



Concept Guide

FortiCloud



DEFINE / DESIGN / DEPLOY / DEMO



Table of Contents

Change Log	3
Introduction	4
FortiCloud as Fortinet's suite of Cloud portals	4
About this guide	5
FortiCloud account	6
Register products and licenses	7
FortiZTP	7
Pending registration	7
FortiCare Asset Management API	8
Cloud products and services	9
FortiGate management	9
FortiGate Cloud	9
FortiManager Cloud	10
FortiEdge Cloud: FortiAP, FortiSwitch, and FortiExtender management	10
FortiEdge Cloud	10
Managed services	11
SOCaaS	11
Managed FortiGate Service	11
Cloud services	11
Other services	12
User management	16
IAM users	16
External IdP integration	17
Multitenancy	18
Organizations	18
Support services	19
FortiCare	19
Appendix A - Documentation References	20

Change Log

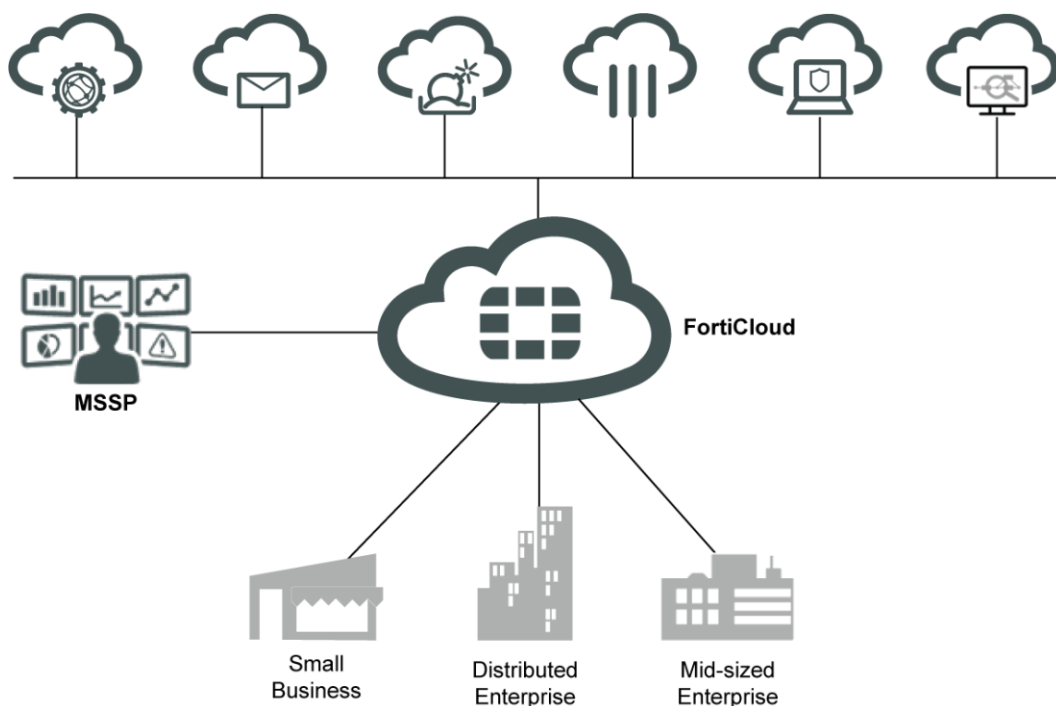
Date	Change Description
2025-05-03	Initial release.

Introduction

This document provides an overview of the FortiCloud Service portals and how it supports and relates to Fortinet Inc. Security-Driven Networking.

FortiCloud as Fortinet's suite of Cloud portals

FortiCloud provides a single point of access to all your Fortinet Cloud portals.



At Fortinet, to best serve our customers with our Security-Driven Networking, we have a range of cybersecurity and secure networking products that can be managed online through a web browser (Security as a Service). These service portals simplify management of our products, and maintain their data and configurations in Fortinet managed secure data centers; a vital service for businesses that would prefer not to maintain their own data centers.

FortiCloud is the umbrella portal for delivering all of Fortinet's cloud-based security and security management services. FortiCloud provides easy single sign on to all Fortinet cloud security services, and unifies those services with FortiCare support, Asset Management and Identity and Access Management (IAM).

The FortiCloud portal does not, of course, preclude using Fortinet products in, or as part of, a cloud-based infrastructure. FortiGate VMs, and other Fortinet VM products, can absolutely be deployed in, and used to secure, public, private, and hybrid cloud infrastructures, including all the major Infrastructure as a Service (IaaS) vendors, including AWS, Azure, Google cloud and others. Nevertheless, this document is focused not on those types of cloud computing, but on FortiCloud portals.

Several FortiCloud Cloud Management solutions are particularly well suited to LAN Edge and SD-Branch solutions, with several options targeting Security-Driven Networks built around FortiGates, FortiSwitches, and FortiAPs/WLANs.

About this guide

This guide aims to provide a broad overview of Security as a Service and FortiCloud concepts. It introduces Fortinet Inc. Cloud products, particularly the Fortinet Inc. Cloud Management products used with Security-Driven Networking devices such as FortiGate, FortiAP, FortiSwitch, and FortiExtender.

FortiCloud account

The FortiCloud account is a centralized login system provided by Fortinet. It serves as a unified authentication mechanism for accessing various Fortinet services and platforms. With a FortiCloud account, users can conveniently log in to multiple Fortinet cloud services and platforms using a single set of credentials. This eliminates the need to create and manage separate accounts for each service, streamlining the login process and enhancing user experience.

The FortiCloud account:

- Provides single Sign On (SSO) authentication to allow access all applications and services that support the FortiCloud account with a single set of credentials.
- Provides single Sign On (SSO) authentication for customized users and external IdP roles that have been configured for specific portal access capabilities.
- Binds all key resources such as hardware and software assets, products, services, users and roles.
- Support multifactor authentication and credential management.

Multiple user accounts and external IdP roles can be created within the account that have their own login credentials. By configuring permission profiles, users and roles can be created with specific access levels for portals, services, and features. This allows for specialized, granular access for those with access to the account through user logins. See [User management on page 16](#).

By leveraging the FortiCloud account, customers can access and manage their Fortinet cloud services, Fortinet support, collaborate within the Fortinet community, and utilize partner-specific resources and tools through a seamless and secure authentication framework.

For more information on creating a new account, see [Creating a FortiCloud account](#) in the FortiCloud Account guide.

Register products and licenses

Products, licenses, and contracts can be registered to your account and managed in the Asset Management portal. The Asset Management portal is an intuitive product registration portal; a place to organize and view all Fortinet products and services in a FortiCloud account. New products, licenses, or contracts are displayed in the *Product List* as well as a customizable folder structure called *My Assets*. The *Account Services* menu lists products, contracts, or licenses applicable at the account level. With *Online Renew*, licenses or contracts can be renewed directly from the portal for supported products and regions.

Asset Management includes:

- The ability to view, arrange, filter, and organize your entire portfolio of Fortinet assets.
- Search assets that can be searched by serial number, contract, or license number.
- The ability to register products and services, and access complete information, including entitlement, location, threat statistics, tickets, enabled Cloud services, license, and keys all in one place.
- *Asset folders* that help organize large number of assets into folder hierarchies.
- Dedicated and filtered views for expired units, decommissioned units on the registered products, and notifications on the assets

For more information, see [Registering assets](#) in the Asset Management guide.

FortiZTP

FortiZTP is a cloud service to manage zero touch provisioning of devices or VMs to cloud or on-premise management solutions from a centralized console. FortiZTP provides following features:

- Bulk provisioning of devices and VMs to a desired cloud service or on-premise management solution
- Visibility of where devices are provisioned
- Deprovisioning devices

FortiZTP automatically loads devices that are registered to Asset Management under the same FortiCloud account and Cloud or FortiDeploy key verification. You must perform the Cloud FortiDeploy key verification during Asset Management registration. If Asset Management does not prompt for the verification step, the Cloud key or FortiDeploy key is invalid in FortiCare. Contact Fortinet Support to inquire on the key status. The centralized FortiZTP service integrates with various FortiCloud services to view the provisioning status and perform actions to provision, deprovision, hide, or change provisioning targets.

See the [FortiZTP Administration Guide](#) for more information.

Pending registration

Unregistered products and devices are listed in the *Pending Registration* page. The registration status can be viewed here for hardware, contracts, and licenses. For more information, see [Pending registration](#) in the Asset Management guide,

FortiCare Asset Management API

FortiCare Asset Management APIs are a set of tools provided by Fortinet that enable programmatic access to asset management functionalities within the FortiCare platform. These APIs allow users to interact with FortiCare's asset management features programmatically, integrating them into their existing systems or workflows.

Key features and capabilities of FortiCare Asset Management APIs include:

Device registration	APIs to register Fortinet devices with the FortiCare platform.
Asset inventory management	APIs for retrieving and managing an inventory of Fortinet devices and their information associated with a FortiCloud account.
Device lifecycle management	APIs to facilitate device lifecycle management tasks, such as decommissioning.
Warranty and support information	APIs to retrieve contract, licenses, and support information for Fortinet devices, including warranty expiration dates, support entitlements, and service contract details.

By leveraging FortiCare Asset Management APIs, customers can automate and streamline their asset management processes, ensuring that their Fortinet devices are properly registered, maintained, and supported throughout their lifecycle. This can lead to improved efficiency, better resource utilization, and enhanced support experiences for users.

See the [Fortinet Developer Network \(FNDN\) Asset Management API](#) page for more information.

Cloud products and services

FortiCloud is Fortinet's Security as a Service platform for cloud-delivered security and security management services. FortiCloud provides customers with a simple way to connect, protect, and deliver their data and applications both on premises and in the Cloud. The FortiCloud offering suite is a set of cloud portals and services enabling customers to access and manage a range of Fortinet solutions and services from an easily accessible website.

FortiCloud provides integration of and single sign on for four categories of services:

- Cloud management and analysis for Fortinet Security-Driven Networking products
- Asset and account management
- FortiCare support services
- Cloud services for other Fortinet Security Fabric products

No two enterprises are identical, and neither are their networks or their security needs. FortiCloud provides multiple Management Portals to accommodate different customer needs. The following topic provides information on cloud products and services:

- [FortiGate management on page 9](#)
- [FortiEdge Cloud: FortiAP, FortiSwitch, and FortiExtender management on page 10](#)
- [Managed services on page 11](#)
- [Cloud services on page 11](#)
- [Other services on page 12](#)

FortiGate management

FortiGate in FortiCloud is managed with the following services:

- [FortiGate Cloud on page 9](#)
- [FortiManager Cloud on page 10](#)

FortiGate Cloud

FortiGate Cloud is an ideal way for a wide range of customers to easily add simplified cloud management to FortiGate based sites, whether a single campus or SD-Branch, or a highly distributed business with many sites. It is specifically aimed at sites utilizing SMB to mid-size FortiGate models, typically a FortiGate 40-200. A multi-tenant option is available, typically used by MSSPs who service such customers.

With a FortiGate Cloud account, you get:

- Simple and secure remote management of FortiGates and all downstream Fortinet devices, including FortiAPs, FortiSwitches, and FortiExtenders.
- One year of hosted log storage.
- Analytics, both on-demand and scheduled reporting.
- Zero-touch provisioning using FortiDeploy.
- Automation options, including:

- Run and schedule CLI scripts across one or multiple FortiGates.
- Cloud REST API.
- Automatic backups (stored in the cloud).
- Integrated FortiSandbox for zero-day threat detection.
- Optional integrated Indicator of Compromise (IOC) service.

FortiGate Cloud is the solution for adding cloud advantages to FortiGate and Fortinet Security-Driven Networking for small and midsize enterprises.

See the [FortiGate Cloud](#) documentation for more information.

FortiManager Cloud

FortiManager Cloud brings a cloud version of our flagship management tool, FortiManager, to our FortiCloud suite for centralized management. FortiManager Cloud is ideal for enterprise customers using high-end FortiGates (including any FortiAPs, FortiSwitches, and FortiExtenders managed by them) who need maximum automation and control across multiple sites. FortiManager Cloud supports a single ADOM (Administrative Domain) and is best suited to single enterprise customers, as MSSPs will usually want to host their own instances of multi-ADOM FortiManager.

Choose FortiManager Cloud when:

- A single ADOM works.
- FortiGates are typically top-end models.
- The highest level of remote automation is needed.
- Configurations across multiple FortiGates are very repetitive.
- Analytics across a network, rather than per site, are needed.

See the [FortiManager Cloud](#) documentation for more information.

FortiEdge Cloud: FortiAP, FortiSwitch, and FortiExtender management

Fortinet Security-Driven Networking products can be used independently from a FortiGate or in combination with a FortiGate as a total solution where the whole is greater than the sum of the parts.

FortiEdge Cloud

FortiEdge Cloud is a hosted cloud-based management platform for the Fortinet Secure LAN Edge (FortiSwitch and FortiAP), and FortiExtender 5G/LTE Gateways, offering zero touch deployment, configuration management, reporting and analytics for standalone LAN and WAN gateway extension deployments.

FortiEdge Cloud offers a simple, intuitive, easy-to-use interface to manage standalone FortiAP, FortiSwitch, and FortiExtender deployments that is available from anywhere at any time. Able to scale from a small handful of devices to thousands across multiple geographically distributed sites, FortiEdge Cloud enables you to improve productivity, customize notifications, and enhance the reliability and intelligence of your network and business operations.

FortiEdge Cloud offers a suite of advanced capabilities, including:

- Global multi-instance deployment for distributed network environments
- Robust REST API for effortless integration with existing systems

- Intuitive provisioning and monitoring tools
- Flexible Organization and OU structure supporting multi-tenant architectures

See [FortiEdge Cloud](#) documentation for more information.

Managed services

The following sections provide information on cloud management without a FortiGate:

- [SOCaaS on page 11](#)
- [Managed FortiGate Service on page 11](#)

SOCaaS

FortiCloud SOCaaS analyzes security events generated from FortiGate appliances, performs alert triage, and escalates verified threat notifications to the security team. SOCaaS complements incident response monitoring life cycles by providing continuous cyber awareness and control of the Fortinet Security Fabric. It provides security teams with enrichment of received FortiGate events through the application of standard event handlers, playbooks, and severity classification while distilling the FortiGuard threat research capability and vulnerability database.


Managed FortiGate Service

Managed FortiGate Service (MFGS) is a remote cloud-based managed network operations service run by Fortinet NOC experts to help organizations manage their network infrastructure efficiently.

Cloud services

FortiCloud has an extensive selection of additional cloud-delivered security and analytic tools. The following portals and tools relate to Cloud application security.

Cloud application	Description
FortiCamera Cloud	FortiCamera Cloud is a cloud-based Video Surveillance as a Service (VSaaS) platform. FortiCamera Cloud provides management and analytical capabilities across your entire FortiCamera deployment, and you can use it to deploy, set up, and view video streams from your FortiCamera devices. Permissions can be fine-tuned with organization-level and site-level privileges.
FortiCASB	FortiCASB is a cloud-native Cloud Access Security Broker (CASB) subscription service that is designed to provide visibility, compliance, data security, and threat protection for cloud-based services being used by an organization. It secures SaaS applications in use by your organization.
FortiDevSec	FortiDevSec offers a cloud and SaaS-based continuous application security testing built from the ground up to natively focus on software developers and DevOps.
FortiPhish	FortiPhish is a phishing simulation service to analyze how internal users interact

Cloud application	Description
	with phishing emails. Use FortiPhish to create custom phishing email campaigns and monitor how users respond to them. The FortiPhish portal contains dashboards with intuitive data analysis monitors to view responses across campaigns and monitor improvements over time.
FortiSandbox PaaS	<p>FortiSandbox executes suspicious files in a cloud VM host module to determine if the file is high, medium, or low risk based on the behavior observed. The rating engine scores each file from its behavior log gathered in the VM module to determine a risk level.</p> <hr/> <div>  <p>FortiSandbox PaaS is bundled with FortiGate Cloud.</p> </div>
FortiSASE	FortiSASE is a Secure Access Service Edge solution that can ensure remote, off-net endpoints are protected with the same security policies as when they are on-net, no matter their location.
FortiToken Cloud	FortiToken Cloud enables FortiGate and FortiAuthenticator customers to add multi-factor authentication (MFA) for their respective users, with no additional hardware or software required. It protects local and remote FortiGate and FortiAuthenticator administrators as well as firewall and VPN users.

Other services

The following table includes a list of other services included in the FortiCloud Services.

Cloud application	Description
FortiAppSec Cloud	FortiAppSec Cloud integrates Web Application Firewall, advanced bot protection, global load balancing, and threat analytics to offer centralized management, visibility, and policy consistency.
FortiCare Elite	FortiCare Elite Portal is a centralized monitoring platform for FortiGates that are registered to your FortiCloud account. The centralized service integrates with FortiGates to view statuses and provide recommendations. FortiCare Elite Portal only supports FortiGates and does not support other services and products registered to your FortiCloud account.
FortiCNP	FortiCNP is Fortinet's Cloud-Native Protection (CNP) service. FortiCNP Cloud Protection continuously monitors and tracks all security components, including configurations, user activity, traffic flow log, and data storage in public cloud environments.
FortiConverter	Migrating old, complex device configurations to new, next-generation solutions can be very challenging and require a lot of time. Errors are often introduced during this process as well. FortiConverter service provides the customer with a restorable configuration file converted from FortiGate, FortiWiFi, or third party firewalls, for use on the specific FortiGate or FortiWifi the service is registered against.

Cloud application	Description
FortiCWP	FortiCWP is Fortinet's cloud-native Cloud Workload Protection (CWP) service. FortiCWP integrates with APIs provided by cloud vendors including AWS, Azure, and Google Cloud Platform to monitor and track all security components, including configurations, user activity, and traffic flow logs.
FortiDAST	FortiDAST is a cloud enabled service that performs web application vulnerability testing through an intensive process of comprehensive and criteria based automated scanning and analysis. It adopts an organised technical approach of assessing your web applications running in an HTTP/HTTPS environment, to identify loopholes and vulnerabilities.
FortiDeceptor DaaS	FortiDeceptor DaaS integrates with your existing third-party security tools as well as with Fortinet Security Fabric – FortiGate, FortiEDR, and FortiNAC, providing a unified, automated threat mitigation, as well as with FortiSIEM, FortiSoar, and FortiAnalyzer, delivering comprehensive visibility and enriched threat intelligence data for fast analysis and accelerated response.
FortiDevice	FortiDevice is a platform that offers businesses a comprehensive security visibility in their network, with coverage for both managed and unmanaged systems. It merges asset, network, software, vulnerabilities, and user data from IT and security solutions to give insights into which systems lack essential security measures and which systems are not included in vulnerability management programs.
FortiDLP	FortiDLP protects organizations' networks, devices, applications, and data against insider and outsider threats. It blends active user behavior analytics and data loss prevention technologies to accelerate detection and response.
FortiEDR/XDR	FortiEDR provides multi-layered, post- and pre-infection protection that stops advanced malware in real time. FortiEDR recognizes that external threat actors cannot be prevented from infiltrating networks, and instead focuses on preventing the exfiltration and ransomware of critical data in the event of a cyber-attack.
FortiGate-as-a-Service	FortiGate-as-a-Service (FGaaS) is a hardware-as-a-service offering FortiGate next generation firewalls on various locations to securely maintain firewall infrastructure and deliver a wide range of network security capabilities, provided on-demand for users anywhere.
FortiGate CNF	FortiGate Cloud-Native Firewall (CNF) is software-as-a-service that simplifies cloud network security while providing availability and scalability. FortiGate CNF reduces the network security operations workload by eliminating the need to configure, provision, and maintain any firewall software infrastructure while allowing security teams to focus on security policy management. FortiGate CNF offers you the flexibility to procure on demand or use annual contracts.
FortiGuard ABP	FortiGuard ABP (Advanced Bot Protection) is a Fortinet SaaS advanced bot mitigation solution designed to detect and protect against sophisticated bots that may be used to conduct malicious automated attacks on your online applications, such as data harvesting, credential stuffing, account take-over attempts, DDoS attacks, and other fraudulent activities.
FortiMail	FortiMail Cloud email security is an independently validated and top-rated secure email gateway solution delivering >99% catch rate, multiple layers of

Cloud application	Description
	malware detection, and an extremely low false positive rate. Fully managed by Fortinet, FortiMail Cloud allows the customer to focus on business goals by relying on a trusted security expert to manage this key infrastructure security component.
FortiMonitor	FortiMonitor allows you to monitor your public and private infrastructure.
FortiPresence	FortiPresence combines Wi-Fi and analytics to understand customer behavior. Visitor smartphones automatically probe for wireless networks. FortiPresence uses existing, deployed Fortinet access points to detect these customer Wi-Fi signals to record location and movements of foot traffic. When combined with social network login portals (Facebook, Google, Instagram, LinkedIn), FortiPresence enables new forms of customer engagement.
FortiSIEM	FortiSIEM brings together visibility, correlation, analytics, UEBA, discovery and reporting into a single solution. It reduces the complexity of managing network and security operations to effectively free resources, improve incident detection, and even prevent breaches. FortiSIEM Cloud simplifies the implementation and ongoing management for organizations and MSSP's, allowing them to focus on incident detection and management.
FortiSOAR	FortiSOAR maximizes your SOC team efficiency and productivity by automatically taking actions and executing playbooks, visualizing your SOC team's workload, calculating average MTTR across resolved alerts and incidents, reporting overall SOC team health, and producing a final remediation report of incidents with tagged VIP assets.
FortiTrust Identity	FortiTrust Identity provides Identity and Access Management as a service (IdaaS), including passwordless FIDO, MFA, Adaptive Authentication, OIDC, SAML, and Certificate Management.
FortiRecon	FortiRecon Digital Risk Protection (DRP), a SaaS-based service, includes: External Attack Surface Management, Brand Protection, and Adversary Centric Intelligence. Part of the Fortinet Inc. SecOps Platform, FortiRecon shows what adversaries are seeing, doing, and planning to help counter attacks at the reconnaissance phase and significantly reduce the risk, time, and cost of later-stage threat mitigation.
FortiVoice Cloud	FortiVoice Cloud is a secure cloud-based unified communications solution with all-inclusive calling and conferencing features. You can deploy this solution without the expertise in private branch exchange (PBX) and activate user services from an intuitive cloud platform.
FortiZTP	FortiZTP is a cloud service to manage zero touch provisioning of devices or VMs to cloud or on-premise management solutions from a centralized console.
Lacework FortiCNAPP	Lacework FortiCNAPP delivers end-to-end visibility into what's happening across your cloud environment, including detecting threats, vulnerabilities, misconfigurations, and unusual activity, so you can innovate with speed and safety.
Overlay-as-a-Service	Overlay-as-a-Service (OaaS) is a cloud-based Software-as-a-Service solution for provisioning and monitoring new SD-WAN Overlay networks using FortiGate physical or virtual appliances.

OTHER SERVICES

Cloud application	Description
Security Awareness and Training	Security Awareness and Training (SAT) is a cloud-based Software-as-a-Service solution that provides you with the ability to deploy and maintain a cybersecurity awareness training program within your company.

User management

Multiple users and external IdP roles can be created within a single account in the Identity and Access Management (IAM) portal. The IAM portal enables granular access control by allowing you to create and assign customized permission profiles to the users and roles. Permission profiles define the portals and level of access a user or role has when accessing FortiCloud portal and services. This then complements account management for all of an organization's FortiCloud portals and assets.

Use the portal to manage users, authentication credentials, and asset permissions. See [User management models](#) in the IAM guide.

This section includes the following:

- [IAM users on page 16](#)
- [External IdP integration on page 17](#)

IAM users

The IAM User Model utilizes portal and role-based permission profiles to manage users' access and asset permissions effectively. Instead of simply assigning Full Access or Limited Access, IAM administrators select access types defined by the portal and roles when creating permission profiles. This approach allows for a more nuanced control over user access and asset permissions.

The following table demonstrates key concepts:

Permission profiles	IAM administrators create permission profiles within the IAM portal, defining access types for users. These profiles are tailored to match the specific needs of different user roles within the organization.
Permission scope	Asset permissions are based on the organizational structure or asset folders within the Asset Management (AM) portal. This enables a granular combination of access and asset permissions, ensuring users only have access to the assets relevant to their role.
Master user (Account Owner)	The master user, or Account Owner, has access to the IAM portal and sets permissions for IAM users. This centralizes control and ensures consistent management of user access across the organization.
User groups	IAM supports user groups, streamlining the process of creating new users by applying predefined permissions. This saves time and ensures consistency in access control.
Two-Factor Authentication (2FA)	IAM provides support for two-factor authentication at the account level, enhancing security by requiring an additional verification step for user logins.
Granular permission granting	Users are granted access only to the portals and assets they require for their roles. This ensures least privilege access and minimizes the risk of unauthorized access to sensitive information.
Asset Management folder structure	Permissions can be assigned based on the folder structure of the organization's Asset Manager, allowing for easy alignment of access controls with the organization's workflow.

API users	IAM supports API users for programmatic access tailored to each portal, enabling automation and integration with other systems.
External Identity Provider (IdP) integration	IAM offers support for external Identity Provider (IdP) authentication, allowing organizations to integrate their existing identity controls seamlessly.

Resources for Further Information:

- For more detailed information on Identity & Access Management (IAM), additional guidance, and best practices, refer to the [Identity & Access Management \(IAM\) guide](#).
- Explore [External IdP integration on page 17](#) for instructions on integrating external identity providers.

By leveraging these features, organizations can effectively manage user access and permissions within their IAM framework, enhancing security and productivity across their digital ecosystem.

External IdP integration

Customers can integrate their own IdP with FortiCloud. FortiCloud supports fine grained permission profile for external IdP users through external IdP IAM role. External IdP roles allow external users to log in to a 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 page where they can select the cloud portals 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. With IdP initiated authentication, customers can access FortiCloud Products, Services and Support.

If connected to the Organization's root account, external IdP users can be granted permissions to manage member accounts within Organizations.

See [External IdP](#) and [External IdP roles](#) in the IAM guide.

Multitenancy

FortiCloud Services' infrastructure supports multitenancy solutions for [managed security service providers \(MSSP\)](#).

Organizations

FortiCloud Organization serves as a centralized hub for MSSPs, Partners, or customers to manage multiple FortiCloud accounts efficiently. It acts as a control center where accounts are consolidated and organized for streamlined management.

Within the portal, users can create Organizations and Organizational Units (OUs) to categorize and group accounts based on their needs. Each account represents a unique set of Fortinet devices and services.

Users gain access to a unified dashboard, providing visibility into all managed assets and cloud services across their accounts. They can invite new accounts to join their managed services, structure accounts hierarchically, and assign access roles to team members as needed.

With the FortiCloud Organization portal, MSSPs, Partners, or customers can enhance their operational efficiency, ensure compliance, and deliver superior services to their clients or users. It serves as a versatile tool for orchestrating managed services and optimizing cloud management efforts effectively.

See the [Organization Portal](#) guide for more information.

Support services

FortiCloud Services provides support customer support in the FortiCare ticketing portal.

FortiCare

The FortiCare portal is a user-friendly ticketing system, designed to streamline your ticket management process. The new comprehensive ticketing web interface supports various workflows based on the ticket types to efficiently submit, track, prioritize, and resolve tickets with ease.

Key features include:

- Creating new tickets of various types:
 - Technical support
 - Customer service
 - DOA/RMA
 - Anti Virus and FortiGuard Service
 - FortiConverter
- Searching, viewing status, and commenting
- Exporting ticket information

See the [FortiCare](#) guide for more information.

Appendix A - Documentation References

The following documentation resources are available:

- [FortiCloud solution hub](#)
- [FortiCloud Services documentation](#)



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 SVP Legal and above, 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.