OpenText™ Active Directory Administrator

Use

Version : 1.0

PDF Generated on : 30/04/2025

Table of Contents

1. Use

The *User's Guide* provides information about the tasks the users can perform in the Active Directory Administrator web console.

Intended audience

This book provides information for the following:

- **Chief Information Security Officers (CISOs)**: Responsible for monitoring domains, their service accounts, and their activities.
- **Admin Group Users**: Responsible for the administering the product and conducting tasks such as configuring, updating, deleting domains and updating their service account discovery details.

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.

Installation and Administrator's Guides
Provides information about the installation and administration of the Active Directory Administrator.

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. Introduction

In any organization having a Windows environment, services, applications, and programs need appropriate permissions to run on the operating systems. This is achieved with the help of service accounts in the organization.

Service accounts in Active Directory (AD) are special types of user accounts that are specifically created and used by applications, services, or operating systems to interact with other network services. They are designed to provide a secure and controlled way for these entities to access network resources without using the credentials of individual users. Service accounts are assigned special permissions to perform critical operations in the organization, including changes to the Active Directory. Service accounts are, therefore, an integral part of any organization. So, it is essential to manage and monitor them. However, the following are some challenges in managing service accounts:

- Service accounts can exist and run on any number of client machines, server machines, and domain controllers in the organization's domain. Therefore, manually monitoring the details and activities of service accounts is a tedious process.
- When a service account password expires or is changed, the services, applications, and programs dependent on the service account stop functioning till they are reconfigured with the new password. If the administrators do not have information on where a service account is used, then, manually checking every machine and application that uses the service account and updating the application with the new password is time-consuming and susceptible to errors. Setting a service account to never expire, increases the chances of the account being compromised.
- Service accounts are typically created for the purpose of executing services in most of the environments and these accounts exclude any user-related function. Hence, there might be instances that the service accounts are overlooked in terms of management.

Because of these challenges, the task of managing service accounts in organizations is often not conducted, paving the way for security attacks.

Active Directory Administrator as a solution helps overcome these challenges.

The OpenText Active Directory Administrator is a powerful solution that provides a visualization of the service accounts and their activity, including changes to the Active Directory, and the activities done by the service account in an organization. This helps administrators gain insights into how robust their organization is against security threats and take necessary actions to preempt potential threats.

1.2. Understanding the product

The Active Directory Administrator, as a product, is a solution to monitor the service accounts and their activities in the domain, thereby assisting the admin to take a corrective action.

The following section describes the terms and entities used in the context of the product:

- **Domain:** In the context of computer networking and Active Directory, a domain refers to a group of network resources such as computers, users, and printers that share a common directory database and security policies. A domain is typically controlled by a centralized server known as a domain controller, which manages authentication, authorization, and other network services within the domain.
- **Service Account:** A service account is a non-user account that is created in the Active Directory. It is associated with one or more windows services, enabling them to run on the windows operating systems. It establishes their access and permission levels to the local and network resources, including the Active Directory.
- **Services:** In the context of computing, ‘services’ refer to software programs or processes that run in the background and provide specific functionality to users or programs. Services are often designed to operate continuously, without direct user interaction, and they can perform a wide range of tasks, such as handling network communication, managing system resources, or executing scheduled tasks.
- **Service Account Activity:** Activity of a service account refers to the account managing the objects of the Active Directory or modifications being made to the account.
- **Service Account without Activity:** A service account without activity indicates that it has not made any modifications to the user objects of the Active Directory and that modifications have not been made on the service account.
- **Service Account Modifications:** Service account modifications refers to the number of modifications that it does to the user objects of the Active Directory or the number of modifications done to the service account.

1.2.1. Roles and responsibilities

Getting started as the Admin

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: This includes tasks such as configuring, updating, deleting domains and updating their service account discovery details.
- Monitor 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.

Getting started as the Chief Information Security Officer (CISO)

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.
- 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.

1.2.2. Functions of the product

The following section describes the functions of the product and how the product helps the Active Directory administrators of an organization:

- **Configuring domains and service accounts:** It enables administrators to add domains and child domains, and enable the discovery of their service accounts.
- **Discovering service accounts:** It enables the administrators and the Chief Information Security Officers (CISOs) to get a list all the service accounts in a domain. It also provides a visual representation of the service accounts and their activity in a domain.
- **Configuring domains and discovering their service accounts:** It enables the configuration of domains and the discovery of their service accounts. The discovery of service accounts enables the product administrators and the Chief Information Security Officers (CISOs) to get a list of all the service accounts in a domain. The product also provides a visual representation of the service accounts and their activity in a domain.

  Note

  Only an Admin group user can configure domains and enable discovery of their service accounts.

- **Monitoring service account activity:** It helps the product administrators and CISOs track the services running through a service account or a service account itself making any changes to the user objects of the Active Directory, such as adding a new user account, granting privileges to service accounts, changing user account credentials, and changing user properties are also captured as an activity of the service account. This enables the product administrators and CISOs to quickly identify changes and determine any suspicious activity on the users and groups in the Active Directory. This search happens in the current data page that is being displayed and is only applicable to even's grid. In addition, the product also provides the following functions:
  - **Viewing service account details:** It provides information such as the machines where a service account is installed and the services with which the account is associated. This makes it easier for administrators to know where a service account is used so that when the account's password is changed, all the places where the account is used can be reconfigured with the new password seamlessly.
  - **Monitoring service account passwords and identifying service accounts not performing any activities:**
    - It provides a snapshot of the password expiration status of the service accounts of a domain. It also lists the password expiration date of each of the service accounts. This feature helps administrators in identifying service accounts that have not been in use for long and taking appropriate actions.

- It helps administrators in determining the last activity related to a service account to understand if the account has become obsolete and poses a risk of being compromised.

1.3. Monitoring Service Accounts

For a domain, the product provides a visual snapshot of the service accounts and their activities. As a CISO group user, you can gather important information on the behaviors and the security standing of the service accounts such as if 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 a CISO 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.

1.3.1. Insights provided by the Overview Dashboard

The **Overview** dashboard provides a holistic view of service accounts and details related to the accounts.

Service Account 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

The Top Accounts by Activity is a graphical chart that displays the service accounts and the number of modifications the accounts have gone through, for the selected time period. The vertical axis shows the names of the service accounts and the horizontal axis displays the 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.

When you click a bar, you will be directed to the Service Account Details dashboard and the selected service account is highlighted.

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.

The pie chart categorizes and displays the service accounts as **Expired**, **Expiring in 7 days**, **Expiring after 7 days and within 15 days**, and **Expiring after 15 days**.

Service Accounts

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

- **Account Name:** The name of the service account.
- **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.
- **Email Notification:** An option to notify the service account manager through email on the password expiration status of the service account.

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, hide or show the details for the service accounts that need to be displayed, and export the listed service accounts along with their details. When you click an **Account Name**, you will be directed to the **Service Account Details** dashboard.

Service Account details for monitoring

The **Service Account Details** window provides detailed insights into the service accounts. The following details are displayed:

- The name and the manager of the service account.
- The password expiration date and an option to notify the account manager on the password renewal action.
- The password expiration date and an option to notify the account manager and other key members on the password renewal action.
- 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.
- 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. Service account details are listed as **Event Name**, **Initiator User Name**, **Target Data Container**, **Target Host Name**, and **Event Time**.
- On the click of an event in any of the tabs, a window appears which displays in-depth information about the modification 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. It also displays what the change was and where was it implemented.
    - **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, hide or show the details for the events that need to be displayed, and export the listed events along with their details.

opentext™

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