ManageEngine
RecoveryManager Plus

A guide to **performing domain controller restoration** using RecoveryManager Plus

www.recoverymanagerplus.com

What is domain controller recovery?

Domain controller recovery is the process of restoring a domain controller from scratch in the event of a complete breakdown. Without a potent disaster recovery plan, unforeseen events such as hardware failure or ransomware attacks can impede routine IT work and business processes.

In this guide, we'll explain how you can configure a domain controller for backup and the steps you can take to perform its restoration.

Domain controllers have two modes of restoration:

- ✓ **Non-authoritative restoration:**
  This method just restores the file from a backup. All changes made to AD after the backup point will be synchronized to the restored domain controller from the other domain controllers in the domain via replication.

- ✓ **Authoritative restoration:**
  In this method, the restored domain controller replicates and overwrites the AD database of all other domain controllers in the domain, erasing all AD changes made after the backup.

  A domain controller can only be authoritatively restored after non-authoritative restoration is complete.

Performing domain controller backups and restorations using RecoveryManager Plus

Creating a domain controller backup and performing restoration is a three-step process:

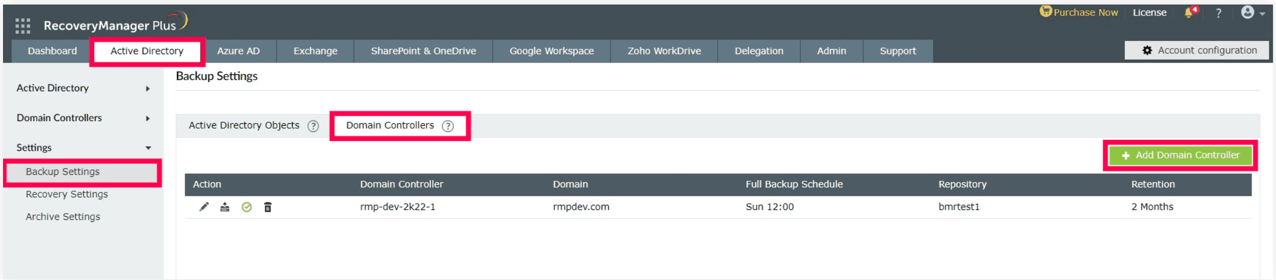
1. Configuring a backup schedule
2. Creating a bootable recovery media
3. Performing the restoration

1. Configuring a backup schedule

To perform a successful domain controller restoration, the backup should contain all parts of the domain controller, including the system state (sysvol folder), boot volume, and the AD database (Ntds.dit); all data in the domain controller must also be backed up.

To perform domain controller restoration, you'll need at least one valid domain controller backup. The following steps illustrate how you can configure a domain controller for backup using RecoveryManager Plus.

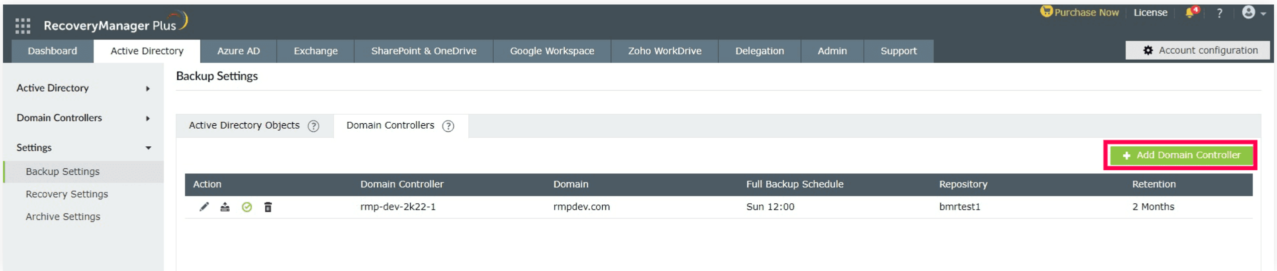
1. Log in to **RecoveryManager Plus** as an administrator.
2. Navigate to the **Active Directory** tab > **Settings > Backup Settings > Domain Controllers.**



Action	Domain Controller	Domain	Full Backup Schedule	Repository	Retention
	rmp-dev-2k22-1	rmpdev.com	Sun 12:00	bmrtest1	2 Months

Figure 1: The domain controller's backup settings page in RecoveryManager Plus.

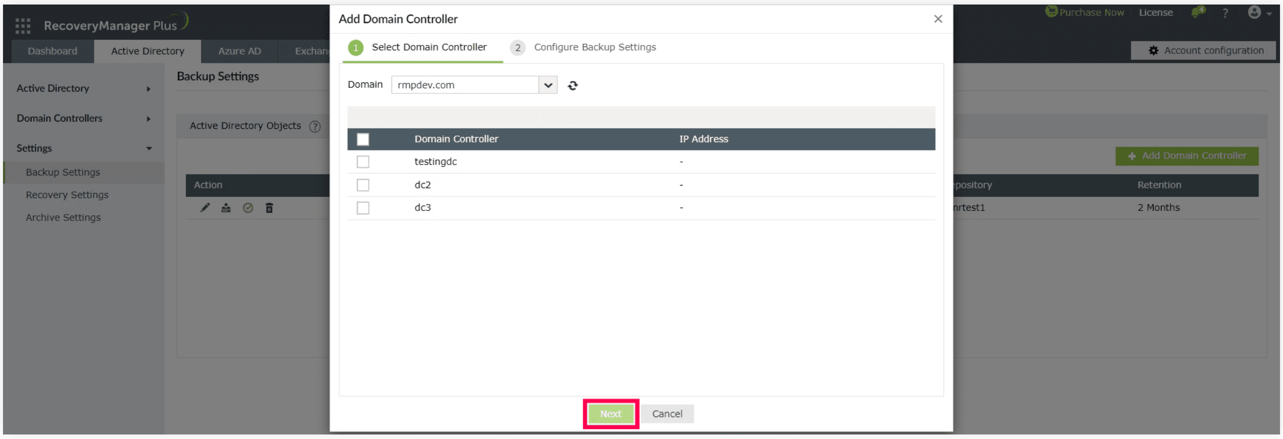
3. Click **Add Domain Controller** in the top-right corner.



Action	Domain Controller	Domain	Full Backup Schedule	Repository	Retention
	rmp-dev-2k22-1	rmpdev.com	Sun 12:00	bmrtest1	2 Months

Figure 2: Adding domain controllers.

4. A list of all domain controllers present in the selected domain will be listed in the pop-up.
5. Select the domain controller(s) that you wish to configure for backup and click **Next.**



Domain: rmpdev.com

□	Domain Controller	IP Address
□	testingdc	-
□	dc2	-
□	dc3	-

Figure 3: Selecting domain controllers for backup.

6. Configure the backup settings for the selected domain controllers in the Configure Backup Settings section.

   i. From the **Select Backup Repository** drop-down menu, select the backup repository from the list of all available repositories. If no repositories are available, click the 📁 icon to add a new repository. In the pop-up that appears, click **Yes** to proceed to add a new repository.

a. Select **NAS/Shared** and click **Add Repository** in the top-right corner.

b. In the *Repository Name* field, enter a name for the repository.

c. In the *Repository Path* field, enter the path of the location where you wish to save the backups.

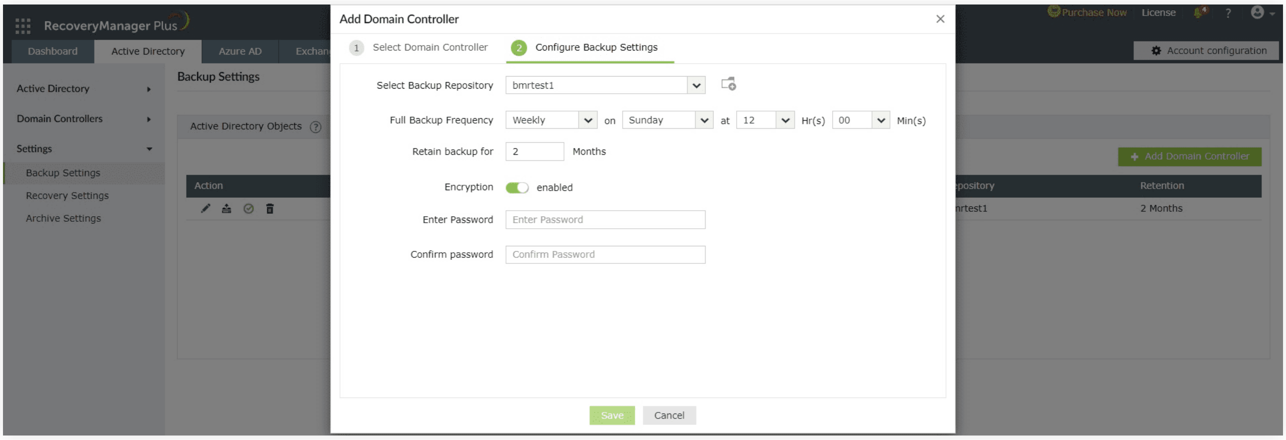
d. Enter the **User Name** and **Password** of a user that can read and write the content in the specified storage location and click **Save.**

ii. In the **Full Backup Frequency** field, specify the frequency (monthly or weekly) at which full backups must be made.

iii. In the **Retain backups for** field, enter how long backup data should be retained.

iv. Select **Encryption** if you wish to encrypt your backups. Enter and confirm the password for your encryption.

v. Click **Save** to complete setting up the domain controller for backup.



Add Domain Controller

1 Select Domain Controller   2 Configure Backup Settings

Select Backup Repository: bmrtest1

Full Backup Frequency: Weekly on Sunday at 12 Hr(s) 00 Min(s)

Retain backup for: 2 Months

Encryption: enabled

Enter Password: Enter Password

Confirm password: Confirm Password

Save   Cancel

Figure 4: Configuring backup settings for domain controllers.

The backup agent will now be installed in the selected servers and domain controllers.

A backup of the selected domain controller will be made at the time specified in the configuration. To manually trigger the creation of a backup of the server as soon as the configuration has been set, click the icon under the Actions column of the configured backup schedule.

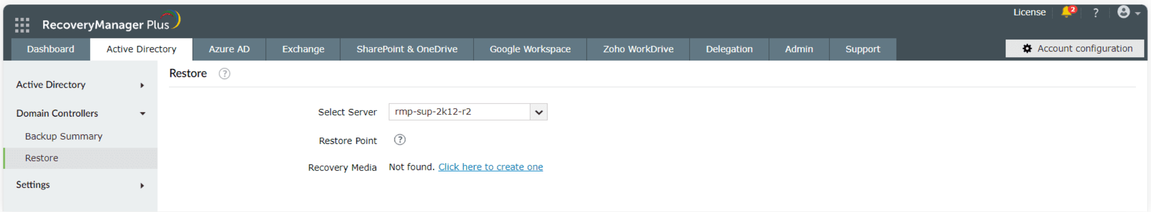
Once you've created a domain controller backup, you can use that to perform a domain controller restoration.

2. Creating a bootable recovery media

A recovery media e is a minimal OS with limited functionalities that contains all data required to boot your machine and run RecoveryManager Plus' restoration wizard. Once created, it can be used to restore multiple domain controllers. Irrespective of the physical machine's version, you will only need one recovery media for all the domain controllers in your environment.

Prerequisite: Make sure you have the Windows Assessment and Deployment Kit (Windows ADK) and Windows PE installed. If not, download them here.

1. Log in to the RecoveryManager Plus web console as an administrator.
2. Navigate to the **Active Directory** tab > **Domain Controllers** > **Restore.**
3. In the **Recovery Media Path** field, select **Click here to create one** to create a recovery media.



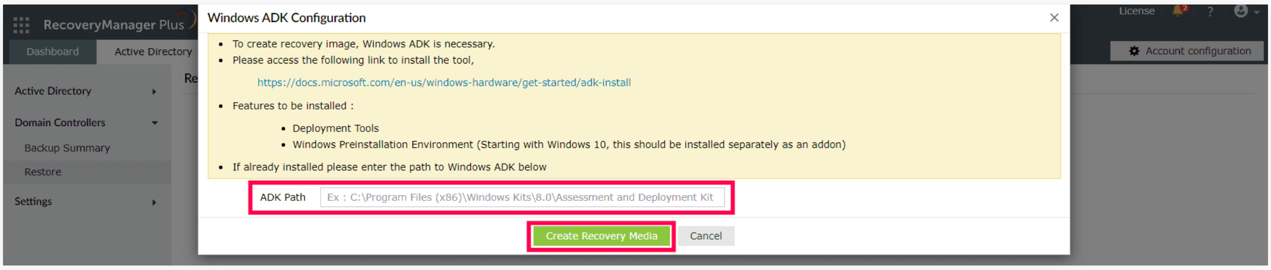
Select Server: rmp-sup-2k12-r2

Restore Point

Recovery Media: Not found. Click here to create one

Figure 5: Creating recovery media.

4. In the pop-up that appears, enter the location (local or shared path) where Windows ADK is installed and click **Create Recovery Media**.



Windows ADK Configuration

- To create recovery image, Windows ADK is necessary.
- Please access the following link to install the tool,

  https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install

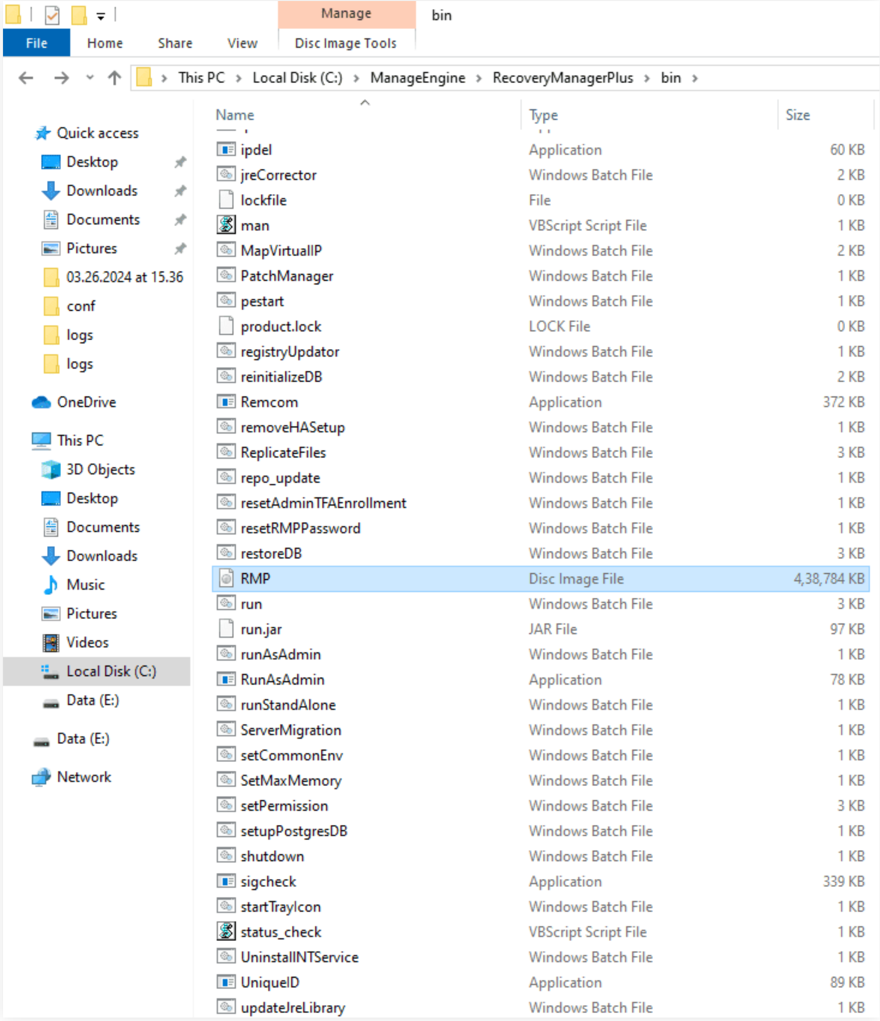
- Features to be installed :
  - Deployment Tools
  - Windows Preinstallation Environment (Starting with Windows 10, this should be installed separately as an addon)
- If already installed please enter the path to Windows ADK below

ADK Path: Ex : C:\Program Files (x86)\Windows Kits\8.0\Assessment and Deployment Kit

Figure 6: Providing the Windows ADK path.

Note: If the entered location is a shared path, select **Authentication** and provide the credentials of a user who can access the location.

5. The recovery media will be created with the name **RMP.iso** and can be found in the **<Installation_directory>\bin.**



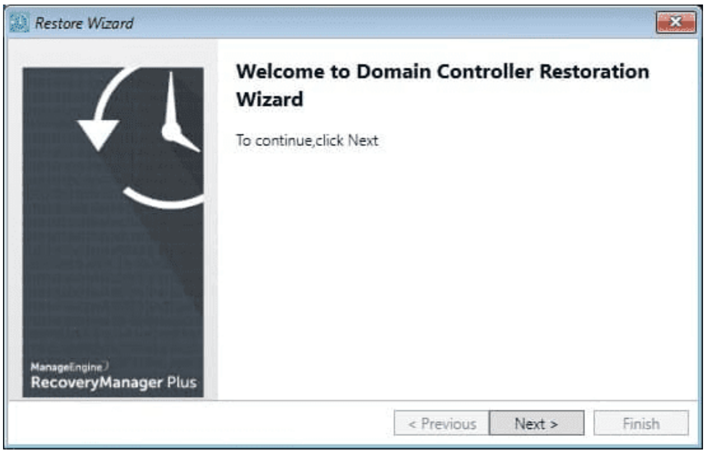
Name	Type	Size
ipdel	Application	60 KB
jreCorrector	Windows Batch File	2 KB
lockfile	File	0 KB
man	VBScript Script File	1 KB
MapVirtualIP	Windows Batch File	2 KB
PatchManager	Windows Batch File	1 KB
pestart	Windows Batch File	1 KB
product.lock	LOCK File	0 KB
registryUpdator	Windows Batch File	1 KB
reinitializeDB	Windows Batch File	2 KB
Remcom	Application	372 KB
removeHASetup	Windows Batch File	1 KB
ReplicateFiles	Windows Batch File	3 KB
repo_update	Windows Batch File	1 KB
resetAdminTFAEnrollment	Windows Batch File	1 KB
resetRMPPassword	Windows Batch File	1 KB
restoreDB	Windows Batch File	3 KB
RMP	Disc Image File	4,38,784 KB
run	Windows Batch File	3 KB
run.jar	JAR File	97 KB
runAsAdmin	Windows Batch File	1 KB
RunAsAdmin	Application	78 KB
runStandAlone	Windows Batch File	1 KB
ServerMigration	Windows Batch File	1 KB
setCommonEnv	Windows Batch File	1 KB
SetMaxMemory	Windows Batch File	1 KB
setPermission	Windows Batch File	3 KB
setupPostgresDB	Windows Batch File	1 KB
shutdown	Windows Batch File	1 KB
sigcheck	Application	339 KB
startTrayIcon	Windows Batch File	1 KB
status_check	VBScript Script File	1 KB
UninstallNTService	Windows Batch File	1 KB
UniqueID	Application	89 KB
updateJreLibrary	Windows Batch File	1 KB

Figure 7: Recovery media created.

3. Performing the restoration

RecoveryManager Plus can restore the backup of a domain controller to the same or a different physical machine. You can also use the product to restore the backup of a domain controller to a virtual machine. Once the recovery media is created, follow the steps below for non-authoritative restoration of domain controllers.

1. Log in to RecoveryManager Plus as an administrator.
2. Navigate to the **Active Directory** tab > **Domain Controllers > Restore.**
3. From the **Select Domain Controller** drop-down, select the domain controller that has to be restored.
4. Select the restore point to which you wish to restore from the **Restore Point** drop-down menu.
5. Once you boot the server to be restored using the recovery media, the RecoveryManager Plus *Domain Controller Restoration Wizard* (see Fig. 8 below) will start. Click **Next.**



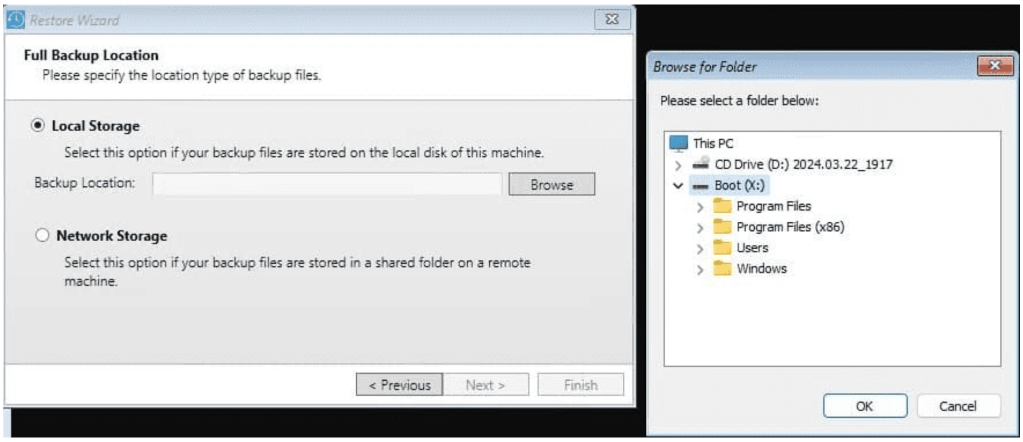
Restore Wizard

Welcome to Domain Controller Restoration Wizard

To continue,click Next

Figure 8: The Domain Controller Restoration Wizard.

6. Provide the location of the full backup in the *Backup Location* field. The location of the full backup can be stored in the local machine or in shared network storage. If the backup is in a shared network, provide the credentials of a user who has permission to access the location and click **Next.**



Restore Wizard

Full Backup Location

Please specify the location type of backup files.

● **Local Storage**

Select this option if your backup files are stored on the local disk of this machine.

Backup Location:

○ **Network Storage**

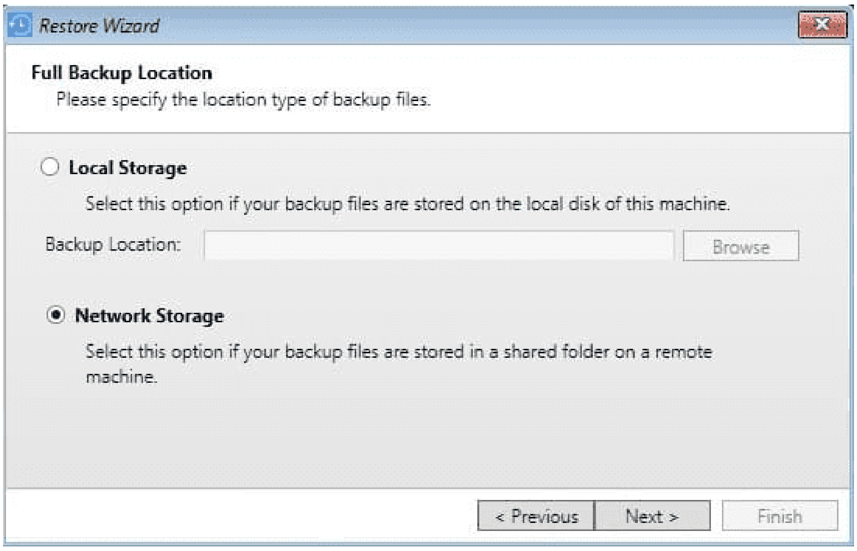
Select this option if your backup files are stored in a shared folder on a remote machine.

Browse for Folder

Please select a folder below:

- This PC
  - CD Drive (D:) 2024.03.22_1917
  - Boot (X:)
    - Program Files
    - Program Files (x86)
    - Users
    - Windows

Figure 9: Providing the location of your full backup (local path).



Restore Wizard

Full Backup Location

Please specify the location type of backup files.

○ **Local Storage**

Select this option if your backup files are stored on the local disk of this machine.

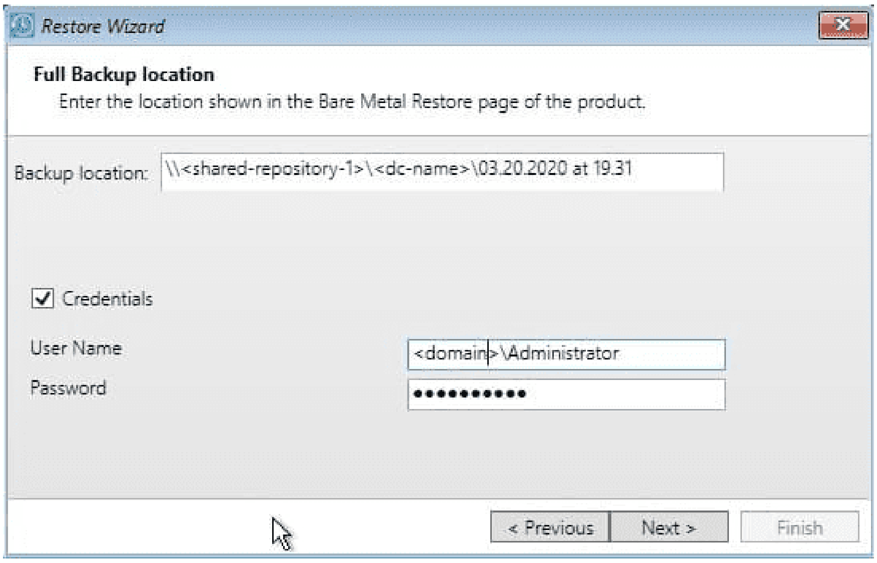
Backup Location:

● **Network Storage**

Select this option if your backup files are stored in a shared folder on a remote machine.

Figure 10: Providing the location of your full backup (network share).

7. Enter the User Name and Password for accessing the network location.



Restore Wizard

Full Backup location

Enter the location shown in the Bare Metal Restore page of the product.

Backup location: \\<shared-repository-1>\<dc-name>\03.20.2020 at 19.31

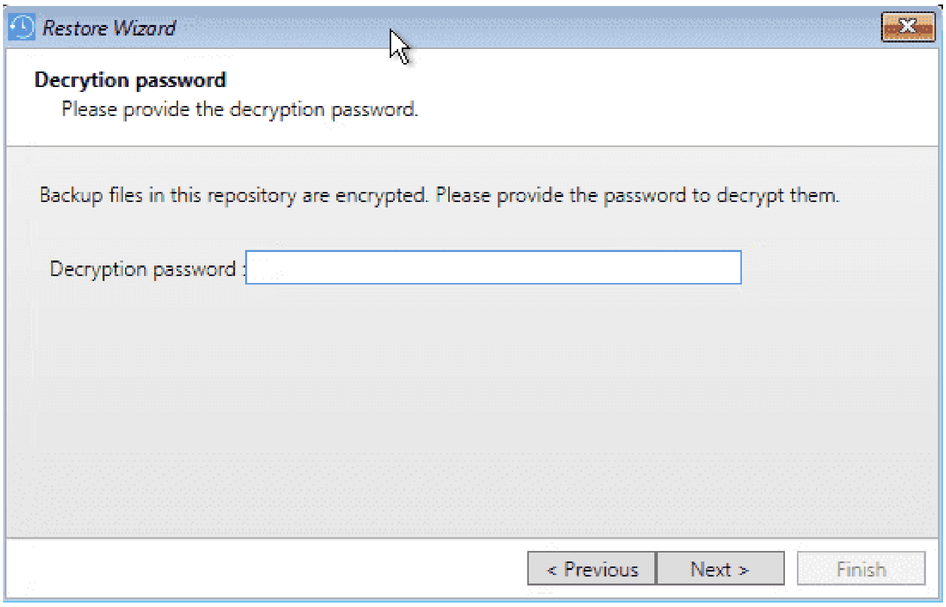
☑ Credentials

User Name: <domain>\Administrator

Password: ●●●●●●●●●●●

Figure 11: Providing the credentials for accessing the network location.

8. If you configured your backups to be encrypted, you'll be prompted to provide a decryption password. Click **Next.**



Restore Wizard

Decryption password

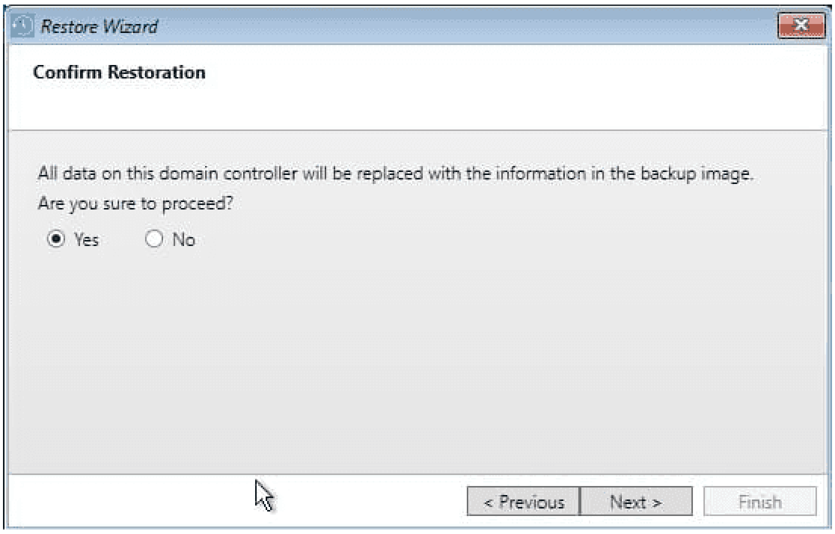
Please provide the decryption password.

Backup files in this repository are encrypted. Please provide the password to decrypt them.

Decryption password :

Figure 12: Providing the decryption password.

9. Select **Yes** and click **Next** on the **Confirm Restoration** screen to begin the restoration. The domain controller has now been restored to its backed-up state.



Restore Wizard

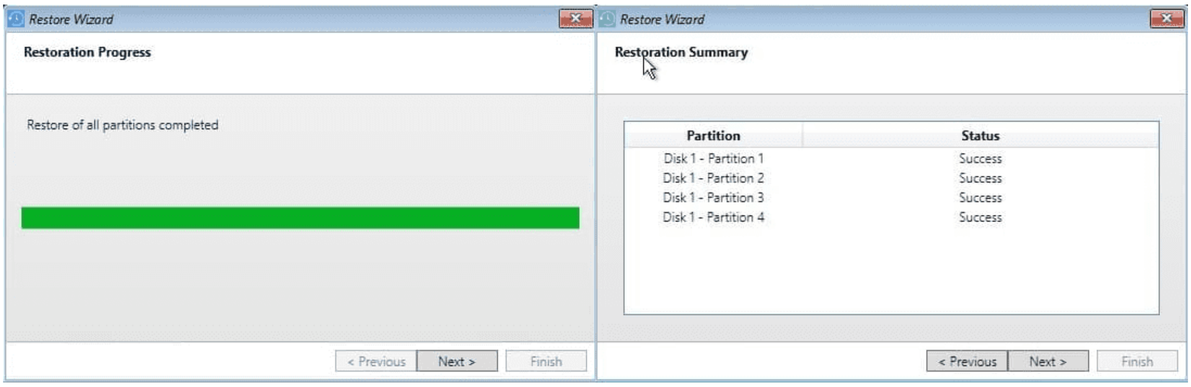
Confirm Restoration

All data on this domain controller will be replaced with the information in the backup image.

Are you sure to proceed?

● Yes ○ No

Figure 13: Confirming the domain controller restoration process.



Restore Wizard

Restoration Progress

Restore of all partitions completed

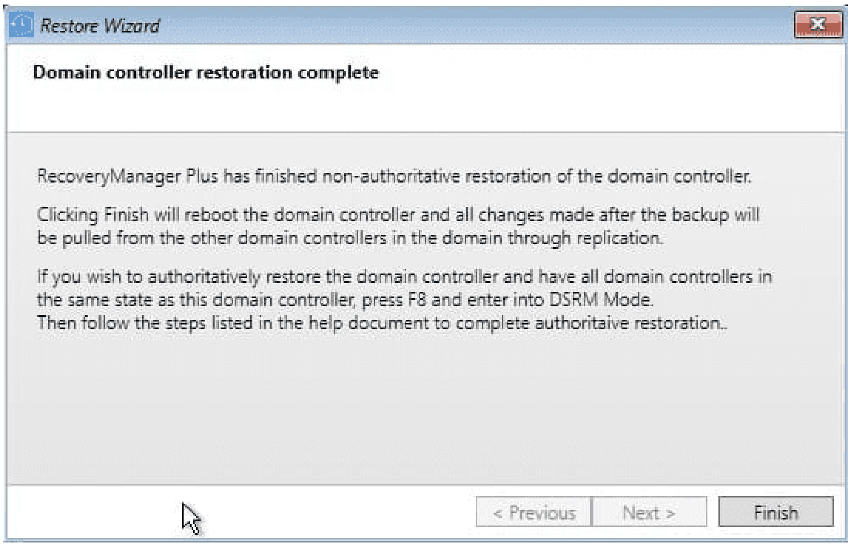
Restore Wizard

Restoration Summary

Partition	Status
Disk 1 - Partition 1	Success
Disk 1 - Partition 2	Success
Disk 1 - Partition 3	Success
Disk 1 - Partition 4	Success

Figure 14: Domain controller restoration process completion and Restoration Summary.

10. Clicking **Finish** will reboot the restored domain controller. All other domain controllers in the domain will replicate all the AD changes made since the backup to the restored domain controller.



Restore Wizard

Domain controller restoration complete

RecoveryManager Plus has finished non-authoritative restoration of the domain controller.

Clicking Finish will reboot the domain controller and all changes made after the backup will be pulled from the other domain controllers in the domain through replication.

If you wish to authoritatively restore the domain controller and have all domain controllers in the same state as this domain controller, press F8 and enter into DSRM Mode.
Then follow the steps listed in the help document to complete authoritaive restoration..

Figure 15: Domain controller restoration complete.

To stop the restored domain controller from receiving changes via replication, and to make all the other domain controllers in the domain have the same state as the restored domain controller, perform an authoritative restoration by following the steps listed below.

Authoritative restoration of a domain controller

Note: A domain controller can be authoritatively restored only after non-authoritative restoration is complete. Follow the steps listed in the previous section to complete non-authoritative restoration before proceeding with authoritative restoration.

1. Once non-authoritative restoration is complete, manually boot the domain controller in **Directory Services Restore Mode** (DSRM) by repeatedly pressing the F8 key immediately after the BIOS POST screen. In the text menu that appears, use the up or down arrow keys to select **Directory Services Restore Mode** or **DS Restore Mode.**
2. Log in with the DSRM account and password.
3. Open a **Command Prompt** and type **ntdsutil.**
4. Type **activate instance ntds.**
5. Type **authoritative restore.**
6. Determine the **distinguished name** of the domain, the subtree of objects, or the object that you wish to authoritatively restore.

   Syntax: CN=value,OU=value,DC=value,DC=value.

   a. To authoritatively restore an entire domain, enter:

   restore subtree <distinguished name of the domain>

   b. To authoritatively restore a subtree of objects, enter:

   restore subtree <distinguished name of the subtree>

   c. To authoritatively restore a single object, enter:

   restore object <distinguished name of the object>
7. Click **Yes** to confirm.
8. Reboot the domain in normal mode to complete authoritative restoration.

Once restoration is complete, all domain controllers in the domain will be in the same state as the restored domain controller.

Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus

ADSelfService Plus | M365 Manager Plus

About RecoveryManager Plus

ManageEngine RecoveryManager Plus is a comprehensive backup and recovery solution that empowers administrators to back up and restore their Active Directory, Entra ID, Microsoft 365, Google Workspace, on-premises Exchange and Zoho WorkDrive environments. With its incremental backups, flexible retention policies and multiple modes of restoration—such as domain controller recovery and object-, item- and attribute-level restoration—RecoveryManager Plus delivers a holistic solution for backing up data that is critical for your enterprise to function. For more information, visit www.manageengine.com/ad-recovery-manager.

$ Get Quote   ⤓ Download