FortiClient - Compliance Guide

Version 6.4

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

November 25, 2021
FortiClient 6.4 Compliance Guide
04-640-620107-20211125

TABLE OF CONTENTS

Deployment options

You can deploy FortiClient in one of the following scenarios:

- FortiClient in the Security Fabric on page 4. This scenario allows FortiClient to participate in the Fortinet Security Fabric.
- FortiClient with EMS on page 6. In this scenario, FortiClient does not participate in the Security Fabric.

FortiClient in the Security Fabric

In this scenario, FortiClient Telemetry connects to EMS to receive a profile of configuration information as part of an endpoint policy. EMS is connected to the FortiGate to participate in the Security Fabric. EMS sends FortiClient endpoint information to the FortiGate. The FortiGate can also receive dynamic endpoint group lists from EMS and use them to build dynamic firewall policies. EMS sends group updates to FortiOS, and FortiOS uses the updates to adjust the policies based on those groups. This feature requires FortiOS 6.2.0 or a later version.

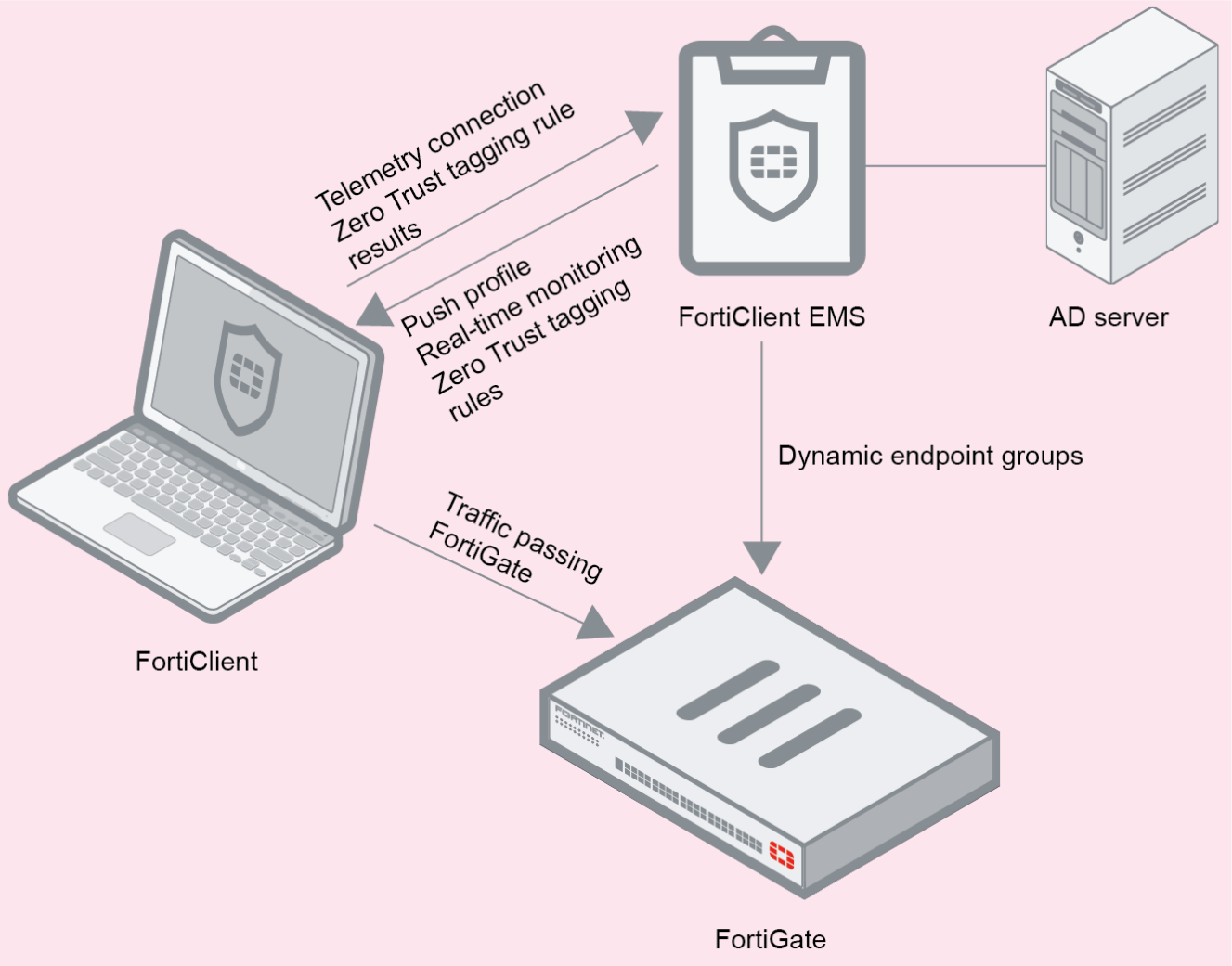
FortiClient 6.4 does not directly connect to FortiOS. FortiOS receives FortiClient data only from EMS.

FortiGate does not provide configuration information for FortiClient and the endpoint. An administrator must configure FortiClient using an EMS endpoint policy.

Following is a summary of how the FortiClient Telemetry connection works in this scenario:

1. EMS is connected to the FortiGate as a participant in the Security Fabric.
2. FortiClient Telemetry attempts connection to EMS. Based on the EMS configuration, FortiClient may receive an SSL certificate from EMS to verify the connection. If the certificate is valid, FortiClient Telemetry connects to EMS.
3. EMS sends the endpoint information received via FortiClient Telemetry to FortiOS.
4. FortiClient receives a profile of configuration information from EMS as part of an endpoint policy.
5. EMS sends Zero Trust tagging rules to the endpoint.
6. FortiClient checks the endpoint using the provided Zero Trust tagging rules and sends the results to EMS.
7. EMS receives the results from FortiClient and dynamically groups the endpoints according to the results.
8. FortiOS pulls the dynamic endpoint group information from EMS. You can use this data to build dynamic firewall policies.
9. EMS sends dynamic endpoint group updates to FortiOS. FortiOS uses the updates to adjust the policies based on those groups.

For details about configuring dynamic endpoint groups in FortiOS, see the *FortiClient EMS Administration Guide*.



FortiClient follows the endpoint profile configuration that it receives from EMS. EMS locks FortiClient settings so that the endpoint user cannot manually change FortiClient configuration.

Only EMS can control the connection between FortiClient and EMS. You can only disconnect FortiClient from EMS.

The EMS server's IP addresses are embedded in FortiClient deployment packages created in EMS. This allows the endpoint to connect FortiClient Telemetry to the specified EMS server.

EMS sends the following endpoint information to FortiOS:

- User profile:
  - Logged-in username
  - Full name
  - Email address
  - Phone number
- User avatar
- Social network account IDs
- MAC address
- OS type
- OS version

- FortiClient version
- FortiClient UUID

EMS also sends the following endpoint information to FortiAnalyzer:

- Telemetry/system information
- User avatar
- Software inventory
- Processes
- Network statistics

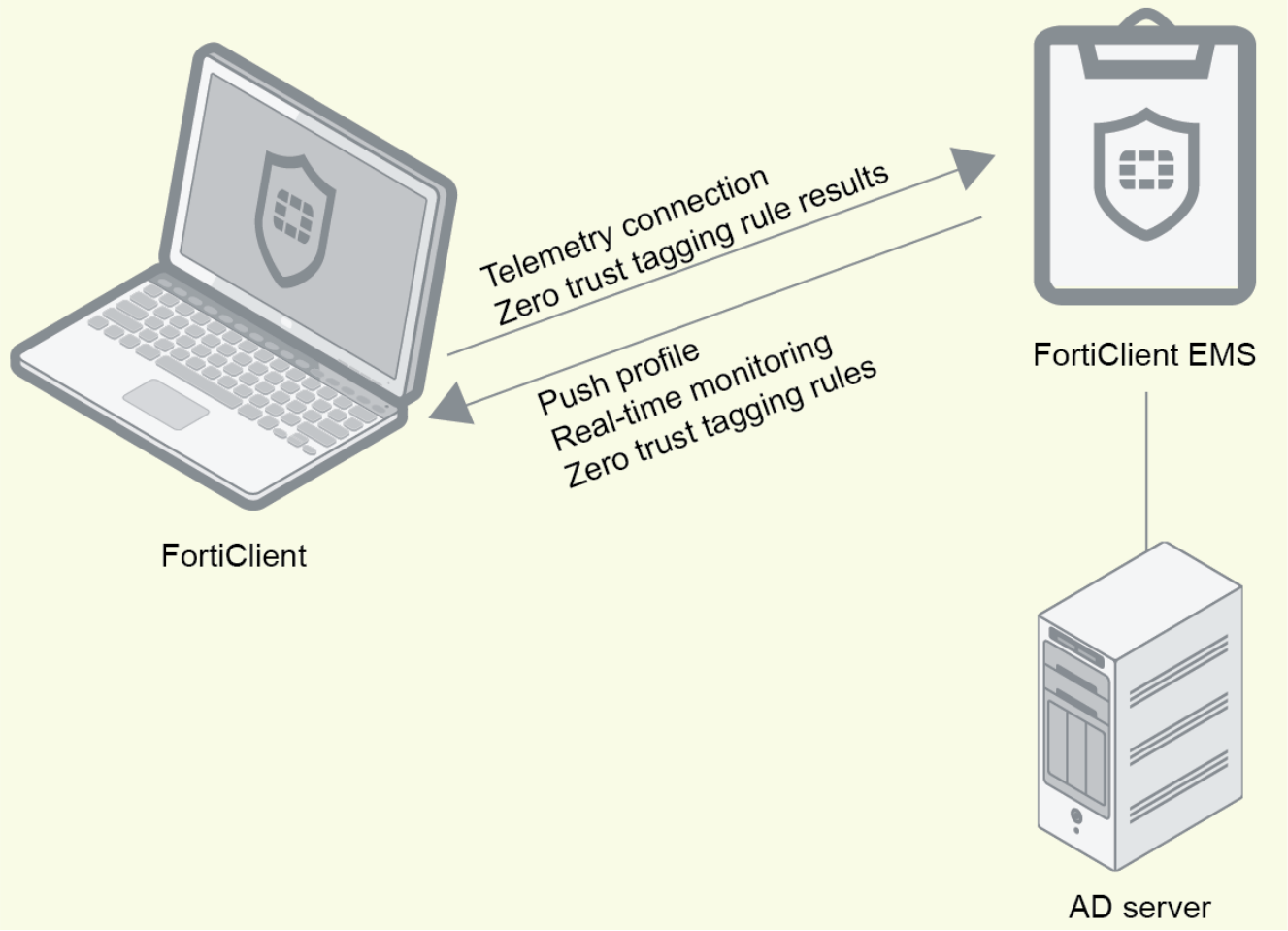
FortiClient directly sends the following information to FortiAnalyzer:

- Logs
- Windows host events

FortiClient with EMS

In this scenario, EMS provides FortiClient endpoint provisioning. FortiClient connects Telemetry to EMS to receive configuration information in an endpoint profile as part of an endpoint policy from EMS. EMS also sends Zero Trust tagging rules to FortiClient, and use the results from FortiClient to dynamically group endpoints in EMS. Only EMS can control the connection between FortiClient and EMS. You must make any changes to the connection from EMS, not FortiClient. When FortiClient is connected to EMS, EMS locks FortiClient settings so that the endpoint user cannot change any configuration. To disconnect FortiClient from EMS, the EMS administrator must deregister the endpoint in EMS.

In this scenario, EMS and FortiClient cannot participate in the Security Fabric, since a FortiGate is not present.


Telemetry connection
Zero trust tagging rule results
Push profile
Real-time monitoring
Zero trust tagging rules
FortiClient
FortiClient EMS
AD server

How FortiClient Telemetry connects to EMS

When initially installing FortiClient on an endpoint, FortiClient registers to the EMS that created the deployment package.

After the FortiClient endpoint reboots, rejoins the network, or encounters a network change, FortiClient uses the following methods in the following order to locate an EMS for Telemetry connection:

1. Manually entering the IP address, which means that the endpoint user enters the EMS IP address into FortiClient.
2. Telemetry server list:
   FortiClient Telemetry searches for IP addresses in its subnet in the Telemetry server list. It connects to the EMS in the list that is in the same subnet as the host system.

   If FortiClient cannot find any EMS servers in its subnet in the Telemetry server list, it attempts to connect to the first reachable EMS in the list, starting from the top. FortiClient maintains the list order as configured in the Telemetry server list.
3. Remembered Telemetry server list. You can configure FortiClient to remember server IP addresses when you connect Telemetry to EMS. Later FortiClient can use the remembered IP addresses to automatically connect Telemetry to EMS.

Silent registration

When silent registration is enabled, FortiClient connects and reconnects Telemetry to EMS without any user interaction. FortiClient does not notify the user about the connection, and the user is not required to confirm the connection.

By default, silent registration is enabled in endpoint profiles in EMS. If desired, you can disable silent registration in EMS.

Reregistration

The EMS administrator can assign an endpoint policy that includes a Telemetry server list to endpoints. Receiving the Telemetry server list triggers FortiClient to connect to an EMS server using the order in How FortiClient Telemetry connects to EMS on page 8, even if FortiClient Telemetry is already connected to EMS.

Change log

Date	Change Description
2020-05-12	Initial release.
2021-11-25	Updated FortiClient in the Security Fabric on page 4.