ESET Tech Center

Create a new certificate or certificate authority in ESET Remote Administrator (6.x)

Ondersteuning | ESET Nederland - 2017-12-04 - Reacties (0) - 6.x

https://support.eset.com/kb3617

Issue

Certificates are used to authenticate products distributed under your license and identify computers on your network. This ensures secure communication between your ERA Server and clients, and helps secure communication with ERA Web Console. Your Certificate Authority (CA) is used to legitimize certificates distributed from your network. In an enterprise setting, a public key can be used to automatically associate client software with the ERA Server during the remote installation of ESET products.

In some cases, you might want to create a new certificate to set specific parameters for a certain group of client computers, for example create a limited-duration certificate for a group of computers that will only be in use for a limited time.

Solution

Permissions changes in ESET Remote

administrator 6.5 and later

Before proceeding, please note important changes to user access rights and permissions in the latest versions of ESET Remote Administrator.

View Permissions Changes

A user must have the following permissions for the group that contains the modified object:

Functionality	*Read*	*Use*	*Write*
Certificates	✓	✓	✓

Once these permissions are in place, follow the steps below.

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 ERA Web Console

1. Open ESET Remote Administrator Web Console (ERA Web Console) in your web browser and log in.
2. Click **Admin** → **Certificates** → **New** → **Certificate**.

Figure 1-1

Click the image to view larger in new window

3. Expand the **Basic** section to display 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.
   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

4. Expand 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 **ERA Virtual Appliance**, you must type the **Certificate Authority Passphrase** in the field. It is the same password you have specified during ERA VA configuration.

5. Expand 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 ERA Web Console

1. Click **Admin** → **Certificates** → **Certification Authorities** → **New**.

2. Expand the **Basic** section to display 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

   > ### Mac OS X 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 Certificate Authority on Mac OS X. The Agent cannot connect, because OS X is unable to accept the Certificate Authority.

3. 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.

Related articles:

Create a new custom certificate or certificate authority for ESET Remote Administrator (6.x)

Export a certificate or public key from ESET Remote Administrator (6.x)

Tags

ERA 6.x