



DEFINE • DESIGN • DEPLOY

FortiCloud

Concept Guide

Version 23.2

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<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>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



May 12, 2023

FortiCloud 23.2 Concept Guide

57-232-890128-20230512

TABLE OF CONTENTS

Change Log	5
Introduction	6
FortiCloud as Fortinet's suite of SaaS portals	6
Intended audience	7
About this guide	7
FortiCloud Security as a Service	8
Cloud management and analytics for security driven networking	8
Fortinet networking products	9
The LAN Edge with FortiSwitches and FortiAPs	9
FortiAPs	10
FortiSwitches	10
The WAN Edge with Integrated SD-WAN and FortiExtender	10
Fortinet Secure SD-WAN	10
FortiExtender	11
FortiCloud Management Portals	12
FortiGate Management	13
FortiGate Cloud	13
FortiManager Cloud	14
WLAN, LAN, WAN Direct Management (without a FortiGate)	15
FortiLAN Cloud	15
FortiExtender Cloud	16
Asset and account management with FortiCloud	17
FortiDeploy	17
Asset Management	18
Identity and Access Management (IAM)	18
FortiCare Support	19
Cloud services and other Security Fabric portals	20
FortiPresence	20
FortiToken Cloud	21
FortiCASB	21
FortiPenTest	21
FortiMail Cloud	22
FortiSandbox PaaS	22
FortiPhish Cloud	22
FortiWeb Cloud	23
FortiInsight	23
OCVPN Portal	23
FortiGSLB	24
FortiCWP	24
FortiConverter	24
SOCaaS	25

FortiVoice	25
FortiSASE	25
FortiDevSec	26
Appendix A - Documentation References	27

Change Log

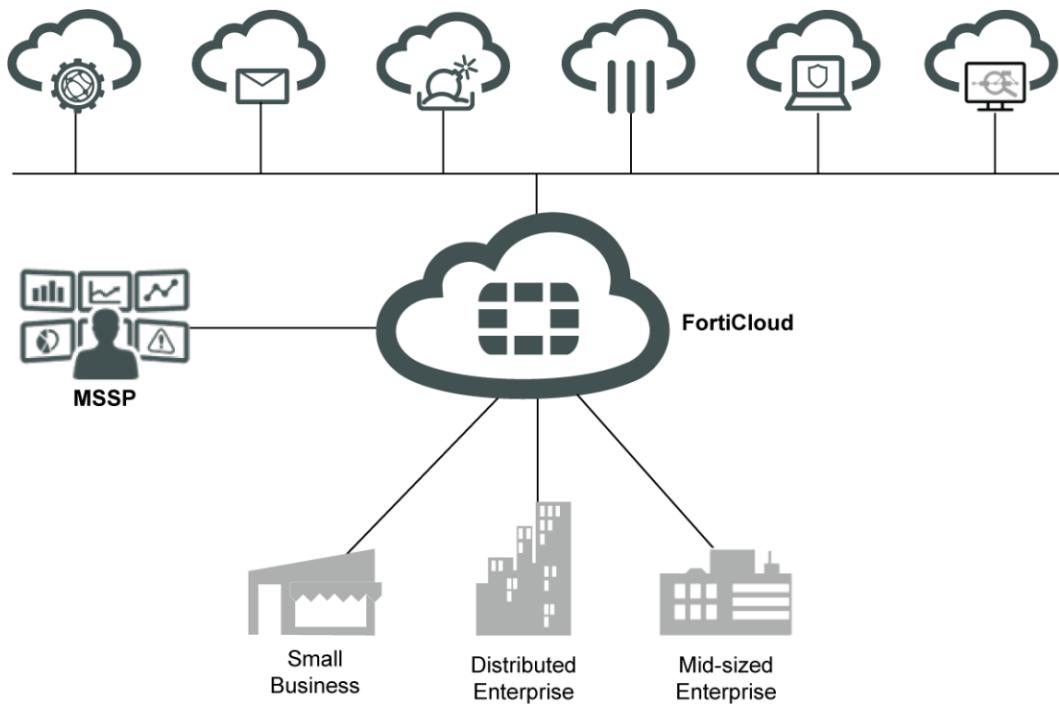
Date	Change Description
2023-04-29	Initial release.
2023-05-12	Updated FortiSandbox PaaS on page 22.

Introduction

This document provides an overview of the FortiCloud SaaS (Security as a Service) portal and how it supports and relates to Fortinet Security-Driven Networking.

FortiCloud as Fortinet's suite of SaaS portals

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



“Cloud” is the go-to word for computer companies these days. It can be confusing figuring out exactly what a cloud option is, because context matters and Cloud Services versus Cloud Infrastructure versus Cloud Platforms are, in fact, different things. All those variations can obscure the fact that when we are talking about computers and not fluffy white things in the sky, “The Cloud” really just means “The Internet.” That is, any cloud interaction is interacting with a computer that someone else owns and is responsible for, instead of an in-house computer that local IT staff are responsible for.

Any use of an Internet service, especially if it involves the user logging in and otherwise controlled access to data on the Internet side, is in fact making use of cloud computing, following the Software/Security as a Service (SaaS) model. Online shopping is cloud computing, as is video streaming services, online banking, customer relationship management, and really, virtually everything on the Internet including Fortinet's [support site](#). In fact, the FortiCare support site is the gateway to FortiCloud services!

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 via 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, Fortinet Asset Management, and Fortinet Identity and User Management (IAM).

The FortiCloud SaaS 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 SaaS portals.

Several FortiCloud SaaS 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.

Intended audience

This guide is intended for an audience which is interested in learning about the FortiCloud Security as a Service portal and its usefulness in managing Fortinet Security-Driven Networking solutions in particular. Readers should have a basic understanding of networking and network security before they begin. Interested audiences may include:

- Network, wireless, and security architects
- Network, wireless, and security engineers

About this guide

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

FortiCloud Security as a Service

FortiCloud is Fortinet's Security as a Service (SaaS) 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

The following topic provides information on cloud security management:

- [Cloud management and analytics for security driven networking on page 8](#)

Cloud management and analytics for security driven networking

Some context is necessary when talking about "Cloud Security Management." It begs the question, "managing what, exactly?" Well, at Fortinet, almost everything starts with the FortiGate.

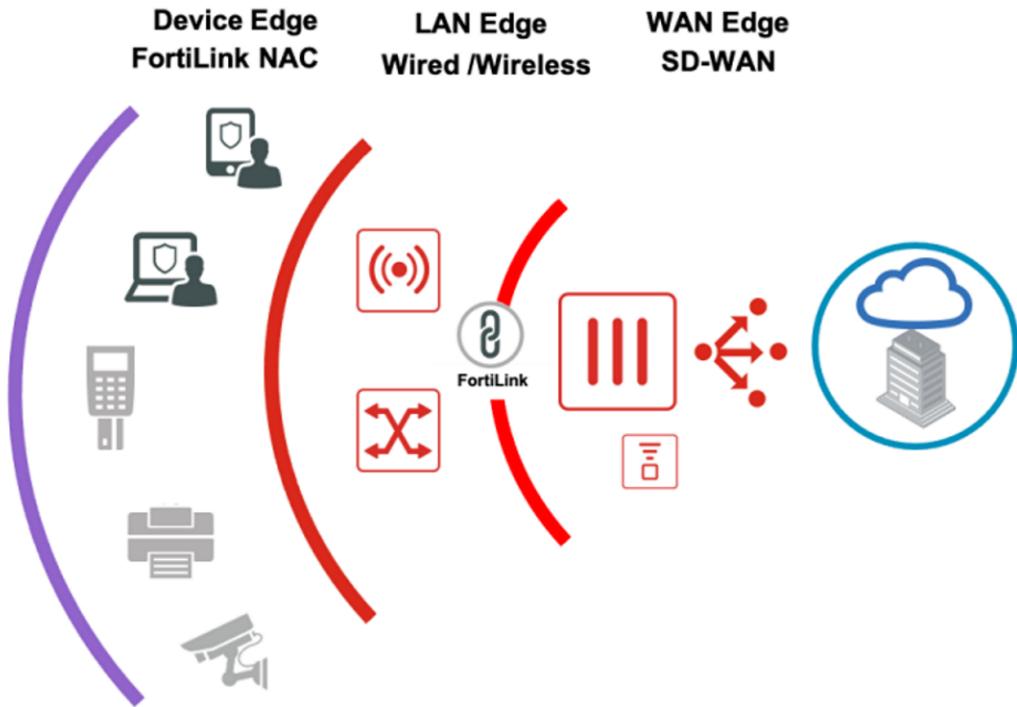
Fortinet's flagship product has always been, and remains, the FortiGate. FortiGate is indisputably one of the industry's top Next Generation Firewalls ([Gartner Magic Quadrant](#)), both as an appliance and as a Virtual Machine. As a total cybersecurity company, Fortinet is simply unmatched, but what is less recognized is just how far FortiGates have evolved as network controllers. A FortiGate is much more than a NGFW. It is a network controller and security appliance.

A FortiGate combines, in a fully integrated form, multiple network controller and security functions. A FortiGate integrates a full-featured WiFi and Switch Controller, a full featured router and SD-WAN solution, a wireless WAN (WWAN) controller that supports 5G and LTE cellular gateways (integrated with SD-WAN) and much more. All such network functions are fully-integrated with the FortiGate's extensive cybersecurity functions. With Security-Driven Networking, inspection of network traffic is not a 'bump in the wire', but part of the wire. There is no additional licensing for any of this extensive additional functionality. It is all included in every FortiGate.

FortiCloud Management Portals provides options for managing the full suite of Fortinet Security-Driven Networking products simply and remotely over the Internet.

Fortinet networking products

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.



Each edge is a security policy enforcement point.

The following topics provide information on enforcement points:

- [The LAN Edge with FortiSwitches and FortiAPs on page 9](#)
- [The WAN Edge with Integrated SD-WAN and FortiExtender on page 10](#)

The LAN Edge with FortiSwitches and FortiAPs

The LAN Edge is the border between end user devices and the LAN, where clients receive authorization and access to network resources. Fortinet has an extensive line of LAN access gear which can be deployed and used independently as any traditional networking gear.

However, when Fortinet LAN Edge equipment is under the direct control of a FortiGate, it converges networking and security into a secure, simple to manage architecture that extends FortiGate NGFW function to every switch port and access point via a fabric tunneling protocol we call FortiLink. All network traffic, regardless of where it comes from, can have a full security stack inspection applied to it.

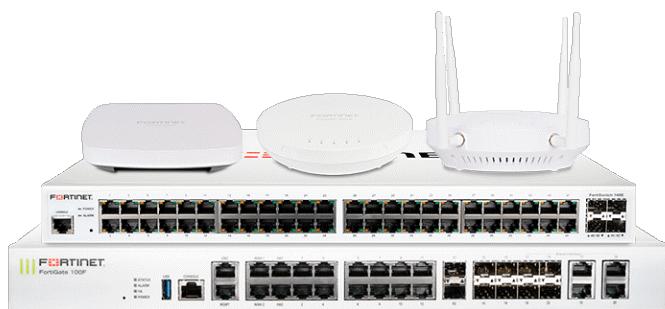
FortiAPs

FortiAPs are high performance purpose-built Wi-Fi 6 access points. They are three radio models, which means they can service both Wi-Fi bands while the third radio serves as a monitor, tracking RF conditions and scanning for neighbor and rogue APs.

FortiAP U-series are premium APs that add two additional features to the above. For Bridge Mode SSIDs, typical of remote deployments, where traffic is bridged directly to the network instead of tunneled to the FortiGate, UTP (Unified Threat Protection) enforcement can be applied directly on the AP. UTP includes options such as Web Filtering, Anti-Virus scanning and others. Additionally, one of the client-serving radios is band selectable so that the AP can have service 2.4 GHz and 5 GHz, or both radios can be set to 5 GHz.

FortiSwitches

FortiSwitches are feature rich yet cost-effective Ethernet switches. FortiSwitches behave similarly to FortiAPs, in that they have the option of forming a fabric with a FortiGate and so extend NGFW functionality throughout the LAN and to the LAN Edge.



The WAN Edge with Integrated SD-WAN and FortiExtender

Similarly, the WAN Edge is the traditional enforcement point for security functions, the dividing line between the traditional 'trusted' and 'untrusted' networks. In addition to the full SD-WAN functionality that is part of every FortiGate, FortiExtender adds LTE or 5G cellular WAN links to a Security-Driven Network.

Fortinet Secure SD-WAN

Fortinet Secure SD-WAN (Software-Defined Wide-Area Network) is an included feature of all FortiGates. This solution enables enterprises to transform and secure all WAN edges. Our Security-Driven Networking approach allows enterprises to realize superior user experience, enhanced security posture effectiveness with converged networking and security, and achieve operational continuity and efficiency. See [Gartner Magic Quadrant](#) for more information.

FortiExtender

FortiExtender cellular gateways provide ultra-fast LTE and 5G wireless to connect and scale any WAN edge. Get LTE/5G cellular, high availability, out-of-band management (OBM), and advanced threat protection in one solution. Naturally, they fully integrate into FortiGate's Secure SD-WAN.



FortiCloud Management Portals

No two enterprises are identical, and neither are their networks or their security needs. FortiCloud provides multiple Management Portals to accommodate different customer needs.

For instance, although a Fortinet Security-Driven Network is built around a FortiGate, there may be any number of reasons to deploy Fortinet networking products without an on site FortiGate. A customer may want to migrate to a full Fortinet solution, but is unprepared to cycle everything at the same time; or a customer simply loves our FortiAPs but prefers to separate WLAN management from other management systems. So, FortiCloud includes options structured to directly manage FortiGates and, via the FortiGate, indirectly manage on-site FortiAPs, FortiSwitches, and FortiExtenders. However, FortiCloud also includes portals that provide direct cloud management of FortiAPs, FortiSwitches, and FortiExtenders.

Available FortiGate Cloud Management portals include:

- FortiGate Cloud
- FortiManager Cloud

Available Fortinet Networking Cloud Management portals include:

- FortiLAN Cloud for FortiAPs and FortiSwitches
- FortiExtender Cloud

Additional Cloud Management portals include:

- FortiAnalyzer Cloud
- FortiClient EMS Cloud
- FortiSOAR Cloud



FortiGate Management

The following topics provide information on cloud management with a FortiGate:

- [FortiGate Cloud on page 13](#)
- [FortiManager Cloud on page 14](#)

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:

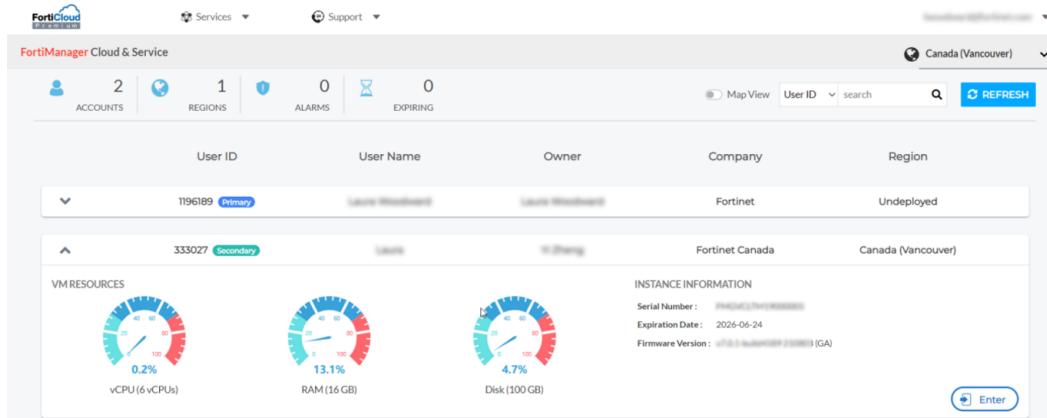
- Simple and secure remote management of FortiGates and all downstream Fortinet devices, including FortiAPs, FortiSwitches, and FortiExtenders.
- One year of hosted log storage.
- Analytics, both on-demand and scheduled reporting.
- Zero-touch provisioning using FortiDeploy.
- Automation options, including:
 - 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 ‘easy button’ for adding cloud advantages to FortiGate and Fortinet Security-Driven Networking for small and midsize enterprises.



FortiManager Cloud

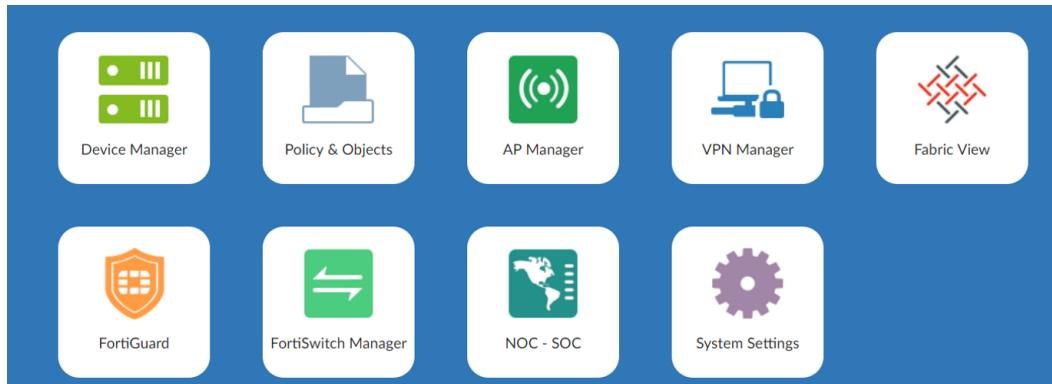
FortiManager Cloud brings a cloud version of our flagship management tool, FortiManager, to our FortiCloud suite for centralized management. FortiManager Cloud is ideal for enterprise customers using high-end FortiGates (and, of course, any FortiAPs, FortiSwitches, and FortiExtenders managed by them)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



The screenshot shows the FortiManager Cloud & Service interface. At the top, there are navigation links for 'Services' and 'Support', and a dropdown for 'Region' set to 'Canada (Vancouver)'. Below this, a summary bar shows 2 ACCOUNTS, 1 REGION, 0 ALARMS, and 0 EXPIRING. A 'REFRESH' button is also present. The main content area displays two users: '1196189 Primary' and '333027 Secondary'. The 'Primary' user is listed under 'User ID', 'User Name', 'Owner', 'Company', and 'Region'. Below this, there are three circular performance meters for 'vCPU (6 vCPUs)', 'RAM (16 GB)', and 'Disk (100 GB)'. The 'vCPU' meter shows 0.2%, 'RAM' shows 13.1%, and 'Disk' shows 4.7%. To the right, there is an 'INSTANCE INFORMATION' section with fields for 'Serial Number', 'Expiration Date' (2026-06-24), and 'Firmware Version'. A blue 'Enter' button is at the bottom right.

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.



WLAN, LAN, WAN Direct Management (without a FortiGate)

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

- [FortiLAN Cloud on page 15](#)
- [FortiExtender Cloud on page 16](#)

FortiLAN Cloud

For direct cloud management of Fortinet's LAN Edge portfolio (FortiAPs and FortiSwitches), there is FortiLAN Cloud. That is, a FortiGate is not required.

FortiLAN Cloud offers a simple, intuitive, easy-to-use interface for managing your LAN that is available from anywhere at any time. FortiLAN Cloud can scale from a small handful of devices all the way up to thousands across multiple sites.

FortiLAN Cloud strengths include:

- Simple and intuitive UI workflow.
- Zero-touch deployment with FortiDeploy that simplifies initial configuration and onboarding.
- High scalability, able to manage deployments from single digits to thousands of devices.
- Multi-tenancy option for MSSPs, with read-only customer accounts and unique customer log reports.
- Multiple dashboards showing key WLAN and LAN statistics (APs, radios, clients, neighbors, and so on).
- Troubleshooting tools with spectrum analysis, RF visibility, and IPerf test tools across wireless and wired.
- Full reporting, including PCI compliance.



FortiExtender Cloud

FortiExtender Cloud is used for direct cloud management of FortiExtender LTE and 5G WAN connections. With FortiExtender Cloud, you can rapidly deploy and dynamically manage LTE internet access at geographically distributed locations.

FortiExtender Cloud includes:

- Scaling to thousands of FortiExtenders anywhere in the world from a single browser.
- Smart grouping functions to manage a large scale of devices.
- Devices automatically showing up in your account with zero-touch provisioning.
- Simple monitoring and reporting of data usage by group, device, or plan.
- Tools to create network and VPN plans according to carrier.

Asset and account management with FortiCloud

For most organizations, management needs go well beyond just direct management of their security and networking devices. Needs typically include tracking where the devices go, what the inventory is, who has access, licensing, and so on. FortiCloud helps simplify and unify this for all of your Fortinet products.

The following topics provide information on asset and account management with FortiCloud:

- [FortiDeploy on page 17](#)
- [Asset Management on page 18](#)
- [Identity and Access Management \(IAM\) on page 18](#)
- [FortiCare Support on page 19](#)

FortiDeploy

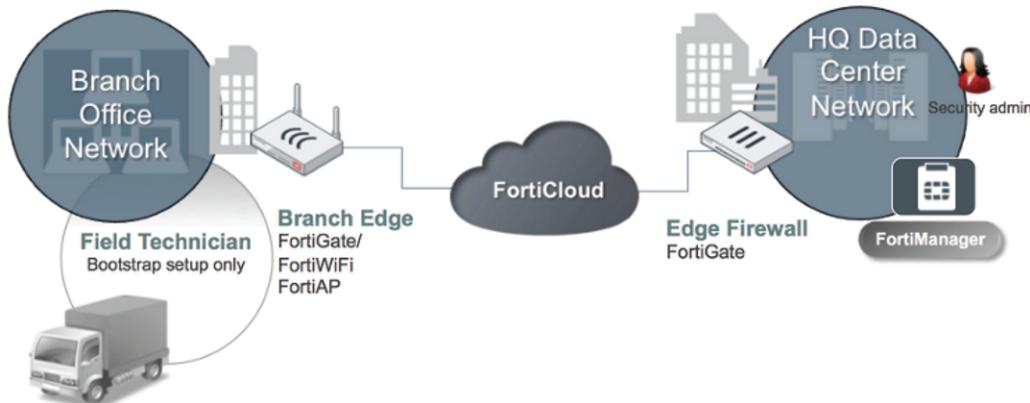
FortiDeploy is a mechanism built into FortiCloud that allows for simplified import and provisioning of any quantity of devices. It allows the user to deploy local or remote installed FortiGates and FortiAPs to their preferred management interface with a few clicks of the mouse. It is particularly efficient with remote deployments to FortiGate Cloud and FortiLAN Cloud.

FortiGates and FortiAPs have a FortiCloud key so that they may be quickly added to a FortiCloud account. Alternately, a FortiDeploy key can be added to a purchase order for bulk deployment of multiple devices.

As devices at remote locations are plugged in, they automatically obtain an IP address via DHCP. These devices then 'call home' to FortiCloud. From there, the device will receive the customer's preconfigured management choice for that device, whether a FortiManager IP or adding the device directly into FortiCloud.



FortiDeploy does not have a specific portal, but Cloud keys and FortiDeploy keys can be entered in different FortiCloud portals, including Asset Management, FortiGate Cloud, and FortiLAN Cloud.



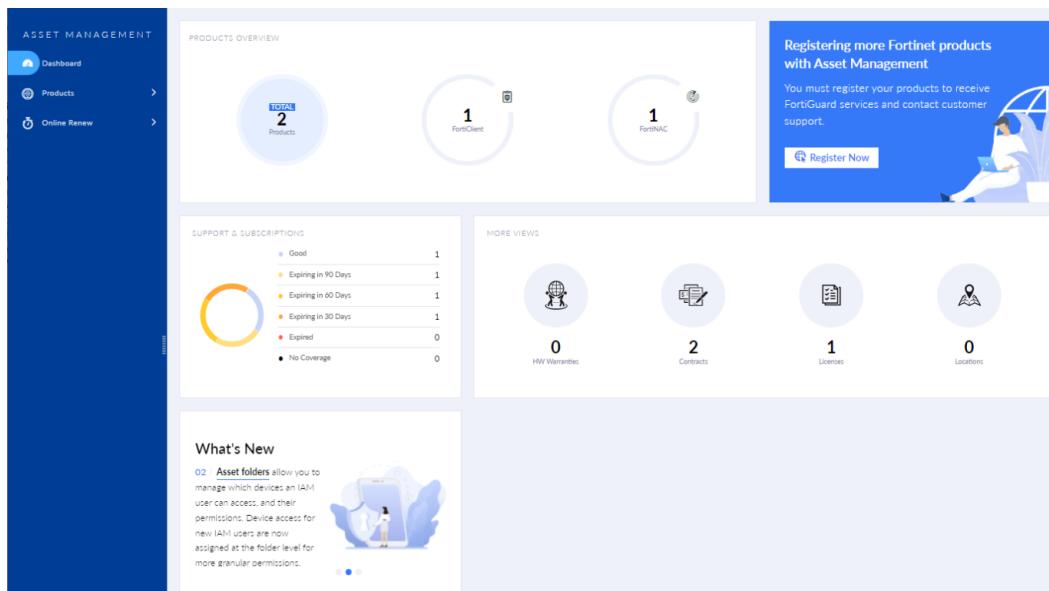
FortiDeploy is a feature in FortiCloud that is able to quickly onboard FortiAP wireless access points and FortiGate firewalls from a centralized, cloud-based management console.

Asset Management

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 can be registered and managed here. Registered products 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 multi-depth folder hierarchies.
- Dedicated and filtered views for expired units, decommissioned units on the registered products, and notifications on the assets.



Identity and Access Management (IAM)

The Identity and Access Management (IAM) portal enables granular access controller and account management for all of an organization's FortiCloud portals and assets. Use the portal to manage users, authentication credentials, and asset permissions.

IAM strengths include:

- User groups that save time when creating new users by applying predefined permissions.
- Support for two-factor authentication down to the account level.
- Granular permission granting users access to only the portals and assets they require.
- Assigning permissions based on the *Asset Manager* folder structure of your organization.
- API users for programmatic access specific to each portal.
- Support for external Identity Provider (IdP) authentication integrates the organizations existing identity controls.

The screenshot shows the 'View Products: 2 Units' section of the FortiCloud Asset Management portal. It lists two items: 'FortClient EMS' and 'FortNAC Control/App VM Server'. A context menu is open over the 'FortClient EMS' row, showing options like 'Add a sub-folder', 'Rename the folder', 'Move the folder', 'Delete all the sub-folders', and 'Bulk import folders'.

FortiCare Support

Of course, the FortiCare support portal is the grandfather of FortiCloud portals. FortiCare is fully integrated with FortiCloud, and directly accessible from every FortiCloud portal. FortiCloud accounts and FortiCare accounts are one and the same thing. That said, the full gamut of support services is easily accessible here.

FortiCare includes the kind of top support to be expected from the world's premier cybersecurity vendor:

- Global 24x7 coverage with 1000+ experts online
- Average wait time of less than five minutes for call
- Download the latest firmware or VM Images
- Create and manage support tickets directly online
- Web chat
- Advanced services available

The screenshot shows the FortiCare support portal. At the top, there are 'Services' and 'Support' dropdown menus. A 'Support' menu is open, showing options like 'Create a Ticket', 'Manage Tickets', 'Ticket Survey', 'Contact Support', and 'Technical Web Chat'. Below the menu, there's a 'Ticket Wizard' and a 'Create Ticket' button. A 'Specify Request Ticket Type' section lists several options: 'Technical Support Ticket', 'Customer Service', 'DOA/RMA Ticket', 'Anti Virus Ticket/FortiGuard Service', and 'Fortinet Converter Ticket'. Each option has a brief description and a play icon.

Cloud services and other Security Fabric portals

Finally, we have the extensive selection of additional cloud-delivered security and analytic tools.

The following topics provide information on other cloud services:

- [FortiPresence on page 20](#)
- [FortiToken Cloud on page 21](#)
- [FortiCASB on page 21](#)
- [FortiPenTest on page 21](#)
- [FortiMail Cloud on page 22](#)
- [FortiSandbox PaaS on page 22](#)
- [FortiPhish Cloud on page 22](#)
- [FortiWeb Cloud on page 23](#)
- [FortiInsight on page 23](#)
- [OCVPN Portal on page 23](#)
- [FortiGSLB on page 24](#)
- [FortiCWP on page 24](#)
- [FortiConverter on page 24](#)
- [SOCaaS on page 25](#)
- [FortiVoice on page 25](#)
- [FortiSASE on page 25](#)
- [FortiDevSec on page 26](#)

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.

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.

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.

FortiPenTest



FortiPenTest provides a cloud-based vulnerability assessment and penetration testing as a service. It simplifies automated detection of critical vulnerabilities in websites and web applications, including those defined by OWASP Top 10. Using FortiPentest can help identify common vulnerabilities and misconfigurations.

FortiMail Cloud



FortiMail Cloud email security is an independently validated and top-rated secure email gateway solution delivering >99% catch rate, multiple layers of 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.

FortiSandbox PaaS



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.



FortiSandbox PaaS is bundled with FortiGate Cloud.

FortiPhish Cloud



FortiPhish is a phishing simulation service to analyze how internal users interact 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.

FortiWeb Cloud



FortiWeb Cloud is a SaaS cloud-based web application firewall (WAF) that protects public cloud hosted web applications from the OWASP Top 10, zero-day threats, and other application layer attacks. FortiWeb Cloud colony of WAF gateways run in AWS, Azure, OCI, and Google Cloud regions allowing to scrub your application traffic within the same region your applications reside addressing performance, regulation concerns, and keeping traffic cost to minimum.

FortiInsight



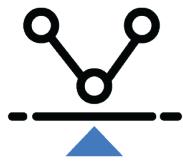
FortiInsight is a unique data security and threat detection solution that delivers advanced threat hunting to help you detect, respond to, and manage risky behaviors that put your organization's business-critical data at risk. It combines powerful and flexible machine learning with detailed forensics around user actions to provide complete visibility of activities around your organization's data. Instantly alerting you to anomalous activities, FortiInsight helps you strengthen your security posture, protect your sensitive information, and support regulatory compliance.

OCVPN Portal



Overlay Controller VPN (OCVPN) is a cloud-based solution to simplify IPsec VPN setup. When OVPN is enabled, IPsec Phase1 interfaces, Phase 2 interfaces, static routes, and firewall policies are generated automatically on all FortiGates that belong to the same community network.

FortiGSLB



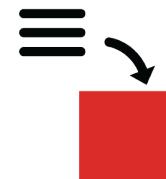
The Global Server Load Balance (GSLB) is a DNS-based solution that allows you to deploy redundant resources around the globe that can be leveraged to keep your business online when a local area deployment experiences unexpected spikes or downtime.

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.

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.

SOaaS



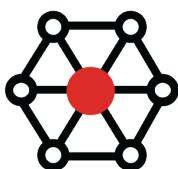
FortiCloud SOaaS analyzes security events generated from FortiGate appliances, performs alert triage, and escalates verified threat notifications to the security team. SOaaS complements incident response monitoring life cycles by providing continuous cyber awareness and control of the Fortinet Security 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.

FortiVoice



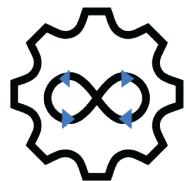
FortiVoice Secure Unified Communications, along with FortiFone IP phones, helps organizations keep up with changing communication needs due to evolving infrastructure, remote or hybrid work, and bring your own device (BYOD). An integrated platform for voice, conferencing, chat, and fax solves these challenges in a way that brings teams together for optimal business efficiency. A mobile-friendly softclient helps connect teams regardless of location. IT has visibility into system performance and the flexibility to optimize communications without increasing resources and costs.

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.

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.

Appendix A - Documentation References

Solution hub:

- [FortiCloud solution hub](#)



www.fortinet.com

Copyright© 2023 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 General Counsel, 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.