Cygna Forest Recovery for Active Directory

Quick Install Guide



For the latest information, visit online documentation at docs.cygnalabs.com

Published 11/2/2026

Version 26.1

Copyright © 2026

Copyright

©2026 Cygna Labs Corp. ALL RIGHTS RESERVED.

Trademarks

Cygna Labs and the Cygna Labs logo are trademarks and registered trademarks of Cygna Labs Corp. in the United States of America and other countries. All other trademarks are property of their respective owners.

Disclaimers

The product documentation is subject to change without notice. For the latest and more detailed documentation, please refer to online documentation at https://docs.cygnalabs.com.

The product functionality described in this document shall not be treated as a public offer or commitment.

The information regarding the use and installation of third-party software is provided to assist you but Cygna Labs Corp. shall not accept any responsibility or liability for any claims or damages caused by incorrect or incomplete information provided about third-party software. For detailed instructions on configuring third-party software components, refer to their respective owners.

Quick Install Guide

This guide lists the machines a Cygna Forest Recovery for Active Directory deployment needs and the steps to install it, with the commands for each step. Cygna Forest Recovery for Active Directory is part of the Cygna Disaster Recovery Suite, so the services and commands it installs carry the suite's short name, Cygna DR, and its installer packages the full name, Cygna Disaster Recovery. It is for administrators who know Windows Server and Active Directory and want to install without reading the background first. Each step names the topic with the full procedure, the options, and the reasons behind each choice.

For the decisions to make before you start, see the Cygna Forest Recovery for Active Directory Planning and Requirements Guide. The full procedures are in the Cygna Forest Recovery for Active Directory User Guide.

Machines

Machine	Operating system	Minimum	Recommended
Manager	64-bit Windows Server 2019 or later	2 processor cores, 4 GB of memory	4 processor cores, 8 GB of memory
Storage machine	64-bit Windows Server 2019 or later	4 processor cores, 4 GB of memory	4 processor cores, 8 GB of memory
Isolated Recovery Host (optional)	64-bit Windows Server 2019 or later, with Hyper-V	4 processor cores, 8 GB of memory	8 processor cores, 32 GB of memory, on a dedicated machine
Candidate machines (optional)	64-bit Windows Server 2019 or later	Enough memory to start the recovery image: its size plus about 1 GB	The processors and memory of the domain controller it replaces
Domain controllers	Windows Server 2016 through Windows Server 2025, Server Core or Desktop Experience	—	—

In addition:

- **Manager and storage machine**—not joined to any domain, never a domain controller, each with a fixed IP address (static, or a DHCP reservation). They can share one machine, but separate machines are recommended. The storage machine needs a volume large enough for the backups you keep, with BitLocker turned on. No IIS, SQL Server, or .NET runtime is needed.
- **Domain controllers**—every domain controller runs the DC agent and needs the Windows Server Backup feature. Back up at least two writable domain controllers in each domain.
- **Isolated Recovery Host**—for test restores only. Not joined to any domain, never a domain controller. Processor virtualization turned on (nested virtualization if it is a virtual machine), and a private IPv4 prefix that is not used elsewhere, for its recovery network.
- **Candidate machines**—spare machines that can receive a full system recovery. Not a domain controller, with the DC agent installed. At least as many disks as the domain controller they replace, each the same size or larger, and the same firmware type (UEFI or BIOS).
- **Operator workstations**—a current web browser, with the Manager's certificate authority (CA) trusted.

Network

These are the default ports. You can change the Manager's ports when you install it.

From	To	Port
Domain controllers, storage machine, candidate machines, Isolated Recovery Host	Manager	TCP 5211. The Manager installer opens it.
Domain controllers, recovery targets, Isolated Recovery Host	Storage machine	TCP 445 (SMB). You add this firewall rule yourself.

From	To	Port
Operator workstations	Manager	TCP 5210 (console, REST API, and `cdr`), and optionally TCP 80 for the redirect to HTTPS.
Manager, or the machine that runs `cdr agent deploy`	Domain controllers, for a push installation	TCP 445 (`ADMIN$`) with the Remote Registry service, plus either WinRM (TCP 5985, with the targets in the installing machine's TrustedHosts) or DCOM (TCP 135 and dynamic RPC ports, with the **Windows Management Instrumentation (WMI-In)** firewall rules enabled).

Have on hand

- **Installer packages**—`CygnaDR.Manager.msi`. The Manager installs a copy of each agent package in the `redist` folder of its program folder, and offers them for download on the **Agents** screen.
- **The license key**—the key Cygna sent you.
- **IP addresses**—of the Manager and the storage machine. Agents use addresses rather than names, so they keep working when DNS is down.
- **A storage path**—an absolute path on the storage volume, for example `E:\CygnaDR`. It cannot be changed later from the Manager.
- **A domain controller administrator account**—a local administrator on each domain controller (Domain Admin in most environments), used to push the DC agent and never stored.
- **Windows Server ISOs**—matching the build, edition, and installation type of each domain controller, for full system recovery.
- **A safe place offline**—for the enrollment token, the break-glass credential, and the recovery passphrase that you create during installation.

Install

Follow the steps in order. Each step needs something that the step before it creates. Run every command in an elevated session.

Step 1: Install the Manager

1. Generate an enrollment token, a random secret that every agent presents to enroll, and record it offline:

   ```
   $bytes = New-Object byte[] 32
   [System.Security.Cryptography.RandomNumberGenerator]::Create().GetBytes($bytes)
   ([System.BitConverter]::ToString($bytes) -replace '-', '')
   ```

2. On the Manager machine, install the Manager:

   ```
   msiexec /i CygnaDR.Manager.msi /qn ENROLLMENTTOKEN=<token>
   ```

3. Read the CA fingerprint from the Application event log. You compare against it in step 3. It is public, so keep a copy with your recovery notes rather than in the safe:

   ```
   Get-WinEvent -LogName Application -MaxEvents 500 |
     Where-Object Message -like '*Cygna DR manager CA fingerprint*' |
     Select-Object -First 1 -ExpandProperty Message
   ```

For details, see *Installing the Manager* in the User Guide.

Step 2: Sign in, claim the Manager, and apply the license

Note: **Important:** Whoever completes the setup page first owns the Manager. Do this step immediately after installing.

1. On the Manager machine, open `https://localhost:5210`.

   The **Set up this manager** page opens.

2. Enter a recovery passphrase of at least 16 characters twice, and select **Create the break-glass account**.

3. Record the break-glass username and password offline with the passphrase, select both confirmations, and select **I have stored both — continue**.

   The password is shown only once.

4. Select **Administration** > **License** > **Apply a license key…**, paste the key, and select **Apply this license**.

   Without a license, the Manager refuses every backup and recovery operation.

5. Select **Administration** > **Operators & Roles**, and create a named account for each person who operates Cygna Forest Recovery. The people setting up the deployment need System Admin and Backup Operator.

6. Sign out, and sign in with your named account. Keep the break-glass account for emergencies.

For details, see *Signing In for the First Time* in the User Guide.

Step 3: Trust the Manager certificate on workstations

On each operator workstation, download the CA certificate, compare its hash with the fingerprint from step 1, and import it only if they match. In PowerShell 7:

```
$trust = Invoke-RestMethod -Uri https://<manager>:5210/api/trust -SkipCertificateCheck
Set-Content -Path .\manager-ca.pem -Value $trust.caCertificatePem
certutil -decode .\manager-ca.pem .\manager-ca.cer
certutil -hashfile .\manager-ca.cer SHA256
certutil -user -addstore Root .\manager-ca.cer
```

Restart the browser. To trust the CA for every user of a workstation, run `certutil -addstore Root .\manager-ca.cer` in an elevated session instead, or distribute it with Group Policy.

For details, see *Trusting the Manager Certificate* in the User Guide.

Step 4: Set up the storage machine

1. Turn on BitLocker with auto-unlock for the storage volume.
2. Create the staging folder, share it, and allow SMB from your domain controllers' networks. Share only the staging folder, never the storage root:

   ```
   New-Item -ItemType Directory -Path E:\CygnaDR\staging
   New-SmbShare -Name CygnaDRStaging -Path E:\CygnaDR\staging -FullAccess
   "BUILTIN\Administrators"
   New-NetFirewallRule -DisplayName "Cygna DR staging (SMB)" -Direction Inbound -Protocol
   TCP -LocalPort 445 -RemoteAddress 10.0.1.0/24,10.0.2.0/24 -Action Allow
   ```

3. Copy `CygnaDR.StorageAgent.msi` from `%ProgramFiles%\Cygna Labs\Disaster Recovery Suite Manager\redist` on the Manager machine to the storage machine.
4. Install the storage agent with the Manager's IP address and CA fingerprint, the storage root, and the enrollment token:

   ```
   msiexec /i CygnaDR.StorageAgent.msi /qn MANAGERADDRESS=https://10.0.0.10:5211
   MANAGERCAFINGERPRINT=<fingerprint> STORAGEROOT=E:\CygnaDR
   ENROLLMENTTOKEN=<token>
   ```

   On **Administration** > **Agents**, the storage machine shows **Connected**. Within a few minutes, **Protection** > **Repository** shows its capacity.

For details, see *Setting Up the Storage Machine* in the User Guide.

Step 5: Deploy the DC agents

1. Install Windows Server Backup on each domain controller:

   ```
   Install-WindowsFeature Windows-Server-Backup
   ```

   Alternatively, leave **Install the Windows Server Backup feature** on (the default) on the **Domain controller agents** tab of **Administration** > **Configuration**, and the agent installs it.

2. Install the agent on one domain controller in each forest. Either run the installer on the domain controller, with the command from **Administration** > **Agents** > **Install agent**:

   ```
   msiexec /i CygnaDR.DcAgent.msi /qn MANAGERADDRESS=https://10.0.0.10:5211
   MANAGERCAFINGERPRINT=<fingerprint> ENROLLMENTTOKEN=<token>
   ```

   Or push it from the Manager machine, in `%ProgramFiles%\Cygna Labs\Disaster Recovery Suite Manager`. `cdr` prompts for the password and the enrollment token:

   ```
   cdr agent deploy dc01.corp.example.com --user CORP\admin --manager-address
   https://10.0.0.10:5211
   ```

   The first agent reports every domain controller in its forest.

3. Select **Active Directory** > **Domain Controllers**, select the domain controllers that have no agent, and select **Deploy the agent to n…**.

4. Enter the administrator account and password, check the Manager address, choose WinRM or DCOM, and select **Install on n machines**.

   Each domain controller shows **Connected** in the **Agent** column.

Candidate machines need the DC agent too. Install it with the same `msiexec` command.

For details, see *Deploying DC Agents* in the User Guide.

Step 6: Set up OS media for full system recovery

1. On the storage machine, create a folder for ISOs and one for recovery images, outside the storage root, and copy your Windows Server ISOs into the first:

   ```
   New-Item -ItemType Directory -Path E:\os-media, E:\recovery-images
   ```

2. Select **Administration** > **Configuration** > **Storage agents**. Set **Media folder** and **Recovery image folder**, and select **Save**.

3. Restart the storage agent:

```
Restart-Service CygnaDRStorageAgent
```

The storage agent builds a recovery image for each operating system that appears in a backup, so images appear after the first backups complete. DC state recovery works without them; full system recovery does not.

For details, see *Setting Up OS Media and Recovery Images* in the User Guide.

Step 7: Create backup policies

No backup policy exists by default. Back up at least two writable domain controllers in each domain, including the PDC emulator.

1. Select **Active Directory** > **Backup Policies**, and select the domain controllers to back up.
2. Select **Edit *n* schedules...**. Set **State** to **Enabled**, **Interval** to **Daily**, and **Backup type** to **Full system**, and select **Save *n* schedules**.

   The first backups are due immediately. To run them outside business hours instead, set **Start time** to **At a set time** and enter a time in the Manager's local time, such as 22:00.
3. Domain controllers you don't back up are shown as **Rebuilt on recovery** and raise no alert; you do not need to exclude them. Make sure every global catalog has the DC agent, because a recovery of another domain in the forest needs it.

For details, see *Creating Your First Backup Policies* in the User Guide.

Step 8: Set up an Isolated Recovery Host (optional)

1. On the storage machine, allow SMB from the host's address, if you limit TCP 445 to your domain controllers' networks:

```
New-NetFirewallRule -DisplayName "Cygna DR Isolated Recovery Host (SMB)" -Direction Inbound -Protocol TCP -LocalPort 445 -RemoteAddress 10.0.0.30 -Action Allow
```

2. From **Administration** > **Agents** > **Install agent**, download `CygnaDR.HostAgent.msi` to the host, and install it:

```
msiexec /i CygnaDR.HostAgent.msi /qn MANAGERADDRESS=https://10.0.0.10:5211 MANAGERCAFINGERPRINT=<fingerprint> ENROLLMENTTOKEN=<token>
```

   The agent installs Hyper-V if it is missing and, on a dedicated host, restarts the host five minutes later. It then creates the isolated recovery network.

3. On **Administration** > **Agents**, check that the host panel shows **Ready to run verification**. If it does not, follow the instructions in the panel.

For details, see *Setting Up an Isolated Recovery Host* in the User Guide.

Verify the deployment

When the first backups have completed, check that:

- **Administration** > **Agents** lists every agent as **Connected**.
- **Protection** > **Restore Points** lists a restore point for each domain controller you back up.
- The **Dashboard** shows each domain and forest as covered.
- On **Active Directory** > **OS Media**, the **Operating systems** tab shows **Available** in the **Recovery image** column for each operating system.
- If you set one up, the Isolated Recovery Host is ready.
- The **Configuration backups** card on the **License** screen shows a backup stored on the storage machine.
- The enrollment token, break-glass credential, and recovery passphrase are recorded together offline, and the CA fingerprint is in your recovery notes.

For everything else to do on the first day, see *Manager Day-One Checklist* in the User Guide.