ESET Tech Center

Create a new certificate or certification authority in ESET Security Management Center (7.x)

Anish | ESET Nederland - 2018-09-12 - Comments (0) - 7.x

Issue

- Certificates are used to authenticate products distributed under your license and identify computers on your network to help ensure secure communication between your ESMC Server and clients

Solution

ESET Security Management Center (ESMC) 7 User Permissions

This article assumes that your ESMC user has the correct access rights and permissions to perform the tasks below.

If you are still using the default Administrator user, or you are unable to perform the tasks below (the option is grayed out), see the following article to create a second administrator user with all access rights (you only need to do this once):

- Create a second administrator user in ESET Security Management Center 7.x

View permissions needed for least privilege user access

Default certificates

Peer certificates and Certification Authority created during the installation are by default contained in the static group All.

Create a new Peer Certificate in ESMC Web Console

1. Open ESET Security Management Center Web Console (ESMC Web Console) in your web browser and log in.
2. Click **More → Peer Certificates → New → Certificate**.

Figure 1-1
Click the image to view larger in new window

1. The **Basic** section displays the following basic settings for the certificate:

- **Product**: Select the type of certificate you want to create from the drop-down menu.
- **Host**: Leave the default value (an asterisk) in the **Host** field to allow for distribution of this certificate with no association to a specific DNS name or IP address.

- **Passphrase**: We recommend that you leave this field blank, but if desired you can set a passphrase for the certificate that will be required when clients attempt to activate.

Unsupported characters in Agent Certificate

The certificate passphrase must not contain following characters: **"** **** These characters cause critical error during the initialization of the Agent.

- **Attributes**: These fields are not mandatory, but you can use them to include more detailed information about this certificate.

Figure 1-2
Click the image to view larger in new window

1. Click the **Sign** section and click **<Select Certification Authority>**. Select the CA that you want to use and then click **OK**.

   "Failed to create certificate: Creating and signing peer certificate failed. Check input parameters for invalid or reserved characters, check certification authority pfx/pkcs12 signing certificate and corresponding password"

   When you are creating a new certificate in **ESMC Virtual Appliance**, you must type the **Certification Authority Passphrase** in the field. It is the same password you have specified during ESMC VA configuration.

2. Click the **Summary** section to view details about the certificate and then click **Finish** to create a new one. Your new peer certificate will be displayed in the list of peer certificates.

Create a new Certification Authority in ESMC Web Console

1. Click **More → Certificates → Certification Authorities → New**.
2. You can set the following basic settings for the Certification Authority:

- **Description**: Enter description for the Certification Authority.
- **Passphrase & Confirm passphrase**: You can set a passphrase for your CA according to your preference, but it is not required.
- **Attributes**: The **Common name** field is mandatory, and will be used to refer to this CA in the future.
- **CA Validity**: Set the CA validity dates using the **Valid from** and **Valid to** fields.

Figure 2-1
Click the image to view larger in new window

macOS does not support certificates with validity ending after year 2037

Certificates with a **Valid To** date of 2037 or later are not supported. It is not possible to parse a date variable from the Certification Authority on macOS. The Agent cannot connect, because macOS is unable to accept the Certification Authority.

1. Click **Save** to save your new CA. It will be listed in the Certification Authority list under **Admin → Certificates → Certification Authorities**, and will be ready for use.