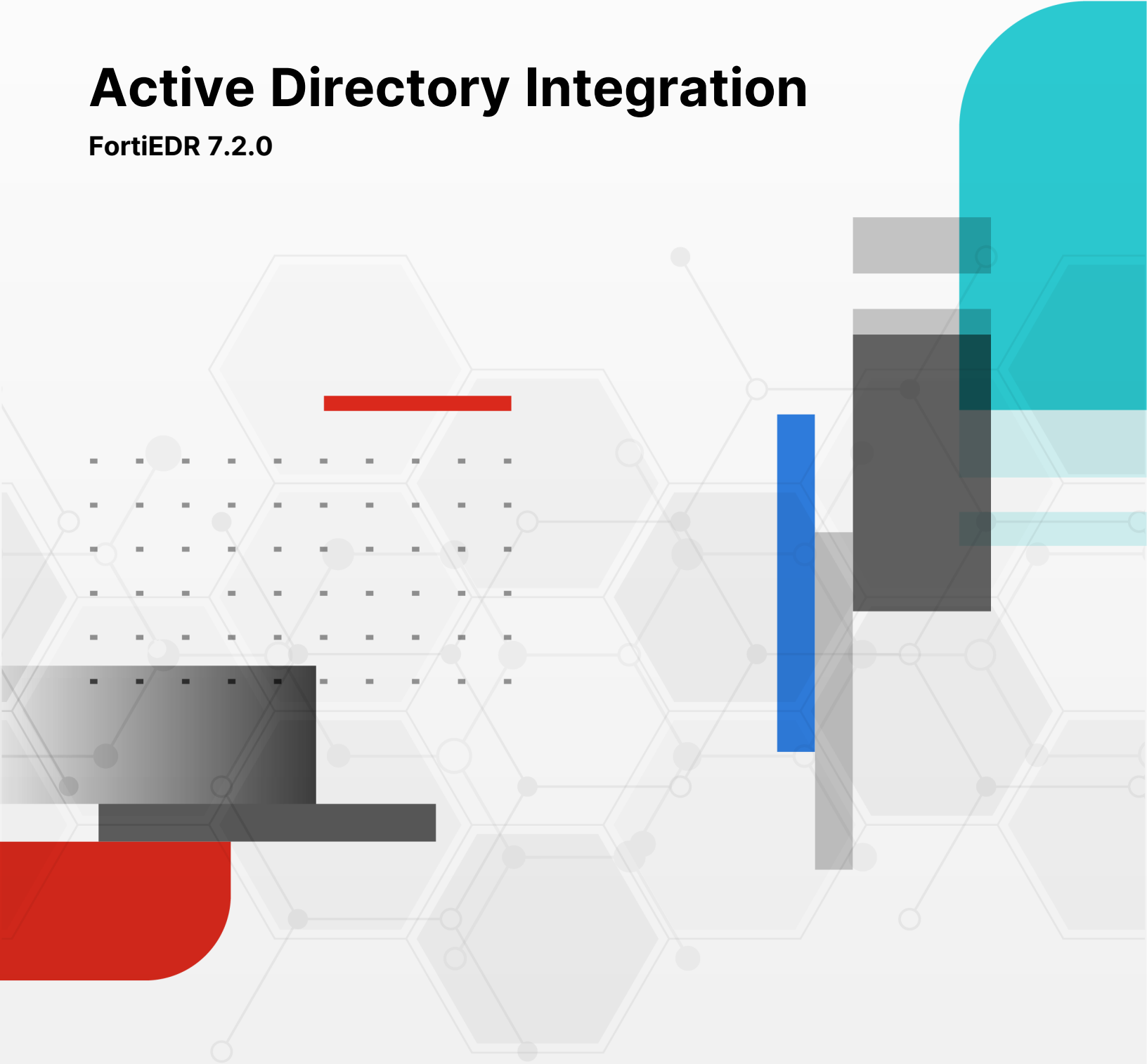


Active Directory Integration

FortiEDR 7.2.0



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



October 10, 2025

FortiEDR 7.2.0 Active Directory Integration

63-720-1214302-20251010

TABLE OF CONTENTS

Change log	4
Overview	5
Prerequisites	6
Configuring Active Directory	7
Configuring FortiEDR	18
Verifying the integration	23

Change log

Date	Change Description
2025-10-10	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:

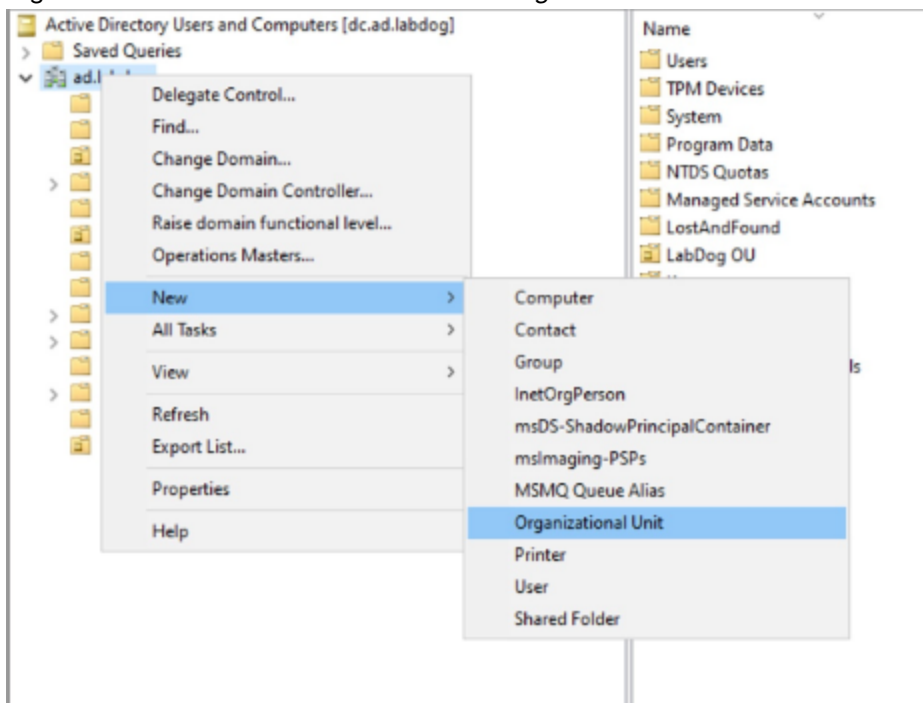
- Your FortiEDR deployment includes a Jumpbox that has connectivity to the Active Directory server.
 - Refer to [Installing the FortiEDR Core](#) for details about how to install a FortiEDR Core and configure it as a Jumpbox.
 - Refer to [Cores](#) for more information about configuring a Jumpbox.
- 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.

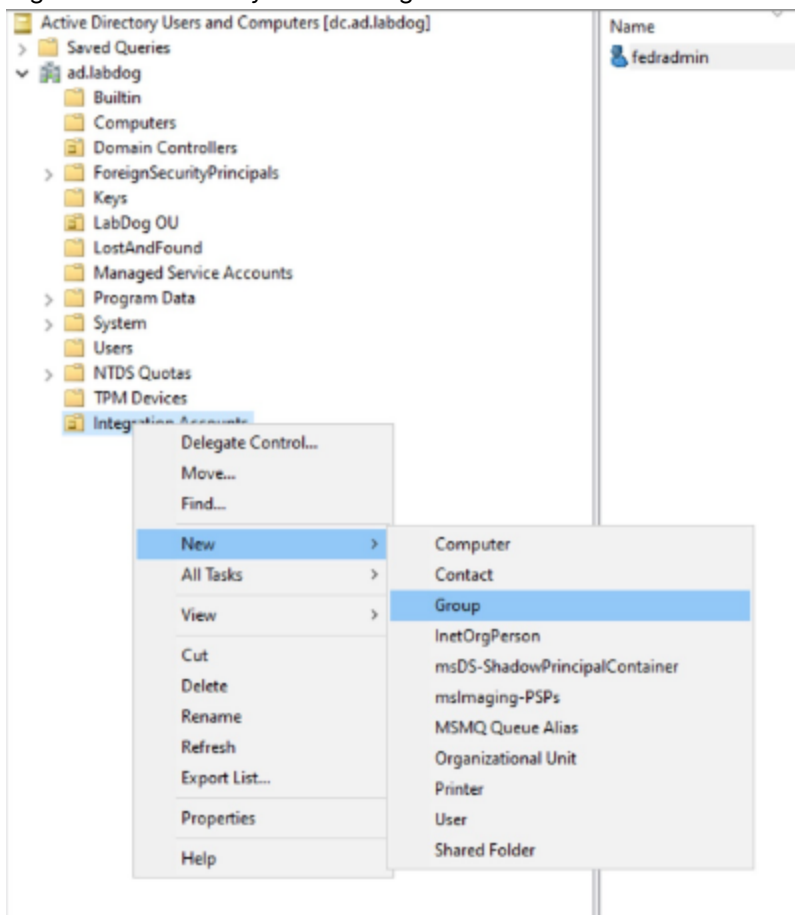
To create an Active Directory admin user for FortiEDR integration:

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

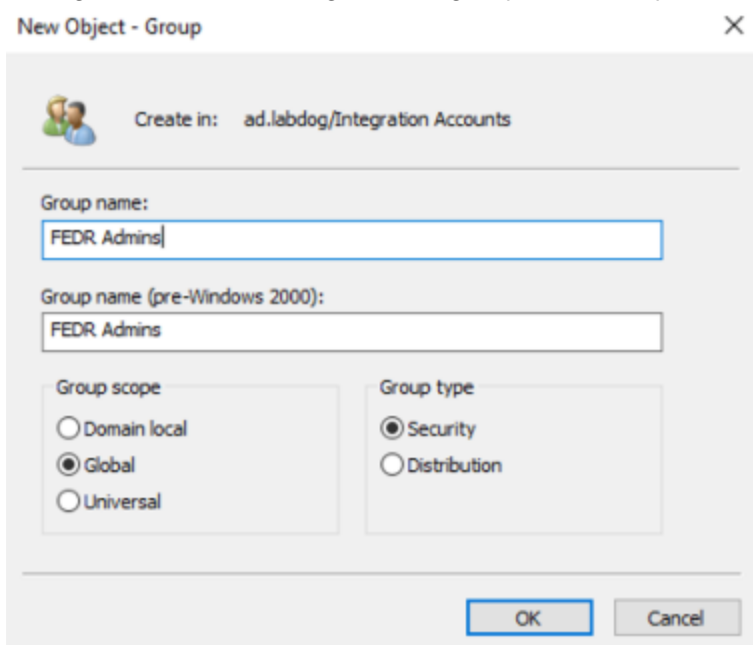


3. Specify the name for the organization unit and save it.

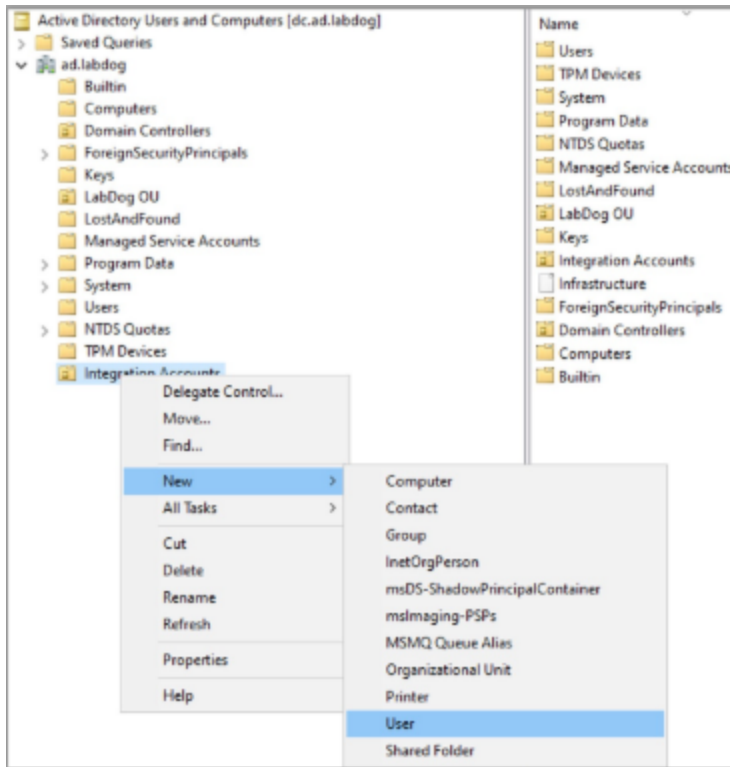
4. Right-click the newly created organization unit and select *New > Group*.



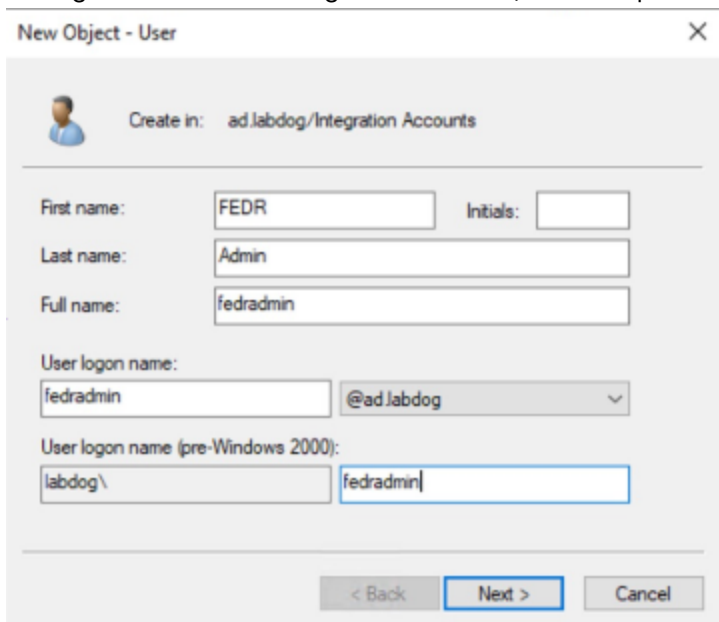
5. Configure the basic settings for the group (see example below).



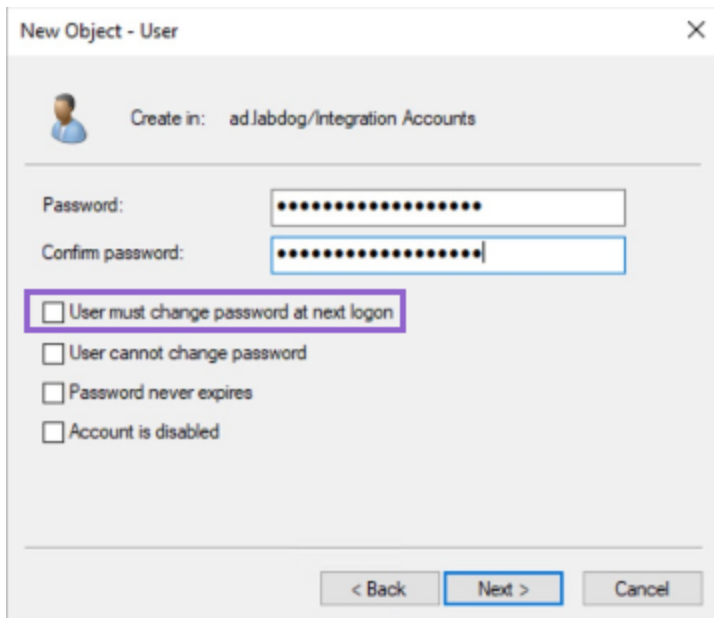
6. Right-click the newly created organization unit and select *New > User*.



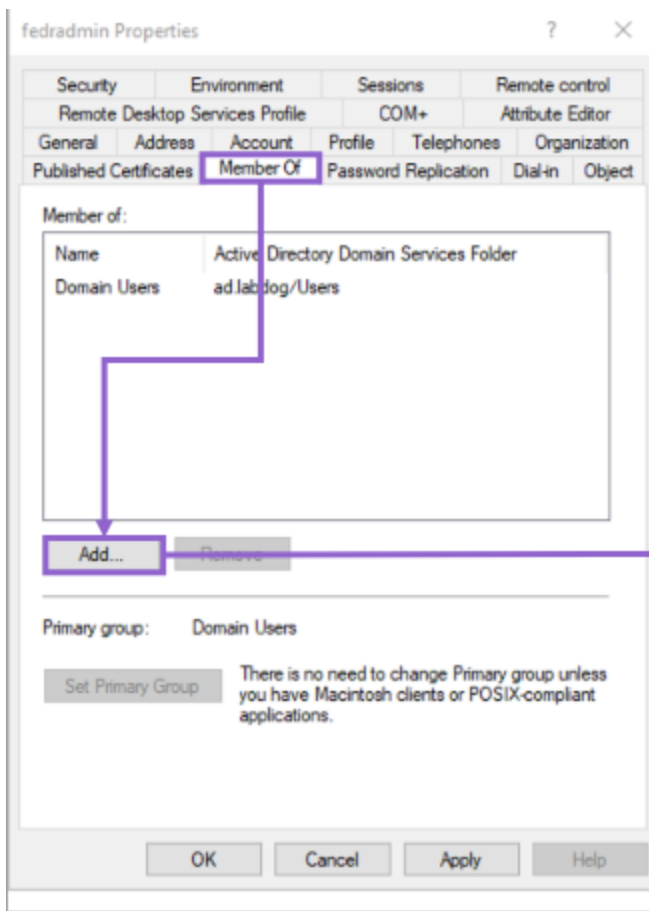
7. Configure the basic settings for the user (see example below) and click *Next*.



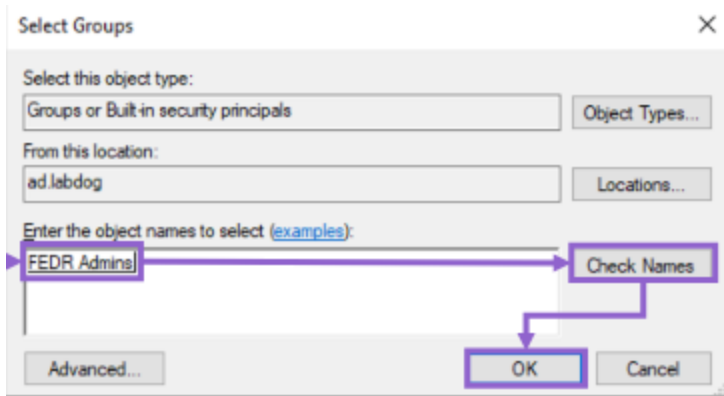
8. Define the password for the user, disable the *User must change password at next logon* option, click *Next* and then *Finish*.



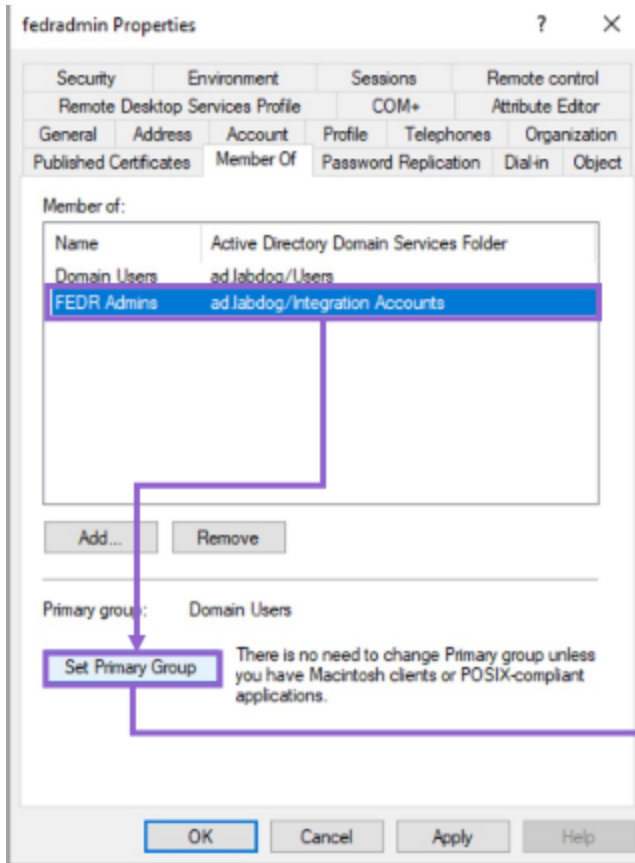
9. Double-click the user you just created to open the *Properties* window.
10. In the *Member Of* tab, click *Add*.



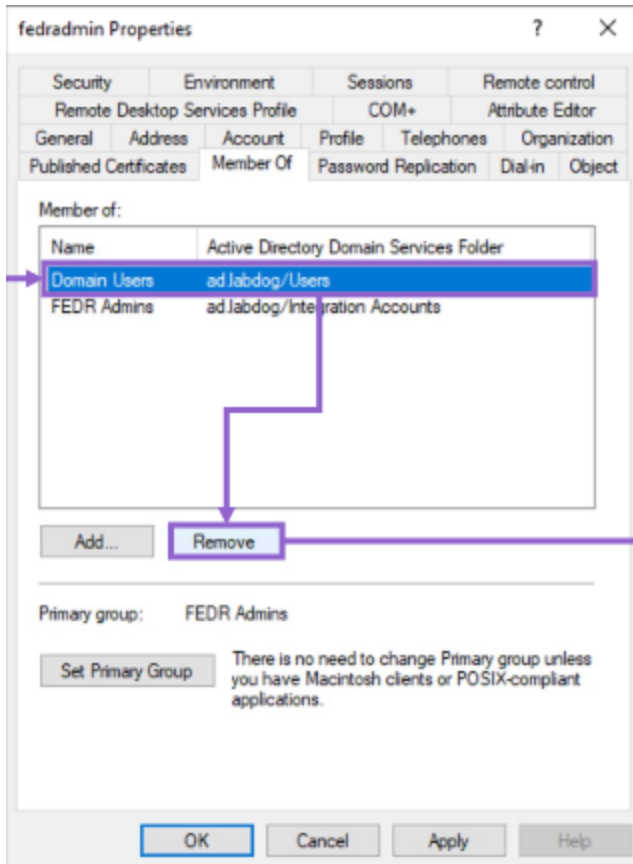
11. Type the name of the group you just created, click *Check Names to verify* and then click *OK*.



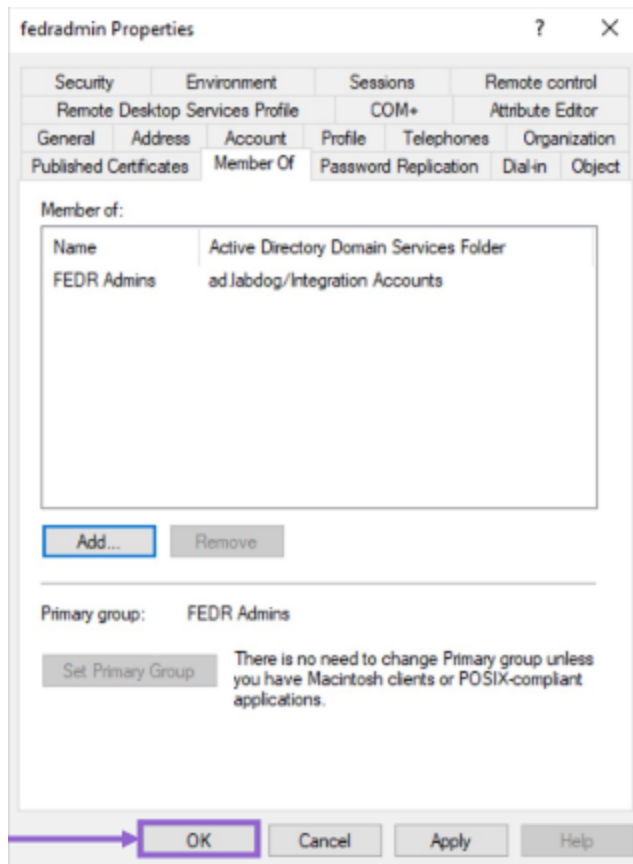
12. Select the the assigned group and click *Set Primary Group*.



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

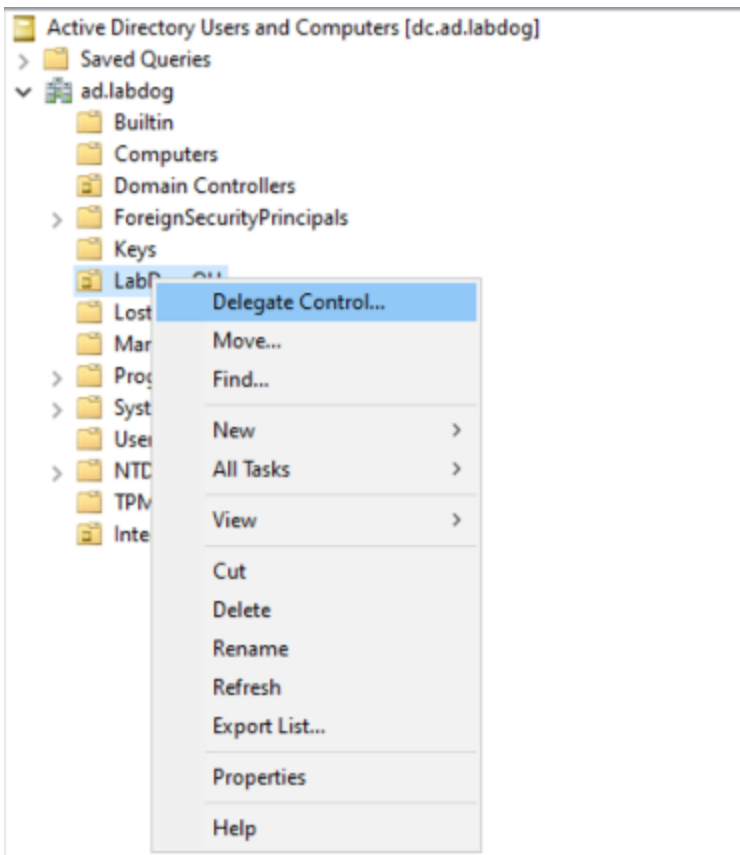


14. Click OK to save the changes.

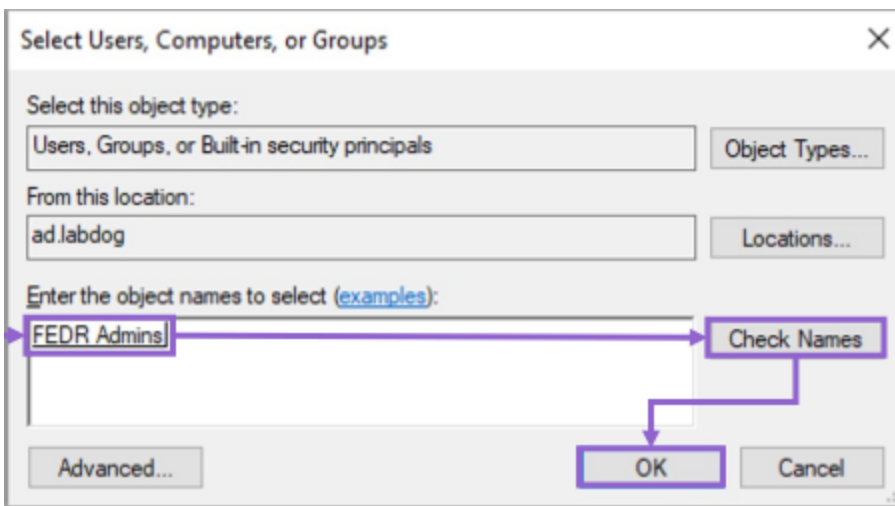


15. Click Save.
16. Configure the target organizational unit or container so that FortiEDR has delegated permissions to reset passwords and disable accounts:

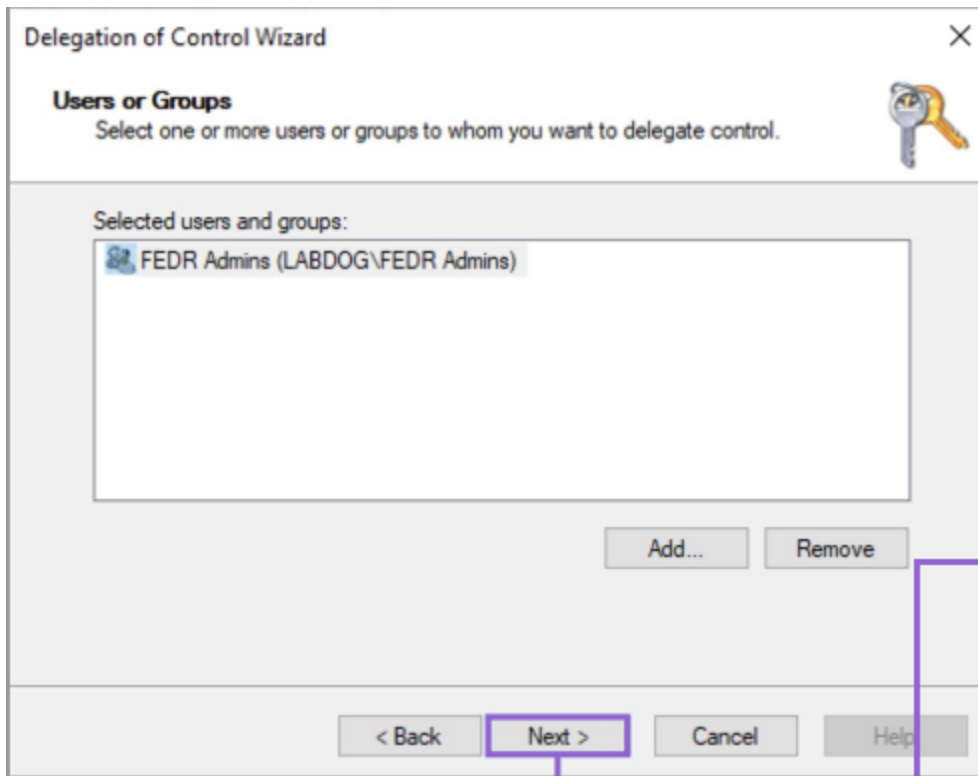
- a. Right-click the organization unit or container and select *Delegate Control*.



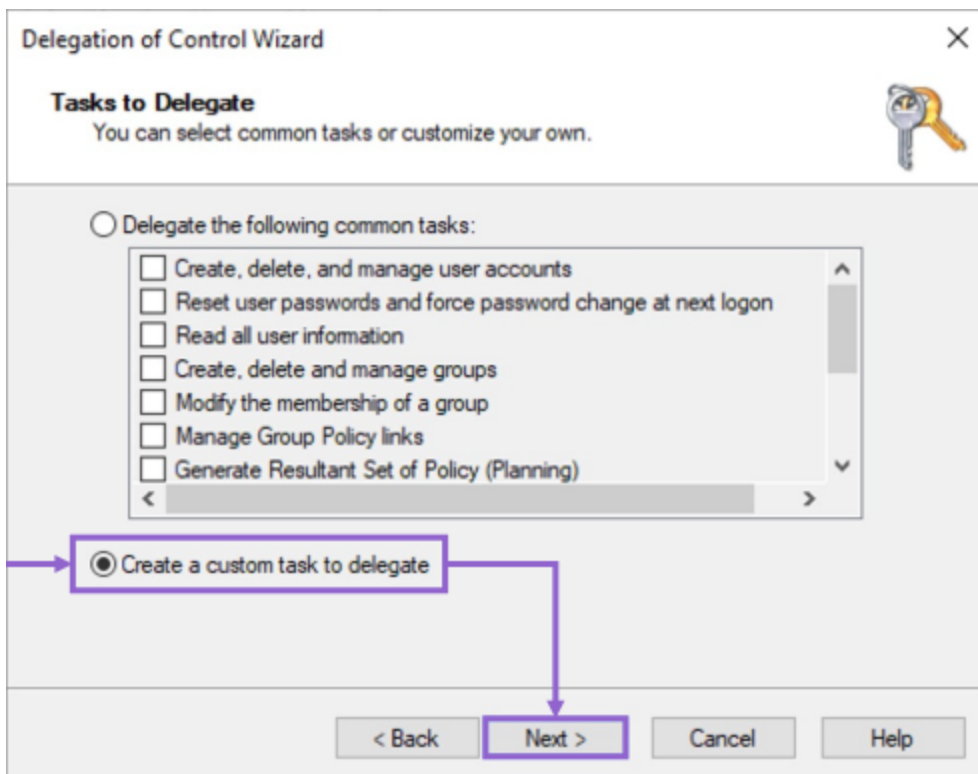
- b. Click *Next* and then click *Add*.
- c. Enter the name of the group that you created earlier, click *Check Names*, and then *OK*.



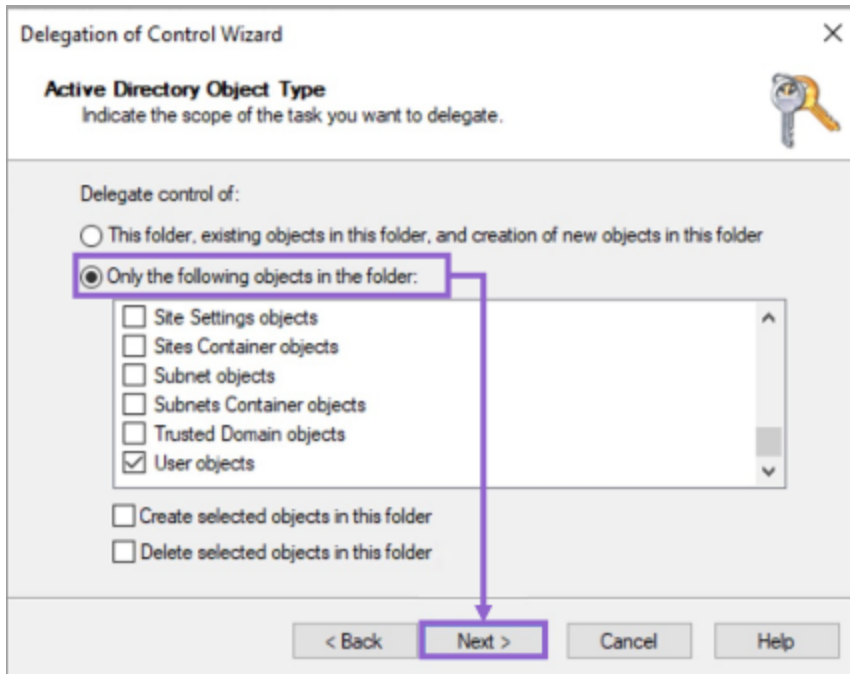
- d. Verify the selected group and click *Next*.



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

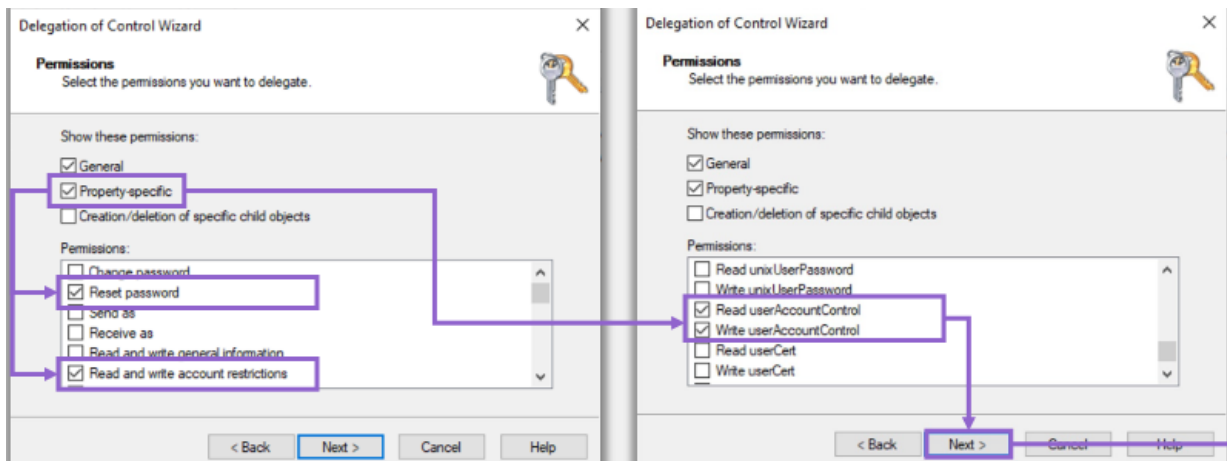


f. Select *Only the following objects in the folder*, select *User objects*, and then click *Next*.

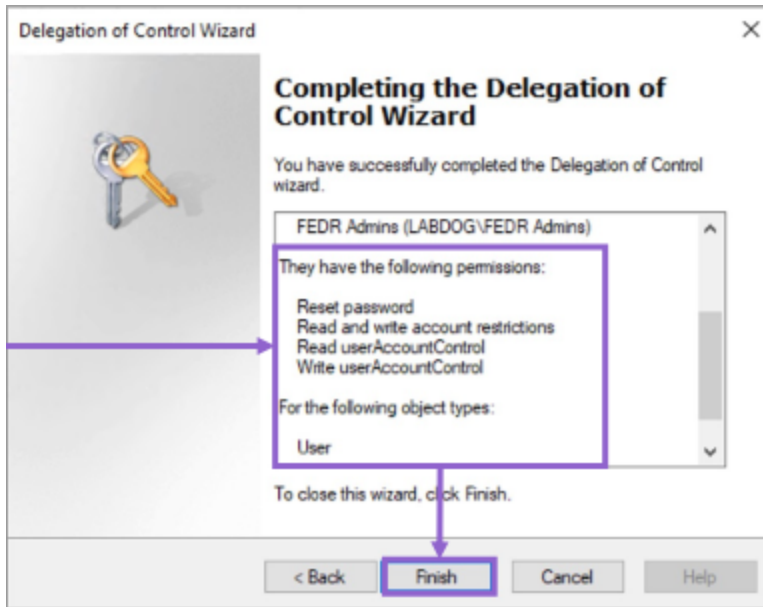


g. Select *Property-specific* under *Show these permissions*, select the following permissions, and click *Next*:

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



h. Verify the permissions list and 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.

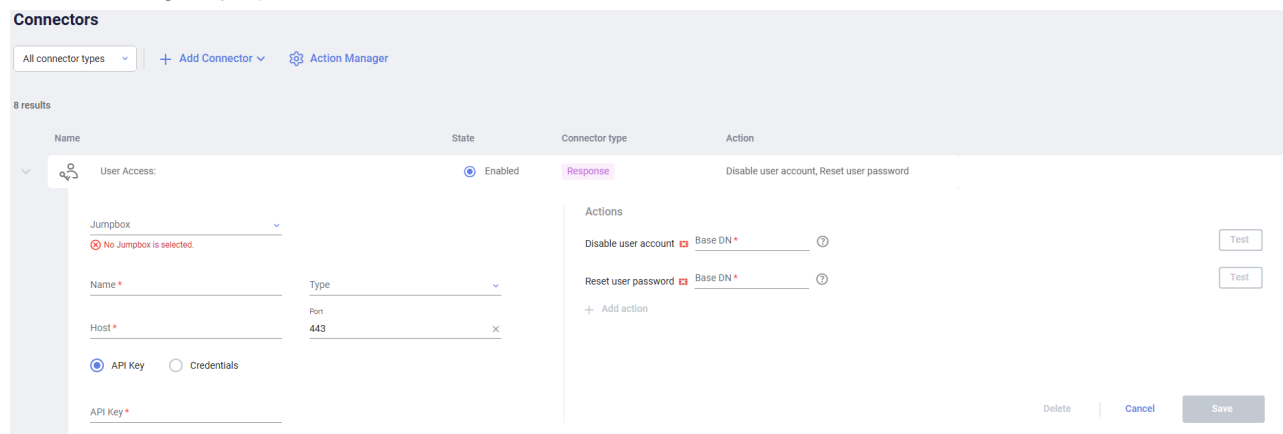
Configuring FortiEDR

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 > Connectors*.
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 <i>Active Directory</i> .
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 .

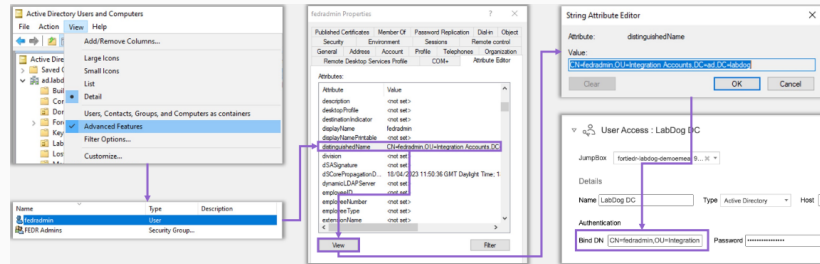
To locate Bind DN information in Active Directory:

1. Click *View > Advanced Features*.

Field	Description
-------	-------------

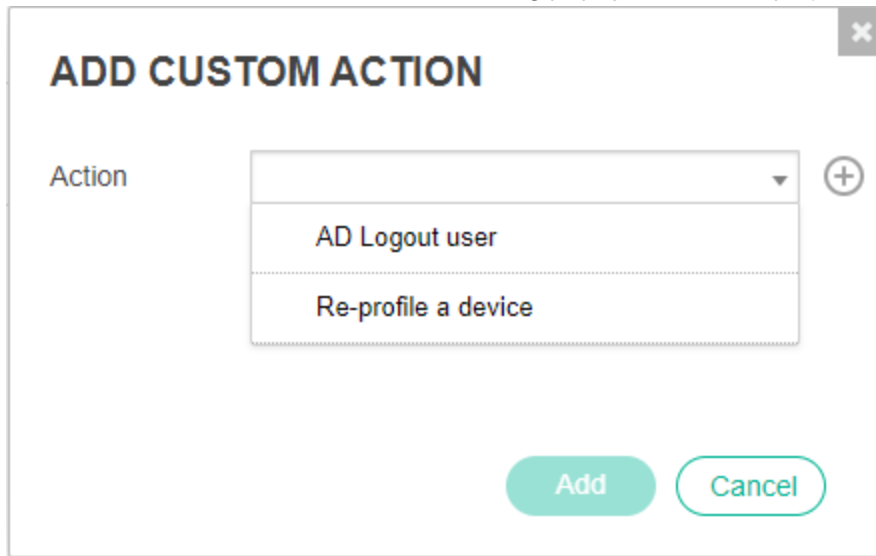
2. Double-click the admin user you created for the FortiEDR integration.
3. In the *Attribute Editor* tab, select *distinguishedName* and click *View*.

The *Value* field include the full Bind DN information that you can copy.



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:

- 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.

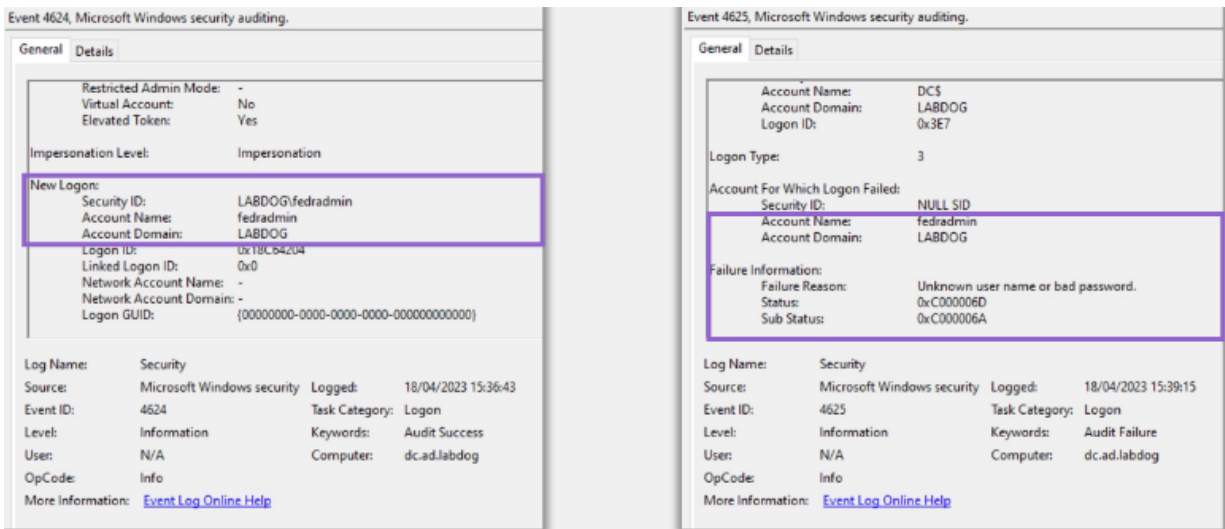
Field	Definition
Upload	<p>Upload a Python script that calls an API from the third-party system in order to perform the relevant action. Python 2.7 or later is supported. The Python script must be created according to the coding conventions that can be displayed by clicking the  icon next to the <i>Action Scripts</i> 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.</p> <div data-bbox="678 558 1425 1150" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Creating A Custom Incident Response Action ×</p> <p>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.</p> <p>Code Conventions</p> <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> ◦ 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: <p style="text-align: center;"> ↓ custom_script.py ↓ config.json </p> <p>Troubleshooting</p> <p>Script execution (either in test mode or as part of a realtime incident response) is defined as</p> <p style="text-align: right;">Close</p> </div>

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.



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:

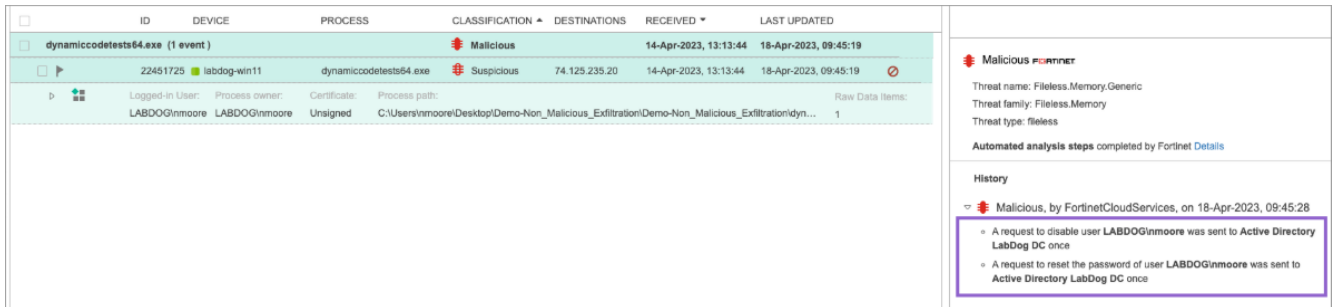
1. Navigate to the *SECURITY SETTINGS > Playbooks* page.
2. Open the Playbook policy that is applied on devices for which you want the automatic incident response to apply.
3. Place a checkmark in the relevant *Classification* column next to the *Disable user* row under the *INVESTIGATION* section or 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.

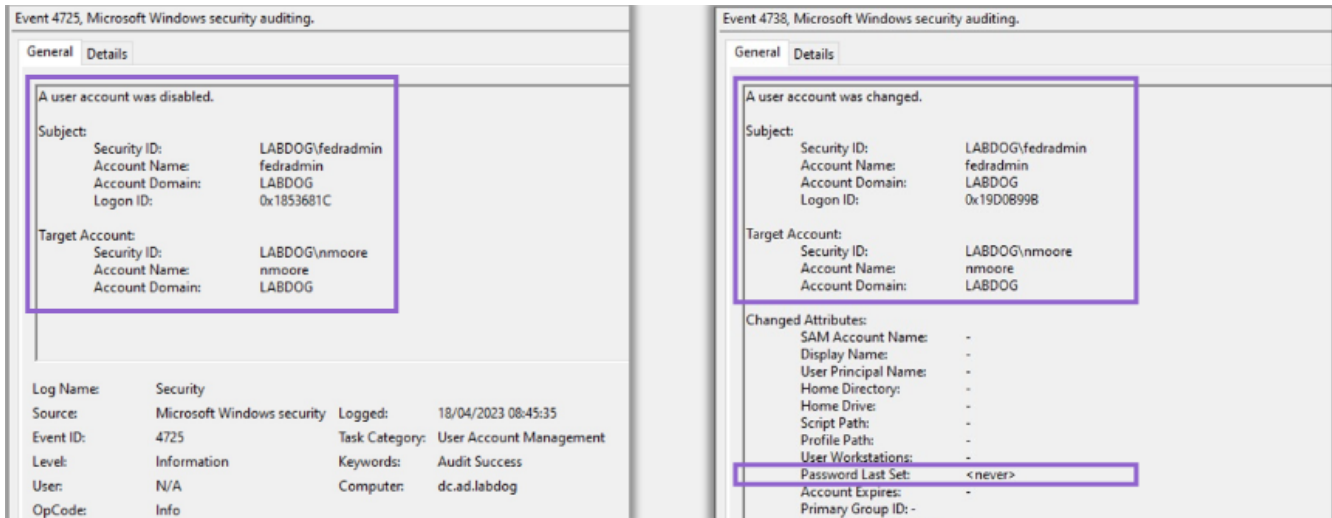
INVESTIGATION						
Isolate device with Collector		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Isolate device with NAC	A NAC connector must be defined under Admin settings					
Move device to the High Security Group		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Disable user	FEDR-QA AD	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Verifying the integration

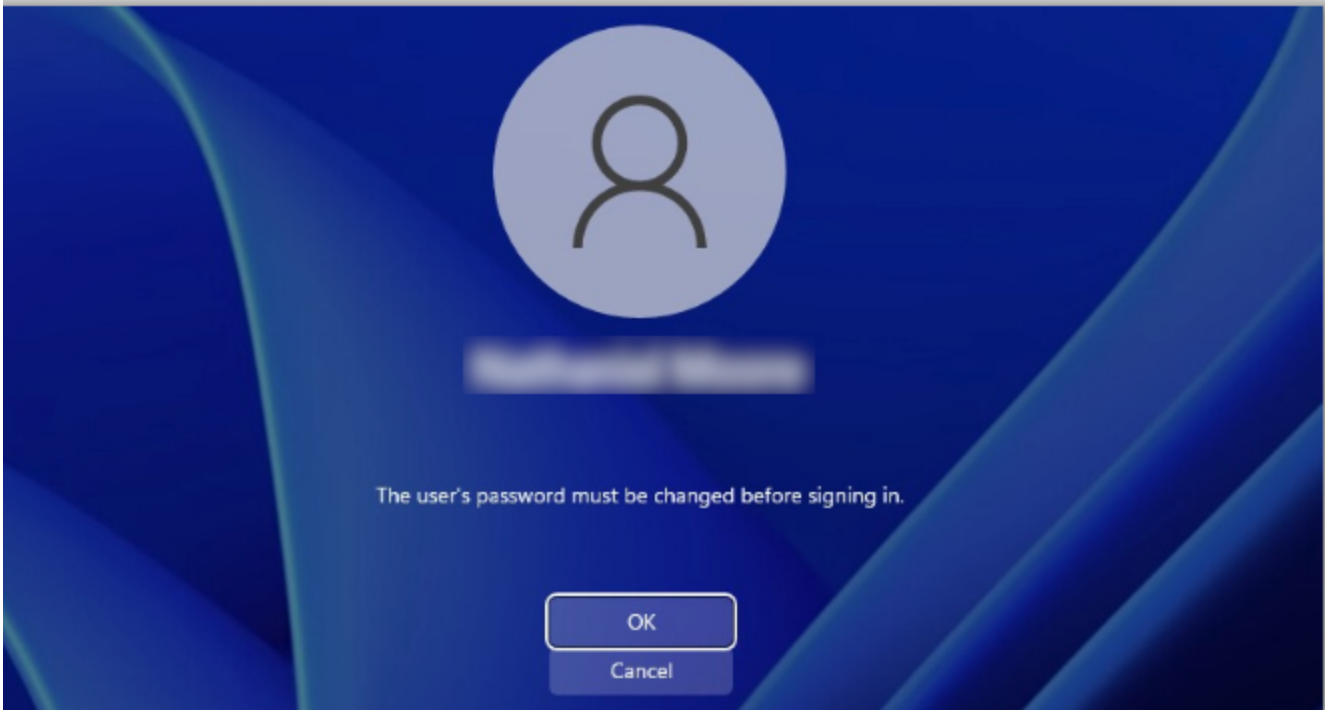
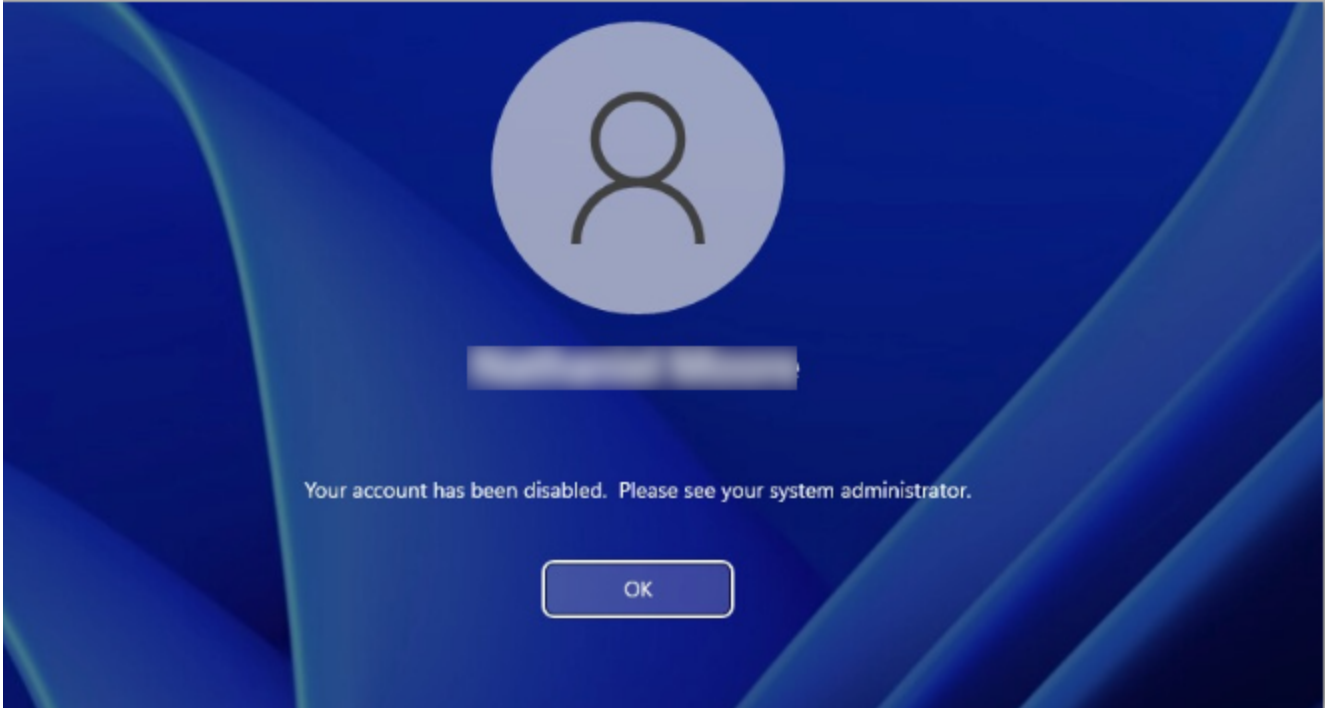
If the integration is successful, in FortiEDR, the *Reset user password* and/or *Disable user account* playbook will be triggered based on the classification trigger defined within the playbook. In the *Incidents* page, you should first see an event classified by *FortinetCloudServices*, similar to the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



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:



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





www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.