ESET Tech Center

How do I enable SSL protocol checking on client workstations? (5.x)

Ondersteuning | ESET Nederland - 2025-03-07 - Reacties (0) - 5.x

https://support.eset.com/kb3560

Issue

Enable / disable SSL protocol checking
Add an exception to SSL protocol checking
A cloud-based service like Dropbox, Google Apps, Quickbooks online or Skype is blocked by ESET SSL scanning
Wireless devices (printers, scanners, etc.) are blocked by ESET SSL scanning

A new version has been released

Version 6 of ESET Remote Administrator (ERA) and ESET business products were released in North America December 11th, 2014, and globally February 25th, 2015. This article applies to version 5.x and earlier ESET business products. For information about what's new in the latest version and how to upgrade, see the following article:

What's new in ESET version 6 business products?

Details

Solution

If you do not use ESET Remote Administrator to manage your network

Perform these steps on individual client workstations.

I. Enable SSL protocol checking on client workstations from the ESET Remote Administrator Console

1. Open the ESET Remote Administrator Console by clicking **Start → All Programs → ESET → ESET Remote Administrator Console → ESET Remote Administrator Console**.

2. Click **Tools → Policy Manager**.

3. Select the policy you want to edit and click **Edit Policy**.

Figure 1-1

Click the image to view larger in new window

4. Expand **Windows desktop v5 → Personal firewall → Settings → SSL**.

5. Click **SSL protocol checking** and select **Always scan SSL protocol** from the **Value** drop-down menu.

Figure 1-2

Click the image to view larger in new window

6. Click **Console → Yes** to save your changes. Click **OK** to exit Policy Manager. SSL protocol checking will be enabled on client workstations assigned to this policy the next time they check in to ESET Remote Administrator.

II. Exclude certificates from SSL protocol checking on client workstations from the ESET Remote Administrator Console

1. Open the ESET Remote Administrator Console by clicking **Start → All Programs → ESET → ESET Remote Administrator**

Console → ESET Remote Administrator Console.

2. Click **Tools → Policy Manager**.

3. Select the policy you want to edit and click **Edit Policy**.

Figure 2-1

Click the image to view larger in new window

4. Expand **Windows desktop v5 → Personal firewall → Settings → SSL**.

5. Click **SSL protocol checking** and select **Ask about non-visited sites (exclusions can be set)** from the **Value** drop-down menu.

Figure 2-2

Click the image to view larger in new window

6. Click **Certificate list: See dialog → Edit**.

Figure 2-3

Click the image to view larger in new window

7. In the **Certificate list** window, select **Excluded certificates** from the **List type** drop-down menu and then click **Add**.

Figure 2-4

8. Browse to the certificate (.cer) file you want to exclude, select it and then click **Open**.

9. Click **OK** to exit the **Certificate list** window.

10. Click **Console → Yes** to save your changes. Click **OK** to exit Policy Manager. SSL protocol checking will be enabled on client workstations assigned to this policy the next time they check in to the ESET Remote Administrator.

Excluding IP addresses and applications from Protocol filtering

To exclude specific IP addresses and applications, see the following Knowledgebase article:

> How do I block or allow a website on client workstations? (5.x)

I. Enable SSL protocol checking on individual client workstations

1. Open ESET Endpoint Security or ESET Endpoint Antivirus. How do I open my ESET product?
2. Press **F5** to access Advanced setup.
3. Expand **Web and email** → **Protocol filtering** and then click **SSL**.
4. Select **Always scan SSL protocol** and click **OK** to save your changes.

Figure 3-1

Click the image to view larger in new window

II. Add an SSL protocol checking exclusion on individual client workstations

1. Open ESET Endpoint Security or ESET Endpoint Antivirus. How do I open my ESET product?
2. Press **F5** to access Advanced setup.
3. Expand **Web and email** → **Protocol filtering**, click **SSL** and then select **Ask about non-visited sites (exclusions can be set)**. Click **OK**.

Figure 3-2

Click the image to view larger in new window

4. Attempt to access the service or device that is being blocked by ESET (for example, open a web app or attempt to print a file).

5. The **Encrypted SSL communication** dialog will prompt you to select an action to take. Select one of the following to allow the communication (in this example **Yes, always** is selected):

    - **Yes, always (recommended)**: This will allow communication with this service or device at all times, but will still examine the certificate before allowing communications.

    - **Exclude**: This will permanently exclude the certificate from SSL scanning. Communication will always be allowed, but your system may be exposed to threats.

    - **Yes**: This will allow communication with the service or device one time. If you select **Yes**, you will need to repeat this action the next time that you attempt to access this service or device.

7. Click **Yes** if you receive a prompt from Windows.
8. Press **F5** to access Advanced setup.

9. Expand **Web and email → Protocol filtering**, click **SSL** and select **Always scan SSL protocol**. Once you are finished, click **OK** to save your changes.

Excluding IP address / application

To exclude specific IP addresses and applications, see the following Knowledgebase article:

> How do I block or allow a website on client workstations? (5.x)

Tags

Endpoint