Active Directory Integration

FortiEDR 7.0.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

April 30, 2025
FortiEDR 7.0.0 Active Directory Integration
63-700-1154339-20250430

TABLE OF CONTENTS

Change log

Date	Change Description
2025-04-30	Initial document release.

Overview

With the integration of FortiEDR and Active Directory, when a security policy assigned to a FortiEDR-protected endpoint triggers the “Reset user password” and “Disable user account” Automated Incident Response (AIR) playbooks, FortiEDR sends an API update to the Active Directory server and automatically resets the user password or disables the user account to prevent further misuse of the compromised account.

After the security incident is resolved and the affected endpoint becomes compliant, the administrator must manually re-enable the account.

Prerequisites

Before you start configuring the integration with Active Directory, verify the following:

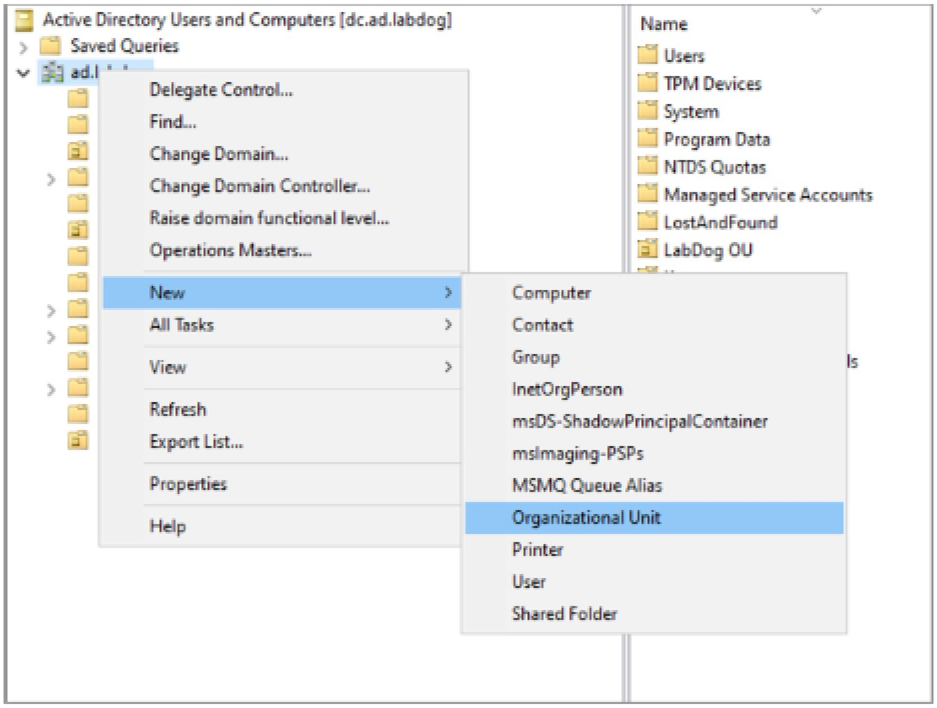
- Your FortiEDR deployment includes a Jumpbox that has connectivity to the Active Directory server.
  - Refer to Installing the FortiEDR Core for details about how to install a FortiEDR Core and configure it as a Jumpbox.
  - Refer to Cores for more information about configuring a Jumpbox.
- The FortiEDR Central Manager has connectivity to the Fortinet Cloud Services (FCS). To verify this, make sure that FCS is in running state (Green) in the *System Components* chart in the Dashboard of the FortiEDR management console.

Configuring Active Directory

To integrate FortiEDR with Active Directory, you must first create an Active Directory admin user with the correct organization, group, and permissions to reset the user password or disable the user account. Fortinet recommends that you create a dedicated Active Directory admin user for FortiEDR integration.

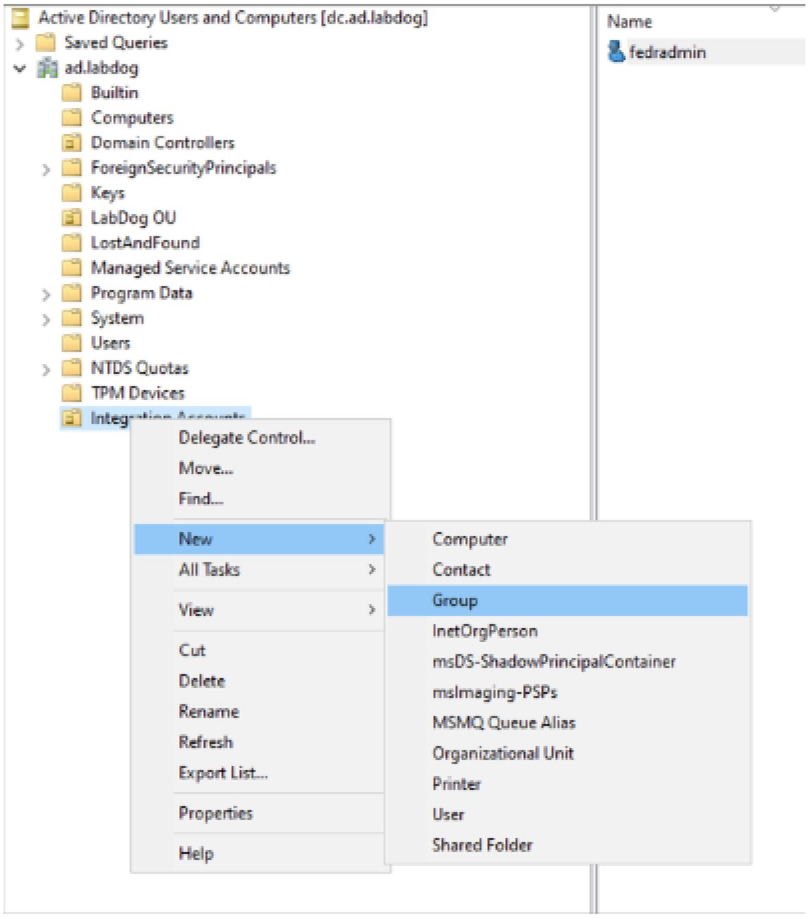
To create an Active Directory admin user for FortiEDR integration:

1. Click *Start* > *Administrative Tools* > *Active Directory Users and Computers*.
2. Right-click the domain and select *New* > *Organization Unit*.

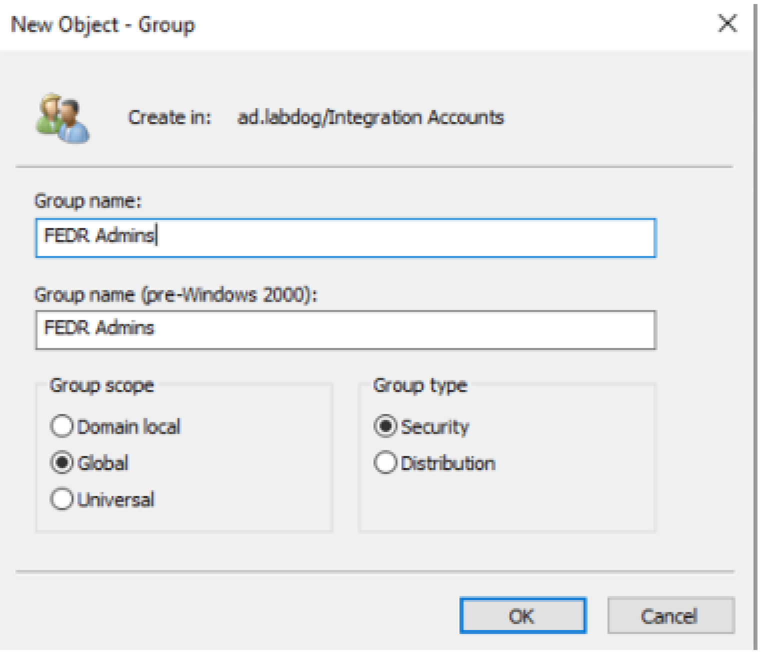


3. Specify the name for the organization unit and save it.

4. Right-click the newly created organization unit and select *New* > *Group*.



5. Configure the basic settings for the group (see example below).



New Object - Group

Create in: ad.labdog/Integration Accounts

Group name: FEDR Admins

Group name (pre-Windows 2000): FEDR Admins

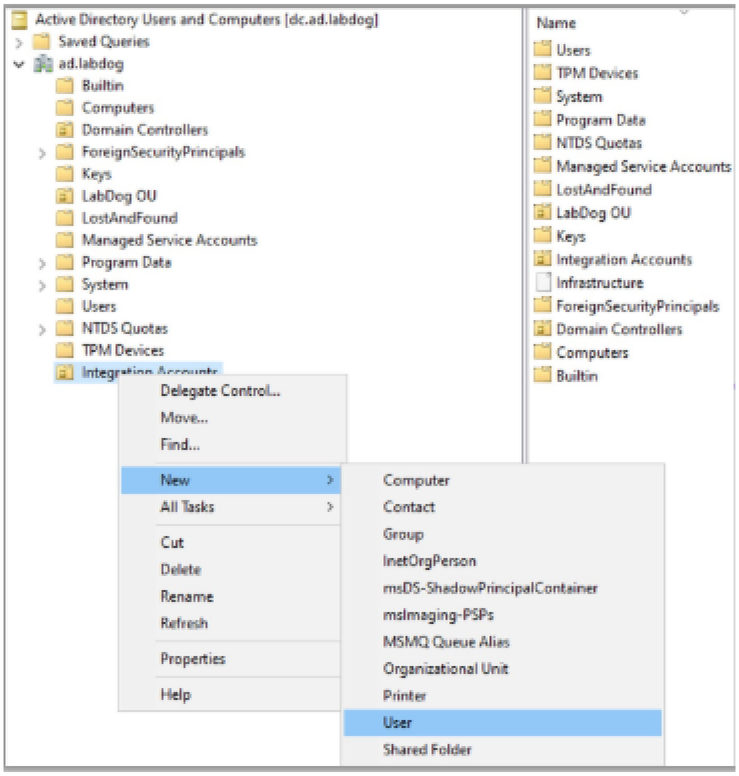
Group scope

○ Domain local
● Global
○ Universal

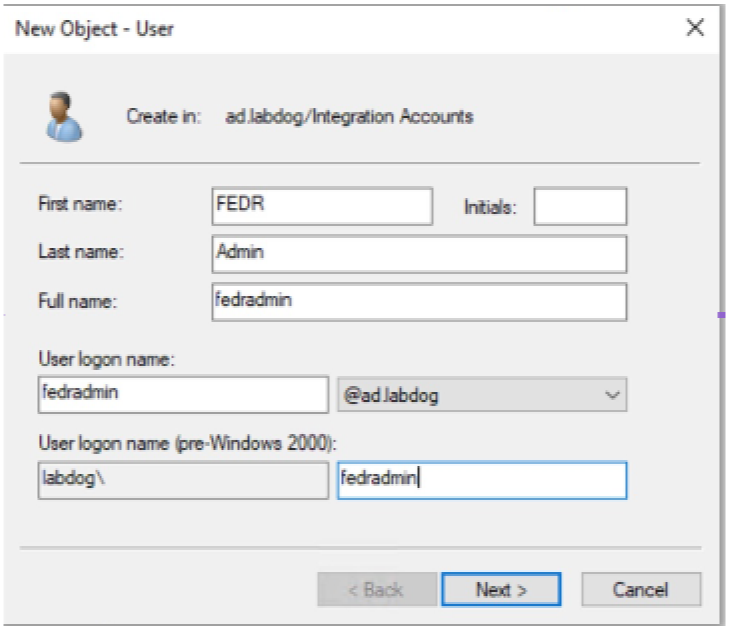
Group type

● Security
○ Distribution

6. Right-click the newly created organization unit and select *New* > *User*.



7. Configure the basic settings for the user (see example below) and click *Next*.



New Object - User

Create in: ad.labdog/Integration Accounts

First name: FEDR

Initials:

Last name: Admin

Full name: fedradmin

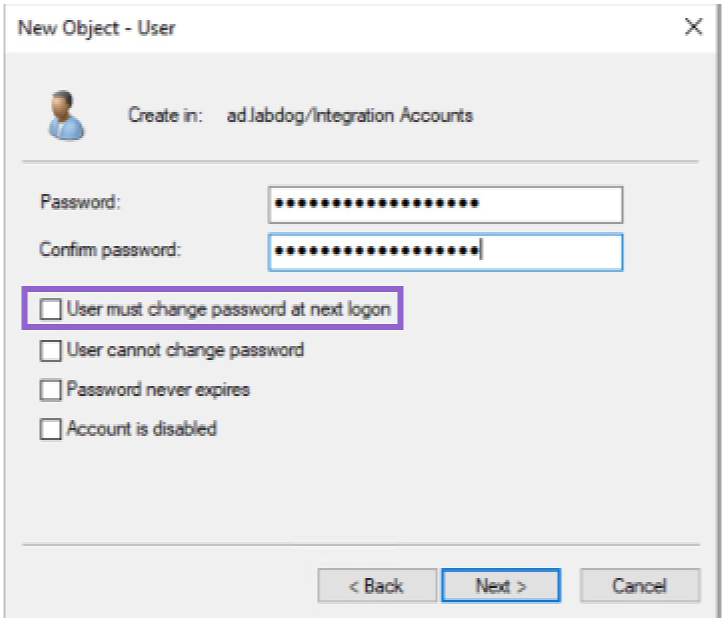
User logon name:

fedradmin @ad.labdog

User logon name (pre-Windows 2000):

labdog\ fedradmin

8. Define the password for the user, disable the *User must change password at next logon* option, click *Next* and then *Finish*.



New Object - User

Create in: ad.labdog/Integration Accounts

Password: ••••••••••••••••••

Confirm password: ••••••••••••••••••

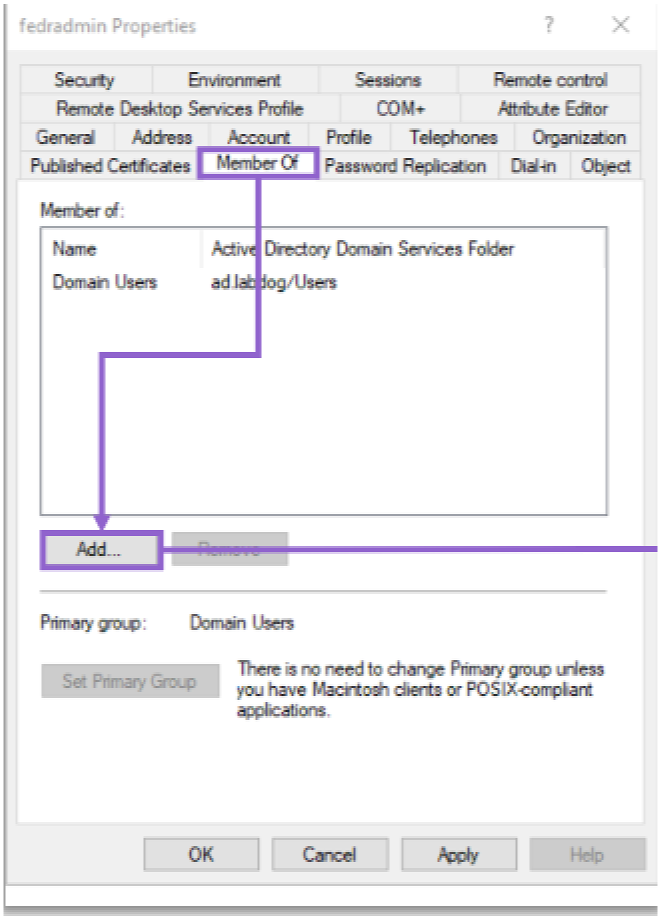
□ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

9. Double-click the user you just created to open the *Properties* window.
10. In the *Member Of* tab, click *Add*.



fedradmin Properties

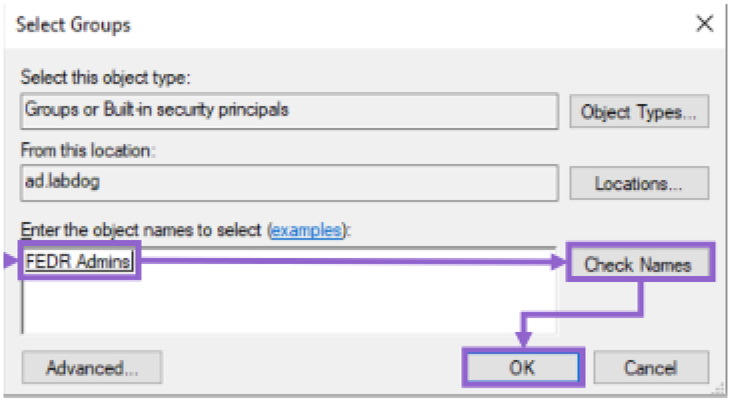
Member of:

Name	Active Directory Domain Services Folder
Domain Users	ad.labdog/Users

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

11. Type the name of the group you just created, click *Check Names to verify* and then click *OK*.

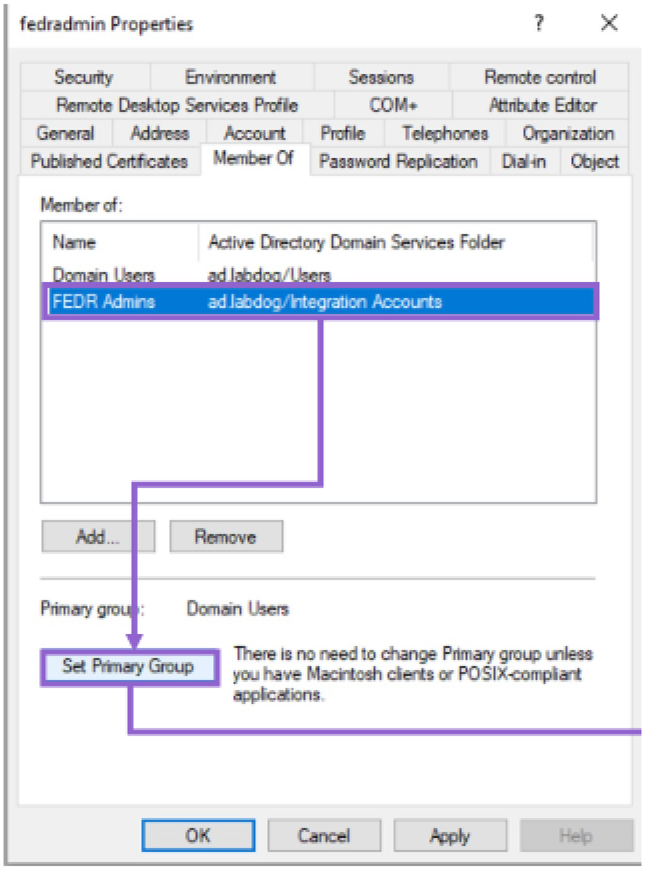


Select this object type:
Groups or Built-in security principals

From this location:
ad.labdog

Enter the object names to select (examples):
FEDR Admins

12. Select the the assigned group and click *Set Primary Group*.



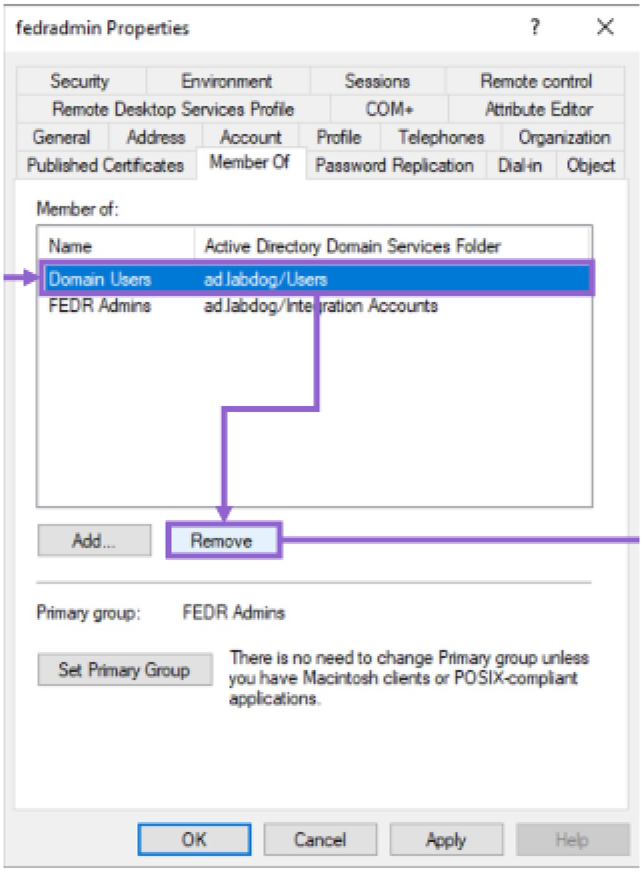
Member of:

Name	Active Directory Domain Services Folder
Domain Users	ad.labdog/Users
FEDR Admins	ad.labdog/Integration Accounts

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

13. Select any other groups assigned to the user and click *Remove*.



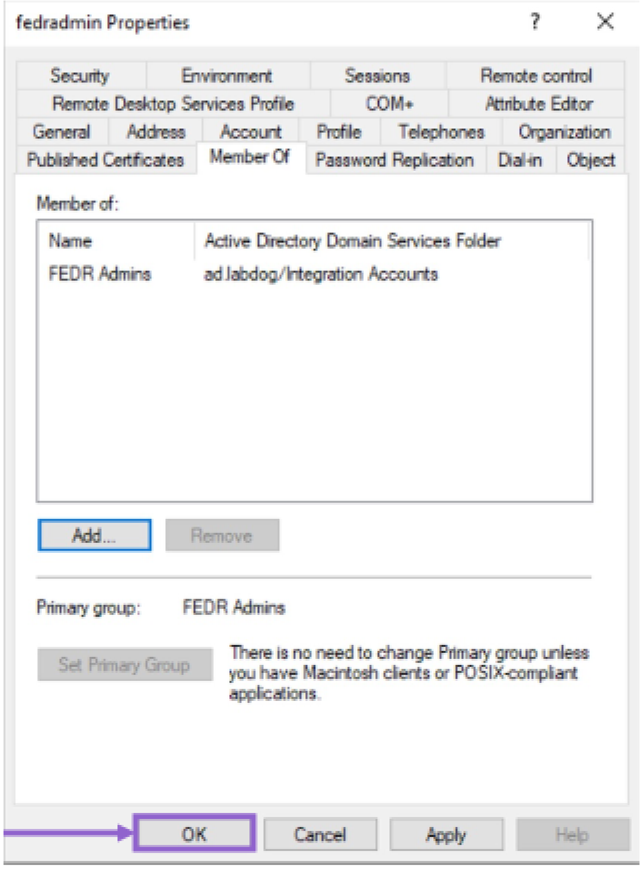
Member of:

Name	Active Directory Domain Services Folder
Domain Users	ad.labdog/Users
FEDR Admins	ad.labdog/Integration Accounts

Primary group: FEDR Admins

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

14. Click *OK* to save the changes.



Member of:

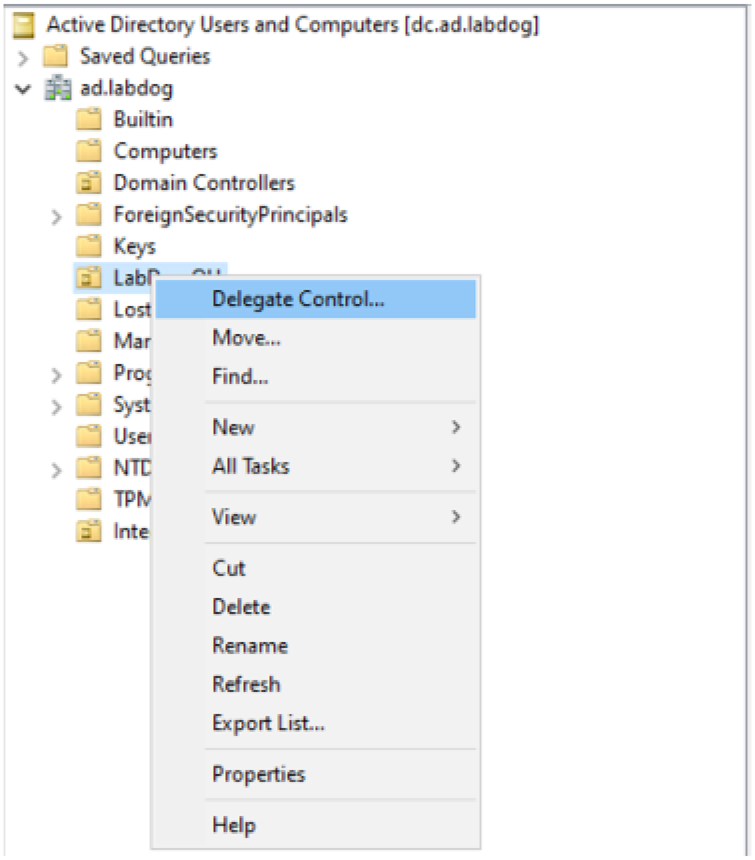
Name	Active Directory Domain Services Folder
FEDR Admins	ad.labdog/Integration Accounts

Primary group: FEDR Admins

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

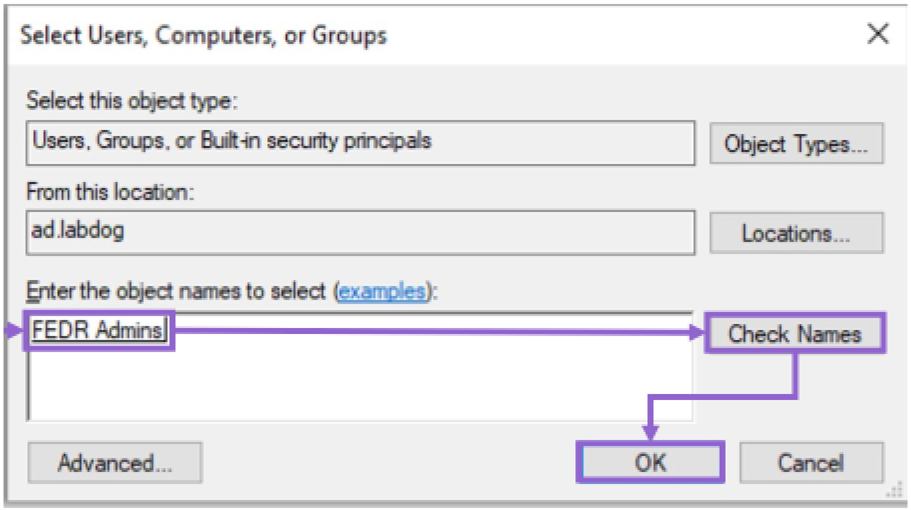
15. Click *Save*.
16. Configure the target organizational unit or container so that FortiEDR has delegated permissions to reset passwords and disable accounts:

a. Right-click the organization unit or container and select *Delegate Control*.



b. Click *Next* and then click *Add*.

c. Enter the name of the group that you created earlier, click *Check Names*, and then *OK*.

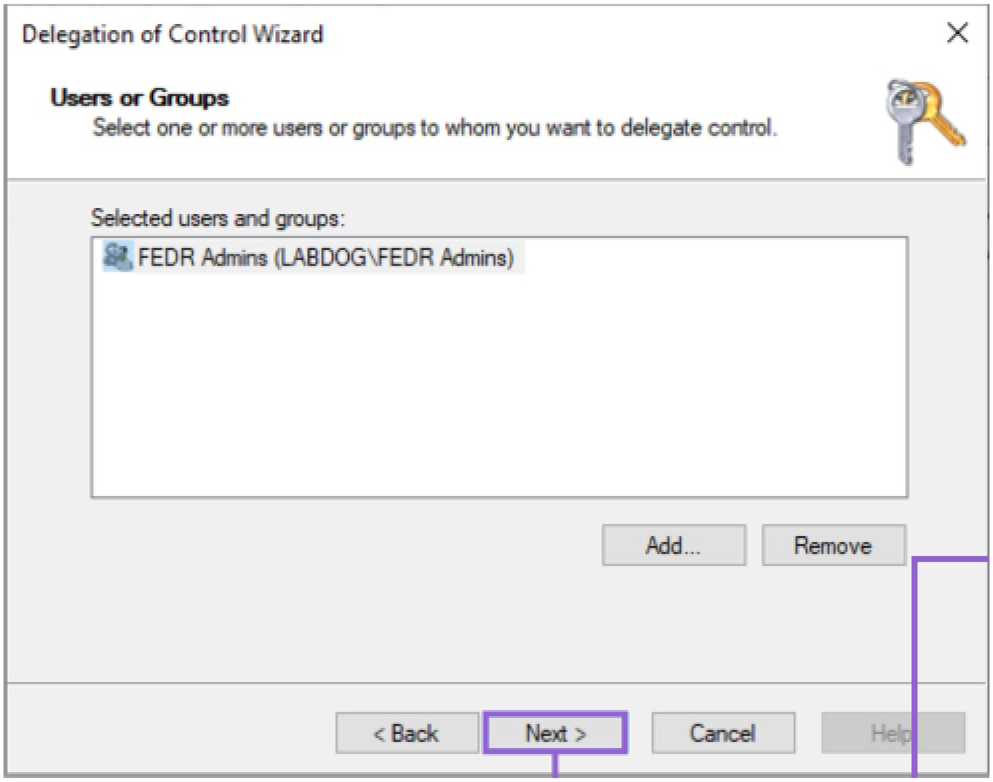

Select Users, Computers, or Groups

Select this object type:
Users, Groups, or Built-in security principals

From this location:
ad.labdog

Enter the object names to select (examples):
FEDR Admins

d. Verify the selected group and click *Next*.



Delegation of Control Wizard

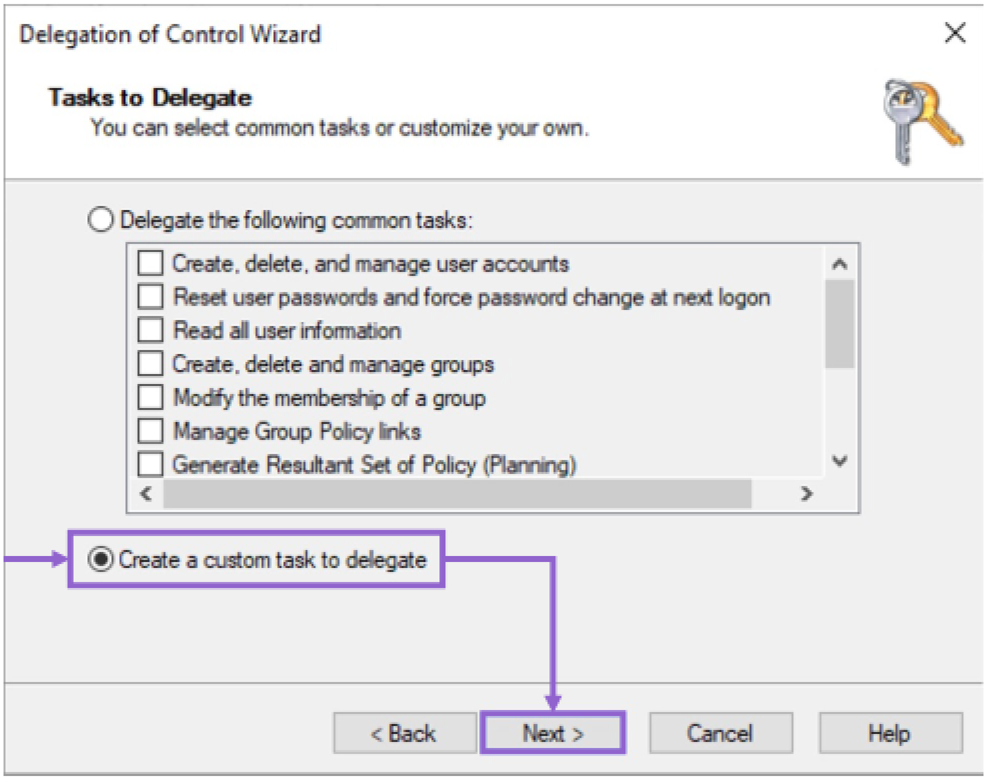
Users or Groups

Select one or more users or groups to whom you want to delegate control.

Selected users and groups:

FEDR Admins (LABDOG\FEDR Admins)

e. Select *Create a custom task to delegate* and click *Next*.



Delegation of Control Wizard

Tasks to Delegate

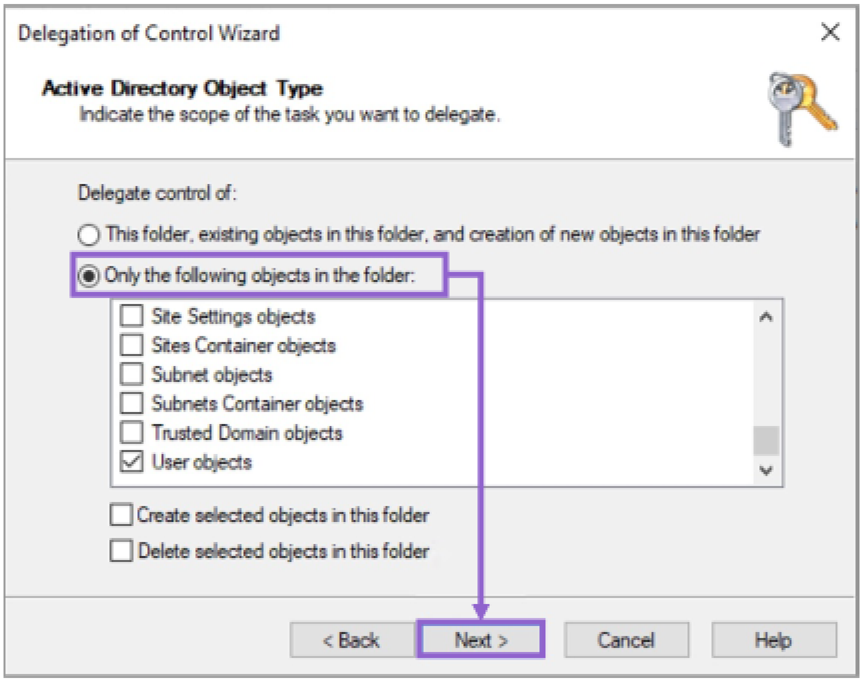
You can select common tasks or customize your own.

○ Delegate the following common tasks:

- □ Create, delete, and manage user accounts
- □ Reset user passwords and force password change at next logon
- □ Read all user information
- □ Create, delete and manage groups
- □ Modify the membership of a group
- □ Manage Group Policy links
- □ Generate Resultant Set of Policy (Planning)

● Create a custom task to delegate

f. Select *Only the following objects in the folder*, select *User objects*, and then click *Next*.



Delegation of Control Wizard

Active Directory Object Type

Indicate the scope of the task you want to delegate.

Delegate control of:

○ This folder, existing objects in this folder, and creation of new objects in this folder

● Only the following objects in the folder:

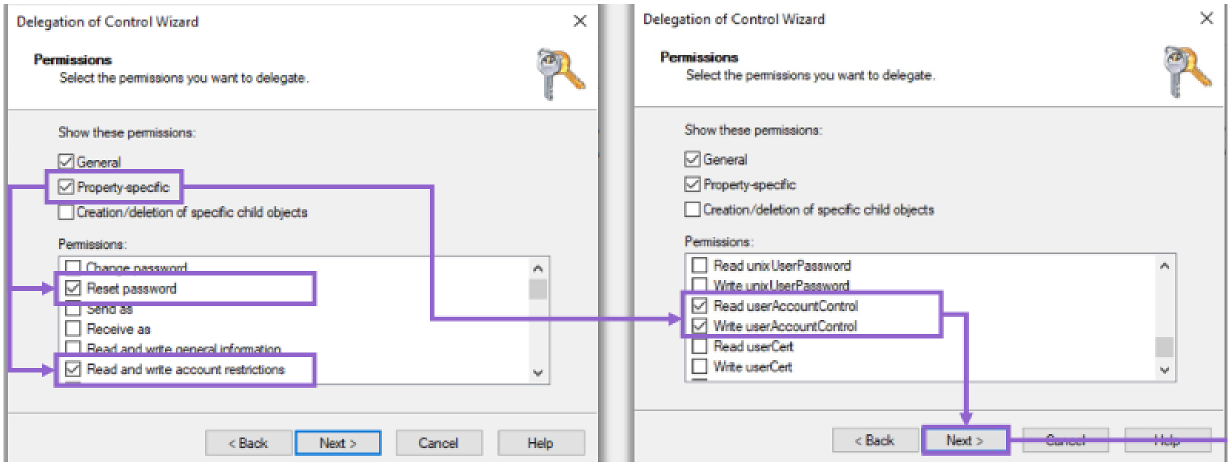
- □ Site Settings objects
- □ Sites Container objects
- □ Subnet objects
- □ Subnets Container objects
- □ Trusted Domain objects
- ☑ User objects

□ Create selected objects in this folder

□ Delete selected objects in this folder

g. Select *Property-specific* under *Show these permissions*, select the following permissions, and click *Next*:

- *Reset Password*
- *Read and write account restrictions*
- *Read userAccountControl*
- *Write userAccountControl*



Delegation of Control Wizard

Permissions

Select the permissions you want to delegate.

Show these permissions:

☑ General

☑ Property-specific

□ Creation/deletion of specific child objects

Permissions:

- □ Change password
- ☑ Reset password
- □ Send as
- □ Receive as
- □ Read and write general information
- ☑ Read and write account restrictions

Delegation of Control Wizard

Permissions

Select the permissions you want to delegate.

Show these permissions:

☑ General

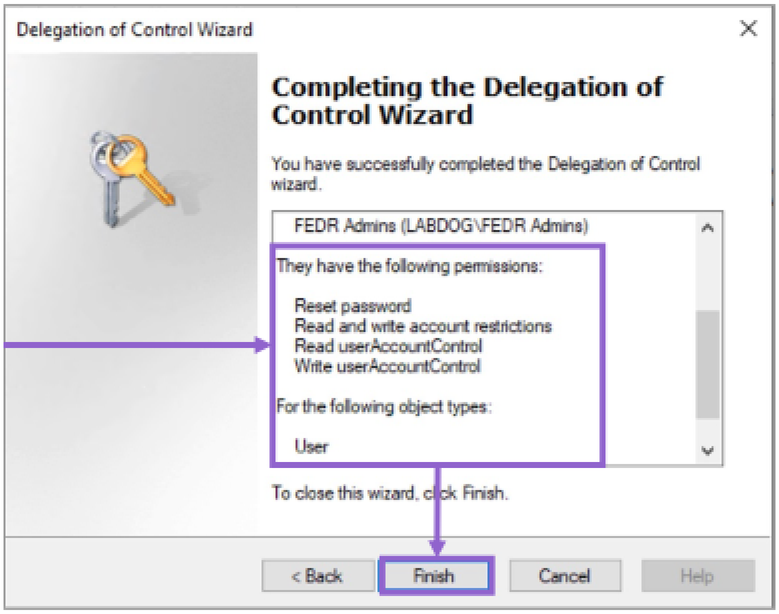
☑ Property-specific

□ Creation/deletion of specific child objects

Permissions:

- □ Read unixUserPassword
- □ Write unixUserPassword
- ☑ Read userAccountControl
- ☑ Write userAccountControl
- □ Read userCert
- □ Write userCert

h. Verify the permissions list and click *Finish*.



Delegation of Control Wizard

Completing the Delegation of Control Wizard

You have successfully completed the Delegation of Control wizard.

FEDR Admins (LABDOG\FEDR Admins)

They have the following permissions:

Reset password
Read and write account restrictions
Read userAccountControl
Write userAccountControl

For the following object types:

User

To close this wizard, click Finish.

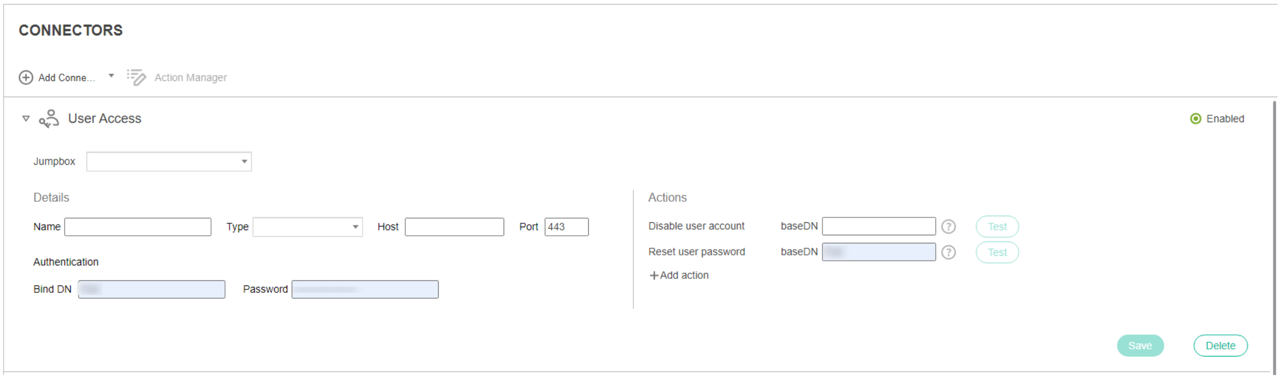
This permission delegation applies to all child objects or users within the target group. To allow FortiEDR to update accounts with elevated privileges, such as Domain Admin, you must manually apply the delegated permissions to these accounts as inheritance is disabled on these accounts by default. See this Microsoft article for more details.

Configuring FortiEDR

To integrate FortiEDR with Active Directory, you must configure a User Access connector and playbook policies for Active Directory in FortiEDR. Automatic incident response actions can then include resetting the user password or disabling the user account on Active Directory upon the detection of a FortiEDR security event.

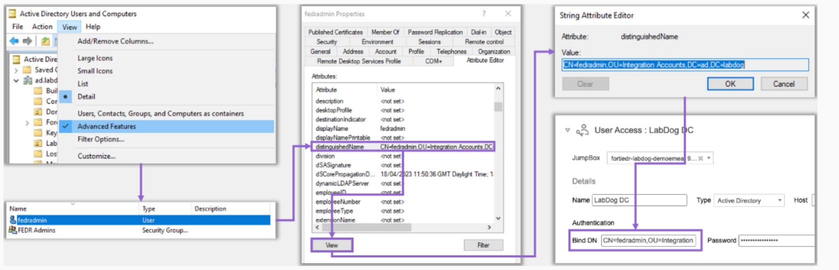
To configure a User Access connector for Active Directory in FortiEDR:

1. In the FortiEDR management console, select *Administration* > *Integrations*.
2. Click the *Add Connector* button and select *User Access* from the dropdown list.
   The following displays:



3. Fill in the following fields:

Field	Description
Jumpbox	Select the FortiEDR Jumpbox that will communicate with the Active Directory server.
Name	Specify a name of your choice to be used to identify the connector for Active Directory.
Type	Select *Active Directory*.
Host	Specify the IP or DNS address of the Active Directory server.
Port	Specify the port that is used for communication with the Active Directory server. Typically port 389 is used for LDAP authentication.
Authentication	Specify the Bind DN and password of the Active Directory admin user you created when Configuring Active Directory on page 7. **To locate Bind DN information in Active Directory:** 1. Click *View* > *Advanced Features*. 2. Double-click the admin user you created for the FortiEDR integration. 3. In the *Attribute Editor* tab, select *distinguishedName* and click *View*. The *Value* field include the full Bind DN information that you can copy.

Field	Description
	

Active Directory Users and Computers
File Action View Help
Add/Remove Columns...
Large Icons
Small Icons
List
Detail
Users, Contacts, Groups, and Computers as containers
Advanced Features
Filter Options...
Customize...
Name Type Description
fedradmin User
FEDR Admins Security Group...
fedradmin Properties
Published Certificates Member Of Password Replication Dial-in Object
Security Environment Sessions Remote control
General Address Account Profile Telephones Organization
Remote Desktop Services Profile COM+ Attribute Editor
Attributes:
Attribute Value
description <not set>
desktopProfile <not set>
destinationIndicator <not set>
displayName fedradmin
displayNamePrintable <not set>
distinguishedName CN=fedradmin,OU=Integration Accounts,DC
division <not set>
dSASignature <not set>
dSCorePropagationD... 18/04/2023 11:50:36 GMT Daylight Time; 1
dynamicLDAPServer <not set>
employeeID <not set>
employeeNumber <not set>
employeeType <not set>
extensionName <not set>
View
Filter
String Attribute Editor
Clear
OK
Cancel
User Access : LabDog DC
Details
Authentication
Host

Attribute: distinguishedName

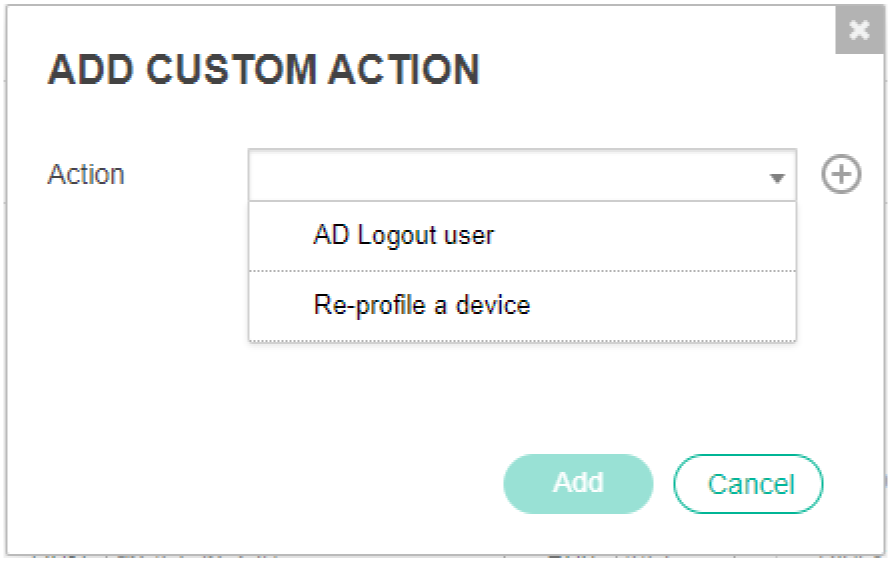
Value: CN=fedradmin,OU=Integration Accounts,DC=ad,DC=labdog

JumpBox: fortiedr-labdog-demoemea 9...

Name: LabDog DC Type: Active Directory

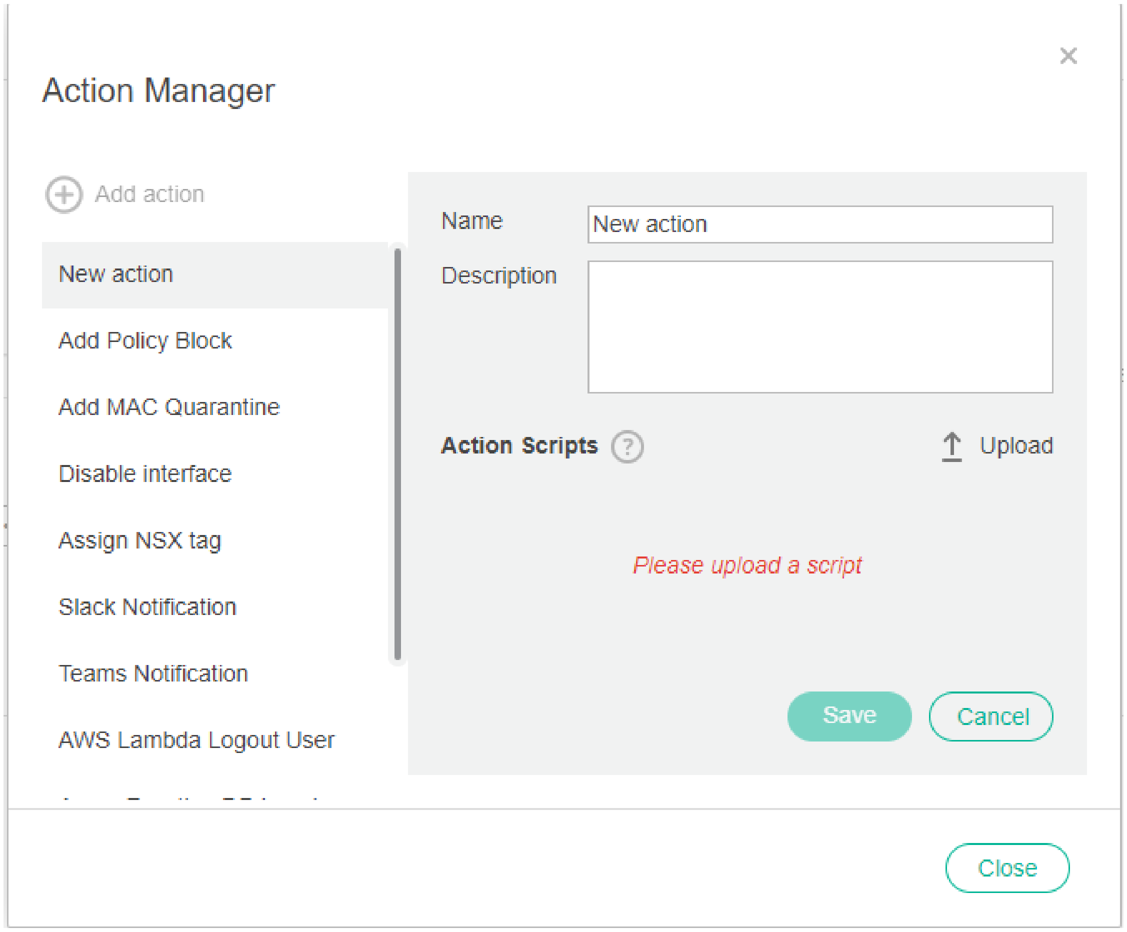
Bind DN: CN=fedradmin,OU=Integration Password: ••••••••••••••••

4. In the *Actions* area on the right, define the action to be taken by this connector:
   - To use an action provided out-of-the-box with FortiEDR (for example, Disable user account on Active Directory), specify the *baseDN* field for *Disable user account* or *Reset user password*, or both according to your needs. The baseDN is the Bind DN without the user name. For example, if the Bind DN is `CN=fedradmin,OU=Integration Accounts,DC=ad,DC=labdog`, the baseDN is `OU=Integration Accounts,DC=ad,DC=labdog`.
   - To use a custom integration action:
     i. Click the + *Add Action* button. The following popup window displays:



     ii. In the *Action* dropdown menu, select one of the previously defined actions (which were defined in FortiEDR as described in Custom integration), or define a new action that can be triggered according to the definitions in the Playbook:

i. Click the *Create New Action* button. The following displays:



Action Manager

Name: New action

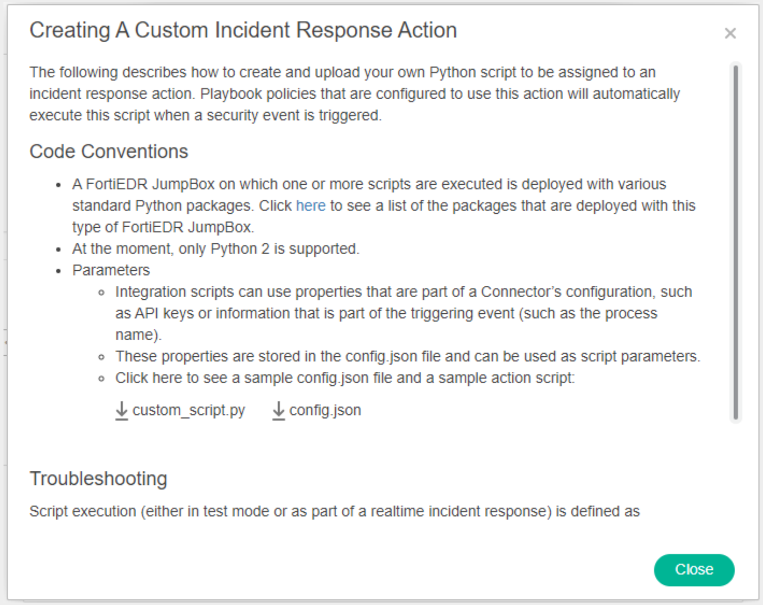
Description:

Please upload a script

ii. Fill out the fields of this window as follows in order to define a new action to be triggered in response to an incident.

In order to trigger this action, a Playbook policy must be defined that triggers this action to execute the script when a security event is triggered. The definition of this new action here automatically adds this action as an option in a Playbook policy. However, this action is not selected by default in the Playbook policy. Therefore, you must go to the Playbook policy and select it in order for it to be triggered when a security event is triggered.

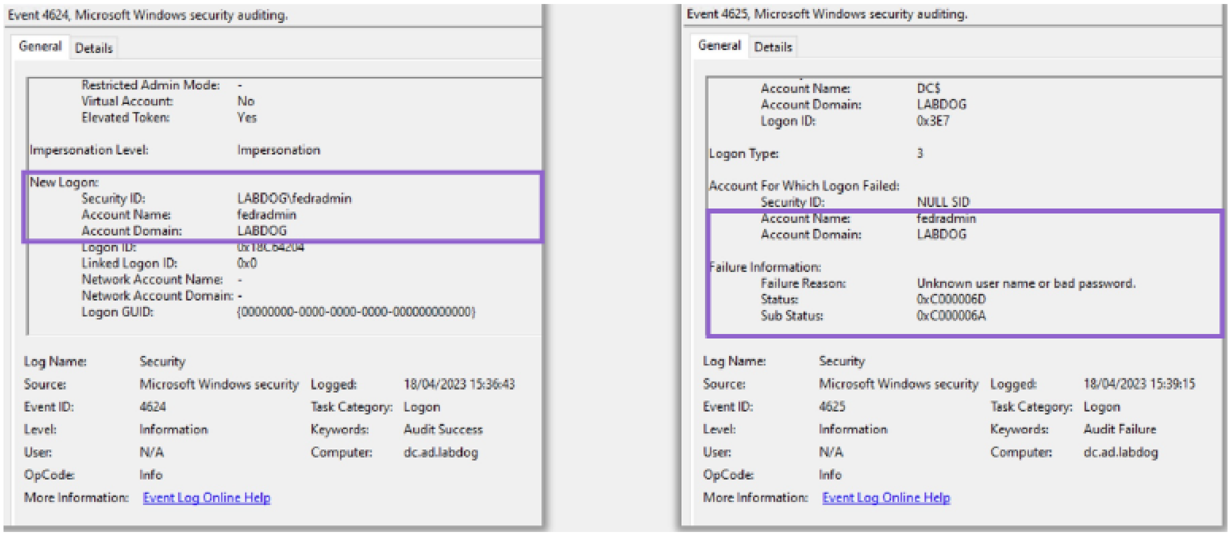
Field	Definition
Name	Enter any name for this action.
Description	Enter a description of this action.

Field	Definition
Upload	Upload a Python script that calls an API from the third-party system in order to perform the relevant action. Python 2.7 or later is supported. The Python script must be created according to the coding conventions that can be displayed by clicking the ? icon next to the *Action Scripts* field. The following displays providing an explanation of the coding conventions and provides various links that you can click to see more detail and/or to download sample files.  Creating A Custom Incident Response Action The following describes how to create and upload your own Python script to be assigned to an incident response action. Playbook policies that are configured to use this action will automatically execute this script when a security event is triggered. Code Conventions • A FortiEDR JumpBox on which one or more scripts are executed is deployed with various standard Python packages. Click here to see a list of the packages that are deployed with this type of FortiEDR JumpBox. • At the moment, only Python 2 is supported. • Parameters ◦ Integration scripts can use properties that are part of a Connector's configuration, such as API keys or information that is part of the triggering event (such as the process name). ◦ These properties are stored in the config.json file and can be used as script parameters. ◦ Click here to see a sample config.json file and a sample action script: Troubleshooting Script execution (either in test mode or as part of a realtime incident response) is defined as

iii. Click *Save*. The new action is then listed in the *Actions* area.

5. Click the *Test* button to test the connectivity. If the test fails, a reason is given.
   You can troubleshoot connection failures in the following ways:
   - Verifying the credentials you entered in step 3.
   - Verify the settings when Configuring Active Directory on page 7.
   - Monitor the Active Directory logs under *Windows Logs* > *Security* in the *Windows Event Viewer*. Search or filter to locate logs related to the test. For example, Event 4624 shows a successful login and Event ID 4625 shows a

failed login.



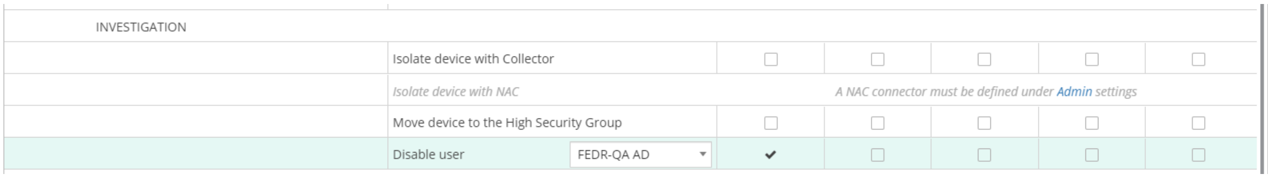
```
Event 4624, Microsoft Windows security auditing.
General  Details

          Restricted Admin Mode:    -
          Virtual Account:          No
          Elevated Token:           Yes

Impersonation Level:                Impersonation

New Logon:
          Security ID:              LABDOG\fedradmin
          Account Name:             fedradmin
          Account Domain:           LABDOG
          Logon ID:                 0x18C64204
          Linked Logon ID:          0x0
          Network Account Name:     -
          Network Account Domain:   -
          Logon GUID:               {00000000-0000-0000-0000-000000000000}

Log Name:          Security
Source:            Microsoft Windows security   Logged:          18/04/2023 15:36:43
Event ID:          4624                         Task Category:   Logon
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        dc.ad.labdog
OpCode:            Info
More Information:  Event Log Online Help
```

```
Event 4625, Microsoft Windows security auditing.
General  Details

          Account Name:             DC$
          Account Domain:           LABDOG
          Logon ID:                 0x3E7

Logon Type:                         3

Account For Which Logon Failed:
          Security ID:              NULL SID
          Account Name:             fedradmin
          Account Domain:           LABDOG

Failure Information:
          Failure Reason:           Unknown user name or bad password.
          Status:                   0xC000006D
          Sub Status:               0xC000006A

Log Name:          Security
Source:            Microsoft Windows security   Logged:          18/04/2023 15:39:15
Event ID:          4625                         Task Category:   Logon
Level:             Information                  Keywords:        Audit Failure
User:              N/A                          Computer:        dc.ad.labdog
OpCode:            Info
More Information:  Event Log Online Help
```

6. Click *Save* to save the connector configuration.

To configure playbook policies to automatically reset the user password or disable the user account upon security event triggering in FortiEDR:

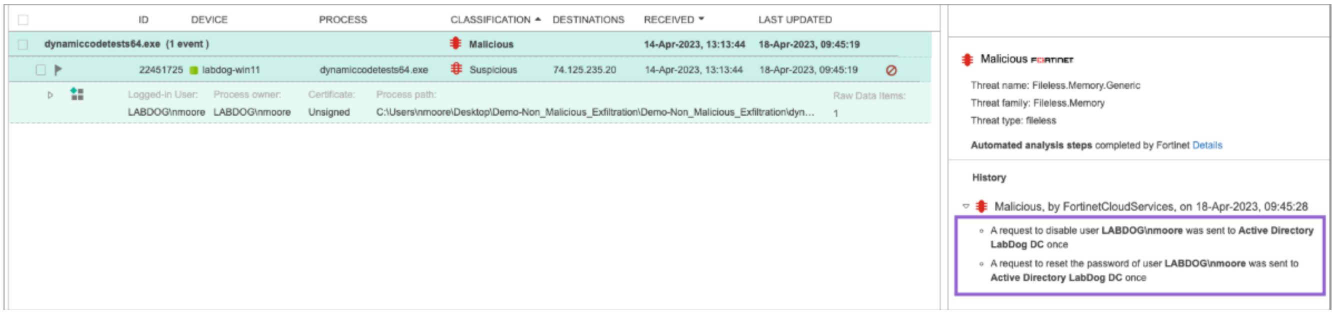
1. Navigate to the *SECURITY SETTINGS* > *Playbooks* page.
2. Open the Playbook policy that is applied on devices for which you want the automatic incident response to apply.
3. Place a checkmark in the relevant *Classification* column next to the *Disable user* row under the *INVESTIGATION* section or the *Reset user password* row under the *REMEDIATION* section.
   FortiEDR is now configured to automatically reset the user password or disable the user account upon security event triggering in FortiEDR.



INVESTIGATION							
	Isolate device with Collector		□	□	□	□	□
	Isolate device with NAC		*A NAC connector must be defined under Admin settings*				
	Move device to the High Security Group		□	□	□	□	□
	Disable user	FEDR-QA AD	✓	□	□	□	□

Verifying the integration

If the integration is successful, in FortiEDR, the *Reset user password* and/or *Disable user account* playbook will be triggered based on the classification trigger defined within the playbook. In the *Event Viewer*, you should first see an event classified by *FortinetCloudServices*, similar to the following:



ID	DEVICE	PROCESS	CLASSIFICATION ▲	DESTINATIONS	RECEIVED ▼	LAST UPDATED
dynamiccodetests64.exe (1 event)			Malicious		14-Apr-2023, 13:13:44	18-Apr-2023, 09:45:19
22451725	labdog-win11	dynamiccodetests64.exe	Suspicious	74.125.235.20	14-Apr-2023, 13:13:44	18-Apr-2023, 09:45:19

Logged-in User:	Process owner:	Certificate:	Process path:	Raw Data Items:
LABDOG\nmoore	LABDOG\nmoore	Unsigned	C:\Users\nmoore\Desktop\Demo-Non_Malicious_Exfiltration\Demo-Non_Malicious_Exfiltration\dyn...	1

Malicious FORTINET

Threat name: Fileless.Memory.Generic

Threat family: Fileless.Memory

Threat type: fileless

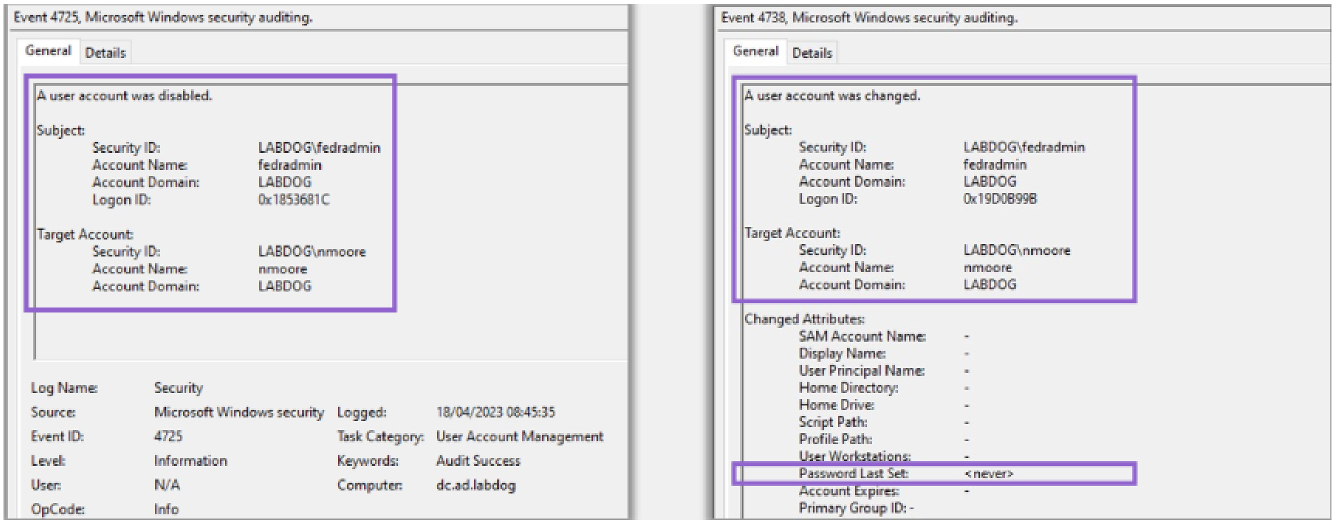
Automated analysis steps completed by Fortinet Details

History

Malicious, by FortinetCloudServices, on 18-Apr-2023, 09:45:28

- A request to disable user **LABDOG\nmoore** was sent to **Active Directory LabDog DC** once
- A request to reset the password of user **LABDOG\nmoore** was sent to **Active Directory LabDog DC** once

Once the playbook is triggered in FortiEDR, an API update will be sent to the Active Directory server to disable the user account and/or mark it as requiring a password reset as per configuration. This activity is shown under *Windows Logs > Security* in the *Windows Event Viewer*. A successful account disable will fall under Event 4725. A successful password reset will fall under Event 4738. See example below:

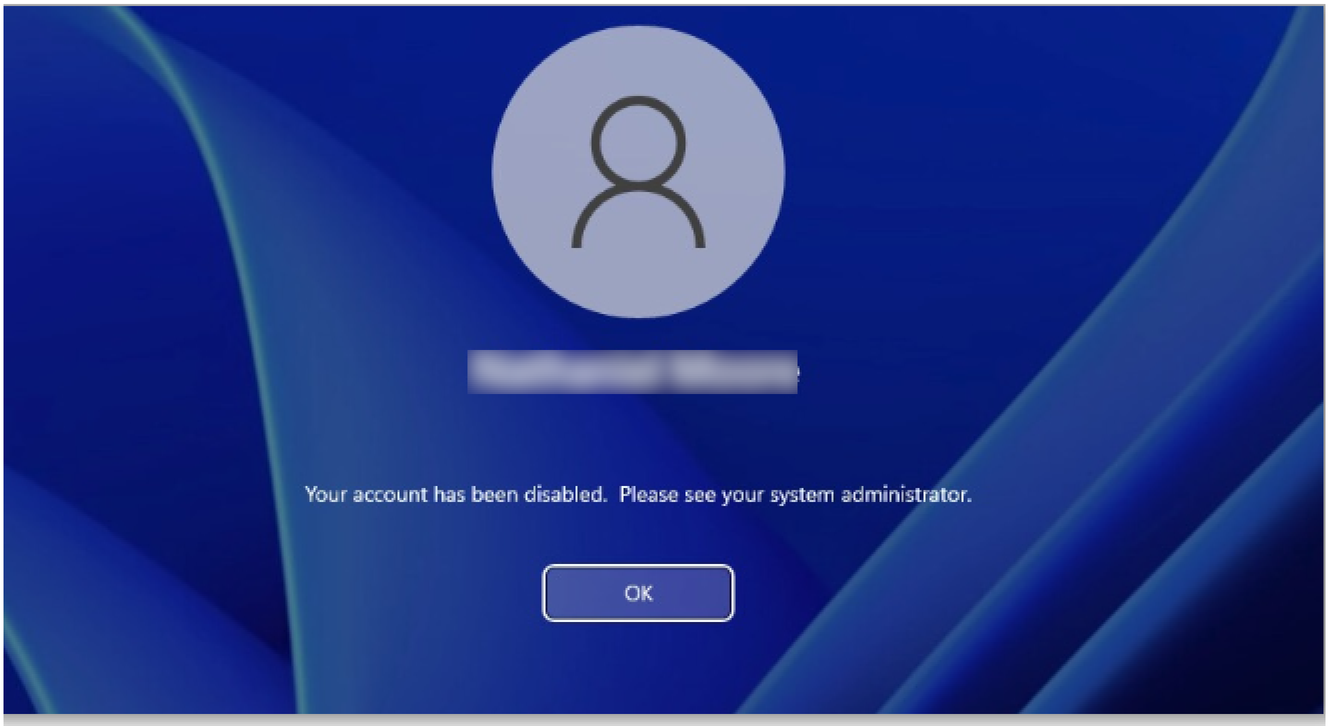


```
A user account was disabled.

Subject:
        Security ID:        LABDOG\fedradmin
        Account Name:       fedradmin
        Account Domain:     LABDOG
        Logon ID:           0x1853681C

Target Account:
        Security ID:        LABDOG\nmoore
        Account Name:       nmoore
        Account Domain:     LABDOG
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	18/04/2023 08:45:35
Event ID:	4725	Task Category:	User Account Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	dc.ad.labdog
OpCode:	Info		

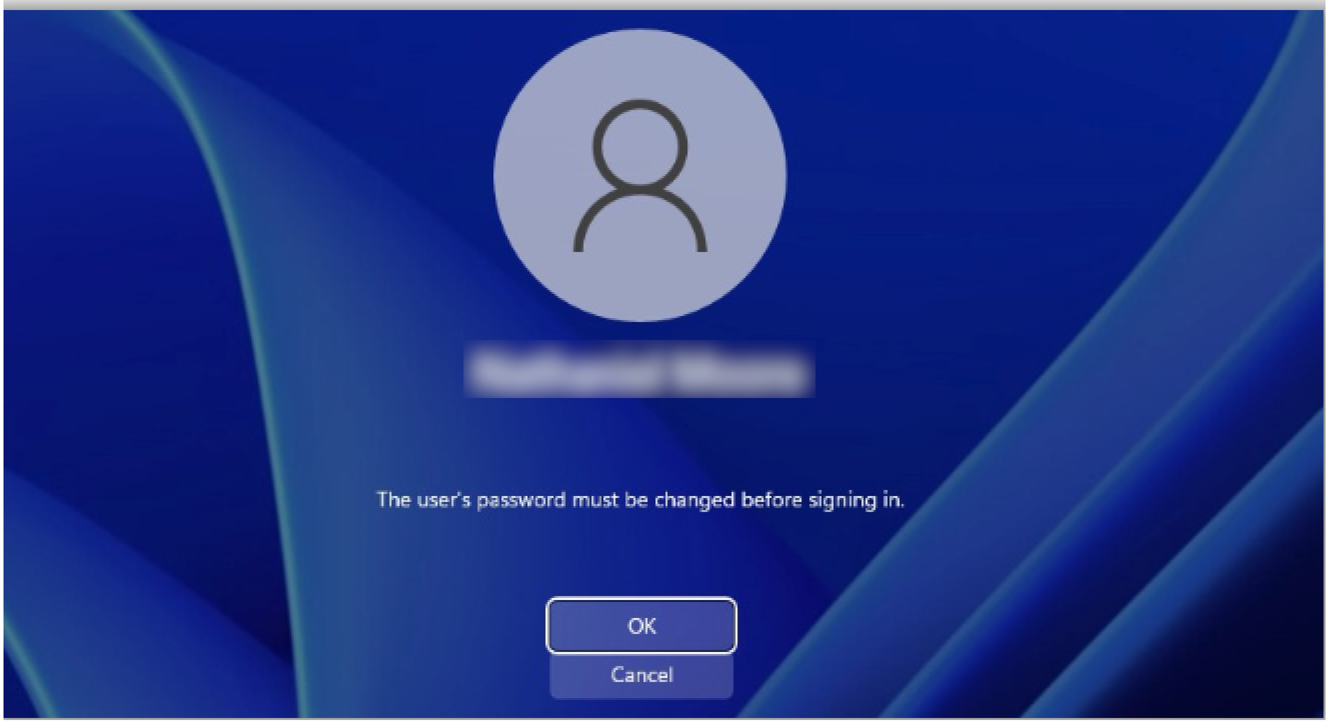
```
A user account was changed.

Subject:
        Security ID:        LABDOG\fedradmin
        Account Name:       fedradmin
        Account Domain:     LABDOG
        Logon ID:           0x19D0B99B

Target Account:
        Security ID:        LABDOG\nmoore
        Account Name:       nmoore
        Account Domain:     LABDOG

Changed Attributes:
        SAM Account Name:       -
        Display Name:           -
        User Principal Name:    -
        Home Directory:         -
        Home Drive:             -
        Script Path:            -
        Profile Path:           -
        User Workstations:      -
        Password Last Set:      <never>
        Account Expires:        -
        Primary Group ID: -
```

During subsequent logins, the user will see an error that the account has been disabled or be prompted to change the password:



[redacted]

Your account has been disabled. Please see your system administrator.



[redacted]

The user's password must be changed before signing in.

www.fortinet.com