OpenText™ Active Directory Administrator

Administer

Version : 1.0

PDF Generated on : 30/04/2025

Table of Contents

1. Administer

The *Administrator Guide* provides planning, installation, configuration, and administration information of the Active Directory Administrator.

Intended audience

This book provides information for users who are responsible for the installation of the Active Directory Administrator and Admin group users who are responsible for administering the Active Directory Administrator.

Additional documentation

The Active Directory Administrator documentation library includes the following resources:

User Guide

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

Release Notes

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

System Requirements Guide

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

This guide is part of the Directory and Resource Administrator documentation set. For the most recent version of this guide and other DRA 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. Configuring the product

After installing the Active Directory Administrator, you need to manage the domain so that it can connect to the Active Directory and start collecting and monitoring the service accounts and their activities on their domains.

1.1.1. Establishing connection with the Active Directories

As a first step in using the product, you need to perform some configurations in it to enable it to connect to and monitor the Active Directory. You establish the connection by configuring domains of an active directory in your product. Along with the domains, you must also provide a pattern for the discovery of the service accounts of the domains.

Configuring Domains and Service Accounts

To configure domains and their service accounts:

1. Log in to the product UI as an Admin group user. If no domains exist, the Domain Configuration page in the **Configuration** tab is displayed.

   > **Note**
   >
   > When one or more domains have already been configured in the product, a visual representation of the service accounts of the first configured domain is displayed in the **Overview** tab. Click **Configuration** in the top pane to navigate to the Domain Configuration page.

2. Click **Add Domain**.

3. Specify the domain details, then click **Test Connection**. When you specify the domain details, select the **Is SSL** check box if the connection to the domain is LDAPS-enabled.

   If you have provided the correct domain details and the domain is up and running, the testing of the connection is successful. If you have provided incorrect domain details or if the domain is not up and running, you get an error message. Depending on the error message displayed, either provide the correct domain details or wait till the domain is up and running and test the connection again.

4. Specify the details for the service account discovery:

   - Select the class, for example, Server, Client, or Both of systems to connect to that will be used to discover the service accounts configured as login accounts for the Windows services, and provide the user credentials to connect to the selected class of systems.

   - To discover service accounts based on a pattern, select **Discovery Pattern**, then specify the pattern and the property.

5. Click **Save**. The domain is added and the details are displayed, along with the machines that serve as the domain controllers.

Updating Domain and Service Account discovery details

To update domain details and the service account discovery details:

1. In the Domain Configuration page of the **Configuration** tab, select the required domain from the list of domains or specify the domain you need to update and then click the domain. The domain details along with the domain controllers are displayed in the right pane.

2. To edit the domain details, click the Edit icon, then update the details and click **Save**.

3. To change the default domain controller, click the **Domain Controller** tab, then click the ... for the domain controller that you need to set as default, and then select **Mark as Default**.

4. To edit the discovery details of the service accounts of the domain, click **Service Account Discovery**, then update the details, and then click **Save**.

Deleting Domains

To delete a domain:

1. In the Domain Configuration page of the **Configuration** tab, select the required domain from the list of domains or specify the domain you need to delete.

2. Click the ... corresponding to the domain you need to delete, then select **Remove Domain**.

1.2. Monitoring Domain activities

This section provides information about monitoring the activities of service accounts of a domain.

- Viewing Domain and Service Account discovery details
- Monitoring Service Accounts

1.2.1. Viewing Domain and Service Account discovery details

To view domain and service account discovery details:

1. Log in to the product UI as an Admin group user. A visual representation of the service accounts corresponding to the first domain configured in the product is displayed in the **Overview** tab.

   Note

   If no domains exist, the Domain Configuration page in the **Configuration** tab is displayed. Ensure that you add a domain to view its details.

2. Click **Configuration** in the top pane to navigate to the Domain Configuration page.
3. In the Domain Configuration page, select the required domain from the list of domains or specify the domain and then click the domain. The domain details along with the domain controllers are displayed in the right pane.
4. To view the discovery details of the service accounts of the domain, click **Service Account Discovery**.

1.2.2. Monitoring Service Accounts

For a domain, the product provides a visual snapshot of the service accounts and their activities. You can gather important information on the behaviors and the security standing of the service accounts such as the service accounts have been involved in any suspicious activities, they have not been in use for long, and their password is about to expire. You can then take appropriate actions based on the data that is displayed to you.

To view and monitor service accounts of a domain:

1. Log in to the product UI as an Admin group user.
2. Click **Overview** in the top pane. By default, a visual representation of the service accounts corresponding to the first domain configured in the product is displayed in the **Overview** tab.
3. Select the domain whose service accounts you need to monitor in the left pane.

A visual representation of the service accounts and their activity is displayed. By default, the accounts' activity for the last 15 days is displayed. You can select the time period for which you need to view the accounts' activity.

Insights provided by graphs

The following aspects of the visual representation help provide insights into the behaviors of the service accounts:

- Service Account Activity Overview
- Top Accounts by Activity
- Service Account Password Expiration Status
- Service Accounts
- Service Account Details for Monitoring

Service Account Activity Overview

For the selected time period, the **Service Account Activity Overview** section, represented as a pie chart, provides a broad, statistical view of the number of service accounts that have engaged in activity and the number of service accounts that have not engaged in any activity. When you click any section in the pie chart, the corresponding accounts are displayed in the Service Accounts section.

Top Accounts by Activity

For the selected time period, the **Top Accounts by Activity** section provides a graphical view of the top service accounts that have engaged in maximum activity (number of modifications made to a service account or the number of modifications the service account has made to the user objects of the Active Directory). A maximum of 10 top service accounts can be displayed.

Service Account Password Expiration Status

The **Service Account Password Expiration Status** section provides a snapshot of the password expiration status of all the service accounts of the domain. The status displayed is for the present time, irrespective of the time period you select. An overall view of the password expiration status in the domain helps you understand how many service accounts need attention for renewal of their passwords.

Service Accounts

For the selected time period, the **Service Accounts** section displays a summary of all the service accounts in the domain. This summary helps you in gaining a broad view of the account details in the selected time range. For each service account, the following details are displayed as part of the summary:

- **Account Name:** The name of the service account.
- **Domain Name:** The child domain to which the service account belongs.
- **Services:** The number of services that run using the service account.
- **Modifications:** The number of changes the service account has made to the objects of the Active Directory or the number of changes that have been made to the service account.
- **Password Status:** Information on whether the service account password has expired, is still active, and so on. This information enables administrators to take timely actions on updating the passwords of the service accounts.
- **Password Expiration Date:** The date when the password expires or has expired. This information along with the information on modifications helps administrators understand if a service account has not been in use for long and is at a risk of being compromised.

There is also a provision to list a specific service account name along with its summary, hide or show the details for the service accounts that need to be displayed, and export the listed service accounts along with their details.

Service Account Details for monitoring

When you click a service account from the list, the **Service Account Details** window is displayed, which provides further insights into the service account. The following details are displayed:

- The manager of the service account.
- The password expiration date and an option to notify the account manager and other key members on the password renewal action..
- An option to notify the service account manager and other key members through email on the password expiration status of the service account.
- The names of the services with which the service account is associated. This information helps in easily identifying which services need to be reconfigured whenever the service account password is updated.
- For the defined period, the activity of the account. All the changes done to the service account and the changes done by the service account are listed in the **Changes Done To Service Account** and **Changes Done By Service Account** tabs respectively. Every change is captured as a single event.
- On the click of an event in any of the tabs, in-depth information on the change is displayed that will help administrators determine if the change is of a suspicious nature and the account deserves attention. You can view the following details:
    - **Overview**: The **Overview** section provides a summary of the initiator of the change and a summary of the change, including the target of the change.
    - **Delta**: The **Delta** section provides a list of the attributes of the target that have been modified in the Active Directory, along with their original and modified values.
    - **All Event Fields**: The **All Event Fields** section provides a list of all the fields of the event, along with their values.

There is also a provision to list a specific event, hide or show the details for the events that need to be displayed, and export the listed events along with their details.

1.3. Archiving audit data

Archiving of audit data is essential as it reduces the primary storage consumption and helps in retaining only the limited data for active use.

Prerequisites:

- The archiving scripts are present in the following install path: **\Active Directory Administrator\Scripts\Audit Archive Data**
- Complete the following configuration before executing the archiving script present in the Install path. This will provide the user with the privilege of running the script.

  Navigate to your custom **CacheDB** folder or the default path **ProgramData** > **OpenText > ADA** > **CacheDB** > **data** > **pg_ident.conf**. Add a new line under the **MapforSSPI** option and specify your system username and domain.

  For example: `MapforSSPI "administrator@opentext.com" postgres`

To archive audit data:

- Open Windows PowerShell.
- Navigate to the `Audit Data Archive` folder.
- Execute the following script:

  `.\DBArchive.ps1`

- Once prompted, set the number of days to retain the data in the active table. The data for the specified number of days will be retained and the rest of the data will be archived. For example, if you set **30** as the number of days, the data of past 30 days will be retained and the older data will be archived.

opentext™

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