ESET Tech Center

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

Anish | ESET Nederland - 2018-09-14 - Comments (0) - ESET Security Management Center

Issue

- Create custom certificates or Certification Authorities (CAs) for ESET Security Management Center (ESMC).

Solution

Prerequisites

- Verify Java is installed. Keytool, included in Java, allows you to create and store certificates.

Solution

Enter the commands shown below to create a new certificate:

1. Open a Command Prompt as the administrator (or root on Linux systems) and navigate to the folder where `keytool` is located:

   ```
   C:\Program Files (x86)\Java\jre1.8.0_40\bin
   ```

   (The directory depends on the OS and JRE version.)

2. Generate a key pair (a public key and associated private key) which will be used as the Certification Authority (CA):

   Linux

   ```
   keytool -genkeypair -v -alias aliasName -keystore keystore.jks -keyalg RSA -keysize 2048 -ext KeyUsage:critical="keyCertSign" -ext BasicConstraints:critical="ca:true" -validity 3650
   ```

   Windows

   ```
   keytool -genkeypair -v -alias "aliasName" -keystore keystore.jks -keyalg RSA -keysize 2048 -ext KeyUsage:critical="keyCertSign" -ext BasicConstraints:critical="ca:true" -validity 3650
   ```

   "aliasName" represents the name of your key in keystore.jks

   Replace aliasName with your alias. It represents the name of your key in the `keystore.jks`

Setting certificate validity

In the example above, the parameter `-validity` represents the duration for which the certificate is valid in days.

The `-validity` parmeter must be greater then other certificates set during certificate creation in ESMC Web Console. Default validity for the ESET Management Agent certificate is 5 years and default validity for ESMC CA is 10 years. ESMC certificate validity must start at least one day after the beginning of the ESMC CA validity. For example, if your CA is valid since April 4, your ESMC certificate can start on April 5.

3. Export the CA from the keystore:

Linux

```
keytool -exportcert -alias "aliasName" -file aliasName.der -keystore keystore.jks
```

Windows

```
keytool -export -alias "aliasName" -file aliasName.der -keystore keystore.jks
```

4. Generate a key pair for the certificate:

Linux

```
keytool -genkeypair -v -alias "aliasName" -keytore keystore.jks -keyalg RSA -keysize 2048 -storepass "yourPassword" -keypass "yourPassword"
```

Windows

```
keytool -genkeypair -v -alias "aliasName" -keytore keystore.jks -keyalg RSA -keysize 2048 -storepass "yourPassword" -keypass "yourPassword"
```

Common name must contain name of ESMC components

The Common Name must contain one of these strings: "server" or "agent".

Unsupported characters in Agent Certificate

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

5. Create a certificate request (`.csr` file) for the certificate:

Linux

```
keytool -certreq -keystore keystore.jks -storepass "yourPassword" -
```

```
alias "aliasName" -file file.csr
```

Windows

keytool -certreq -keystore keystore.jks -storepass "yourPassword" -alias "aliasName" -file file.csr

1. Create a certificate with the certificate request:

Linux

keytool -gencert -keystore keystore.jks -storepass "yourPassword" -alias "aliasName" -infile file.csr -outfile output.cer

Windows

keytool -gencert -keystore keystore.jks -storepass "yourPassword" -alias "aliasName" -infile file.csr -outfile output.cer

1. Create a `.pfx` file from `keystore.jks`:

   Linux

   ```
   keytool -importkeystore -v -srcalias aliasName -srckeystore keystore.jks -srcstorepass yourPassword -srcstoretype JKS -destkeystore aliasName.pfx -destkeypass yourPassword -deststorepass yourPassword -deststoretype PKCS12 -destalias aliasName
   ```

   Windows

   ```
   keytool -importkeystore -v -srcalias "aliasName" -srckeystore keystore.jks -srcstorepass yourPassword -srcstoretype JKS -destkeystore aliasName.pfx -destkeypass yourPassword -deststorepass yourPassword -deststoretype PKCS12 -destalias "aliasName"
   ```

For more information about keytool, visit the Oracle webpage.

KB Solution ID: KB6804 |Document ID: 25666|Last Revised: August 17, 2018