Endpoint communication security improvement

FortiClient Endpoint Management Server (EMS) and FortiClient 6.4.7 add an improvement to endpoint communication security.

FortiClient connects to EMS using Telemetry to:

- Obtain license information
- Send endpoint and management information to EMS
- Receive endpoint configuration
- Receive endpoint commands, the results of which it can send to EMS
- Other similar tasks

The connection from FortiClient to EMS uses TCP and TLS 1.3. During the SSL connection setup, EMS sends a server certificate to FortiClient. The certificate that EMS sends to FortiClient is the one configured in *EMS Settings* > *Shared Settings* > *SSL certificate*. See Adding an SSL certificate to FortiClient EMS.

In 6.4.6 and earlier versions, FortiClient checks the certificate subject name received from EMS to confirm its validity. In 6.4.7, the certificate validation follows industry standards:

- Domain or fully qualified domain name (FQDN) that FortiClient is connecting to matches the domain to which the certificate is issued.
    - Validation process correctly handles wildcards in the domain name in the certificate.
    - Validation process considers both the common name (CN) in the subject or subject alternative name (SAN).
- The certificate expiry date is in the future. The certificate has not expired.
- The certificate issuer or the root certificate in the certificate chain is from a publicly trusted certificate authority (CA). Trusted CAs are read from the operating system.

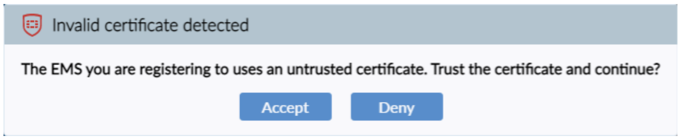
The new endpoint communication security feature allows the EMS administrator to configure endpoint profiles to take different actions based on the validity of the certificate that FortiClient receives from EMS. The EMS administrator configures this feature by enabling *Use SSL certificate for Endpoint Control* in EMS and configuring the desired *Invalid Certificate Action* for each endpoint profile.

When *Use SSL certificate for Endpoint Control* is enabled, FortiClient 6.4.6 and earlier versions cannot connect to EMS. Following the recommended upgrade path as detailed in the following procedure is recommended to ensure that endpoints can connect to EMS. See Recommended upgrade path on page 3.

The following describes the behavior when *Use SSL certificate for Endpoint Control* is enabled:

- If the EMS server certificate is valid, FortiClient silently connects without displaying a message. This is the same connection behavior from 6.4.6 and earlier versions.
- If the EMS server certificate is invalid:
    - If the *Invalid Certificate Action* is configured as *Warn*, FortiClient displays a warning message to the end user. The message warns the user that the EMS to which FortiClient is attempting to connect to has provided an invalid server certificate. The message offers options to allow or deny the connection:
        - If the user allows the connection, FortiClient connects to EMS and remembers the certificate for this EMS. FortiClient no longer prompts the user each time that it connects to this EMS.

  - If the user denies the connection, FortiClient does not connect to EMS by canceling the connection. The next time that the user tries to connect to the same EMS and the server certificate is still invalid, FortiClient displays the same message again.



Invalid certificate detected

The EMS you are registering to uses an untrusted certificate. Trust the certificate and continue?

- If the *Invalid Certificate Action* is configured as *Allow*, FortiClient connects to EMS.
- If the *Invalid Certificate Action* is configured as *Deny*, FortiClient does not connect to EMS.

When *Use SSL certificate for Endpoint Control* is disabled, EMS sends the FortiCare certificate for endpoint control connections to FortiClient. FortiClient considers this certificate invalid and follows the configured *Invalid Certificate Action*.

Recommended upgrade path

Existing FortiClient and EMS users may have a mixture of 6.4.7 and older versions in production. The new endpoint security improvement feature is only available for EMS 6.4.7 and later versions. The EMS administrator configures this feature by enabling *Use SSL certificate for Endpoint Control* in EMS and configuring the desired *Invalid Certificate Action* for each endpoint profile. When the endpoint security improvement feature is enabled in EMS, only FortiClient 6.4.7 and later versions can connect. Therefore, upgrading all FortiClient endpoints to 6.4.7 is recommended.

⚠ When *Use SSL certificate for Endpoint Control* is enabled on EMS, FortiClient 6.4.6 and earlier versions cannot connect to EMS. Following the recommended upgrade path as detailed in the following procedure is recommended to ensure that endpoints can connect to EMS.

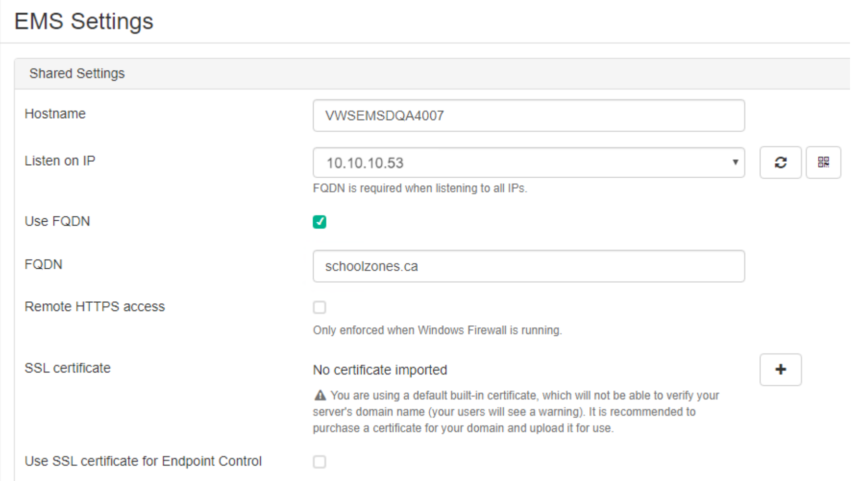
⚠ FortiOS connects to EMS using the configured Fabric connector. Whenever the SSL certificate changes on EMS, you must reauthorize the EMS certificate in FortiOS.

Following is the recommended upgrade path for when FortiClient and/or EMS older than 6.4.7 exists in production. You must complete the following steps:

1. Upgrade EMS to 6.4.7.
2. Upgrade FortiClient to 6.4.7.
3. Apply a valid certificate to EMS.
4. Configure the invalid certificate action as warn.

To upgrade EMS to 6.4.7:

1. Upgrade EMS to 6.4.7 as the Upgrade Path describes.
2. Go to *System Settings > EMS Settings*.
3. Disable *Use SSL certificate for Endpoint Control*.



EMS Settings

Shared Settings

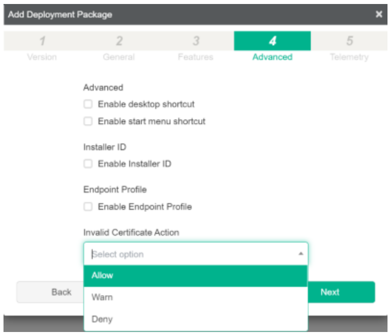
Hostname	VWSEMSDQA4007
Listen on IP	10.10.10.53 FQDN is required when listening to all IPs.
Use FQDN	☑
FQDN	schoolzones.ca
Remote HTTPS access	☐ Only enforced when Windows Firewall is running.
SSL certificate	No certificate imported ⚠ You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). It is recommended to purchase a certificate for your domain and upload it for use.
Use SSL certificate for Endpoint Control	☐

4. Go to *Endpoint Profiles > Manage Profiles*.
5. Select a profile.

6. On the *System Settings* tab, configure *Invalid Certificate Action* as *Allow*.
7. Save the configuration.
8. Repeat steps 4-7 for all profiles.

To upgrade FortiClient to 6.4.7:

1. Create an installer:
   a. In EMS, go to *Deployment & Installers* > *FortiClient Installer*.
   b. Click *Add*.
   c. On the *Version* tab, select *Choose a custom installer*.
   d. Select an existing FortiClient 6.4.7 custom installer from the *Custom Installer* dropdown list, or use the *Add Installer option* to add a new 6.4.7 installer.
   e. Click *Next*.
   f. In the *Name* and *Notes* fields, enter the desired values. Click *Next*.
   g. On the *Features* tab, enable all desired features. Click *Next*.
   h. On the *Advanced* tab, from the *Invalid Certificate Action* dropdown list, select *Allow*. Configure other fields as desired, then click *Next*.



Advanced
☐ Enable desktop shortcut
☐ Enable start menu shortcut

Installer ID
☐ Enable Installer ID

Endpoint Profile
☐ Enable Endpoint Profile

Invalid Certificate Action
Select option
Allow
Warn
Deny

   i. Click *Finish*.
2. Create a deployment configuration:
   a. Go to *Deployment & Installers* > *Manage Deployment*.
   b. Click *Add*.
   c. In the *Endpoint Groups* field, click *Edit*. In the *Add Endpoint Groups* dialog, select all groups that contain endpoints to upgrade to 6.4.7.
   d. For *Action*, select *Install*.
   e. From the *Deployment Package* dropdown list, select the package that you created earlier.
   f. Enable *Start at a Scheduled Time* and configure the desired time.
   g. Ensure that *Enable the Deployment* is enabled.
   h. Configure other fields as desired, then save the deployment configuration.
   At the scheduled time, EMS deploys the FortiClient 6.4.7 upgrade to all endpoints groups that you configured for the deployment. FortiClient upgrades to 6.4.7 on the endpoints. After upgrade, FortiClient reconnects to EMS. FortiClient does not display an error or warning as it reconnects to EMS.

To apply a valid certificate to EMS:

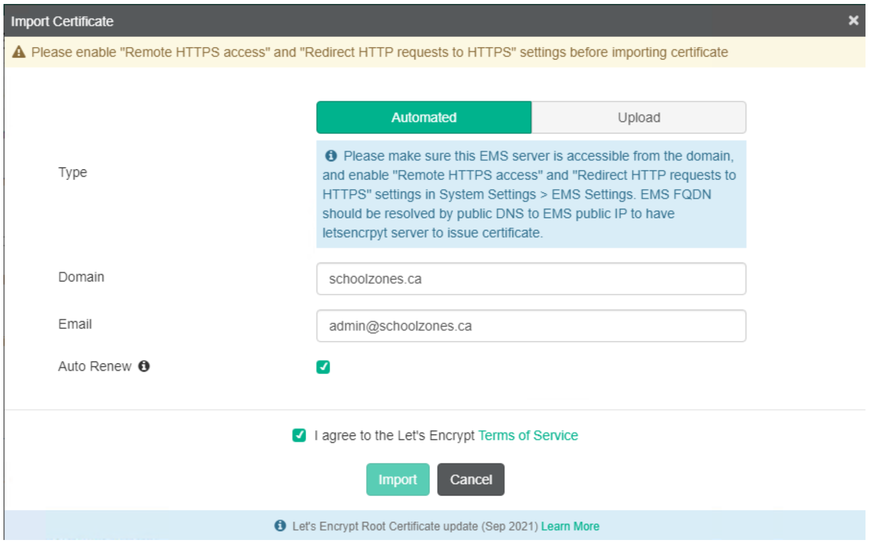
1. In EMS, go to *System Settings > EMS Settings*.
2. You can add an SSL certificate to EMS in one of the following ways:

Method	Description
Automated	The Automated Certificate Management Environment (ACME), as defined in RFC 8555, is used by the public Let's Encrypt certificate authority to provide free SSL server certificates. You can configure EMS to use certificates that are managed by Let's Encrypt.
Upload	Manually upload an SSL certificate.

For either method, you must ensure that the certificate satisfies the criteria in Endpoint communication security improvement on page 1 to ensure that communication between FortiClient and EMS is secure.

Do one of the following:

a. Configure an automated SSL certificate:
   i. Go to *System Settings > EMS Settings*.
   ii. Ensure that *Remote HTTPS access* and *Redirect HTTP request to HTTPS* are enabled.
   iii. Ensure that ports 80 and 443 are accessible from the Internet by going to https://<EMS FQDN> in a browser. If the ports are accessible, the browser displays the EMS login page.
   iv. In the *SSL certificate* field, click the *Import SSL certificate* button.
   v. Select *Automated*.
   vi. In the *Domain* field, enter the EMS FQDN. For the Let's Encrypt server to issue the certificate, the public DNS server must resolve the EMS FQDN to the EMS public IP address.
   vii. In the *Email* field, enter a valid email address.
   viii. If desired, enable *Auto Renew*. When *Auto Renew* is enabled, EMS automatically renews the certificate before expiry.
   ix. Select the checkbox to agree to Let's Encrypt's terms of service. Click *Import*.



⚠ Please enable "Remote HTTPS access" and "Redirect HTTP requests to HTTPS" settings before importing certificate

Type: Automated

Please make sure this EMS server is accessible from the domain, and enable "Remote HTTPS access" and "Redirect HTTP requests to HTTPS" settings in System Settings > EMS Settings. EMS FQDN should be resolved by public DNS to EMS public IP to have letsencrpyt server to issue certificate.

Domain: schoolzones.ca

Email: admin@schoolzones.ca

Auto Renew: ☑

☑ I agree to the Let's Encrypt Terms of Service

Let's Encrypt Root Certificate update (Sep 2021) Learn More

b. Manually upload an SSL certificate:
   i. Go to *System Settings > EMS Settings*.
   ii. In the *SSL certificate* field, click the *Import SSL certificate* button.

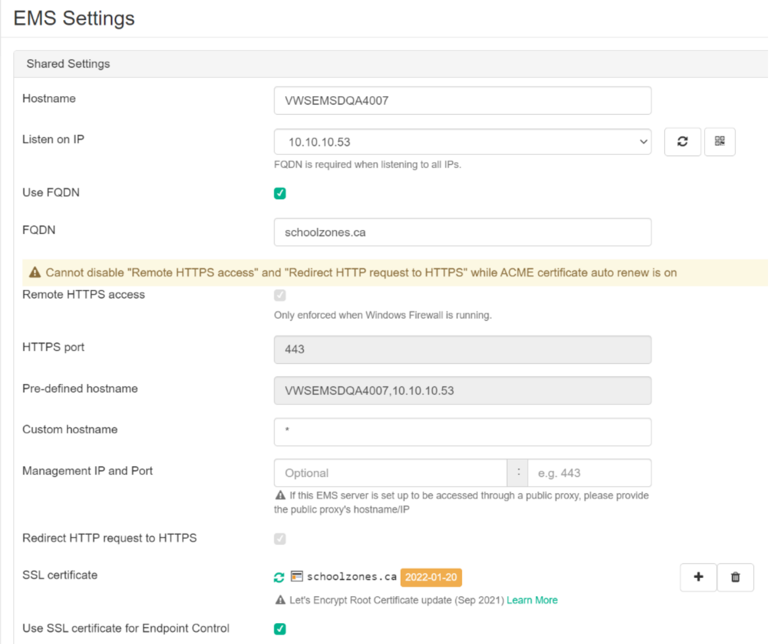
   iii. Select *Upload*.

   iv. In the *Certificate* field, browse to and select the desired certificate.

   v. In the *Certificate Password* field, configure the desired password for the certificate.

   vi. Click *Upload*.

3. After all endpoints have upgraded to FortiClient 6.4.7 and EMS is using a valid certificate, go to *System Settings > EMS Settings* and enable *Use SSL certificate for Endpoint Control*. When you enable this option, endpoints still running FortiClient 6.4.6 and older versions can no longer connect to this EMS. If they were previously connected, they now show as offline.



EMS Settings

Shared Settings

Hostname	VWSEMSDQA4007
Listen on IP	10.10.10.53 FQDN is required when listening to all IPs.
Use FQDN	☑
FQDN	schoolzones.ca

⚠ Cannot disable "Remote HTTPS access" and "Redirect HTTP request to HTTPS" while ACME certificate auto renew is on

Remote HTTPS access	☑ Only enforced when Windows Firewall is running.
HTTPS port	443
Pre-defined hostname	VWSEMSDQA4007,10.10.10.53
Custom hostname	*
Management IP and Port	Optional : e.g. 443 ⚠ If this EMS server is set up to be accessed through a public proxy, please provide the public proxy's hostname/IP
Redirect HTTP request to HTTPS	☑
SSL certificate	schoolzones.ca 2022-01-20 ⚠ Let's Encrypt Root Certificate update (Sep 2021) Learn More
Use SSL certificate for Endpoint Control	☑

To configure the invalid certificate action as warn:

1. In EMS, go to *Endpoint Profiles > Manage Profiles*.
2. Select a profile.
3. On the *System Settings* tab, configure *Invalid Certificate Action* as *Warn*.
4. Save the profile.
5. After FortiClient receives the configuration change, observe if FortiClient displays a warning about the certificate being invalid. If you do not observe connection issues when *Invalid Certificate Action* is set to *Warn*, you can optionally change the setting to *Deny*.

Change log

Date	Change Description
2021-11-25	Initial release.
2021-12-22	Updated Recommended upgrade path on page 3.