FortiClient & FortiClient EMS - New Features Guide

Version 6.2.1

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/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: techdoc@fortinet.com

February 26, 2019
FortiClient & FortiClient EMS 6.2.1 New Features Guide
04-621-548127-20200226

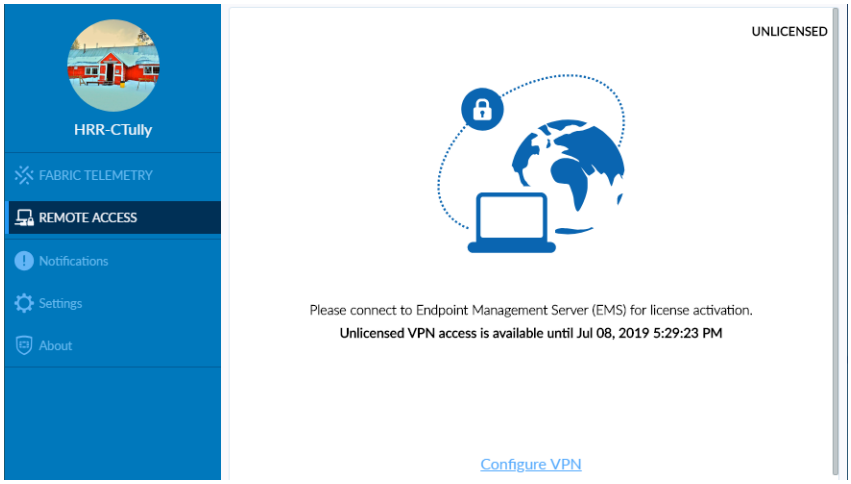
TABLE OF CONTENTS

Other

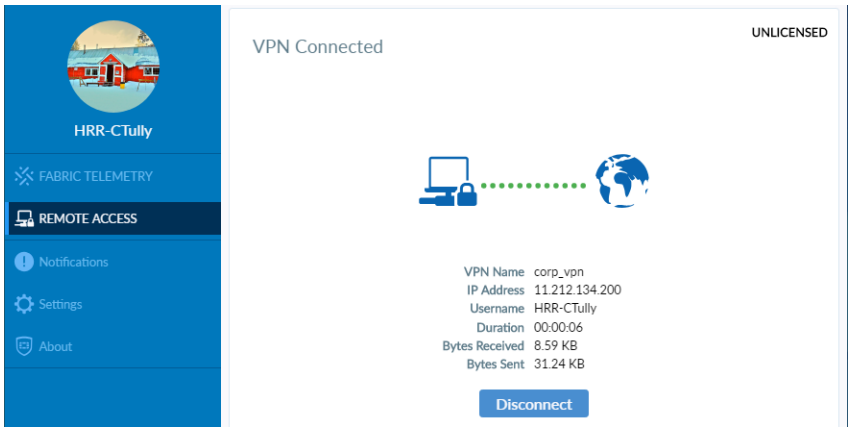
Free three-day VPN access for FortiClient

After you install FortiClient 6.2.1, you get three-day free VPN access so that you can connect to a remote EMS for license activation. You must connect to the remote EMS to activate your license and unlock all supported FortiClient features.

After initial FortiClient installation, if FortiClient has not registered to any EMS, all FortiClient features are disabled except for Remote Access. You can use full FortiClient VPN functionality for three days. The FortiClient GUI shows that it is unlicensed and indicates the time that VPN will be available in this unlicensed state.



You can configure and establish a VPN connection to a FortiGate. This allows the endpoint to reach an EMS behind a FortiGate.



Following successful registration to EMS, FortiClient receives a full license if available from EMS. EMS enables all FortiClient features configured on the assigned endpoint profile, which may include Remote Access.

If FortiClient goes offline after registering to EMS, FortiClient features remain enabled for 30 days. You can still establish a VPN connection to the FortiGate in this scenario.

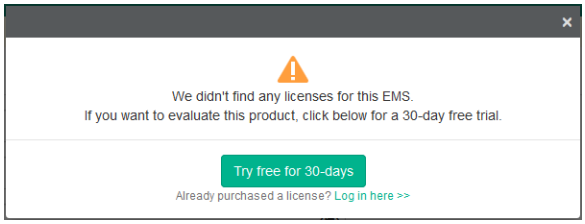
If FortiClient does not register to EMS or obtain a valid Fabric Agent license during the three-day free VPN access, the Remote Access feature becomes unavailable. At this point, the endpoint must be able to reach EMS without a VPN connection to connect to EMS. Upon successfully receiving a license from EMS, EMS enables all FortiClient features configured on the assigned endpoint profile.

30-day free trial support

EMS supports a 30-day free trial. After installing EMS, you can enroll for a 30-day free trial from the EMS GUI. This makes it easier for prospective customers to try the FortiClient product. If you want to extend your trial, you must contact Fortinet sales for an evaluation license.

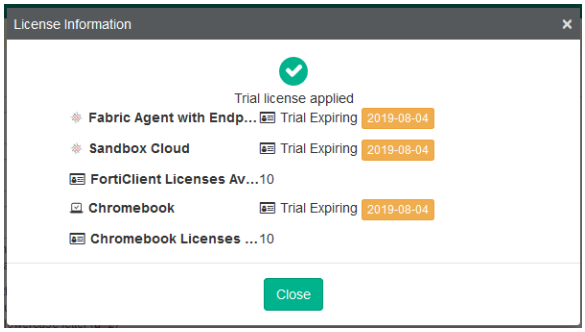
To activate 30-day free trial support:

1. Download an EMS installation file from the Fortinet support site or obtain the file from Fortinet sales.
2. Install EMS.
3. If you do not have a FortiCare account, create a FortiCare account. You can create a FortiCare account in one of two ways:
   a. Register directly on the FortinetOne website.
   b. Register via the link on the EMS GUI. When you install and log in to EMS, EMS displays the following prompt if EMS is unlicensed. Click the *Try free for 3-days* button.

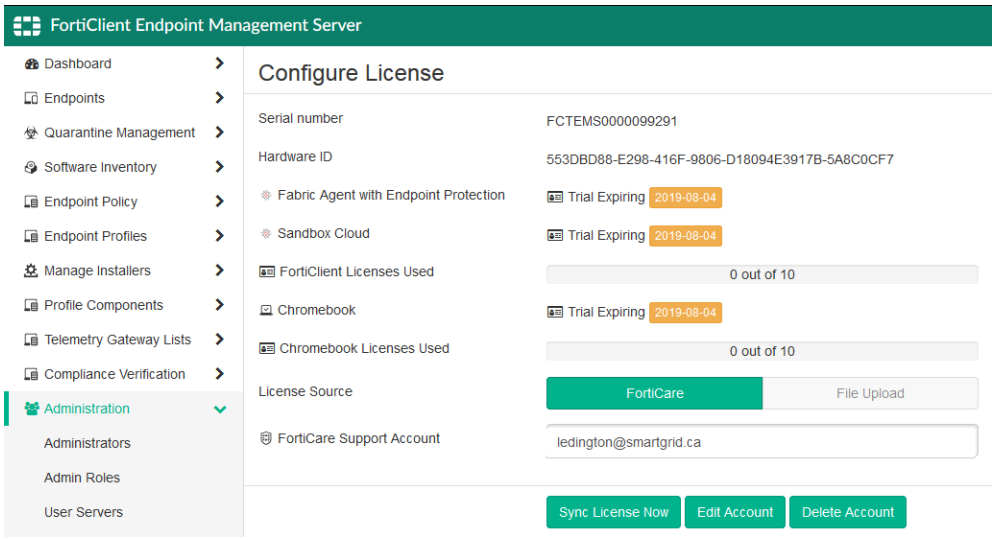
   

   Click *Sign up now* >>.

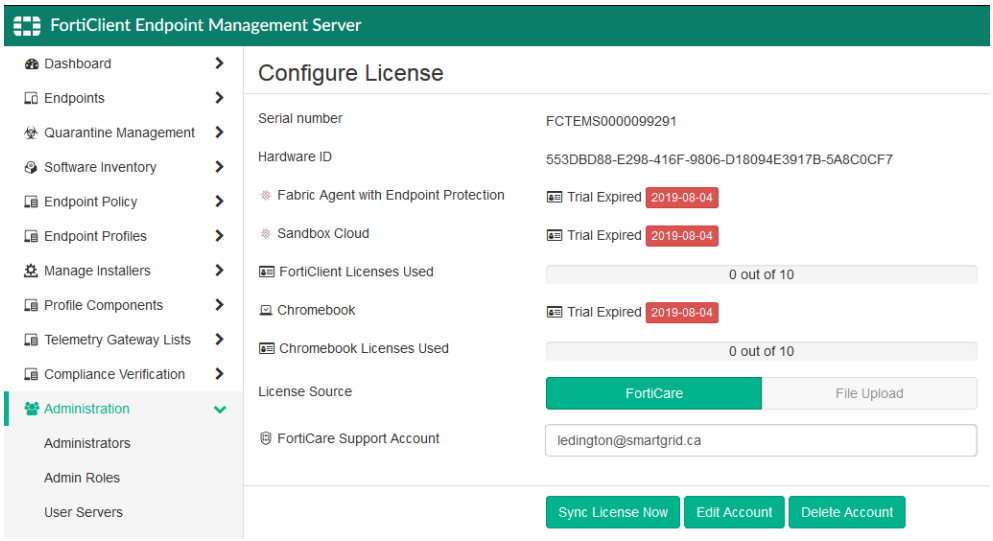
   On the FortinetOne registration page, create an account.
4. In EMS, in the *FortiCare Support Registration* dialog, enter your FortiCare email address and password.
5. Click *Login & Start Trial*. EMS retrieves a trial license from FortiCare. The following shows the trial license information retrieved from FortiCare.

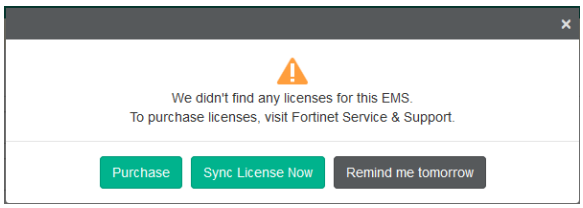
   

6. Go to *Administration* > *Configure License*. Verify that your EMS has a 30-day trial license with ten seats for Windows, macOS, and Linux endpoints, and ten seats for Chromebook endpoints, with all features enabled.



After 30 days, EMS shows that the license expired.





You can purchase a full license before or after the trial license expires. After upgrading to the full license using the FortiCare account created in step 3, go to *Administration* > *Configure License* and click the *Login & Sync License Now* button. EMS checks for and retrieves the full license from FortiCare.

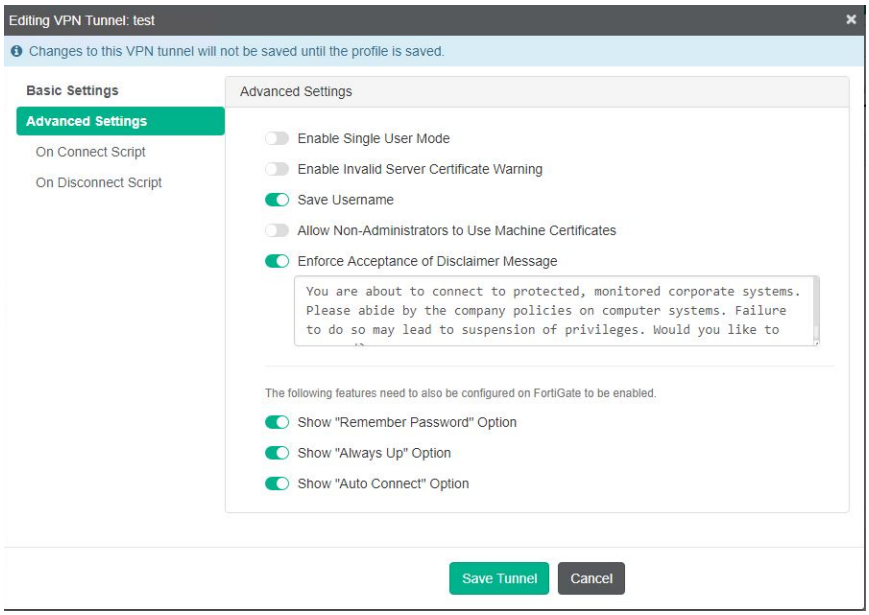
VPN option to enforce disclaimer acceptance

You can enforce acceptance of a disclaimer message before a remote user connects to IPsec or SSL VPN. You can use the disclaimer message to notify the end user of important points to remember when using FortiClient VPN.

This guide assumes that you have configured SSL VPN in FortiOS and it is ready to use.

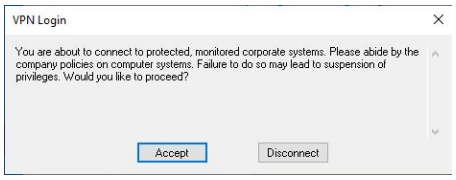
To configure enforcing disclaimer acceptance:

1. In EMS, under *Endpoint Profiles*, select the desired profile.
2. On the *VPN* tab, edit an existing VPN tunnel, or create a new one.
3. On the *Advanced Settings* tab, enable *Enforce Acceptance of Disclaimer Message*. Enter a custom message in the text box.



4. Click *Save Tunnel*.

When a remote user establishes a VPN connection, the disclaimer message displays. If the user clicks Accept, the VPN connection establishes successfully. If the user clicks Disconnect, the VPN connection process terminates.



The disclaimer message displays under the following scenarios:

- When the user attempts to connect to VPN when *Auto Connect* and/or *Always Up* are enabled.
- Before the VPN connection establishes, if the endpoint restarts.
- With resilience configuration, when FortiClient connects to the primary or secondary FortiGate.
- When you have enabled *Show VPN before Logon*.

Change log

Date	Change Description
2019-07-18	Initial release.
2020-02-26	Added VPN option to enforce disclaimer acceptance on page 7.