OpenText™ Active Directory Administrator

Install

Version : 1.0

PDF Generated on : 30/04/2025

Table of Contents

1. Install

The *Installation Guide* provides planning, installation, licensing, and configuration information for the OpenText Active Directory Administrator (ADA) and its integrated components.

This book guides you through the installation process and helps you make the correct decisions to install and configure DRA.

Intended audience

This book provides information for anyone installing ADA.

Additional documentation

The Active Directory Administrator documentation library includes the following resources:

Release Notes
: Provides additional information about the release, resolved issues and known issues.

System Requirements
: Provides the list of hardware and software requirements, and the supported applications.

Administrator Guide
: Provides information about the installation and administration of the Active Directory Administrator.

User Guide
: Provides information about the tasks users can perform in the Active Directory Administrator web console.

This guide is part of the Active Directory Administrator documentation set. For the most recent version of this guide and other ADA documentation resources, visit the DRA Documentation site.

Contact information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the **comment on this topic** link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact Open Text Support for Micro Focus products at https://www.microfocus.com/support-and-services/.

1.1. Preparing for installation

This section provides information about planning Active Directory Administrator installation and upgrade.

- Implementation checklist
- Understanding roles
- Understanding ports used
- Enabling Active Directory monitoring
- Binding SSL certificates

1.1.1. Implementation checklist

Task	See
Understand roles	Understanding roles
Review the hardware and software requirements, and the supported applications	System requirements
Ensure that you meet the following security considerations	Understanding ports used
Enable Active Directory monitoring	Enabling Active Directory monitoring
Binding SSL certificates	Binding SSL certificates

1.1.2. Security considerations

Security considerations ensure a more secure deployment and operation of the OpenText Active Directory Administrator. It is intended for administrators with several configuration guidelines. These guidelines can be used for enhancing the security of the environment.

Pre-installation server configurations

Firewalls

- Open only the necessary firewall ports required for communication between ADA and its connected servers.
- To review the list of ports, see Understanding ports.

FIPS settings

FIPS 140-2 is a standard established by NIST (National Institute of Standards and Technology) and CSE (Communications Security Establishment Canada). FIPS 140-2 pertains to cryptographic modules in software or hardware products.

- Ensure that ADA is configured and enabled to be compliant with FIPS standards for cryptographic modules.
- To enable FIPS on Windows Server:
  - Navigate to Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options.
  - Locate "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing" and set it to "Enabled".

TLS settings

- Windows Server 2016 and 2019: Enable TLS 1.2.
- Windows Server 2022: TLS 1.3 is enabled by default.
- TLS 1.2 settings and configurations can be enabled, refer to Enabling TLS 1.2 configurations.

User Account Control (UAC)

- Ensure that UAC is properly configured to enforce the principle of least privilege.
- Ensure UAC settings are high.
- Configuration Path: Control Panel > System and Security > Security and Maintenance > Security > User Account Control > Change Settings.

Post-installation configurations

Antivirus programs

- For optimal performance, ensure you configure antivirus programs to allow or exclude necessary ADA processes and files.

Antivirus exclusions

- You must exclude the following default locations from antivirus scans; if custom locations are used, exclude those instead:
  - Default ADA installation location: C:\Program Files\Active Directory Administrator
  - Default ADA Cache Data location: C:\ProgramData\OpenText\ADA\CacheDB\
  - Default ADA log location : %programdata%\OpenText\ADA\Logs

General security

- User account passwords are encrypted by default in the persistence store.

Certificates

Use trusted certificates for all secure communications to prevent attacks.ADA is compatible with SSL, CA or third party certificates; use any one. You can also change certificates post installation.

Note

ADA stores certificate information in in a json file available at: `<your installation location>\SeedData\common.settings.json`.

To change SSL certificates

1. Copy the following parameters from the new certificate to update the `common.settings.json` file.
   1. Subject
   2. Store
   3. Location
   4. AllowInvalid
2. Use netsh commands to update certificate binding:
   1. Identify the current binding:
      `netsh http show sslcert`
   2. Delete the existing binding:
      `netsh http delete sslcert ipport=0.0.0.0:6666`
   3. Get the new certificate's thumbprint:
      `Get-ChildItem Cert:\\LocalMachine\\M`
   4. Add the new certificate binding:
      `netsh http add sslcert ipport=0.0.0.0:6666 certhash=NEW_CERT_THUMBPRINT appid={YOUR_APP_ID}`

3. Restart the IIS service.

To change CA certificates

1. Copy the following parameters from the new certificate to update the `common.settings.json` file.
    1. Path
    2. Password
    3. AllowInvalid
2. Use netsh commands to update certificate binding:
    1. Identify the current binding:
       `netsh http show sslcert`
    2. Delete the existing binding:
       `netsh http delete sslcert ipport=0.0.0.0:6666`
    3. Get the new certificate's thumbprint:
       `Get-ChildItem Cert:\\LocalMachine\\M`
    4. Add the new certificate binding:
       `netsh http add sslcert ipport=0.0.0.0:6666 certhash=NEW_CERT_THUMBPRINT appid={YOUR_APP_ID}`
3. Restart the IIS service.
4. For third party CA certificates, import into the trusted root certificate store, if not already:
   `Import-Certificate -FilePath "path/to/ca_certificate.cer" -CertStoreLocation Cert:\\LocalMachine\\Root`

1.1.3. Understanding roles

The product provides two roles: Admin and Chief Information Security Officer (CISO). Users must belong either to an Admin group or a CISO group in the Active Directory to use the product. The users in the Admin group have the Admin role and the users in the CISO group have the CISO role.

Important

Ensure that the Admin and CISO groups have been created in the Active Directory and the Active Directory users have been assigned to any or both the groups. Only those groups that have Domain local as their group scope and Security as their group type are supported.

Admin Group User

As an Admin group user, you are responsible for administering the product. You can perform the following tasks in the product:

- Establish connection with the Active directories. The Admin user can be created by adding the user to the ADA admin group created while installing Change Guardian. This includes tasks such as configuring, updating, deleting domains and updating their service account discovery details.
- Monitoring Domain Activities. This includes tasks such as viewing domains and their service account discovery details, viewing the password expiration status of the accounts and notifying service account managers accordingly, and monitoring the service account activity to identify accounts that are not performing activities or suspicious accounts, which pose a risk of being compromised.

Chief Information Security Officer Group User

As a Chief Information Security Officer (CISO) group user, you are responsible for monitoring domains and their service accounts, and their activities that will help you determine which service accounts are suspicious or at a risk of being compromised. Some of the monitoring activities that you can perform in the product are as follows:

- View the number of service accounts that have engaged in activity and which have not. The CISO user can be created by adding the user to the ADA CISO group created while installing Change Guardian.
- View the top ten service accounts that have engaged in maximum activity. This information helps you determine if any of these service accounts require close monitoring.
- View the password expiration status of the service accounts and notify service account managers accordingly.
- Monitor the service account activity to identify the accounts not performing any activities and hence pose a risk of being compromised.
- Monitor the service account activity to identify suspicious accounts, which pose a risk of being compromised.
- View the names of the services with which a service account is associated, which helps in understanding which services need to be reconfigured whenever the service account password is updated.

1.1.4. Understanding ports used

Ensure that the following ports are open:

Note

These ports are not configurable while installing ADA. You must keep the mentioned ports unused and open in the firewall enabled setup. Or else, you will have to edit the corresponding json files with your custom ports after installing ADA.

Protocol and port	Direction	Destination	Usage
TCP/UDP 389	Outbound	Microsoft Active Directory domain Controllers	Active Directory object management (LDAP)
TCP/UDP 53	Outbound	Microsoft Active Directory domain controllers	Name resolution
TCP 636  **Important** • This port needs to be opened only if SSL is enabled on the Active Directory.	Outbound	Microsoft Active Directory domain controllers	Active Directory object management (LDAP SSL).
HTTP 5985 HTTPS 5986	Outbound	Microsoft Active Directory Member Servers or Clients	Used to collect Service Accounts and associated service details.

Protocol and port	Direction	Destination	Usage
HTTPS 50501	Inbound	OpenText ADA Gateway Service	API Gateway for the Active Directory Administrator server.
HTTPS 6681	Internal Communication	OpenText ADA Configuration Service	Used for internal communication between ADA services (does not need to be opened through the firewall).
HTTPS 6682	Internal Communication	OpenText ADA Collector Service	Used for internal communication between ADA services (does not need to be opened through the firewall).
HTTPS 6683	Internal Communication	OpenText ADA Watcher Service	Used for internal communication between ADA services (does not need to be opened through the firewall).
HTTPS 51103	Internal Communication	OpenText ADA Cache Service	Used for internal communication between ADA services (does not need to be opened through the firewall).

1.1.5. Enabling Active Directory monitoring

You must configure your Active Directory environment to enable the product to monitor the user objects of the Active Directory. Perform the following configurations on all the domain controllers for their operating systems to generate and retain as events the modifications to the user objects of the Active Directory. The product can then monitor and process the events, and display vital information related to service accounts and their activity in the Active Directory.

Configuring the security event log

You must configure the security event log to ensure that Active Directory events remain in the event log until the product monitors the events and processes them.

Set the maximum size of the Security Event Log to no less than 10 MB, and set the retention method to Overwrite events as needed.

To configure the security event log:

1. Log in to a domain controller where you need to configure using a user account with domain administrator privileges.
2. Open command prompt, type `gpmc.msc`, then press **Enter**to start the Group Policy Management Console.
3. Expand **Forest > Domains > domainName > Domain Controllers**.
4. Right-click **Default Domain Controllers Policy**, then select **Edit**.

   

   Note

   Making this change to the default domain controllers policy is important because a GPO linked to the domain controller (DC) organizational unit (OU) with a higher link order can override this configuration when you restart the computer or run gpUpdate again. If your corporate standards do not allow you to modify the default domain controllers policy, create a GPO for your product settings, add these settings to the GPO, and set it to have the highest link order in the Domain Controllers OU.

5. Expand **Computer configuration > Policies > Windows Settings > Security Settings.**
6. Click **Event Log**, then set **Maximum security log size** to a value greater than or equal to 10240 KB (10 MB).
7. Set the value of **Retention method for security log** to **Overwrite events as needed**.
8. Return to the command prompt, type `gpUpdate`, then press **Enter.**

To verify the configuration and ensure Active Directory events are not discarded before processing:

1. Open command prompt, type `eventvwr`, then press **Enter**to start the Event Viewer.
2. Expand **Windows logs**, right-click **Security**, then select **Properties**.
3. Verify that the maximum log size is greater than or equal to 10240 KB (10 MB) and the retention method is set to the value of **Overwrite events as needed**.

Configuring Active Directory auditing

You must configure Active Directory Auditing to ensure that the Active Directory events are logged in the security event log.

Configure the Default Domain Controllers Policy GPO with Audit Directory Service Access set to monitor both success and failure events

To verify or set this configuration:

1. Log in to a computer in the domain you want to configure using a user account with domain administrator privileges.
2. Open command prompt, type `gpmc.msc`, then press **Enter**to start the Group Policy Management Console.
3. Expand **Forest > Domains > domainName > Domain Controllers**.
4. Right-click **Default Domain Controllers Policy**, then select **Edit**.

   

   Note

   Making this change to the default domain controllers policy is important because a GPO linked to the domain controller (DC) organizational unit (OU) with a higher link order can override this configuration when you restart the computer or run gpUpdate again. If your corporate standards do not allow you to modify the default domain controllers policy, create a GPO for your product settings, add these settings to the GPO, and set it to have the highest link order in the Domain Controllers OU.

5. Expand **Computer configuration > Policies > Windows Settings > Security Settings.**
6. Complete the following steps:
   1. In **Security Settings**, expand **Advanced Audit Policy Configuration** > **Audit Policies**.
   2. For ADAAD and ADAGP, click **DS Access**.
   3. For each subcategory, configure or verify the following selections:
      - Configure the following audit events
      - Success
      - Failure
   4. For ADAAD only, define the same configuration for all subcategories of **Account Management** and **Policy Change**.

7. Complete the following steps:
    1. In **Security Settings**, expand **Local Policies** and click **Audit Policy**.
    2. For ADAAD and ADAGP, click **Audit directory service access**.
    3. Configure or verify the following selections:
        - Define these policy settings
        - Success
        - Failure
        - For CGAD only, configure or verify the same selections for Audit account management and Audit policy change.
8. Return to the command prompt, type `gpUpdate` and press **Enter**.

Configuring User and Group auditing

This configuration enables auditing of user logons and logoffs (by both local users and Active Directory users) and local user and group settings. You can configure user and group auditing manually.

To manually configure user and group auditing, complete the following steps.

To configure user and group auditing:

1. Log in to a computer in the domain you want to configure using a user account with domain administrator privileges.
2. Open the Microsoft Management Console, then click **File > Add/Remove Snap-in.**
3. Click **Group Policy Management Editor**, then click **Add**.
4. On the Select Group Policy Object window, click **Browse**.
5. Click **Domain Controllers.FQDN**, where **FQDN** is the Fully Qualified Domain Name for the domain controller computer.
6. Click **Add**.
7. Click **Default Domain Controllers Policy**, then click **OK**.
8. Click **Finish**, then click **OK**.
9. In the Microsoft Management Console, expand **Default Domain Controllers Policy FQDN > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy**.
10. Under **Audit Account Logon Events**, click **Define these policy settings**, then select **Success** and **Failure**.
11. Under **Audit Logon Events**, click **Define these policy settings**, then select **Success** and **Failure**.
12. In the Microsoft Management Console, expand **Default Domain Controllers Policy FQDN > Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Logon/Logoff**.
13. Under **Audit Logon**, click **Audit Logon**, then select **Success** and **Failure**.
14. Under **Audit Logff**, click **Audit Logoff**, then select **Success** and **Failure**.
15. To update Group Policy settings, open a command prompt and type `gpupdate /force`.

Configuring Active Directory Security Access

Control Lists

The Security Access Control List (SACL) describes the objects and operations to monitor. You must configure the SACL to generate events for operations that can result in, or are related to, changes in GPO data stored in Active Directory.

To enable the product to monitor all changes of current and future objects in the Active Directory, see Configuring SACLs for the Product for Active Directory

Configuring SACLs for the product in Active Directory

The Security Access Control List (SACL) describes the objects and operations to monitor. You must configure the SACL to generate events for operations that can result in, or are related to, changes in GPO data stored in Active Directory.If you are running the product for Active Directory in your environment, perform the steps in this section. To enable the product to monitor all changes of current and future objects inside Active Directory, you must configure the domain node.

Note

To use `adsiedit.msc` in Windows Server 2003, you must install the Windows Support Tools. For more information about installing Windows Support Tools, see http://technet.microsoft.com/en-us/library/cc755948%28WS.10%29.aspx.

To verify or set the configuration:

1. Log in to a computer in the domain you want to configure using a user account with domain administrator privileges.
2. Open command prompt, type `adsiedit.msc`, then press **Enter**to start the ADSI Edit configuration tool.
3. Right-click **ADSI Edit**, and then select **Connect to**.
4. In the Connection window, ensure that **Name** is set to `Default naming context`, and **Path** points to the domain to configure..

   

   Note

   You must perform Step 5 through Step 12 three times, configuring the connection points for **Default naming context**, **Schema**, and **Configuration.**

5. In **Connection Point**, click **Select a well known Naming Context**, and then select one of the following:

   - On the first time through this step, select **Default naming context** in the drop-

down list.

- On the second time through this step, select **Schema**.
- On the third time through this step, select **Configuration**.

6. Click **OK**, and then expand **Default naming context** , **Schema**, or **Configuration**.
7. Right-click the node under the connection point (begins with DC= or CN=), then select **Properties**.
8. Click the **Security** tab, then click **Advanced > Auditing > Add**.
9. Perform the following steps to configure auditing to enable monitoring of every user:
    1. (Conditional) For Windows Server 2012, click **Select a principal**.
    2. Specify everyone for **Enter the object name to select**, then click **OK**.
    3. (Conditional) For Windows Server 2012, select **All** for **Type**.
    4. (Conditional) For Windows Server 2012, in the **Permissions** list, select the following:
        - Write All Properties
        - Delete
        - Modify Permissions
        - Modify Owner
        - Create All Child Objects
        - Delete All Child Objects

        

        Note

        When you create or delete child objects, the nodes associated with the child objects are also created or deleted automatically.

    5. (Conditional) For versions of Windows Server other than 2012, In the **Access** list, select **Successful** and **Failed** for the following:
        - Write All Properties
        - Delete
        - Modify Permissions
        - Modify Owner
        - Create All Child Objects

- Delete All Child Objects

Note

When you create or delete child objects, the nodes associated with the child objects are also created or deleted automatically.

10. For **Applies to** or **Apply onto**, select **This object and all descendant objects**.
11. Clear the setting of **Apply these auditing entries to objects and/or containers within this container only**.
12. Click **OK** until you close all open windows.
13. Repeat Step 5 through Step 12 two more times for configuring the connection points for **Schema** and **Configuration** respectively.

Enabling Remote Event Log Management

You must ensure that the Remote Event Log Management rules are enabled to facilitate your product to monitor and process the Active Directory events.

To enable Remote Event Log Management:

1. Log in to a domain controller where you need to enable the Remote Event Log Management service.
2. Open **Control Panel**, select **System and Security**, then select **Windows Defender Firewall** in the middle pane.
3. Click **Inbound Rules**. All the predefined rules are displayed in the middle pane.
4. Look for the **Remove Event Log Management** and **Remote Event Log Management (RPC)** rules and verify that each of them is **Enabled**. If any of the Remote Event Log Management rules is disabled, then right-click the rule, then select **Enable Rule**.

Enabling Remote Procedure Call

The Remote Procedure Call (RPC) service is internally used by multiple Windows services and is set to running by default.

To enable remote traffic, set the firewall by following the steps in the target machine:

- Open Windows Firewall with Advanced Security.
- Navigate to **Inbound Rules** > **Predefined Rules**.
- Select **Remote Event Log Management (RPC)**.

1.1.6. Binding SSL certificates

While creating a self signed certificate, ensure to have the digital signature attribute in the certificate. In case of a CA certificate, ensure to have the SAN attribute for improved security.

Note

During installation of Active Directory Administrator, use a self-signed certificate for REST APIs and the web client. Ensure this certificate is created using PowerShell and is added to the trusted store.

Binding SSL certificates to an IIS Server

To bind SSL certificates to an IIS Server:

1. Open the Internet Information Services Manager (IIS).
2. In the IIS window, under **Connections**, expand your server's name and the required **Sites**.
3. Under **Actions**, click **Edit Site** and then click **Bindings**.
4. Under **Site Bindings** window, select binding for **https** and then click **Edit**.
5. In the **Edit Site Binding** window, enter the following information:

   Table: 1

IP Address	Select **All unassigned** from the drop-down list. If your server has multiple IP addresses, select the one that applies.
Host Name	If you are using Server Name Indication (SNI), enter the host name that you are securing.
Required Server Name Indication	If you are using SNI, select this check box.
SSL Certificate	Select the appropriate certificate from the drop-down list.

6. Click **OK**.

1.2. Installing and verifying

The product runs on Windows and is installed using the Windows installer. This section provides the steps for installing the product and verifying the installation.

- Installing the product
- Verifying the installation

1.2.1. Installing the product

1. Log in to the Microsoft Windows server where you need to install the product.

   

   Important

   Ensure that you have downloaded the installation kit (ADASuiteInstallationKit.zip) to the server and your windows account has domain administrative privileges to install the product.

2. Navigate to the downloaded location of the **ADASuiteInstallationKit.zip** file and extract the file.

3. Run the Setup.exe to start the installation.

   

   Note

   In case of the default path installation the logs can be found at **C:\Programdata\OpenText** folder.

4. Click **Next** to continue with the installation.

5. In the **Prerequisite List** screen, click **Install** against each of the prerequisites that have not been installed already, then click **Next**. You cannot proceed further without installing all the prerequisites.

Note

The following are the considerations for prerequisites:

- When you click **Install**, the prerequisites are installed from the `Prerequisites` folder in the installation kit.
- To know more about the prerequisites, click **Show Report**.
- To know the installation status of the prerequisites, click **Refresh** or click **Show Report** and view the **Result** column in the report.
- To install Microsoft IIS, click **Details** and follow the instructions given in the Prerequisites report.
- For the installation of the Microsoft .NET Framework, you are prompted to close the wizard. After the installation of the framework is complete, relaunch the wizard by performing steps 2 and 3 again, and then follow the instructions in the wizard till you arrive at the **Prerequisite List** screen.
- If you have installed Microsoft ASP.NET Core after installing Microsoft IIS, the status of Microsoft ASP.NET Core is not updated to indicate that the installation is successful, even after you click **Refresh**. In this case, close the wizard, relaunch the wizard by performing steps 2 and 3 again, and then follow the instructions in the wizard till you arrive at the **Prerequisite List** screen. The status of Microsoft ASP.NET Core is updated.
- If the status of Microsoft ASP.NET Core does not change or reflect, restart the machine.

6. Read and accept the terms in the End User License Agreement, then click **Next**.
7. Do one of the following to specify the installation folder:
   - Click **Next** to install the product in the default location of: `C:\Program Files\Active Directory Administrator Suite\`.
   - Click **Change** and choose another location, then click **Next**.
8. Specify the group account names for the Admin and CISO roles.

Important

Consider the following:

- Ensure that the group names you provide during installation match the Admin and CISO group names that you have provided in the Active Directory where you have also added the identified users to any or both the groups.
- Only those groups that have Domain local as their group scope and Security as their group type are supported.

9. Specify unique ports in the range of 50000-63335 for the Active Directory Administrator services to use, then click **Next**.
10. Do one of the following to specify the cache data location for the Active Directory Administrator cache service:
    - Click **Next** to cache the data in the default location of: `C:\ProgramData\OpenText\ADA\CacheDB\`.
    - Click **Browse** and choose another location, then click **Next**.
11. Select an SSL certificate for the REST Service, then click **Next**.

Note

The **REST Service SSL Certificate** field lists certificates from both the WebHosting store and Personal store.

12. In the **Active Directory Administrator Web Console Wizard**, ensure to select the option **Use an existing SSL Certificate**. An existing SSL certificate that is bind to IIS will be displayed. For more information on how to create the certificate and bind it to IIS, see the section Binding SSL Certificate to IIS Server under Creating Self-Signed Certificate. Then click **Next**.

Note

The existing SSL certificate list contains certificates from both the WebHosting store and Personal store.

13. Review your installation settings before you begin with the installation, then click **Install**.
14. Wait till the installation is complete, then click **Next**. The product is successfully installed.
15. Click **Finish** to exit the wizard.

1.2.2. Verifying the installation

Post install, you need to verify that your installation is successful.

To verify the installation:

1. In a web browser, specify the following URL to access the UI of the product:

   `https://<FQDN>/adminsuiteclient`, where FQDN is the fully-qualified domain name of the product. The Login page is displayed.

2. Enter your credentials by providing your user name and password, and then click **Log in**. Any of the following screens is displayed:

   - If you are a user with the Admin role, the Domain Configuration page in the **Configuration** tab is displayed.
   - If you are a user with the CISO role, the Overview page in the **Overview** tab is displayed.
   - If you are a user not assigned to any of the product roles, you cannot log in to the product.
   - While logging in to the **UI**, if it shows the “Something went wrong (502)” **error**, then restart the machine where the ADA is installed.

opentext™

For more info, visit https://docs.microfocus.com