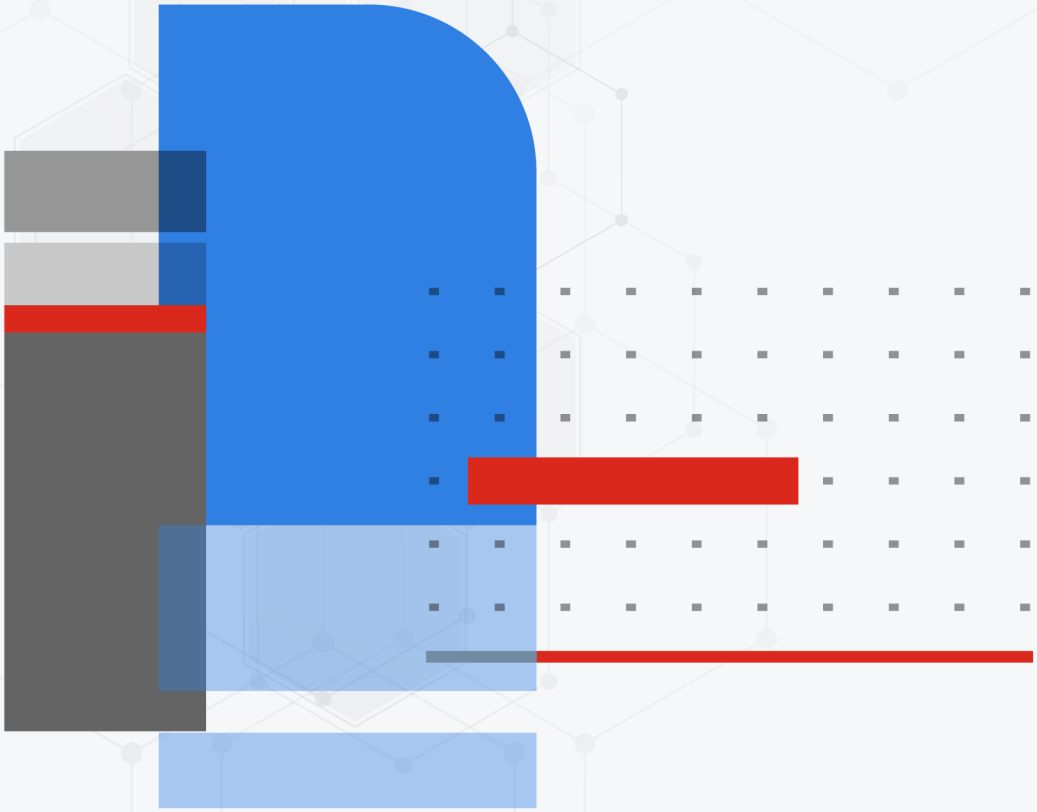
# User Access Control

FortiEdge Cloud 25.4.0



**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

Nov 05, 2025
FortiEdge Cloud 25.4.0 User Access Control
53-254-1222893-20251105

# TABLE OF CONTENTS

# Change log

| Date | Change description |
| --- | --- |
| 2025-11-05 | FortiEdge Cloud 25.4.0 release version. |

# Types of User Access

Creating multiple different types of users with unique access control attributes is a key feature of FortiLAN Cloud. These user types are created to govern role and permission based authorization and access to FortiLAN Cloud assets and data. You can create and manage different types of users from FortiCloud (**IAM and external IdP**) and from FortiLAN Cloud (**email users**) as well. The following users/access types are supported in FortiLAN Cloud.

- IAM Users
- External IdP
- API Users
- Email Users

## IAM Users

Identity & Access Management (IAM) is a service to help you control access to FortiCloud portals and assets. The IAM user type provides more control and flexibility when assigning user permissions. Save time creating new users by applying the permissions of an existing user to a new user or adding the user to a group. Account administrators can temporarily disable vulnerable IAM users and enforce Two-Factor Authentication at the account level. Access the IAM service from the FortiCloud portal using the master FortiLAN Cloud account.

## External IdP

External IdP roles allow IdP users to log in to a cloud portal with their organization's ID provider. External IdP roles allow you to create one role for many users while leveraging all of the benefits of the IAM user type. One account can have more than one external IdP role. User accounts with multiple roles are required to select a role before they can access a portal. This is useful for enterprises that need to secure their user credentials and hence provision FortiLAN Cloud access through their own Identity Provider.

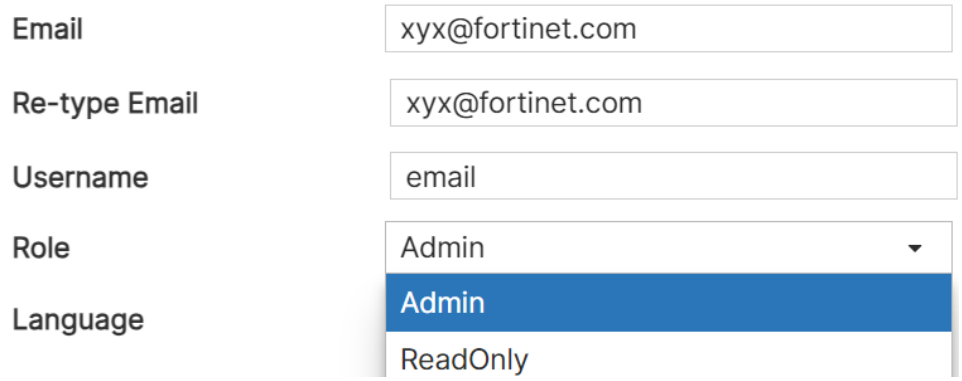
## API Users

API users can access FortiCloud services through APIs. API users can only use OAuth 2.0 for authentication then access web service APIs provided by each FortiCloud service portal.

# Email Users

The legacy email users are created and managed in FortiLAN Cloud using the registered user email address.They have access at the FortiLAN Cloud account level only and to no other FortiCloud service.

You can create an email user in the **Manage User Access** page of the FortiLAN Cloud portal. Click **Add Email User (Legacy)**.




Based on your user access requirement, assign Admin or ReadOnly permissions to each user, granting full access or restricted access to various networks and assets.

You can migrate the legacy email users to IAM users following the user migration procedure in the FortiLAN Cloud portal.

### Detailed Documentation References

To migrate legacy email users to IAM users, see Migrating legacy email users.

# User Access Control

This section describes the role of permission profiles in adding IAM users and external IdP roles in FortiCloud and authenticating various users on FortiLAN Cloud.



## Permission Profiles

You can define permission profiles to manage users' access and asset permissions. Instead of assigning full access permissions or limited access for the user account, you can select the access types described in this section when creating a permission profile. This allows for a more granular combination of access and asset permissions when creating users in FortiCloud. The permission model is multi-dimensional to provide fine grained control and easy of use.

- **Permission Profile** - Defines the enables portals and access permissions available to an assigned user. Instead of assigning portal permissions directly when creating an IAM user, external IdP role, and so on, the user is assigned to a permission profile. Ensure to create a permission profile for FortiLAN Cloud before assigning a user; you can assign a permission profile to multiple users and user groups. The following access types are supported for FortiLAN Cloud.
  - **Admin** - This provides full access to the FortiLAN Cloud portal that includes network monitoring and all configuration.
  - **Read-Only** - This provides limited access to the FortiLAN Cloud portal that includes *only* monitoring. Users are not allowed to configure features.
  - **Guest Manager** - This provides access to only manage (add and delete) guest users logging in into FortiLAN Cloud.
- **Permission Scope** - The permission scope defines the scope of access within the account. Management of the account is dependent on the available and selected scope.

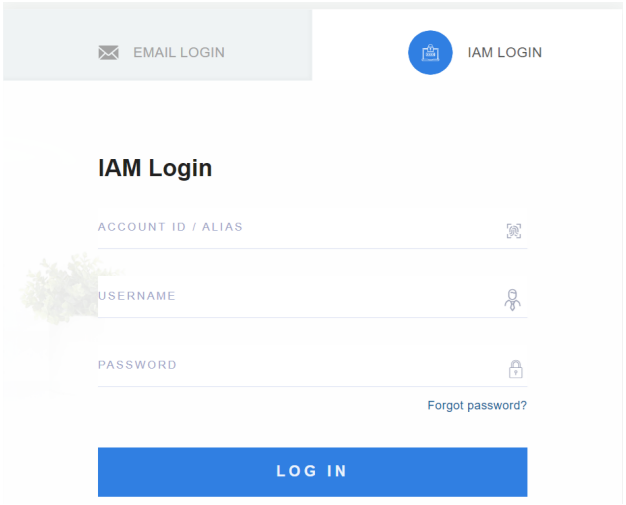
For more information, see Permission profiles.

## Adding and Authentication Users

You can add and authenticate users via the FortiLAN Cloud/FortiCloud portals.

### IAM Users

The IAM users can access FortiLAN Cloud with a FortiCloud account. Each IAM account requires an *Account ID/Alias*, *User Name*, and *password* to log in to a portal. Administrators can assign permission profiles to an IAM user or to an IAM user group. Login credentials are shared after an IAM user is added in FortiCloud.




In the **Manage Account Access** page of the FortiLAN Cloud portal, you can migrate the legacy email users to IAM users. This migration procedure is applicable to only those FortiLAN Cloud email users who are present in FortiCloud.

### Detailed Documentation References

- To add and manage IAM users from FortiCloud, see IAM users.
- To migrate the users to FortiCloud IAM, see Migrate legacy FortiLAN Cloud users to FortiCloud IAM.

## External IdP roles

External IdP roles allow external users to log in into cloud portal using their organization's ID provider. External IdP roles are authenticated with a custom login page. After the user is authenticated, they are redirected to a jump page where they can select the cloud portal(s) assigned to their account. One account can have more than one external IdP role. User accounts with multiple roles are required to select a role before they can access a portal. Users with no roles assigned to their account are blocked.

### Detailed Documentation References

- To create external IdP roles in FortiCloud, see External IdP roles.
- To add and manage external IdP roles in FortiLAN Cloud, see External IdP authentication.

## API Users

API user IDs and passwords are generated by the IAM service portal. One FortiCloud account can have multiple API users. The IAM service administrator can define which cloud portals the user can access, as well as the user's read/write permissions.

### Detailed Documentation References

- To add and manage API users, see API Users.
- For more information on FortiLAN Cloud REST APIs, see API Access.

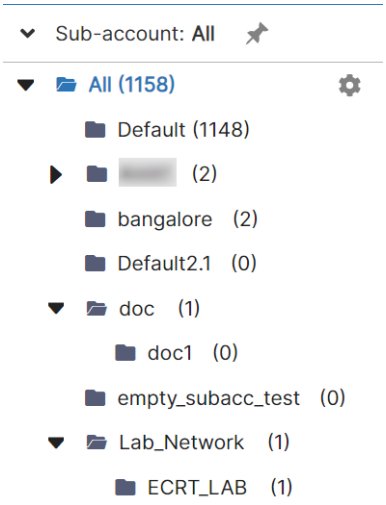
# Managed Security Service Providers (MSSP)

FortiEdge Cloud will no longer support multi-tenancy license extensions after December 31, 2026. Any multi-tenancy license extended will have its expiration date set to December 31, 2026, regardless of the start date.

If you currently use multi-tenancy feature, you must now transition to use the *FortiCloud Organization* feature for managing multiple entities within FortiEdge Cloud. See FortiCloud Organization.

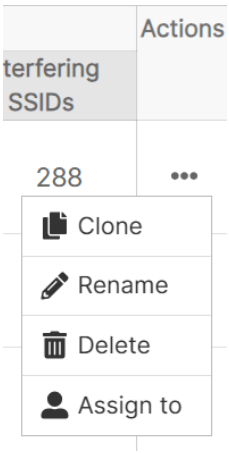
In an MSSP enabled FortiLAN Cloud setup, you can restrict the access of all users (email/external IdP) to specific sub-accounts, thereby selectively providing full access (admin) or read-only permissions to users over specific networks. The multi-tenancy account is designed for MSSPs, wherein, you can create and manage multiple sub-accounts and add or move devices between these sub-accounts. Each account can have its own administrators and users, allowing more control over a managed service's provisioning.

MSSP sub-accounts are added at the network view level and are considered as sites/sub-sites. An hierarchical tree view is formed as more sub-accounts are added, each sub-account can have users assigned to them at different levels in the hierarchy. The sub-account users are given regular user permissions and can have access to more than one sub-account. A sub-account user can only view the sub-accounts and monitor the networks that it is associated with.




- You are required to create email users to assign administrative rights to their respective sub-accounts.
- The primary account is the master account (MSSP) for all sub-accounts.

You can assign/modify the access permissions to sub-accounts in the **Manage Account Access** page of the FortiLAN Cloud portal; edit a listed user and assign sub-accounts. By default, a new network is created in the default account, you are required to manually assign it to one or multiple sub-accounts. This is based on your requirement of providing full or limited access control over the network. In the dashboard, select **Assign to** in the **Actions** column for the network and select the sub-accounts to assign the network to.




### FortiCloud Organization

FortiCloud supports a centralized account management feature called *FortiCloud Organization* that consolidates multiple FortiCloud accounts into **Organization (O)** or **Organizational Units (OU)**. It allows FortiLAN Cloud Premium license holders to create accounts in FortiCloud. FortiCloud Organization is a central management service in that it is common platform across all Fortinet cloud portals. FortiLAN Cloud supports FortiCloud Organization feature in addition to the existing MSSP (multi-tenancy) feature. For more information, see the Organization Portal.

### Detailed Documentation References

To activate and manage MSSP, see Multi-tenancy.

# Resource/Task-Based Access Control (RTBAC)

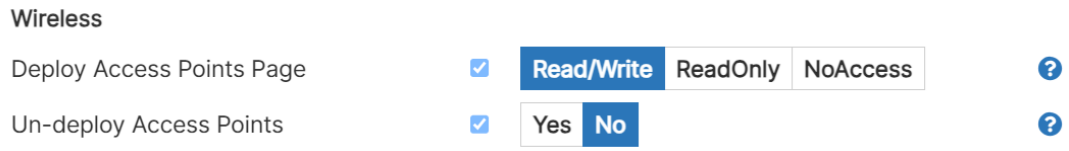
RTBAC enables you to control the tasks/operations and resources that a user can have access to, thus providing a more granular level of control over user access. RTBAC offers flexibility in defining access control policies to control the set of GUI pages served to different users. This feature aims at providing heightened data security with the ability to define multiple different profiles to restrict access as per your network requirements and efficiently assigning these access profiles to multiple users.

In the **Manage Account Access** page of the FortiLAN Cloud portal, you can associate access permissions with both users and specific tasks they intend to perform on resources, in addition to the assigned role in FortiCare for an account.

- **RTBAC profiles** – Create the profile to define resources and their configured permissions. You can set access permissions (**Read/Write**, **ReadOnly**, **NoAccess**) for specific GUI pages/features. Consider the following example, here the configured RTBAC profile provides varying access to the user in the **Devices** page.

  The user cannot view the account inventory details as there is no access to the **Inventory Devices** tab and can only view the deployed devices in the **Deployed Devices** tab. In the following example, a wireless user can deploy FortiAPs in the **Deploy APs** page but does not have permission to un-deploy them.

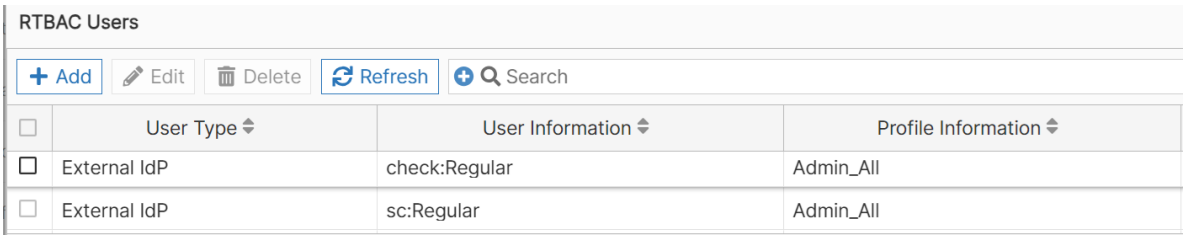
  You can use the **Apply template** option to reset all permissions configured for the **Resources/Tasks** and grant blanket permissions.

  **Notes**:

  - The permissions configured in this page are overridden by the **Access Type** set in the FortiCare account. For example, if the user **Access Type** is **ReadOnly** in FortiCare then all **Read/Write** permissions are reset to **ReadOnly**.
  - The resources/tasks with un-configured permissions on this page are granted access based on the **Access Type** (Admin/ReadOnly) configured in FortiCare.
- **RTBAC users** - You can assign an RTBAC profile to one or multiple FortiLAN Cloud users, and every account can have multiple RTBAC profiles. You can assign RTBAC profiles to an RTBAC user, external IdP, email, and IAM users are supported. In the following example, the same RTBAC profile is assigned to

two users.




For detailed configuration information, see RTBAC.

www.fortinet.com