View Progress**.
- b. On the Configuration page for the Recovery Plan, select **View Progress** in the toolbar.

For each domain controller in the Recovery Plan, the following information related to task progress is displayed in the table:



NOTE: This topic only documents fields and other elements on this page that either are not self-explanatory or require additional information.

- **Status** – The status of the ongoing or completed task on the domain controller. The possible status entries include the following:
 - Verification
 - **Starting DC Verification** – The verification operation is in the process of starting.
 - **DC Verification in Progress** – The verification operation is in progress.
 - **DC Verification Completed** – The verification operation has been completed.
 - **Verification Completed with Warnings** – The verification operation has been completed, but one or more operations have warnings. For more information, see [Domain Controller Operations](#).
 - **DC Verification Failed** – The verification operation has failed.
 - **DC Verification Canceling** – The verification operation is in the process of being canceled.
 - **DC Verification Canceled** – The verification process has been canceled.
 - Recovery
 - **Starting DC Recovery** – The recovery operation is in the process of starting.
 - **DC Recovery in Progress** – The recovery operation is in progress.
 - **DC Recovery Completed** – The recovery operation has been completed.
 - **DC Recovery Completed with Warnings** – The recovery operation has been completed, but one or more operations have warnings. For more information, see [Domain Controller Operations](#).
 - **DC Recovery Failed** – The recovery operation has failed.
 - **DC Recovery Canceling** – The recovery operation is in the process of being canceled.
 - **DC Recovery Canceled** – The recovery process has been canceled.
 - **Waiting For Other DCs** – The operation is waiting for other domain controllers to finish their operations.

By clicking the status entry in the **Status** column, you can open the domain controller Operations page. This page lists all operations performed on the domain controller during verification or recovery, including any configuration errors or warnings. For more information, see [Domain Controller Operations](#).

- **Current Operation** – The operation currently running or last run. If there are configuration errors or warnings, the operation during which the error occurred is displayed in this column.



NOTE: Using Filters

- You can select to filter the list by domain, domain recovery method, domain controller recovery method, or status.

Domain Controller Operations

By selecting the entry in the **Status** column of a domain controller in progress view, you can open the domain controller Operations page. This can only be accessed during or after verification or recovery.

i | **NOTE:** If the Recovery Plan configuration has been edited, the Recovery Plan summary and domain controller operations will be cleared. You can view the operations that took place during recovery on the **Events** page.

The Operations page details the operations performed on a domain controller when verifying a Recovery Plan or performing recovery.

Above the toolbar, you can see the progress of both the domain controller and the Recovery Plan.

- On the left side of the status bar, you can view the status of the domain controller, including the:
 - Progress of the verification or recovery
 - Number of errors and warnings
 - Number of canceled, completed, and pending operations

i | **NOTE:** Icons are displayed only for statuses that include one or more operations in that category.

- On the right side of the status bar, you can view the status of the Recovery Plan, including the:
 - Overall summary of the Recovery Plan
 - Overall time taken for the verification or recovery

You can view the following information for the domain controller on the Operations page:

- **Operations** – Selecting the link of an operation entry opens a flyout with a description of the operation, including details about any warnings or errors.
- **Elapsed Time** – The total duration the operation took to run.
- **Completion Date** – The date and time when the operation finished.

You can perform the following actions on the Operations page:

- **Skip and Continue** – Allows you to skip the current failed recovery step for the domain controller you selected and continue with the recovery of the domain controller. This action is recommended only if you have manually completed the failed recovery step on the domain controller.
- **Retry Last** – Allows you to rerun the failed recovery step on the domain controller you selected. This action is recommended when you manually fixed the issue that had caused the recovery step to fail.
- **Cancel** – Cancels the recovery or verification operation for the selected domain controller.

! | **CAUTION:** Canceling a recovery operation may result in a corrupt forest.

- **View Events** – Opens the list of events for the domain controller for the latest or currently running task of the Recovery Plan.

Events Management

The **Events** page displays events that occurred while performing tasks such as backups, verification, and recovery. You can perform the following actions on this page:


- Use the **Filters** button to filter events by severity or the date the event was created.
 - To filter by severity, select the relevant checkboxes to filter by one or more of the following severities: **Information**, **Warning**, or **Error**.
 - To filter by the date the event was created, select the desired date and time range and then select **Apply**.
- Use the **Refresh** button to display the most up to date events.
- Use the **Export** button to export the events data into a .csv format.
- Use the **Edit Columns** button to include or exclude one or more columns.
- Change the forest by using the dropdown menu on the top right side of the page.


Task Management

The **Tasks** page allows you to view a log of tasks, including their statuses and when they were created.

You can perform the following actions on this page:

- Use the **Filter** button to filter tasks by their status or the date the task was created.
 - To filter by status, select the relevant checkboxes to filter by one or more of the following statuses: **Queued, In Progress, Completed, Failed, Canceling, or Canceled**.
 - To filter by the date the task was created, select the desired date and time range and then select **Apply**.
- Use the **Refresh** button to display the most up to date tasks.
- To stop tasks that are in progress, select the checkboxes for the tasks you want to cancel and then select **Cancel**.

 **NOTE:** To cancel all tasks, you must select the checkbox in the table header on each page of the list.

 **CAUTION:** Canceling a recovery task may result in a corrupt forest.

- Use the **Edit Columns** button to include or exclude one more columns.
- Change the forest by using the dropdown menu on the top right side of the page.

Quest Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit www.quest.com or follow Quest Software on [X \(formerly Twitter\)](#) and [LinkedIn](#).

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