Admin Guide

FortiAuthProxy 1.1.1

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

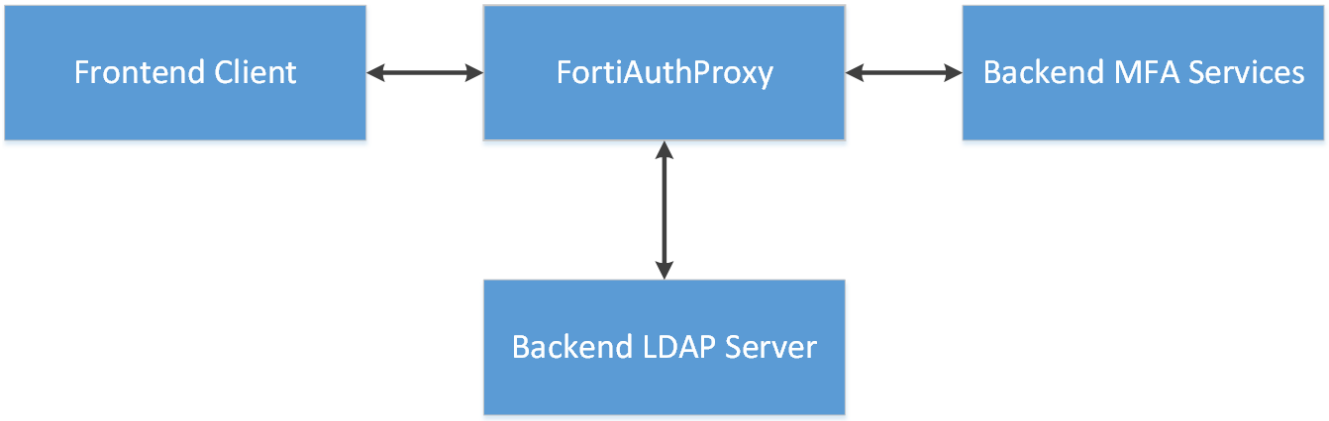
FEEDBACK
Email: techdoc@fortinet.com

December 7, 2025
FortiAuthProxy 1.1.1 Admin Guide

TABLE OF CONTENTS

Introduction

FortiAuthProxy is a software application that adds multi-factor authentication (MFA) support to common authentication protocols such as LDAP. It's an OVA file that can be installed on a VMware ESXi server.



- Frontend client — Firewall/VPN gateway managing LDAP authentication or generic LDAP client.
- FortiAuthProxy — The LDAP proxy software of this project.
- Backend LDAP server — Microsoft Active Directory (AD) or OpenLDAP.
- Backend MFA services — FortiIdentity Cloud (FIC).

When a frontend client sends an authentication request, it first goes to FortiAuthProxy. FortiAuthProxy then checks the user's credentials with the backend LDAP server. If the credentials are correct, it forwards the request to the backend MFA service, which is FIC. The user can then approve the auth by either pushing with FMT or entering their token to complete the authentication process.

Installing FortiAuthProxy

This software has undergone rigorous internal validation to ensure it functions as documented. We strongly recommend using the product in its original, unmodified form. Issues arising from any alterations to the shipped product are not supported.

Prerequisites

To obtain the latest FortiAuthProxy installer, contact our support team at cs@fortinet.com.

FortiAuthProxy 1.1.1 requires the following prerequisites to install and operate:

- VMware ESXi 6.7.0 or later.
- The latest version of Google Chrome or Mozilla Firefox.

Upgrading FortiAuthProxy 1.1.0 to 1.1.1

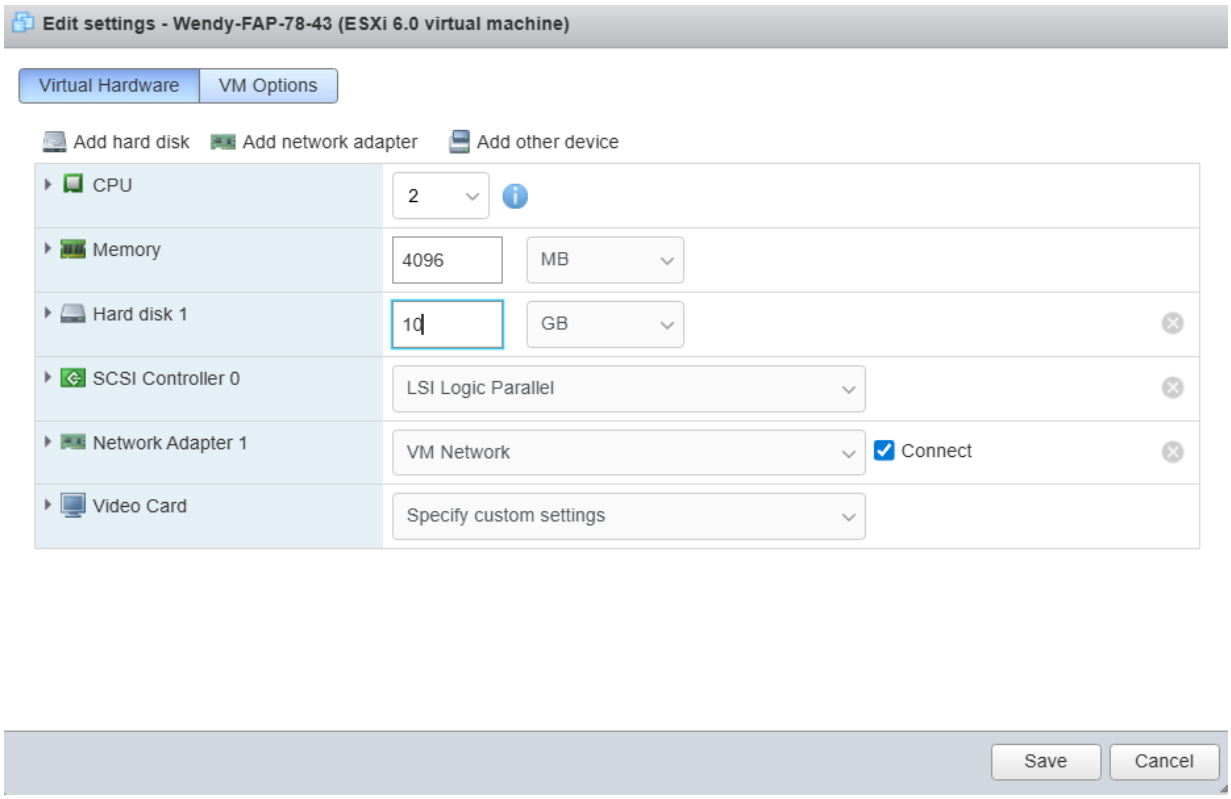
1. Before running FortiAuthProxy (FAP) 1.1.1, stop your FAP 1.1.0 service by running:
   ```
   sudo systemctl stop fortiauthproxy
   ```
2. Double-check to ensure that the FAP 1.1.0 proxy is disabled by running:
   ```
   sudo systemctl status fortiauthproxy
   ```
   ```
   root@priya247:/home/admin-k8s# sudo systemctl status fortiauthproxy
   ● fortiauthproxy.service - FortiAuthProxy
        Loaded: loaded (/etc/systemd/system/fortiauthproxy.service; enabled; vendor preset: enabled)
        Active: inactive (dead) since Fri 2025-08-15 17:12:30 UTC; 3 days ago
       Process: 2199048 ExecStart=/usr/bin/python3 /opt/fortiauthproxy/current/iamproxy/fortiauthproxy.py (code=exited, status=0/SUCCESS)
      Main PID: 2199048 (code=exited, status=0/SUCCESS)

   Aug 15 17:10:43 priya247 systemd[1]: Started FortiAuthProxy.
   Aug 15 17:12:30 priya247 systemd[1]: Stopping FortiAuthProxy...
   Aug 15 17:12:30 priya247 systemd[1]: fortiauthproxy.service: Succeeded.
   Aug 15 17:12:30 priya247 systemd[1]: Stopped FortiAuthProxy.
   root@priya247:/home/admin-k8s#
   ```
3. Now configure FAP 1.1.1 by following the steps in Deploying FortiAuthProxy in ESXi on page 6, save the configuration, and run FAP 1.1.1.

To ensure a seamless upgrade, be sure to use the same client id and its secret as those used in your FAP 1.1.0 configuration. If the client id's secret has been changed, you must use the new secret for this client id.

Deploying FortiAuthProxy in ESXi

1. Download the OVA file.
2. Log into ESXi.
3. Register/Create a new VM by deploying the OVA file.
4. **(Highly recommended) Extend the original disk size to a minimum of 10 G (because the original disk size is only 6 G and could be filled up quickly with logs):**
   a. Extend the disk size in ESXi.



   b. Shut down the VM if it's still running, and power it on again to let the changes in ESXi take effect.
   c. Log into the backend with the username `"ubuntu"` and the password `"ubuntu".`
   d. Run `sudo expand-root-lvm`. You should be able to see the changes in disk size get allocated.

```
ubuntu@ubuntu-server:~$ sudo expand-root-lvm
[2025-09-12T18:32:50+00:00] Root fs=ext4 | LVM=1 | Disk=/dev/sda | Part=/dev/sda3 | Part#=3
+ growpart /dev/sda 3
NOCHANGE: partition 3 is size 17297375. it cannot be grown
[2025-09-12T18:32:51+00:00] growpart non-zero (often ok if already max)
+ partprobe /dev/sda
+ udevadm settle
+ pvresize /dev/sda3
  Physical volume "/dev/sda3" changed
  1 physical volume(s) resized or updated / 0 physical volume(s) not resized
+ lvextend -r -l +100%FREE /dev/mapper/ubuntu--vg-ubuntu--lv
  Size of logical volume ubuntu-vg/ubuntu-lv unchanged from <8.25 GiB (2111 extents).
  Logical volume ubuntu-vg/ubuntu-lv successfully resized.
resize2fs 1.45.5 (07-Jan-2020)
The filesystem is already 2161664 (4k) blocks long.  Nothing to do!

[2025-09-12T18:32:53+00:00] Done.
Filesystem                         Size  Used Avail Use% Mounted on
/dev/mapper/ubuntu--vg-ubuntu--lv  8.1G  2.8G  4.9G  37% /
```

5. After the VM is up and running, configure the network with `netplan` by updating the `/etc/netplan/00-installer-config.yaml` file as follows:
   a. Run `ip addr`, and configure the Ethernet interface under ethernets in the `yaml` file. In the following illustration, it's `ens32`.

```
ubuntu@ubuntu-server:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens32: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:0c:29:65:c0:3e brd ff:ff:ff:ff:ff:ff
```

   b. Configure the FortiAuthProxy address under `addresses`. (This is where you want your proxy to run.)

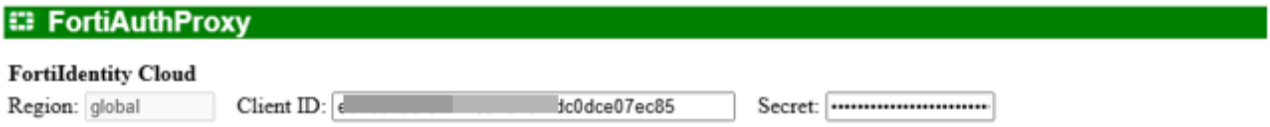
```
ubuntu@ubuntu-server:/etc/netplan$ cat 00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  version: 2
  ethernets:
    ens32:
      dhcp4: no
      addresses:
         - 10.160.[redacted]/24
      nameservers:
         addresses: [8.8.8.8, 1.1.1.1]
      routes:
         - to: default
           via: 10.160.[redacted]
```

   c. Run `sudo netplan apply`
6. Verify that your FortiAuthProxy is up and running to the configured static IP address, as illustrated in the following screenshot.

7. Remember the default FortiAuthProxy portal Username/Password: `admin/fortinet123`

Configuring FortiIdentity Cloud for FortiAuthProxy

1. Log into `fic.fortinet.com`.
2. Create a realm and a Web application, and assign the Web application to the realm.
3. Copy the Client ID and secret access key. (**Note**: Be sure to note down the Client ID and secret because they cannot be retrieved. If they are changed, be sure to update them in FortiAuthProxy as well.)
4. Start the FortiAuthProxy portal, and paste the Client ID and secret of the Web application into their respective boxes, as illustrated in the following screenshot.



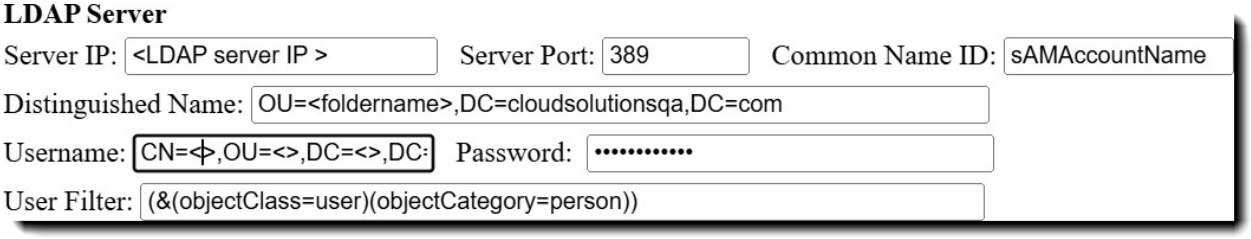
If you already have an existing realm configured with FortiAuthProxy, make sure to use the same client and secret from the same realm in the new FortiAuthProxy.

You can't have more than one FortiAuthProxy instances using the same secret. This will overlap the LDAP sync, so you must shut down the old instance before starting a new one.

Configuring LDAP for FortiAuthProxy

Configuring LDAP server

1. On the FortiAuthProxy portal, configure the LDAP server by entering the following:
   a. Server IP
   b. Server Port
   c. Common Name
   d. Distinguished Name, etc.
2. Refer to the following screenshot, if needed.



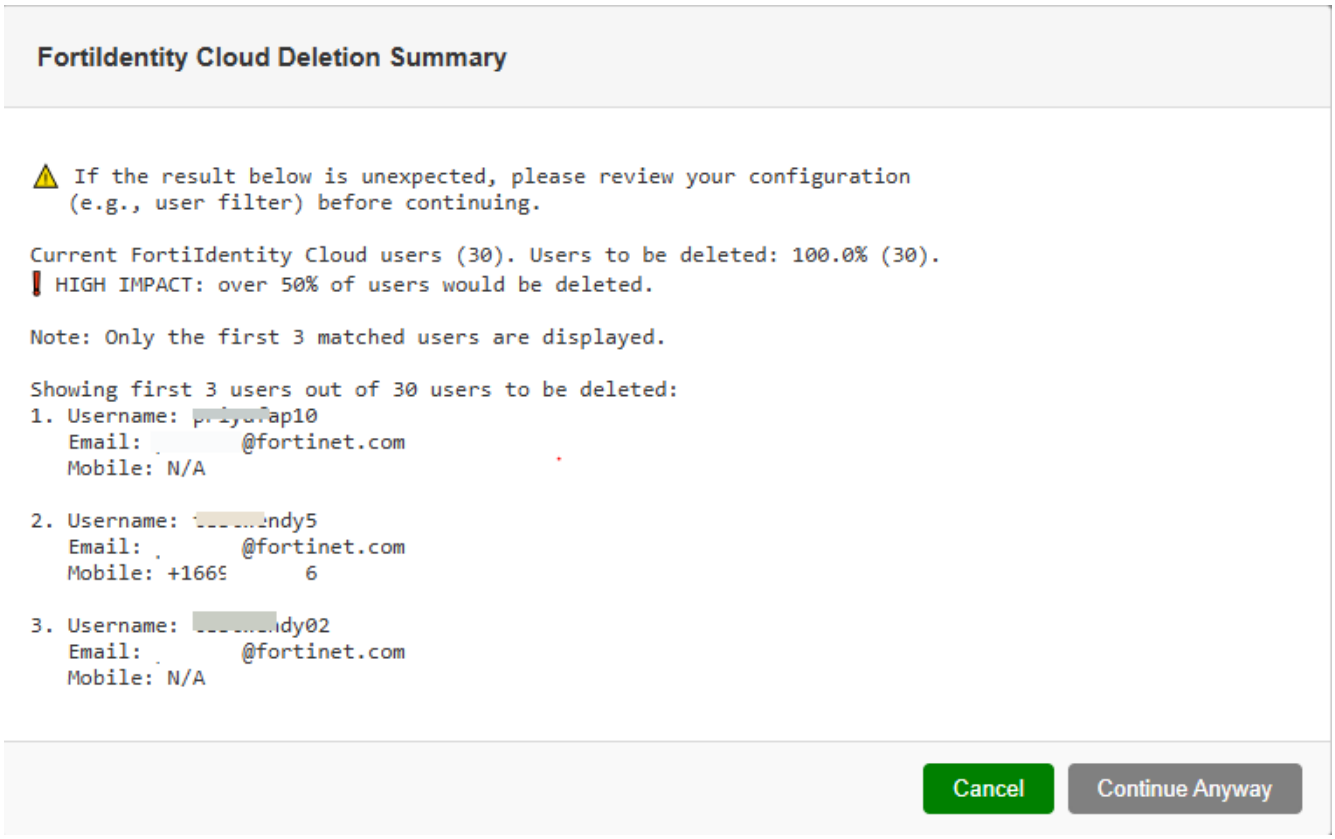
3. Pay attention to the LDAP user filter conditions for the security group:
   - `(&(objectClass=user)(memberOf=CN=<security group name>, OU=Security,DC=example,DC=com))`
   - Logical OR condition:

```
(&(objectClass=user)(|(memberOf=CN= Group1,OU=Security,DC=example,DC=com)(memberOf=CN=
     Group2,OU=Security,DC=example,DC=com)))
```

   - Logical AND condition:

```
(&(objectClass=user)(memberOf=CN= Group1, OU=Security,DC=example,DC=com)(memberOf=CN=
     Group2,OU=Security,DC=example,DC=com))
```

The LDAP user filter can delete the users on FIC if it not set incorrectly. A warning message will pop up when *Delete User in Background* is selected. It will ask you for permission to continue the action or to cancel it. Make sure that the user filter is set correctly to prevent accidentally deleting users on FIC.



You can check your configuration from the backend at `/etc/fortiauthproxy/fortiauthproxy.conf`. You can use the same configuration file if you want to rebuild the VM instance.

Configuring LDAP proxy

1. Configure the *Proxy Port*.
2. Specify a *Sync Interval*.

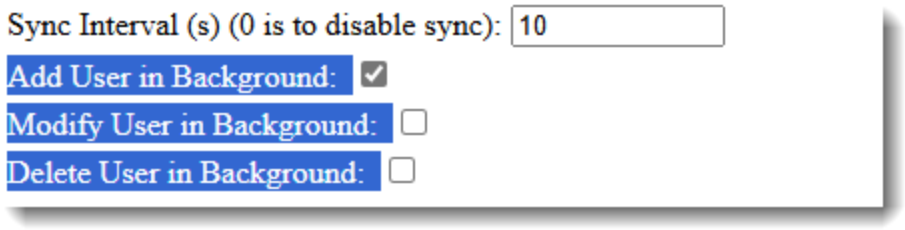
- The *Sync Interval* determines how frequently the system checks for changes. A value greater than 0 means periodic syncing is enabled.

3. Select the actions (Add/Modify/Delete User in Background) to be performed:

a. *Add User in Background: allows background processing of user additions.*

New users added to LDAP will automatically be detected and added to your system in the background during the next scheduled sync which is 10 seconds in the following illustration. The following screenshot shows that the system syncs with the LDAP server for newly added users once every 10 seconds. Because both *Delete User in Background* and *Modify User in Background* are disabled, it will not delete or modify users.

- FortiAuthProxy LDAP configuration:



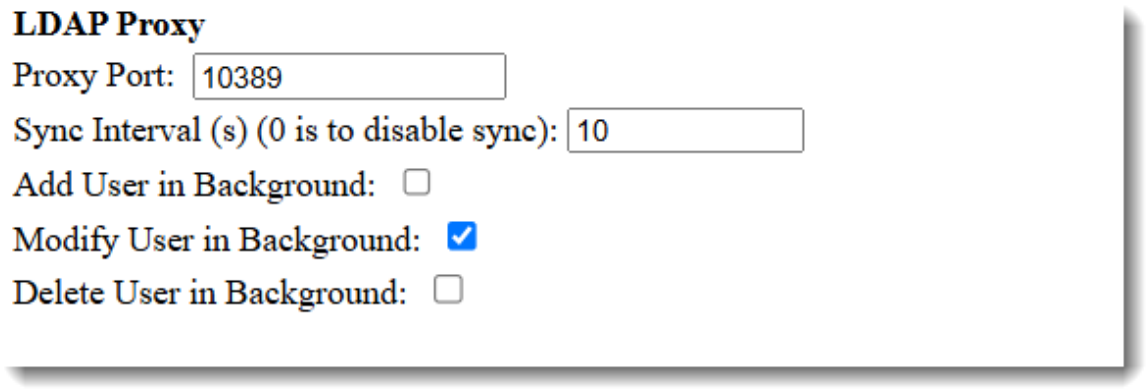
- FortiIdentity Cloud Management log page:

- The FortiAuthProxy log for user addition:

```
Number of users to be added to fortiIdentity-cloud:1
2025-          5:55 1 username:te          , email:          t@yahoo.com, mobile:
2025-          5:55 Number of users added to fortiIdentity-cloud:1
2025-          5:56 fp_sync_user -> user filter: (&(|(objectClass=person)(objectClass=user)(objectClass=inetOrgPerson))(sAMAccountName=*))
2025-          5:56 API: ftc_get_user, found users
2025-          5:58 fp_sync_user -> user filter: (&(|(objectClass=person)(objectClass=user)(objectClass=inetOrgPerson))(sAMAccountName=*))
2025-          5:58 API: ftc_get_user, found users
2025-          5:58
```

b. *Modify User in Background:* allows background processing of user modification, for example, modification of email and/or contact number.

- FortiAuthProxy LDAP configuration:



- FortiIdentity Cloud Management log for user modification:

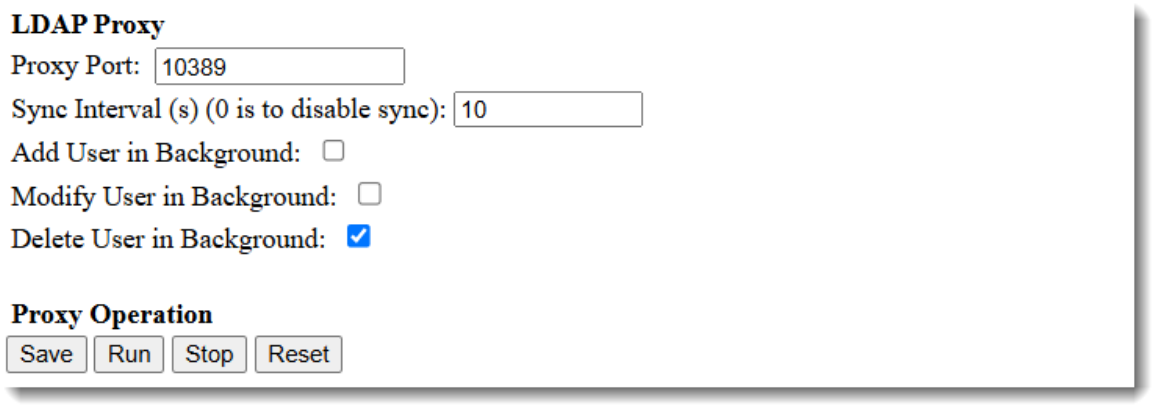
- FortiAuthProxy log for user modification:

```
Number of users to be modified in fortiIdentity-cloud:1
2025-08-21 23:35:58 1 username:      tFAP, email:      t@yahoo.com, mobile:+1      28
2025-08-21 23:35:58 Number of users modified in fortiIdentity-cloud:1
2025-08-21 23:36:00 fp_sync_user -> user filter: (&(|(objectClass=person)(objectClass=user)(objectClass=inetOrgPerson))(sAMAccountName=*))
2025-08-21 23:36:00 API: ftc_get_user, found users
```

If you want to change the user name in LDAP, you must enable *Add User in Background* and *Delete User in Background* as well.

c. *Delete User in Background:* allows background processing of user deletion.

- FortiAuthProxy LDAP configuration:

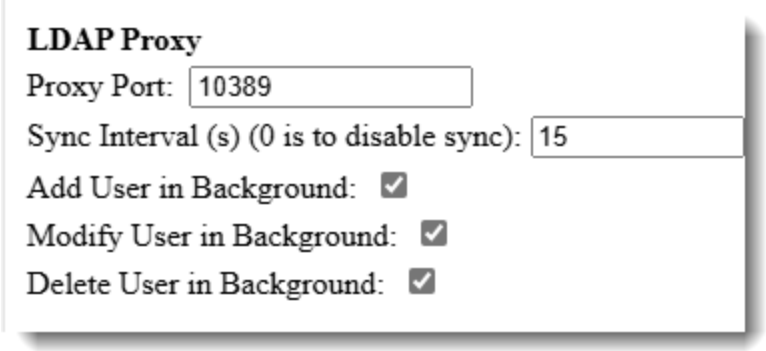


- FortiIdentity Cloud Management log for user deletion:

- FortiAuthProxy log for user deletion:

```
2025-08-21 23:42:57
Sync: number of users to be deleted from fortiIdentity-cloud: 1
2025-08-21 23:42:57 1 username:      AP, email:      @yahoo.com, mobile: +16
2025-08-21 23:42:57 Sync: number of users deleted from fortiIdentity-cloud:1
```

If the sync interval is set to a value greater than 0, the Add, Modify, and Delete options will take effect when selected. However, if the sync interval is set to 0, these options will not have any effect even if they are selected.



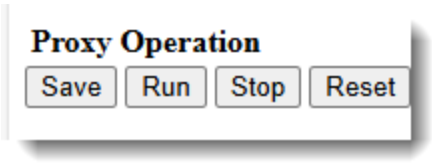
4. Save the configuration.

Keep the following in mind when configuring LDAP proxy:

- By default, the *Proxy Port* is 10389.
- The *Sync Interval* is in seconds.
- The *Add User in Background/Modify User in Background/ Delete User in Background* flags must be enabled to be effective.
- The *Sync Interval* can be determined by the time interval that the LDAP server uses to sync with FortiAuthProxy.
- Clicking *Run* starts background sync and authentication when the LDAP sync interval is greater than 0.
- No manual LDAP search is needed.
- An email attribute must exist for a user to be created in FIC.

FAP will only prompt the LDAP configuration check results when *Delete User in Background* is enabled. Be sure to check the log to ensure that the LDAP connection works as expected if this is not selected.

Making configuration changes



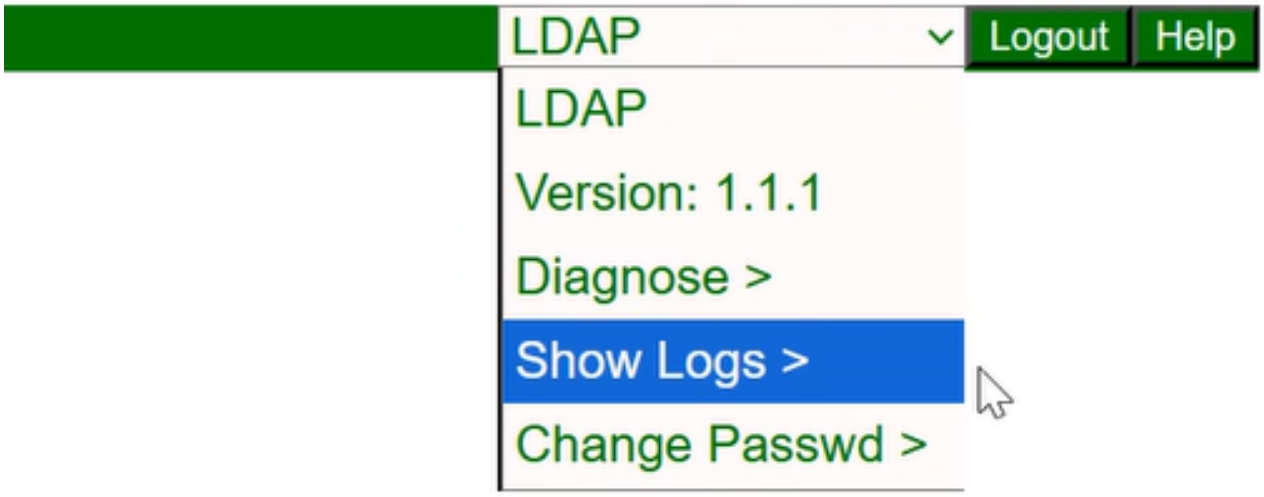
1. Locate the *Proxy Operation* panel.
2. Click *Stop* to pause FortiAuthProxy.
3. Make the intended configuration changes.
4. Click *Save*.
5. Click *Run* to restart FortiAuthProxy.

- Be sure to stop FortiAuthProxy before attempting to make changes. Changes made to FortiAuthProxy configuration will not be saved if you do not stop FortiAuthProxy before making the changes.
- Stopping FAP won't affect adding, modifying, or deleting users from FIC with debug commands.

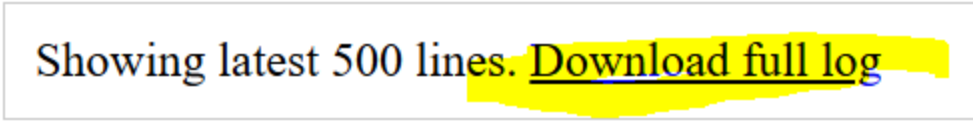
6. To reset the configuration file, click *Reset*.

Viewing logs

1. Click the down arrow in the upper-right corner of the FortiAuthProxy portal.
2. From the drop-down menu, select *Show Logs*.



3. You can also download the logs by clicking the *Download full log* link.



Currently, logs rotate at 10 MB, keeping three backups. Once it reaches the threshold, approximately 40 MB, the oldest log is deleted.

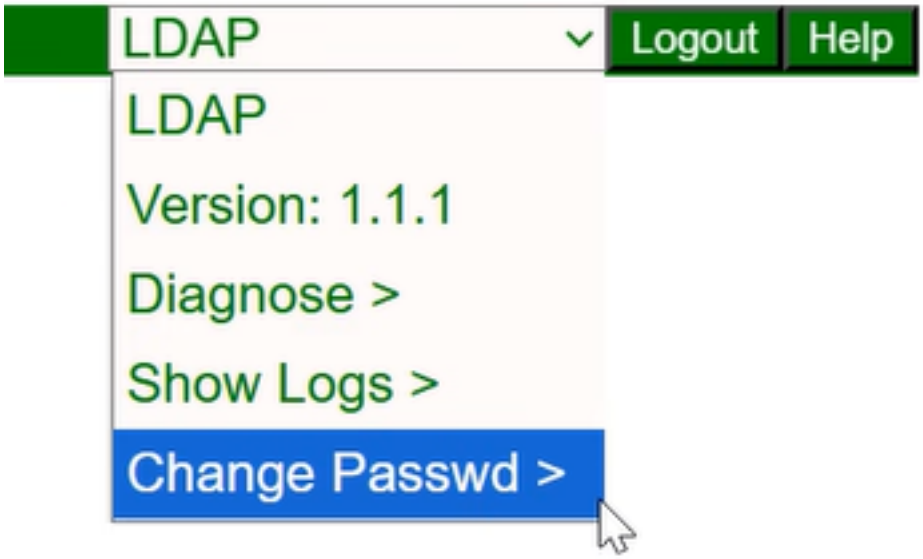
4. You can access the logs from the backend at - `/var/log/fortiauthproxy/fortiauthproxy.log`

```
ubuntu@ubuntu-server:/var/log/fortiauthproxy$ ls -al
total 31944
drwxrwx---+  2 fortiauthproxy fortiauthproxy     4096 Sep 12 17:02 .
drwxrwxr-x+ 11 root          syslog             4096 Sep 11 23:34 ..
-rw-rw----+  1 fortiauthproxy fortiauthproxy        0 Sep 11 23:07 cmderr.txt
-rw-rw----+  1 fortiauthproxy fortiauthproxy    14453 Sep 11 23:07 cmdout.txt
-rw-rw----+  1 fortiauthproxy fortiauthproxy  1219919 Sep 12 17:05 fortiauthproxy.log
-rw-rw----+  1 fortiauthproxy fortiauthproxy 10485642 Sep 12 17:02 fortiauthproxy.log.1
-rw-rw----+  1 fortiauthproxy fortiauthproxy 10485698 Sep 12 16:35 fortiauthproxy.log.2
-rw-rw----+  1 fortiauthproxy fortiauthproxy 10485376 Sep 12 16:09 fortiauthproxy.log.3
-rw-rw----+  1 fortiauthproxy fortiauthproxy      371 Sep 11 23:07 forti_event.log
ubuntu@ubuntu-server:/var/log/fortiauthproxy$
```

Changing the password

For the current release, FortiAuthProxy has only one administrator user which is `'admin'`.

1. From the drop-down menu, select *Change Password*.

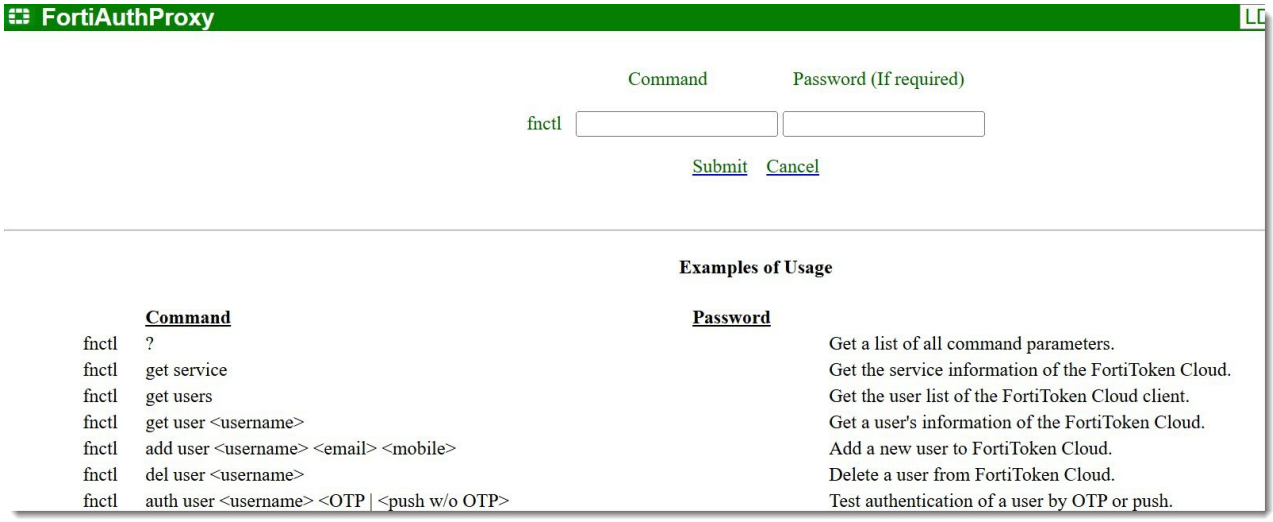


2. Update the password, and click *Submit*.
3. To factory-reset the password, log into the FortiAuthProxy VM through SSH, and run `fnctl reset password`.

- If you cannot reset the password, check to see if the hard disk is full by running – `df -kh`
- If the disk space is 100% full, extend the disk size. For more information, see Deploying FortiAuthProxy in ESXi on page 6.

Using Diagnose commands

1. Click the down arrow in the upper-right corner of the FortiAuthProxy portal.
2. Select *Diagnose* from the drop-down menu.
3. Use any of the `fnctl` commands to diagnose FIC from FortiAuthProxy, as shown in the following screenshot.



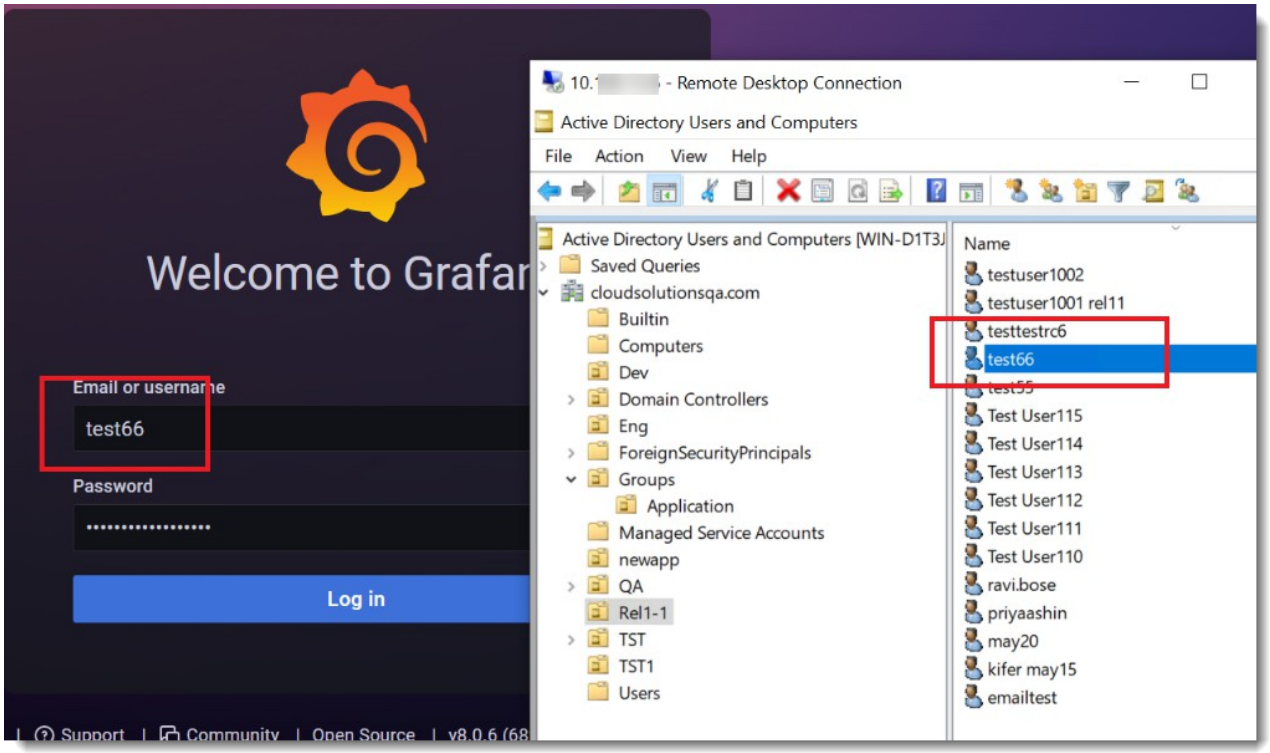
Client-side LDAP login using FortiAuthProxy

The following steps are based on a fictitious instance for illustration purposes only.

1. Configure *Grafana* as a client with FortiAuthProxy using LDAP.

```
apiVersion: v1
data:
  ldap.toml: |-
    [[servers]]
    # Ldap server host (specify multiple hosts space separated)
    host = "[redacted]"
    # Default port is 389 or 636 if use_ssl = true
    port = 10389
```

2. In FIC, set the default authentication method to FTM for the associated realm and enable user synch.
   Note: If user sync is not enabled, the token activation email will be sent to the user when the user tries to log in for the first time.
3. Once the token is activated, the user can use FTM for MFA.



By using FortiAuthProxy, *Grafana* is able to authenticate users from the LDAP and leverage FIC's MFA capability for added security.

Logging in using MFA

Logging in with Push Notification

1. In FortiIdentity Cloud, set the end user's MFA method to *FTM*.
2. Activate the token by scanning the QR code or manually entering the activation code.
3. In the web application, enter the username and password.
4. Click *Push Notification* that appears in the mobile device on which the token has been activated (Refer to Step 2 above).
5. Click *Approve*.

Logging in with OTP from a mobile device

1. In FortiIdentity Cloud, set the end user's MFA method to *FTM*, and disable *Push Notification* for it.
2. Activate the token by scanning the QR code or manually entering the activation code.
   (**Note**: The system will send an OTP to the end user's FTM app shortly.)
3. Enter the username and password and the OTP in the web app.

Logging in with OTP through email

1. In FortiIdentity Cloud, set the end user's MFA method to Email.
2. In the web application, enter the username and password. (**Note**: The system will email the end user an OTP shortly.)
3. Enter the username and password and the OTP, and log in again.

Logging in with OTP through SMS

1. In FortiIdentity Cloud, set the end user's MFA method to SMS.
2. In the web application, enter the username and password. (**Note**: The system will send an OTP to the end user through SMS shortly.)
3. Enter the username and password and the OTP, and log in again.

Troubleshooting

Issue	Solution
Why can't I find any users?	Check to see if the LDAP DN has been set up correctly. A wrong DN could reach different dictionaries where the user information does not exist.
Why can't I verify synced user credentials?	Check to see if the end users' passwords have been entered correctly. You can verify if the users are in FortiIdentity Cloud using the following command: `fnctl get users`
Why can't a user receive OTP in email?	On the FortiIdentity Cloud *Users* page, check to see if the email address has been entered correctly. The user may also want to check their spam or trash folders.
Why can't a user receive OTP in SMS?	On the FortiIdentity Cloud *Users* page, check to see if the mobile number has been entered correctly, including the country code. You may also want to check if the FortiIdentity Cloud account has enough SMS quota to use SMS messaging services. Keep in mind that SMS rates vary by country. For more information, see SMS Rate by Country.
Why can't I sync more users between LDAP server and backend MFA services?	First of all, check to see if you have enough user quota in your FortiIdentity Cloud account to sync a large number of end users. Then, check to see if the realm of the web app has been assigned enough user quota when Share-Quota Mode is disabled. For more information, see Share-quota Mode. To check your account user quota, execute the following command: `fnctl get service`
Why did I get an invalid login access error?	First of all, make sure that the username and password are correct. If they are correct, check the VM disk size in the backend with the command `df -kh`. If the disk is full, add more disk size for the image in ESXi and allocate the new size in the backend. Always remember to restart FortiAuthProxy from the frontend using the Stop button and then the Start button after rebooting the VM, even if it shows running in the frontend.
How to reboot FortiAuthProxy?	 Currently, you can reboot FortiAuthProxyfrom ESXi only.. 1. On the GUI, stop FortiAuthProxy by clicking the *Stop* button. 2. Reboot the VM from ESXi. 3. After the VM is up, restart FortiAuthProxy by clicking the *Start* button on the GUI.

Issue	Solution
	 If you do not stop FortiAuthProxy before rebooting from ESXi, FortiAuthProxy may not function normally. In that case, you should restart FortiAuthProxy from the GUI by clicking the *Stop* button and then the *Start* button.
Why is the login process so slow?	Check your LDAP server and make sure that it is working as expected. Degraded LDAP response time could slow down the authentication process.

Change Log

Date	Change Description
December 7, 2025	Initial release.

www.fortinet.com