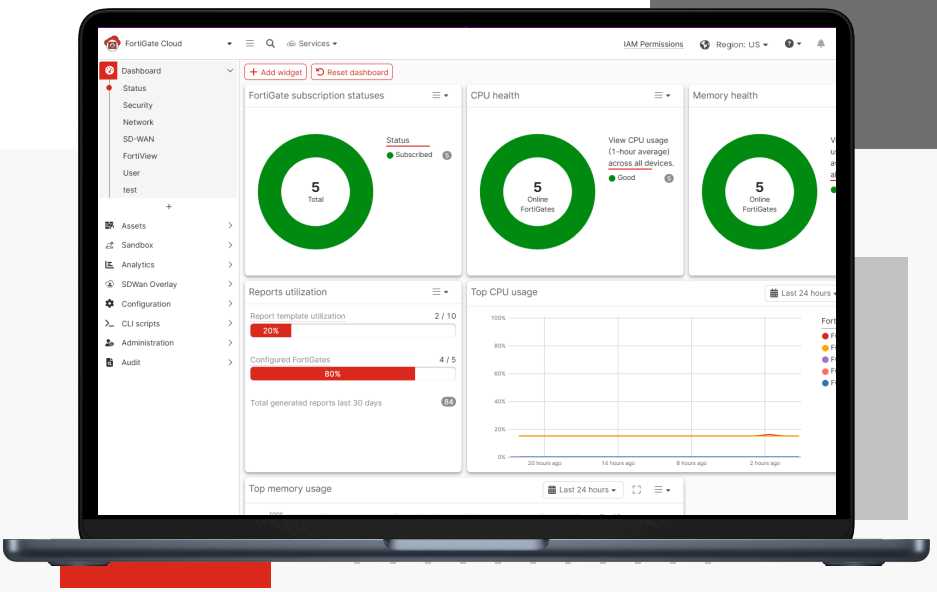
FortiGate Cloud



Highlights

- Zero touch provisioning
- Simplified FortiGate network and security management
- Unrestricted device configuration management
- Firmware upgrades, configuration backups, and scripting
- Monitoring, cloud logging and security Analytics
- Automated reporting and event handlers
- Cloud Sandbox
- Indicators of Compromise (IOC)
- Multitenancy
- SD-WAN Overlay as a service

Cloud Management and Analytics for FortiGate Firewalls

FortiGate Cloud is a cloud-based service offering simplified management, security analytics, and reporting for Fortinet's FortiGate next-generation firewalls to help you more efficiently manage your devices and reduce cyber risk. It simplifies the initial deployment, setup, and ongoing management of FortiGates and downstream connected devices such as FortiAP, FortiSwitch, and FortiExtender, with zero-touch provisioning. FortiGate Cloud can grow with your requirements from a single FortiGate to a complete MSP management solution for thousands of devices across multiple customers.

Highlights

International Cloud Management

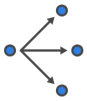
- Isolated instances for Europe, America, and Asia ensure data separation for privacy laws
- Simultaneously provision devices in multiple regions

Zero Touch Provisioning

- Zero touch provision FortiGates with FortiCloud key
- Bulk import and provisioning with FortiDeploy key

Network Visibility and Cloud Management

- Comprehensive overview of network, assets, device health, and statistics
- Management firewall configuration from cloud including security profiles, firewall policies, cloud config backups, CLI scripts, API access, and firmware upgrades



SD-WAN

- Configure SD-WAN interfaces
- Set up and manage application prioritization
- Deploy and manage the entire SD-WAN deployment

SD-WAN Overlay

- Easily provision new SD-WAN overlay networks
- Define and deploy the site, ISP, and subnet for the hub in the SD-WAN network
- Monitor link performance and quality across devices in the SD-WAN network

User Management

- FortiCloud integrated single-sign on, secure 2FA controls, and external IDP support
- Fine grained access control for IAM Users and APIs. Access to audit logs for compliance

Security Analytics and Reporting

- View cloud log analysis and visibility to traffic, security, event logs, and FortiView monitors
- Set up event handlers and schedule from curated reports

IoC (Indicators of Compromise)

- Identify risky devices and users
- Re-scan logs for threat hunting

Multitenancy

- Manage multiple customers with hierarchal tenant structure
- User management with access controls
- Central visibility for admins to manage tenant network

FortiGate Cloud Subscription

- FortiGate Cloud offers subscription for cloud management, security analytics, and one-year hosted log retention
- Devices without subscription are limited to seven days of logs, one report, and no cloud config management

FortiGate Cloud Advanced Subscription

- The FortiGate Cloud advanced subscription also offers SD-WAN Overlay as service and extended SecOps features (IoC)

Challenges

How FortiGate Cloud Addresses Key Security Challenges

Challenge	Solution
Facilitating turnkey provisioning of FortiGates at remote sites when on-site configuration expertise is unavailable.	FortiGates include FortiGate Cloud registration functionality in their firmware that allows an individual or multiple devices to provision themselves with minimal on-site expertise.
Keeping initial investment costs down and preference for consumption-based, OPEX model.	FortiGate Cloud uses Software-as-a-Service (SaaS) model that eliminates the need for upfront capital purchases.
Maintaining a single pane of glass management for overseeing security infrastructure.	FortiGate Cloud provides control over FortiGates while providing granular visibility and reporting at the same time.
Investing in a future-proof security solution that will scale with your business.	FortiGate Cloud can grow as your business grows and will accommodate additional log storage as needed.
Deploying different configurations across multiple sites and setup access control.	Role-based access control provides flexibility in managing users. Multitenancy enables the management of customers and users with simplicity and ease.

Features

Zero Touch Provisioning

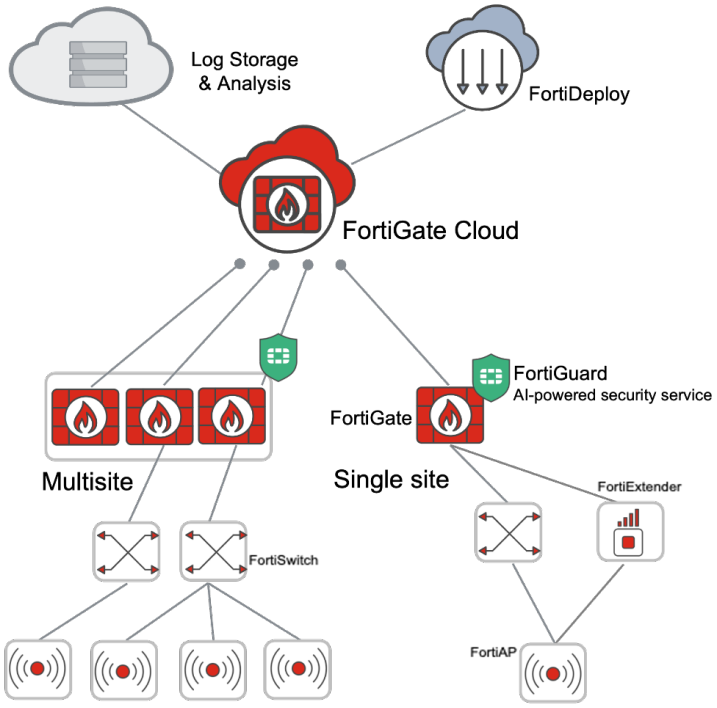
Initial configuration of firewalls, switches, and access points can be a tricky proposition, often requiring expert staff on-site to configure each device individually. Zero touch provisioning greatly simplifies local or remote onboarding of devices for the initial configuration. FortiCloud key provides an easy mechanism to import FortiGates into FortiGate Cloud with the automatic connection of FortiGates to be managed by FortiGate Cloud.

Hundreds of FortiGates can be provisioned using a bulk FortiCloud key in distributed environments, such as large retail or education networks. Once a communication tunnel is established, FortiGate Cloud provisions the FortiGate to the designated account, enabling settings, cloud logging, and device management from the cloud.

Features continued

Configuration and Device Management from a Single Pane of Glass

Consistent configuration of devices within your network is essential for ensuring that security policies are correctly applied. FortiGate Cloud provides a web-based management console to control FortiGates and downstream connected devices. Device settings such as SD-WAN interfaces/SLAs/rules, IP addresses, or service set identifiers (SSIDs) can be configured for FortiGate Cloud managed devices. Configuration backups are kept in FortiGate Cloud to assist with replacement or recovery efforts. Device firmware updates and scripts can be performed on multiple FortiGates, enabling automation and allowing customers to take advantage of the latest features.



FortiGate Cloud Network Security Management

Fabric Integration with FortiSwitch, FortiAP, and FortiExtender

FortiGate Cloud has the added benefit of provisioning, configuring, and managing your extended infrastructure through the FortiGate. Not only can you manage your entire infrastructure from a single cloud management interface, but by allowing FortiGate to manage your FortiSwitch, FortiAP, and FortiExtender, it can extend its functionality into them.

For example, the switch ports inherit the same properties as the firewall, making them extensions of the firewall — the same principle goes for the FortiAP. This unique Fabric integration enables this cross-product functionality. It can further allow automation in the face of a threat. When an infected client is detected through Indicators of Compromise (IOCs), the switch or AP can block the device until the problem is remediated.

Features continued

Deployment and Management of SD-WAN

Deploying SD-WAN need not be a complicated and expensive endeavor — FortiGate Cloud allows you to roll out and manage your SD-WAN deployment easily using zero touch deployment through its interface either manually or automatically as the FortiGates come online. Once your interfaces are up, you can move on to setting up the SD-WAN rules to optimize application prioritization on the WAN interfaces.

SD-WAN Overlay as a Service

IT teams are expected to keep up with ever-expanding networks and new technology deployments, often without the skills or experience to work efficiently. Setting up secure overlay networks may require complicated approaches using a variety of technologies such as IPsec and BGP to facilitate communication across the WAN. FortiGate Cloud offers streamlined and swift provisioning of a new SD-WAN region, taking the burden off overwhelmed IT staff. Operating as a cloud-hosted service, it significantly reduces deployment time and costs, while also eliminating expenses associated with hosting and management.

Account and User Management

Providing secure access to administrators for managing the FortiCloud account, assets, and services is a key factor in efficient operations. FortiGate Cloud provides granular resource-based access controls to reduce security risks by assigning only the necessary permissions to carry out specific tasks for designated personnel. Integrated with FortiCloud IAM (Identity and Access Management), secure 2FA authentication, permission profiles for authorization, admins can securely control access to FortiCloud assets and features for your users. Additionally, integrated with FortiCloud external IdP, customers can leverage external IdP user management and manage access to FortiGate Cloud.

Instant Security Intelligence and Analytics

To place better security controls on your network, you must first know how it is being utilized. FortiGate Cloud's extensive set of dashboards gives you an immediate view of FortiGate usage, including a breakdown of network traffic and bandwidth usage. FortiGate Cloud analytics provides you with drill-down and filtering functionality to instantly determine how applications, websites, users, and threats impact your network.

Hosted Log Retention and Cloud-based Storage

Log retention is an integral part of any security and compliance best practice, but administering a separate storage system can be burdensome and costly. FortiGate Cloud takes care of this automatically and stores your valuable log information securely in the cloud.

Depending on your device, you can easily store and access different logs, including traffic, system, web, applications, and security events. FortiGate Cloud provides seven days of log retention for devices without subscription while the subscription service extends this to one full year of logs.

Features continued

Indicators of Compromise

Identifying suspicious usage and artifacts on the network and intrusions with higher confidence is critical to keeping the systems secure. FortiGate Cloud Indicators of Compromise (IOC) feature provides intelligence and information to help security analysts identify risky devices and users based on these artifacts. The IOC package includes a large number of indicators and delivers it via our Fortinet Developers Network (FNDN). Analysts can also re-scan historical logs for threat hunting and identify threats based on new intelligence, as well as review users' aggregated threat scores by IP addresses, hostname, group, OS, overall threat rating, a location Map View, and a number of threats.

Exceptional Network Visibility with FortiGate Cloud Reporting

A periodic review of network and security activity is essential to keep costs down and security breaches at bay. Reporting allows you to be proactive about optimizing your network and satisfying executive staff scrutiny. FortiGate Cloud provides preconfigured reports to give you the information you need for your specific reporting and compliance requirements. A wide variety of rich canned reports such as a 360-degree Activity Report, Fortinet Security Best Practices Report, Application Usage Report, or Cyber Threat Assessment Report, amongst others, can be run on-demand or scheduled (daily, weekly, or monthly), giving you complete visibility with actionable outcomes. Devices without subscription receive only the 360-degree Activity Report.

Multitenancy Management

Large scale tenant management requires mature and complex deployment structures with increased flexibility and a streamlined process for resource provisioning in different locations for customers. FortiGate Cloud multitenancy can be leveraged via FortiCloud Organizations. FortiCloud Organizations based multitenancy provides unified tenant management across FortiCloud services and helps to structure accounts, assets, and implement fine-grained access controls across multiple accounts. FortiGate Cloud provides a centralized dashboard for the Organization and Organizational Units with visibility of the tenant accounts, devices, licenses, easy access to manage tenant network and security.

FortiGate Cloud Transport Security and Service Availability

FortiGate Cloud encrypts all communication including log information between your FortiGate devices and the cloud. Fortinet deploys redundant data centers to give the FortiGate Cloud service its high availability. Fortinet has also used its years of experience in protecting sophisticated networks worldwide to implement operational security measures that make sure your data is secure and only you can view or retrieve it.

Ordering Information

FortiGate Cloud Subscriptions

FortiGate Cloud subscription per device is available for FortiGates (40 ~ 3700 series), FortiGate-VM/VM-S series, and FortiWiFi (40 ~ 81 series) for cloud management, analytics, and one year rolling log storage.

Product	SKU	Description
FortiGate Cloud Subscription	FC-10-00XXX-131-02-DD	FortiGate Cloud Management, Analysis, and One Year Log Retention (XXX = model code)
FortiGate Cloud Advanced Subscription	FC-10-XXXXX-1125-02-DD	FortiGate Cloud Advanced including cloud management, analysis, one year log retention plus SD-WAN Overlay-as-Service and extended SecOps (Indicators of Compromise)

Multitenancy

Regular FortiCloud accounts can enable multitenancy with FortiCloud Organizations up to 10 accounts. For more than 10 accounts, FNDN basic account should be registered (no additional license needed).

For customers who would like to add bulk provisioning for multiple devices, add the following SKU to the purchase order*.

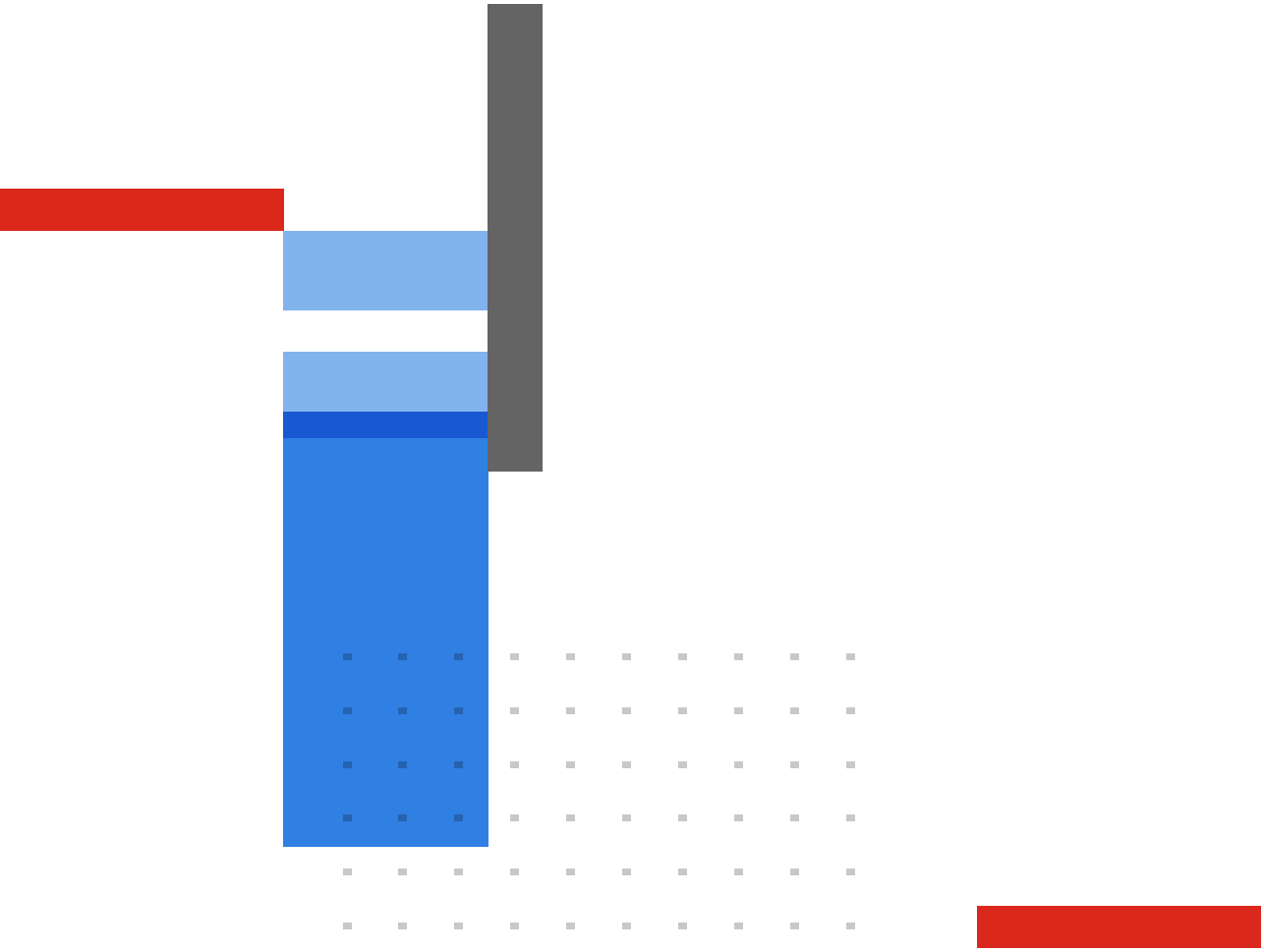
Product	SKU	Description
FortiDeploy	FDP-SINGLE-USE	Enables zero touch bulk provisioning for your FortiGate, FortiWiFi, or FortiAP products with FortiGate Cloud. Must be purchased with every PO.

* This feature is only available on devices running FortiOS 5.2.2 and above.

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

March 5, 2025

FG-CL-DAT-R8-20250304