FortiClient - Compliance Guide

Version 6.2

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 COOKBOOK
https://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

FORTINET®

April 16, 2019
FortiClient 6.2 Compliance Guide
04-620-546335-20190416

TABLE OF CONTENTS

Introduction

This document describes using FortiClient in the following configurations:

- FortiClient with FortiGate and EMS on page 5
- FortiClient with EMS on page 7

Deployment options

This section describes the following deployment options: FortiClient with FortiGate and EMS and FortiClient with EMS.

FortiClient with FortiGate and EMS

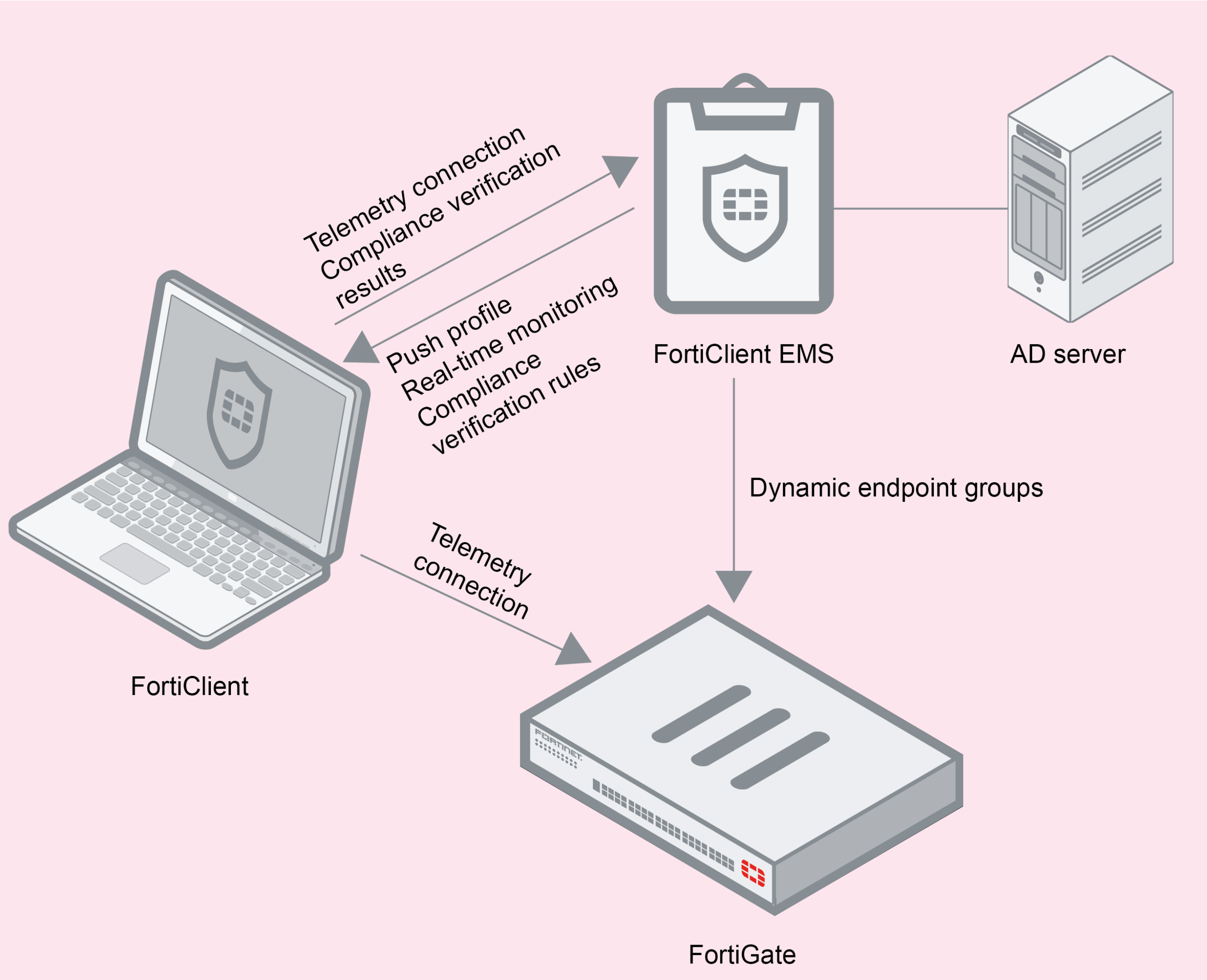
In this scenario, FortiClient Telemetry connects to EMS to receive a profile of configuration information as part of an endpoint policy and to FortiGate to participate in the Fortinet Security Fabric. The FortiGate can also receive dynamic endpoint group lists from EMS and use them to build dynamic firewall 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.

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

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

- FortiClient Telemetry connects to EMS.
- FortiClient receives a profile of configuration information from EMS as part of an endpoint policy.
- FortiClient Telemetry connects to the FortiGate using a Telemetry gateway list received from EMS. This allows the endpoint to participate in the Security Fabric.
- EMS sends compliance verification rules to the endpoint.
- FortiClient checks the endpoint using the provided compliance verification rules and sends the results to EMS.
- EMS receives the results from FortiClient and dynamically groups the endpoints according to the results.
- FortiOS pulls the dynamic endpoint group information from EMS. You can use this data to build dynamic firewall policies.
- 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 received from EMS. FortiClient settings are locked so the endpoint user cannot change any configuration.

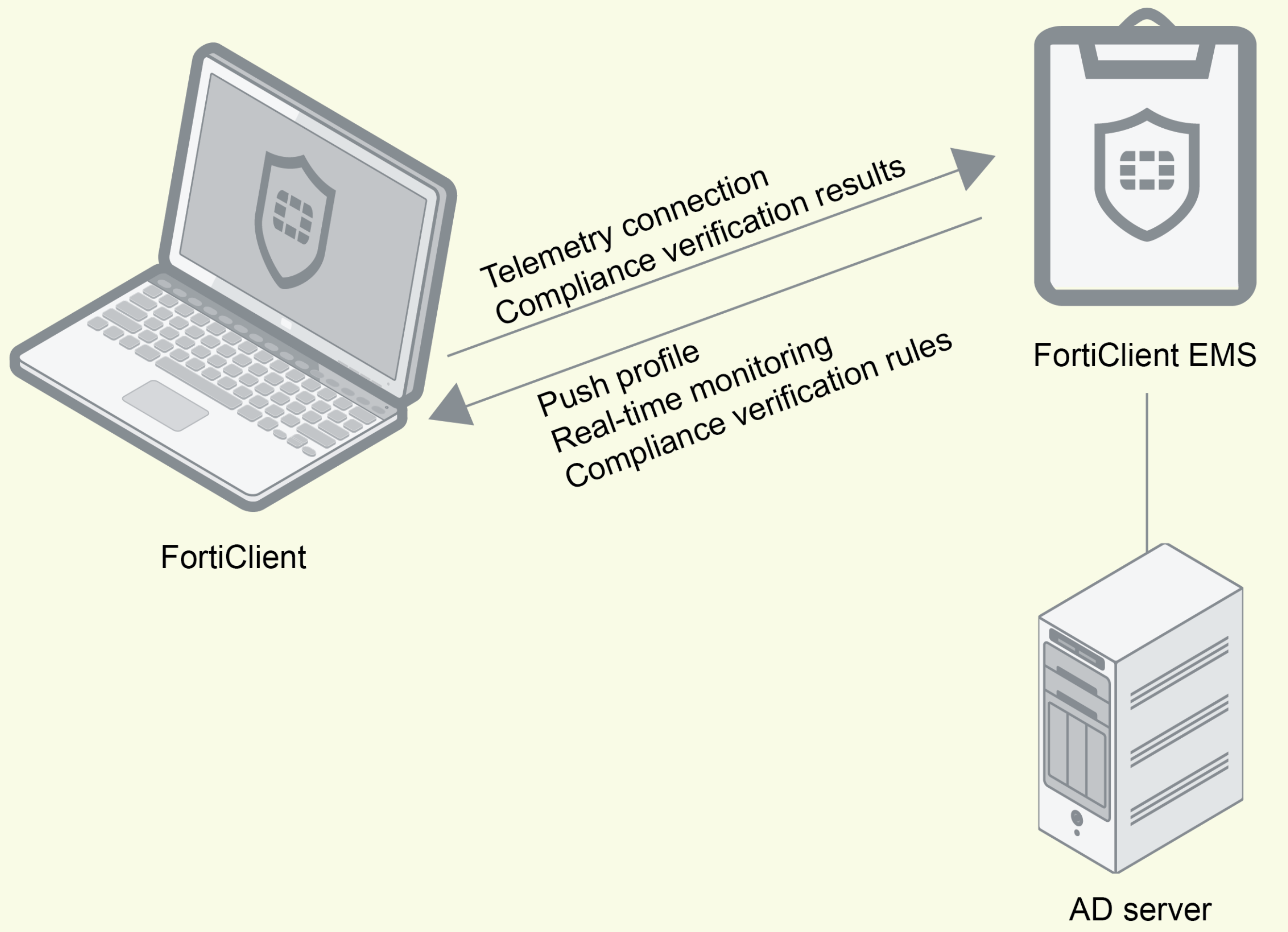
Only EMS can control the connection between FortiClient and EMS. Disconnecting FortiClient from EMS can only be done in EMS.

FortiClient installers created in EMS are embedded with the EMS server's IP address. This allows the endpoint to connect FortiClient Telemetry to the specified EMS server. The administrator can also embed a Telemetry gateway list in the installer that contains FortiGate IP addresses. This allows the endpoint to connect FortiClient Telemetry to a FortiGate. FortiClient only registers to a FortiGate if all of the following is true:

- FortiClient is registered to EMS.
- FortiClient has received a Telemetry gateway list from EMS.
- EMS has allocated a Fabric Agent license to the endpoint. A Fabric Agent license is required to register to the FortiGate. See the *FortiClient EMS Administration Guide*.

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 compliance verification 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. Any changes to the connection must be made from EMS, not FortiClient. When FortiClient is connected to EMS, FortiClient settings are locked so the endpoint user cannot change any configuration. To disconnect FortiClient from EMS, the EMS administrator must deregister the endpoint in EMS.



How FortiClient Telemetry connects to IP addresses

When initially installing FortiClient on an endpoint, FortiClient registers to the EMS server that created the deployment package. FortiClient also registers to a FortiGate using the Telemetry gateway list configured in the installer, if present.

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

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

  If FortiClient cannot find any FortiGates in its subnet, it will attempt to connect to the first reachable FortiGate in the list, starting from the top. The order of the list is maintained as it was configured in the gateway IP list.
- Remembered gateway IP list. You can configure FortiClient to remember gateway 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 or EMS and the FortiGate 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 gateway IP list to endpoints. Receiving the gateway IP list triggers FortiClient to connect to a server using the order in How FortiClient Telemetry connects to IP addresses on page 8, even if FortiClient Telemetry is already connected to EMS or EMS and the FortiGate.

Change log

Date	Change Description
2019-04-16	Initial release

Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.