# FortiCloud v3.1.2
## Frequently Asked Questions

FortiCloud v3.1.2 Frequently Asked Questions

March 14, 2017

32-25-185514-20170314



| | |
|---|---|
| Technical Documentation | docs.fortinet.com |
| Knowledge Base | kb.fortinet.com |
| Customer Service & Support | support.fortinet.com |
| Training Services | training.fortinet.com |
| FortiGuard | fortiguard.com |
| Document Feedback | techdocs@fortinet.com |

# Table of Contents

# General Questions

## What is FortiCloud?

FortiCloud is a hosted wireless and UTM infrastructure management solution and log retention service for FortiGate®, FortiWiFi® and FortiAP® devices. It gives you centralized configuration management, location-based analytics and reporting, and log retention without the need for additional hardware and software. The feature set includes:

- One-touch provisioning of large scale security and wireless networks
- Configuration and device management from a single pane of glass
- Cloud-managed FortiAPs
- Hosted log retention and cloud-based storage
- Wireless health and oversight at your fingertips
- Cloud management of wireless guest access
- Social media account login for Guest WiFi
- Rogue access point detection and analytics
- Built-in protection from APTs with FortiGuard sandboxing technology
- Location-based analytics with FortiPresence
- Instant security intelligence and analytics with FortiView
- Network health and utilization-based analytics and reporting
- Wireless configuration including security profiles per SSID for the Smart AP

## What functions does FortiCloud have?

- Centralized Dashboard: system and log widgets plus real-time monitors
- FortiView Log Viewer: real-time log viewing with filters and download capability
- Drilldown Analysis: real-time location, user, and network activity analysis
- Report Generator: create custom report templates, and schedule reports in different formats to display location-based analytics or illustrate network usage patterns
- Device Management: configuration backup and history, script management, and alert profiles for real-time monitors
- AV Submission: shows the status of suspicious files undergoing cloud-based sandbox analysis
- Wireless Health Monitoring: bandwidth, usage, clients, interference, failed login and rogue APs
- Wireless Security Logs & Events: Authentication, Antivirus, IPS, Web Access, PCI compliance
- Wireless Configuration: SSIDs (including IPS, Antivirus and Web Filtering configuration), Authentication, Captive Portal, Platform Profiles, Tags and Network Settings
- Guest Management: ability to add guests and notify them if credentials via SMS or email
- Social Media Account Integration: ability for guests to connect to wireless accounts via social media

## How does FortiCloud work?

One or multiple FortiGate/FortiWiFi/FortiAP units are registered with FortiCloud under a single account. This is done via the licensing widget in the device dashboard or at www.forticloud.com. The logs from each device are periodically sent to FortiCloud and stored.

Logs are sent automatically to FortiCloud for storage and processing. You configure what to log, including just Traffic and Event logs or including security logs such as Antivirus, Application Control, IPS, etc.

From the recorded logs, reports can be generated to indicate trends within network traffic, individual user activity, and security threats across different applications. Drilldown capability and real-time alerting are also available.

FortiCloud also creates copies of FortiGate/FortiWiFi/FortiAP configurations that can be used for backup and restore or to provision new devices. A VPN tunnel can be used to bring up the console of a device behind a firewall, allowing you to perform configuration or policy changes remotely.

## How does FortiCloud compare with FortiPortal and FortiAnalyzer?

FortiCloud is an ideal solution for customers who do not want to implement a separate hardware solution such as the FortiAnalyzer 200D series. However, it does not have all the features of a FortiAnalyzer. A high-level comparison is shown below:

| **Feature** | **FortiCloud** | **FortiPortal** | **FortiAnalyzer** |
|---|---|---|---|
| Business size | Small Branches/Large Campus/Distributed Enterprise | MSSP | Enterprise/MSSP |
| Summary | Fortinet-hosted cloud-based reporting, management and client sandboxing | End customer/MSSP portal, overlaid on existing local infrastructure. Hosted in the MSSP's datacenter. | Premises-based log collection, reporting and alerting system |
| Per-Site Licensing | Licensing is based on a per-device basis. | Licensing is based on number of devices and add-ons. Devices can be FG/VDOM/wireless. No limits on scaling factors, distributed architecture. | Typical licensing for FAZ hardware. Max device limit set per model, VM and cloud-based options available. |
| Sandboxing | FortiSandbox Cloud included in AV bundle. FortiCloud gives visibility in cloud to uploaded files. | No support in the current release. Must use FortiSandbox. | No support. Must use FortiSandbox. |
| Supports external authentication for administrative access | No | Yes | Yes |
| Storage quota | Unlimited storage with 1 year log retention. | Based on MSSP's datacenter storage availability. | Depends on model. Up to 48 TB for the appliance, and 24 TB for the VM. |

| Feature | FortiCloud | FortiPortal | FortiAnalyzer |
|---|---|---|---|
| Centralized logging | Real-time for disk-less models. Batch upload for disk models. | Real-time for security and wireless, analytics and reports. | Real-time for disk-less models. Batch upload for disk models. Log aggregation and forwarding. CEF compliant logging. |
| Aggregated reports | No | Yes | Yes |

## How do I confirm which version of FortiCloud is currently in use?

The version number is displayed at the bottom of the screen after login.

## How can I provide feedback or request improvements to FortiCloud?

On the top right of every screen is an envelope icon, which will open a feedback submission form. Feedback is greatly appreciated, but Fortinet cannot guarantee individual responses to any requests.

## Which languages are supported by FortiCloud?

FortiCloud currently supports two languages: English and Japanese. These can be selected via the web portal login page. Other languages may be available in other regions.

## Is there any way for me to choose which Data Center my logs are stored in?

Yes. When you initially create your account in FortiCloud, it will offer you the choice of which data center to use. If you change your mind, you will need to create a new account and transfer your devices.

No existing logs can be transferred between data centers.

## Is there a European FortiCloud instance?

Yes. As if Q2 2016, the FortiCloud service has been available through our new Regional FortiCloud Datacenter, geographically aimed at our European customer base, and is completely isolated from the North American instance.

All analysis, reporting, management and storage capabilities are provided locally, with full access to our global threat intelligence databases, with the dual benefit of isolating intercontinental data and providing performance improvements and lower latency to the end device.

## If I am an existing customer in EMEA, will my data be transferred to the new Datacenter, or will it remain in its current location?

Any existing units will remain logging to their original destinations. If you wish to change this, please contact our Customer Services. No existing logs will be moved as part of this process.

## What are the new features in Version 3.1?

All the new 3.0 features that were available for free, are still free.

Two-Factor Authentication has been added to the management interface. FortiGate management remains as a public beta service in the 3.1 release, but has been expanded to allow importing of the current configuration from a deployed FortiGate. Sandbox functionality has also been improved, showing the number of files waiting for processing.

A new Enterprise-level license is now available as a paid upgrade for connected APs, covering a number of advanced RF settings, and blocking of intra-SSID traffic. This license includes support for the FAP-S series APs, with included FortiGuard subscription and Bonjour relaying.

## Were there any functionality changes between the 2.5 and 3.0 versions of FortiCloud?

Yes, location-based analytics with FortiPresence have been added in 3.0. To support FortiPresence features, social media logins for Guest WiFi Accounts have been integrated into FortiCloud. Also new in 3.0 is enhanced FortiOS management, Fast Roaming between AP units, and enhanced AP configuration in NAT Mode.

## Were there any functionality changes between the 2.43 and 2.5 versions of FortiCloud?

Yes, multi-tenancy was added as a feature in 2.5; and a series of wireless-related features such as guest management, external captive portals, security per SSID (for the Smart AP), AP location floor plan and AP radio adjustment. Also added were PCI compliance reports and integration with Advanced Threat Protection.

# Licensing and Registration

## Is there an easy way to test drive FortiCloud?

Yes, you can test drive FortiCloud by visiting the FortiCloud portal, and selecting the *Live Demo* link at the bottom of the FortiCloud login screen. This will show a FortiCloud account with populated devices and logs to simulate a live environment.

## What is the price of FortiCloud?

A no-charge service option is available with unlimited storage is available for one week.

Effective in FortiCloud 3.0, we are replacing the 200Gb-per-device service with a annual-subscription-based service, with one, two, or three-year service terms. The new service provides 1 year of history, regardless of size.

FortiCloud will be available for all FortiGate devices up to the FG3200D.

To activate FortiCloud after the free trial ends, you will need to acquire a subscription license based on the following SKUs, available with 1, 2, and 3-year service terms:

| **Description** | **SKU** |
|---|---|
| **FortiCloud Analysis and 1-Year Log Retention** | |
| FortiGate (Up to 2U) & FortiWiFi | FC-10-000XX-131-02-DD |
| **FortiCloud Enterprise AP Licenses** | |
| FAP/FAP-U/FAP-C | FC-10-000XX-131-02-DD |
| FAP-S | FC-10-90APS-170-02-12 |
| **FortiCloud IOC (Indicator of Compromise)** | |
| FortiGate FGT20-90 models | FC-10-90803-142-02-12 |
| FortiGate FGT100-300 models | FC-10-90804-142-02-12 |
| **Other Services** | |
| FortiCloud - Multi-Tenancy | FCLE-10- |
| FortiDeploy Access | FDP-SINGLE-USE |

Activation on device requires FortiOS 5.4.2 or newer. The Indicator of Compromise (IOC) Service requires an existing FortiCloud subscription.

For pricing information, please contact your Fortinet partner or reseller.

## How do you enable the FortiCloud service for FortiGate and FortiWiFi?

1. Register the FortiGate/FortiWiFi on the Service and Support Portal at https://support.fortinet.com.
2. Create an account in the FortiGate/FortiWiFi dashboard licensing widget.
3. Activate the FortiGate/FortiWiFi within the dashboard licensing widget.
4. Create a firewall policy with logging enabled. Configure log uploading, if necessary.

5. Log into the portal at https://www.forticloud.com.

## How do you enable the FortiCloud service for FortiAP?

1. Register for a FortiCloud account at https://www.forticloud.com.
2. Click the “Add Device” link and enter the unique FortiCloud key located on your FortiAP device.
3. Deploy the FortiAP to an existing AP network or create a new AP network.
4. Associate your FortiAP with an SSID.
5. Connect your FortiAP to an internet connection, and wait for it to self-configure.
6. Log into the portal at https://www.forticloud.com to configure it further.

## Do I need a support contract to enable the service?

No, but you do need to register each FortiGate/FortiWiFi/FortiAP on the Service and Support Portal at https://support.fortinet.com. It’s very important to register each device in your network, or the service (free or subscribed) cannot be enabled.

## How do I subscribe to a FortiGate Analysis and Log Retention contract?

To upgrade to a subscription, you need to:

1. Obtain a license (Contract Number) from your Fortinet reseller.
2. Click on the *Upgrade* icon in the FortiGate/FortiWiFi dashboard licensing widget. Follow the instructions presented.

   If you are running FortiOS 5.0 and higher, you have the option of receiving a scratch-off card/certificate from your Fortinet reseller. Scratch the card to reveal the hidden activation code. Enter this directly into the FortiGate console in the Licensing widget.
3. It takes about 30 minutes for the backend systems to process the subscription.
4. The account type in your FortiGate/FortiWiFi will change from *Free* to *Subscribed*.

## What features do I get access to for subscribing?

Yes. When you upgrade to a subscription, you will no longer have a daily limit on uploads and will be able to create, schedule, and customize reports. You will also be able to subscribe to more advanced features, like the FortiCloud IOC (Indicator of Compromise) Service, FortiPresence Analytics, and FortiOS Management.

You also gain the ability to analyze more files per day with FortiCloud Sandboxing (the free version limits you to 10 files per day.) The actual daily limit of files is based on the model of FortiGate deployed.

## How do I subscribe to the Enterprise License?

1. Place an order, and receive a Support Contract from your selected partner.
2. Per the Service Entitlement Summary on the contract, apply the Contract Registration Code on support.fortinet.com.
3. Select the applicable FortiAP (S) serial number.
4. Complete the registration process.
5. Product Entitlements will now display Support Coverage for ‘FortiCloud FAP Management Service’ with a 1-year subscription.

## What features do I get access to for subscribing to the Enterprise License?

FortiAP-C benefits from 8x5 support and 1-year log retention.

FortiAP and FortiAP-U also gain advanced wireless features which grant control over transmitted data rates.

FortiAP-S benefits from the additional capability of Bonjour relaying, a subscription to FortiGuard services, and intra-SSID isolation of specific clients.

More subscriber-only features will be added in future releases of FortiCloud.

## What happens if I lose my password?

You can reset your password on the FortiCloud portal at https://www.forticloud.com.

## Can I use Two-Factor Authentication for FortiCloud?

Yes. As of 3.1, Two-Factor Authentication is offered as part of the base free service, using the FortiToken app available on mobile devices. To enable two-factor authentication, ensure your entered email address is correct, as you will be sent an email withe setup instructions. Then enable '2-Factor' in the 'My Account' section.

## What is a Multi-Tenancy Account and what is the process to activate it?

A Multi-Tenancy Account is a one-year service for an administrator to create and manage multiple sub-accounts. It also allows devices to be moved between these accounts. Each of the sub accounts can be allocated administrators, with full or read-only access, allowing you more control over the provision of a managed service.

To activate a Multi-Tenancy Account, please request a quote for the following SKU:

"FCLE-10-FCLD0-161-02-DD"

through your Fortinet Partner or Reseller.

## How do you configure service once it is activated?

The configuration of the service is done via the web portal at https://www.forticloud.com. The logs will automatically start appearing in the logs and archives section.

Select the gear icon on any page to edit that page's settings.

Select the gear icon next to the administrator email in the top right to edit user settings.

## For how long are logs retained?

FortiCloud will automatically delete logs older than the length of the support contract to make space for new log data. Email and pop-up reminders will be sent periodically (30 days, 14 days, 7 days, and 24 hours) before logs are deleted and before the contract term comes to an end.

## When a device subscription lapses, what happens to the year's worth of logs?

Any logs that are associated with the licensed device older than 1 year will be automatically purged. For the free service, logs older than 7 days will be purged.

There is no grace period, so please ensure you are properly renewed so that your logs are retained.

## What if I want to unsubscribe from the service and stop uploading logs?

You can disconnect your account from the dashboard in your FortiGate/FortiWiFi. In the Licensing and Information widget in the FortiGate interface, click on the *Log-out* button. This will detach the FortiGate/FortiWiFi from the account and stop the logs from uploading.

# Technical Questions

## What security and redundancy has been built into the service?

Logs are transferred between devices and the FortiCloud storage are transmitted via an encrypted link. All system elements are duplicated for redundancy.

## How do I verify my network is PCI compliant?

FortiCloud makes it easy to deploy, monitor and verify PCI compliance. FortiCloud's security feature set addresses PCI Data Security Standards 3.0, helping customers to build and maintain a secure network, protect cardholder data, maintain a vulnerability management program, implement strong control measures, and monitor network security.

## Does my FortiGate unit require a hard drive to use FortiCloud?

The FortiGate does not require a hard drive if logs are being uploaded to FortiCloud in real-time, which can be enabled in the *Log Setting* page in the FortiGate interface. FortiCloud is a convenient alternative to a hard drive for devices too small to contain one, such as FortiWiFi units.

## Does FortiCloud support devices from other vendors?

FortiCloud only supports FortiGate, FortiWiFi and FortiAP products. It does not currently support other company's products for log retention.

## Which FortiGate and FortiWiFi models does FortiCloud support?

### FortiGate

All 2U (3200D) and smaller FortiGates are supported by the FortiCloud environment.

### FortiWiFi

All FortiWiFi models 20 to 90 support FortiCloud natively through the dashboard Licensing widget.

### FortiAP

All FortiAP, FortiAP-S, and FortiAP-C models are supported by FortiCloud. FortiAP-U will be supported by Q3 2017.

## Which versions of FortiOS does FortiCloud support?

FortiCloud is available for all devices at FortiOS version 4.3 or later, but for full feature support, the most current available version should be deployed. Devices running FortiOS version 4.2 or earlier may not be able to access FortiCloud. Consult your device's documentation for more information.

## What port numbers are used by FortiGate devices connecting to FortiCloud?

Please note that these should be required by OUTBOUND traffic only. On request, we can supply the destination IP addresses to add to an outbound policy, if required.

| Purpose | Protocol/Port |
|---|---|
| Syslog, Registration, Quarantine, Log & Report | TCP/443 |
| OFTP | TCP/514 |
| Management | TCP/541 |
| Contract Validation | TCP/10151 |

## When are scheduled reports sent to administrators?

Scheduled reports are sent to administrator email addresses between 2 AM and 6 AM if automatic report delivery (Daily/Weekly/Monthly) is enabled.

## Why can I not see any management functions?

You must first enable the management tunnel on the FortiGate/FortiWiFi device. On the device, use the following commands in the CLI:

```
config system central-management
  set mode backup
    set type fortiguard
end
```

## Can I set up high availability (HA) logging with FortiCloud?

FortiCloud accepts inbound logs from each device independently, and has no means of detecting that connected devices are in an HA cluster. Though multiple HA clustered devices will theoretically send identical logs to FortiCloud, if one device stops logging or is unable to reach FortiCloud, the other devices will not send logs on its behalf.

## Do I need to purchase a subscription for each FortiGate in an HA pair?

Yes. FortiCloud handles each device separately, regardless of configuration.

# FortiCloud Sandbox

## How does Cloud Sandboxing and AV Submission work?

In a proxy-based antivirus profile on a FortiGate, the administrator selects *Inspect Suspicious Files with FortiGuard Analytics* to enable a FortiGate unit to upload suspicious files to FortiGuard for analysis. Once uploaded, the file will be executed and the resulting behavior analyzed for risk. If the file exhibits risky behavior or is found to contain a virus, a new virus signature is created and added to the FortiGuard antivirus signature database. The next time the FortiGate unit updates its antivirus database it will have the new signature.

FortiGuard Labs considers a file suspicious if it exhibits some unusual behavior, yet does not contain a known virus (the behaviors that FortiCloud Analytics considers suspicious will change depending on the current threat climate and other factors).

The FortiCloud console enables administrators to view the status of any suspicious files uploaded: Pending, Clean, Malware, or Unknown. The console also provides data on time, user, and location of the infected file for forensic analysis.

## Why can I note see a function or tab for AV Submission/Sandboxing?

You must first enable Cloud Sandboxing on the FortiGate device, and then submit a suspicious file to cause the tab to appear.

## What is the turnaround time on Cloud Sandboxing and AV Submission?

It can be anywhere from 10 minutes (for automated sandbox detection) to up to 10 hours (if FortiGuard Labs is involved).

## Is there a service description for FortiCloud Sandbox?

Yes, a full current service description is available online here:

http://docs.fortinet.com/uploaded/files/3429/FortiSandbox-Cloud-Service-Description.pdf

# AP Network

## What is the FortiCloud AP Network feature?

This feature allows administrators to remotely configure APs, modify wireless management settings and visualize wireless-related events. Examples of configuration changes include AP name and SSID configuration, power settings and rogue AP detection. Wireless management settings include RADIUS details, standard users/groups/guests and SSIDs/security. There are a robust set of visualizations including real-time and historical charting of traffic usage, AP client counts and client usage. Think of it as a comprehensive way to manage your wireless infrastructure via the cloud.

## How can I register a FortiAP to my FortiCloud account?

Supported FortiAP models include a sticker with a unique FortiCloud key affixed. This key must be entered into the FortiCloud interface to register the FortiAP to your FortiCloud account.

## What is the recommended FortiAP version to use with FortiCloud 3.1?

We recommend FortiAP version 5.4.3 or later for use with FortiCloud 3.1. It is always our recommendation that you run the latest GA firmware on your FortiAPs.

## What port numbers are used by FortiAPs connecting to FortiCloud?

Please note that these should be required by OUTBOUND traffic only. On request, we can supply the destination IP addresses to add to an outbound policy, if required.

| Device | Purpose | Protocol/Port |
|---|---|---|
| FortiAP, FortiAP-S, FortiAP-C | Initial Discovery | TCP/443 |
| FortiAP, FortiAP-S, FortiAP-C | CAPWAP Tunnel, Event Logs | UDP/5246, UDP/5247 |
| FortiAP, FortiAP-S, FortiAP-C | Syslog, OFTP, Registration, Quarantine, Log & Report | TCP/514 |
| FortiAP-S | FortiGuard | UDP/53, UDP/8888 |

## What happens if my AP loses connection with FortiCloud?

If your AP loses connection to FortiCloud, or in the unlikely event that the FortiCloud service is unavailable, then all functions which are not hosted in FortiCloud will continue to work without interruption. The configuration is held locally on the AP, and will continue to function.

Only SSID's with authentication in FortiCloud will be disrupted: FortiCloud-hosted Captive Web Portals, and FortiCloud User Groups. Open, WPA2 PSK, and WPA2 802.1X RADIUS SSID's that are not using FortiCloud-hosted authentication (such as ones using local RADIUS server or Local Captive Portal) will continue to work uninterrupted.

## I have an older FortiAP that doesn't include a FortiCloud key. Is there some way I can add my device to a FortiCloud AP Network?

Older FortiAPs that have shipped without a FortiCloud key can be added to FortiCloud. Open the FortiAP management interface, and in *WTP-Configuration* select *FortiCloud*. Enter your FortiCloud credentials, and select *Apply*. Login to FortiCloud and select *Inventory* > *Unused APs* to see the list of FortiAPs. Select *Deploy to AP Network* > *Existing AP Network*.

## What FortiAP models are supported by FortiCloud AP Networks?

The AP Network functionality within FortiCloud is supported by all FortiAP models.

## Does the FortiCloud AP Network feature support FortiWiFi?

FortiWiFi models are not currently supported for wireless configuration.

## Is there a minimum firmware version that I need to run on a FortiAP for the FortiCloud AP Network feature to work?

The FortiAP must be running FortiAP OS 5.2 at a minimum. It is recommended to run the latest software build on the FortiAP to guarantee FortiCloud functionality.

## Does my internal wireless/networking traffic get sent to FortiCloud?

No. Fortinet uses an out of band management architecture, meaning that only management data flows through the FortiCloud infrastructure. No user traffic passes through Fortinet's datacenters, and your data stays on your network.

## Do I need to use a FortiGate in conjunction with a FortiCloud AP Network?

No. We recommend you register your FortiAP to be directly managed by FortiCloud. You do not need to use a FortiGate unit as a proxy to manage FortiAPs from FortiCloud.

## Is there different pricing/licensing for AP Network functionality?

There are no additional fees or licensing required to manage FortiAPs from FortiCloud.

## Can FortiAP devices be managed by FortiCloud and work with FortiPresence?

Yes, FortiPresence is supported by FortiAPs and managed by FortiCloud in version 3.1.

For location analytics, the APs will use a Push API to talk to the FortiPresence cloud. You can configure this under *AP Network* > *Configuration* > *Miscellaneous*.

## Is there a maximum number of FortiAPs that can be managed via FortiCloud?

There is no licensing limit for the number of FortiAPs that can be managed with FortiCloud.

## How does roaming work for a FortiCloud managed AP?

Starting with FortiAP 5.4 and FortiCloud 3.0, APs which are in the same management subnet will talk to each other using encrypted communications and share station and authentication information. This means that when a client connected via Captive Web Portal, 802.1X or PSK moves from one access point to another, there is no re-authentication required and a session transition should happen once the client decides to roam.

## What is the admin password for my AP?

When you add an AP Network, you are asked to define a password for it. This password is used as the admin password for all APs inside that AP Network. The password can be changed inside the AP Network under *Configuration* > *Miscellaneous*.

## What is Social Media Captive Web Portal?

Social Media Captive Web Portal is the functionality that creates a Captive Web portal where a user's social media login is used as authentication. This is hosted in FortiCloud, and currently supports Facebook, Google+, LinkedIn and Twitter accounts. The Captive Web Portal can be customized with different colors and logos. We recommend a Terms of Use be added to the Captive Web Portal, matching with the legal requirements of your jurisdiction. Please see the disclaimer on the configuration page for more details.

## What is the NAT IP Subnet of my AP SSID Configuration?

If you want each AP to provide its own AP NAT boundary rather than bridge users directly onto the local network, you can now assign the Subnet for the APs to use in the SSID configuration.

Note: A known limitation is that the subnet will be assigned only on the 2.4Ghz radio. The 5Ghz radio will use a subnet 17 octets higher. For example, if the 2.4Ghz radio is set to use 10.10.10.1/24, the 5Ghz radio will use 10.10.17.1/24. This limitation will be addressed in a future software release.

## What is Floorplan in Maps?

In FortiCloud 3.0, you can now add a Floorplan, and zoom into it to place your APs and see their statistics and RF information. Previously, you could use Google Maps integration to see a floorplan overlaid over a building, but now full zoom and positioning controlls have been added.

## What are Folders?

Folders are a simple way to group AP's together for management purposes, and can be used to organize APs into groups, sites or any other organization you see fit. You can create subfolders and also assign new addresses and locations to APs.

## How do Dynamic VLANs work?

RADIUS servers can be configured to pass class attributes back in response to a successful authentication. One of these attributes is the VLAN to which the client should be assigned. With an Enterprise license and this feature enabled, it is possible to place different types of users connected to the same SSID into different VLANs, based on their user credentials.

## What is Bonjour Relay?

Bonjour is a protocol where (typically Apple) devices broadcast their services. For example, an Apple TV sends a Bonjour broadcast, so that an iPad knows it is there and can connect to it.

The issue is that these broadcasts are layer 2 – so if the iPad and the Apple TV are on different VLANs, then they will not be able to talk. Bonjour Relay is a simple mechanism to fix this. The FAP-S series of APs can be set to operate with a service network (where the Apple TV is), and a client network (where the iPad is), allowing the FAP-S to re-transmit the Bonjour requests from the service network onto the client network, allowing the iPad to learn where the Apple TV is and create a session.

To set it up, enter one or more services as Service VLAN and Client VLAN, along with a definition of the service, e.g. you may choose to only send the information about the Apple TV to a meeting room, and not the printer in reception. Once these services have been defined, simply select the AP that will perform the Bonjour Relay function.

## What is Blocking of Intra-SSID Traffic?

This feature blocks all traffic from one client to another on the same SSID. This helps to avoid a common issue of clients sending data between themselves on the same SSID, without traversing and being protected by the firewall.

## Why do I need to change my Radio Rates in the Enterprise Management section?

Wireless operates at many different data rates based on the quality of the radio signal. For example, an 802.11n 2.4GHz client is capable of running at 450 Mbs on a 3x3 AP, but it is equally capable of running at 1 Mbps.

Inconsistent radio rates can lead to clients remaining connected to an AP long after they should have reconnected to a better AP. A client running at 1 Mbps has great range, but its slow throughput will have a degrading effect on the network performance as a whole. The new data rate control feature in 3.1 allows you to restrict which data rates are allowed, to ensure clients that are too far away are not slowing down the overall system.

# Indicator of Compromise (IOC) Service

## What is the FortiCloud Indicator of Compromise Service feature?

FortiCloud Indicator of Compromise (IOC) Service is a new service that alerts administrators about newly-found infections and threats to devices in their network. By analyzing UTM logging and activity, the service can provide a comprehensive overview of threats to the network.

## What kind of threats can the IOC Service detect?

IOC can detect three types of threats, based on our evolving FortiGuard database:

- Malware — Malicious programs residing on infected endpoints.
- PUP — Potentially unwanted programs, such as Spyware, Adware, and toolbars.
- Unknown — Threats detected by signature but not associated with any known malware.

## How do I get access to the IOC Service?

The IOC is currently being developed as a beta, and will be rolled out to existing FortiCloud customers over time.

## Does the IOC Service require a subscription?

The basic form of the IOC is free, which will alert you to threats and automatically prepare a comprehensive threat report.

You can purchase a subscription for the complete IOC by opening the *Plan* page in the FortiCloud IOC site, selecting *Buy Online*, and completing the purchase process.

A subscription grants you access to IP Whitelisting, which allows you to narrow your malware search by excluding safe IPs and domains, and Alert Emails, which notify you directly of detected network threats. It will also allow you to view the IPs of infected devices, allowing you to better control their access to your network.

## How do I register my subscription code once I've purchased one?

You will receive your subscription code by email. Visit the Fortinet Support portal at http://support.fortinet.com, and log into your customer account. On the *Asset* page, register the subscription code as if it were a product serial number, and then enter the serial number of the FortiCloud-connected device that you want the service to monitor.

# FortiDeploy

## What is FortiDeploy?

FortiDeploy is a product built into FortiCloud as a feature, for one-touch provisioning when devices are deployed, locally or remotely. FortiDeploy provides deployment for FortiAPs into a Cloud AP Network, and automatic connection of FortiGates to be managed by FortiCloud or a FortiManager unit.

## What features does FortiDeploy provide?

- One touch deployment for FortiAPs into a Cloud AP Network
- One touch deployment for FortiGates to be FortiCloud managed or mananged by a FortiManager IP

## How does FortiDeploy work?

When you visit forticloud.com and enter the Bulk FortiCloud Key, you will see a list of serial numbers from the order that contained the FortiDeploy SKU. Once you confirm that the devices are connected, you can perform some basic configuration on the devices remotely, such as sending a FortiManager IP to all remote FortiGate devices, so they can be managed remotely.

## How do I purchase FortiDeploy?

At time of purchase, order a FortiDeploy SKU in addition to your other purchases, and enter it in FortiCloud. Once the FortiGate's serial number is associated with your customer account, you have the option to deploy the devices in either FortiCloud or FortiManager. FortiDeploy can also push an IP to each FortiManager. Support starts the moment you send an email to cs@fortinet.com.

## What is the price of FortiDeploy?

FortiDeploy must be purchased on every PO using FDP-SINGLE-USE SKU. The nominal fee is $100/PO.

## What happens if you forget to order FortiDeploy on the PO?

If you forget to order FortiDeploy on the PO, please send an email to the Fortinet Customer Service and Support Team: cs@fortinet.com, and they can manually register your serial numbers and generate a Bulk FortiCloud Key.

## Will my FortiGuard and FortiCare services start automatically?

No. FortiGuard and FortiCare services will start only after you register your serial numbers. Bulk registration of FortiGuard and FortiCare is available, but you will need to send a direct request after registration to cs@fortinet.com.

## What are the devices supported by FortiDeploy?

- All FortiGates up to 2U (3200D), and all FortiWiFi devices
- All FAPs

## Which versions of FortiOS does FortiDeploy support?

FortiDeploy is available for FortiGate/FortiWiFi devices at FortiOS version 5.2.2 or later, and FortiAP devices at version 5.0.9 or later.

## Are there any complications if I've recently upgraded FortiOS?

From FortiOS 5.2.3 onward, the CLI command `auto-join-forticloud` is enabled by default, and must be enabled for FortiDeploy to function correctly.

But upgrading the FortiOS firmware from 5.0.x to 5.2.2 or later automatically disables `auto-join-forticloud`, which will need to be re-enabled or FortiDeploy will not function.

You can re-enable it through the CLI or by factory resetting your device (but factory resetting will reset all firewall configuration).

```
config system fortiguard
  get
    set auto-join-forticloud enable
  end
end
```

After changing this setting, restart the device and ensure that traffic is being sent to FortiCloud to verify that it has been configured correctly.

## What if I am connected to FortiCloud but the device is not cloud-managed?

Double-check that central management is set to FortiGuard.

In the CLI console:

```
config system central-management
  set type fortiguard
end
```

Reboot the device, login to FortiCloud and try to manage the device.

## What if a device is deployed behind a NAT device (such as a cable modem)?

A FortiGate's default "internal" IP is in the 192.168.1.0/24 subnet, and so IP conflicts can occur with FortiDeploy-managed devices. The solution is to unset the default IP for each of the devices in the CLI console:

```
config system interface
  edit internal
    unset ip
  end
end
```

Or change the internal interface's IP in the web-based management interface.