



From
BT-SC/ESB

Our Reference

Tel

Grasbrunn
21 April 2020
No. 1.3 public

Report

Issue **1.3**
Topic **Certificate distribution in the large system for BVMS recording authenticity feature**

Description

From
BT-SC/ESB

Our Reference

Tel

Report

Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

Index

1	Introduction.....	3
1.1	Purpose of this document.....	3
1.2	BVMS recording authenticity feature.....	3
1.3	Solution concept and system security.....	5
1.4	Required system components	6
1.5	Versions	6
2	Create camera certificates.....	6
2.1	Using CA certificate from Domain Controller in Configuration Manager	7
2.2	Using MicroCA from Configuration Manager.....	9
2.2.1	MicroCA certificate on Windows Certificate Store	10
2.2.2	MicroCA certificate on USB stick	11
2.3	Replacing CA certificates in Configuration Manager	13
2.4	Bulk creation of camera certificates using Configuration Manager.....	14
3	Distribute CA certificates to BVMS Operator Client computers	19
3.1	Create AD computer group for BVMS Operator Client workstations	19
3.2	Configure a domain policy for workstations group.....	24
3.3	Distribute CA certificate	28
4	Restrictions.....	34
5	Glossary	36

From
BT-SC/ESB

Our Reference

Tel

Report

Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

1 Introduction

1.1 Purpose of this document

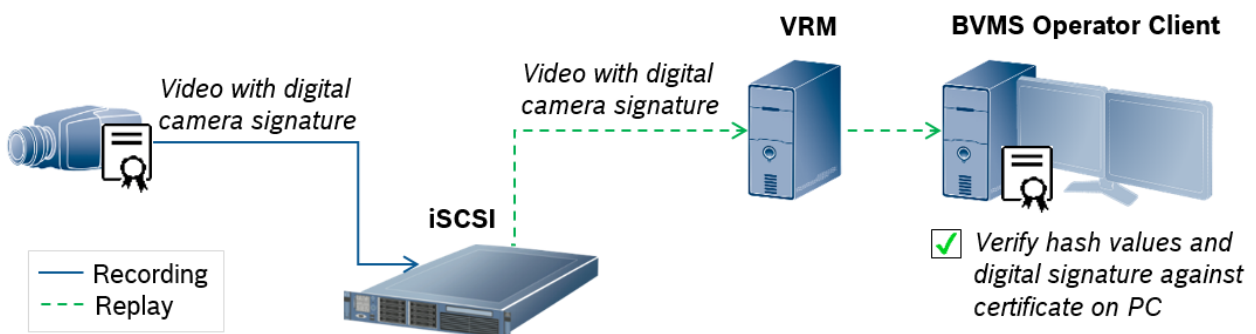
This document provides a step by step description of how to create certificates and configure their distribution in the large systems. For some of the steps a domain controller and optionally a Windows Certification Authority are required. It is assumed that these components already exist in the system as setting up of them is out of this document scope.

The document is written in a way that it makes it easier to troubleshoot the functions, but it does not necessarily mean that it offers the fastest way to set up the system. For faster system configuration some steps may be performed in a different order and workstations may be rebooted once all configuration steps are completed.

1.2 BVMS recording authenticity feature

In case any incident in a public building happens, the security officer needs to export a video clip and provide it to police as an evidence. Therefore the security system is required to provide a possibility to check that the exported video was not altered. As per most of the tenders this has to be achieved by hashing combined with certificates.

The implementation of this requirement in BVMS is following.



The camera is signing the hash values with the private key of its HTTPS certificate and saves the video together with the certificate on the iSCSI. During the video authenticity check BVMS

From
BT-SC/ESB

Our Reference

Tel

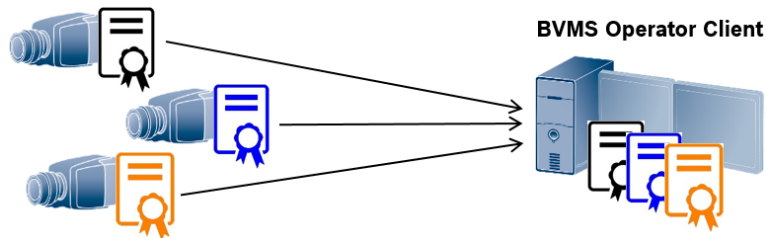
Report

Issue 1.3

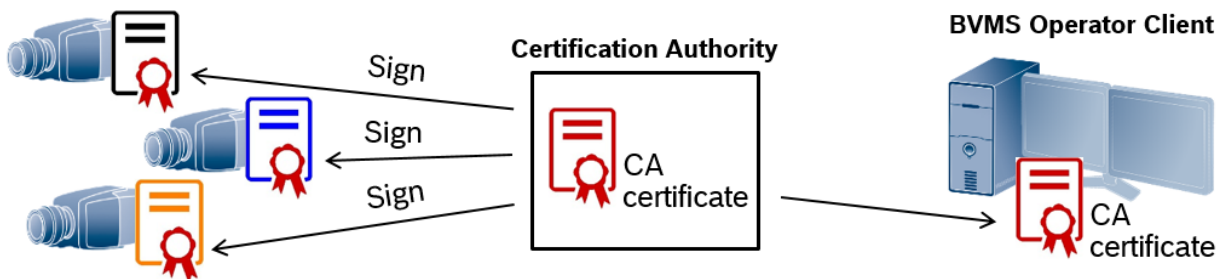
Topic Certificate distribution in the large system for BVMS recording authenticity feature

Operator Client makes a replay and checks the hash values against the received video footage and verifies the digital camera signature against the certificate installed in its Windows Certificate Store. It uses the certificates installed under trusted root certificates path. The system can handle certificates that are self-signed or signed by a Certification Authority (CA).

Self-signed certificates are easier to create, but they are not so secure and that also would mean that each BVMS Operator Client should have each of the self-signed certificate from each camera installed on its Windows Certificate Store. Taking into account that a system can consist of more than 500 cameras and 50 BVMS Operator Clients, the manual setup and maintenance of such a system requires an unacceptable amount of time.



When using a CA signed certificate an effort of creating such a certificate for each camera is higher. This however provides a higher security and only 1 CA certificate has to be distributed on each BVMS Operator Client. Nevertheless executed manually for each single large system component this method also consumes an unacceptable amount of time.



From
BT-SC/ESB

Our Reference

Tel

Grasbrunn
21 April 2020
No. 1.3

Report

Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

1.3 Solution concept and system security

In order to configure authenticity check in BVMS system, each camera has to have a certificate assigned to its HTTPs server. The certificate has to be installed on each BVMS Operator Client that should be able to verify the video.

Out of the box all cameras have a default certificate, however due to a higher security level and a lower efforts of certificate installation on the Operator Client computer a CA signed certificate is more suitable for large systems.

In this solution description camera certificates are created using Configuration Manager (CM). As CA certificate for signing the camera certificates CM can use a certificate from Domain Controller (DC) Windows Certification Authority or create its own MicroCA. Certificates of CM MicroCA can be saved in Certificate Store of the local computer or on a USB stick.

The DC certificate is available in Local Machine Certificate Store. The CM MicroCA certificate can be saved in the Current User Certificate Store. In both cases certificates with their private keys are available directly on the computer and CM has to be installed on the same machine in order to use them. Saving a private key directly on the computer that is constantly online introduces a risk as this key might be extracted by an unauthorized person who manages to access the network. Therefore it is recommended to use the CA certificate from a Windows Certificate Store only if computer can be put offline once the certificate creation is completed. In case it is not possible, please make sure that the network is properly secured.

A higher security level can be reached by saving a CM MicroCA certificate with its private key on the USB stick. The USB stick can be secured with encryption and removed from computer once it is not needed. In this case please consider creating a backup USB stick with the copy of CA certificate in case the original one is damaged.

Once camera certificates are signed and created, the CA certificate has to be distributed to each BVMS Operator Client. In this solution concept it is done using Active Directory (AD). The CA certificate has to be exported by CM and imported to the group policy settings of AD. The exported CA certificate introduces low risk as only a certificate with public key is extracted in this case.

From
BT-SC/ESB

Our Reference

Tel

Grasbrunn
21 April 2020
No. 1.3

Report

Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

1.4 Required system components

In order to configure a bulk certificate creation and distribution, following components have to be available in the system:

- CM version 7.10 or higher – for creating CA signed certificates in the cameras.
- Configured Windows Certification Authority (Optional) – in case the domain certificate should be used for signing camera certificates. Setting up and configuring a Certification Authority is not within the scope of this document.
- Domain Controller with an Active Directory – for distributing the CA certificate to the workstations.

1.5 Versions

This step by step description was created using following system component versions:

- BVMS 10.0.0
- CM 7.10
- Camera firmware: 5.70 to 7.50
- Server OS: Windows Server 2012; Windows Server 2016
- Workstation OS: Windows 10

2 Create camera certificates

In order to create CA signed camera certificates a CA certificate has to be available in CM. In the solution described in this document there are 3 types of CA certificates recommended:

1. CA certificate from DC Certification Authority
2. CM own MicroCA certificate that is saved on the same computer in the Windows Certificate Store
3. CM own MicroCA certificate saved on a USB stick

From
BT-SC/ESB

Our Reference

Tel

Report

Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

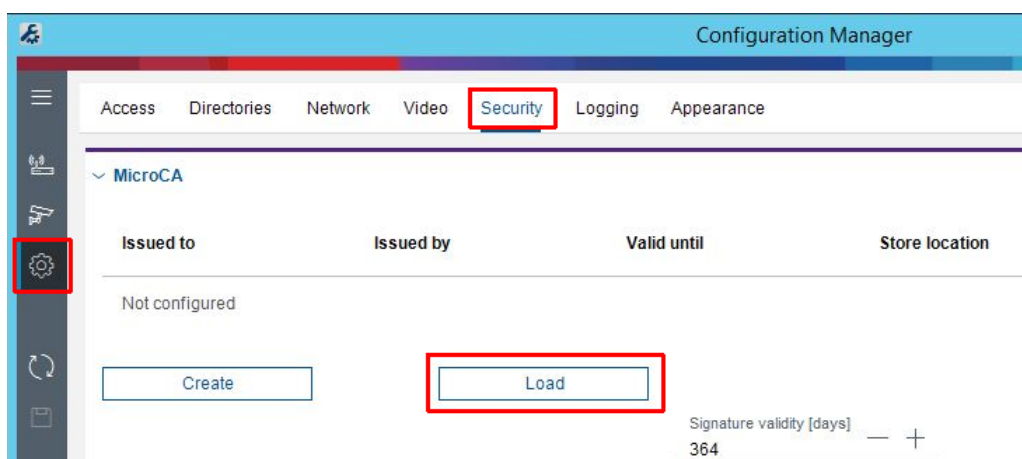
This chapter describes how to load (in case of DC certificate) or create the CA certificates and how to create and sign the camera certificates. Even though CM can handle multiple CA certificates, for a normal operation only one CA certificate can be used.

2.1 Using CA certificate from Domain Controller in Configuration Manager

If a system DC has a Certification Authority with its own CA certificate configured and the network is properly secured, CM can use this certificate for signing the new created camera certificates. Please be aware of the risks described in the chapter 1.3.

DC certificate can be loaded to CM in following way:

1. **Install CM 7.10** or higher on the same computer where the Domain Certification Authority is configured.
2. In CM go to **Preferences / Security** and click on the button **Load**:



From
BT-SC/ESB

Our Reference

Tel

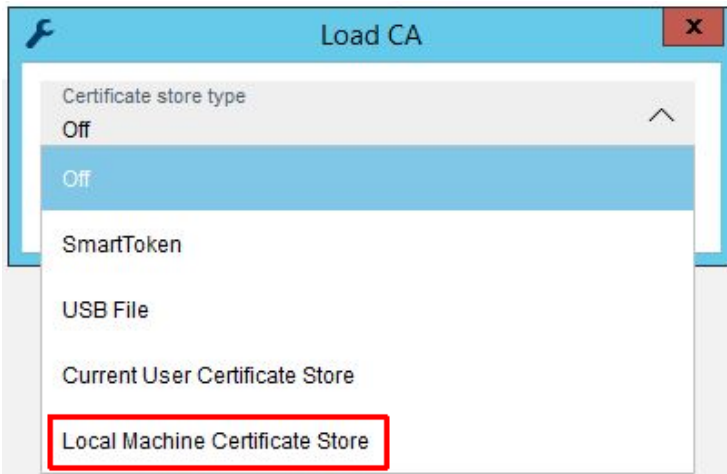
Grasbrunn
21 April 2020
No. 1.3

Report

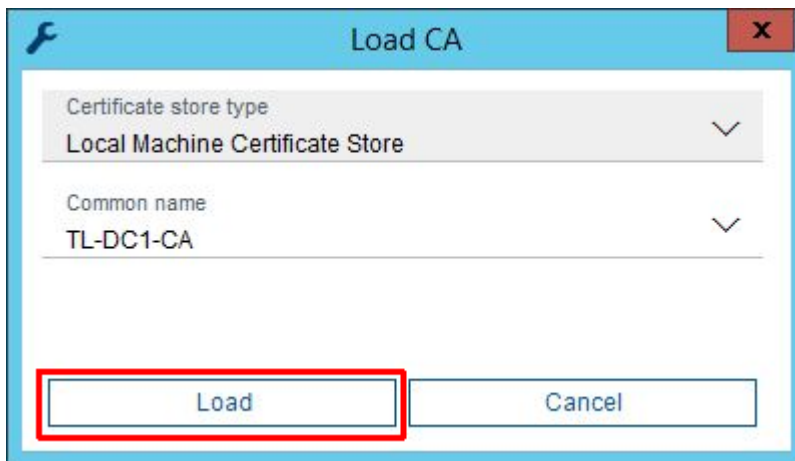
Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

3. In order to use the CA certificate from Domain Certification Authority, choose **Local Machine Certificate Store** in the drop down menu:



Once the right certificate is chosen, press **Load** button.



From
BT-SC/ESB

Our Reference

Tel

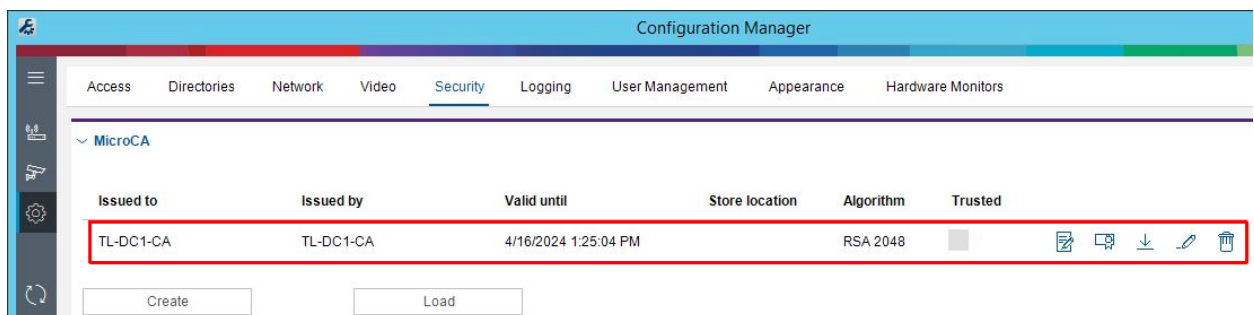
Grasbrunn
21 April 2020
No. 1.3

Report

Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

The loaded certificate is shown under **Preferences / Security**. This certificate will be automatically used for signing the new created camera certificates.



2.2 Using MicroCA from Configuration Manager

CM is capable of creating its own MicroCA and sign camera certificates with it. The MicroCA root certificate can be saved in the local Windows Certificate Store, as a smart token using a smart card or as a file on USB stick. The step by step description in this chapter concentrates on the solution with encrypted USB stick and local Windows Certificate Store.

From
BT-SC/ESB

Our Reference

Tel

Grasbrunn
21 April 2020
No. 1.3

Report

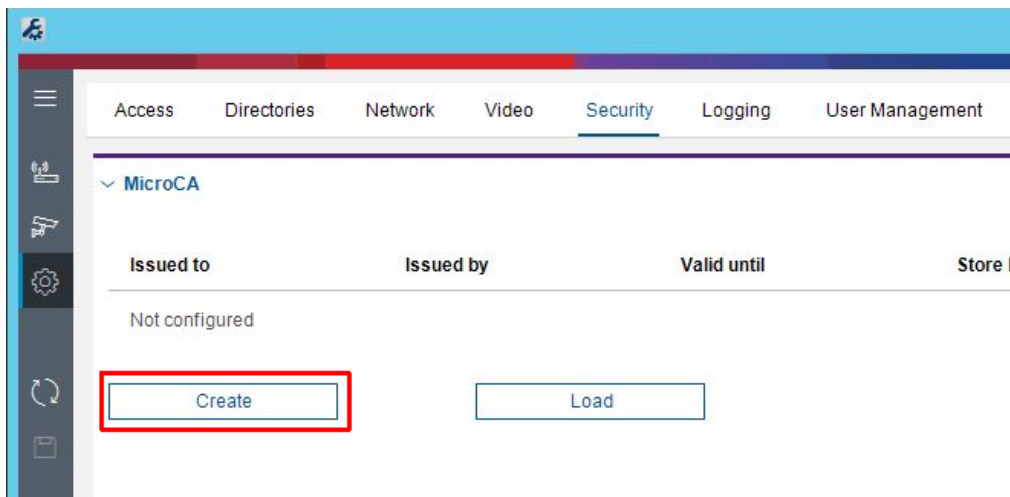
Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

2.2.1 MicroCA certificate on Windows Certificate Store

The CM MicroCA certificate on Windows Certificate Store can be created in the following way. By saving CM certificate on the computer that is meant to be online all the time please be aware of the risks discussed in the chapter 1.3.

1. CM can be installed on any PC that fulfills the requirements from its release letter.
2. In the CM go to **Preferences / Security** and click **Create** button:



From
BT-SC/ESB

Our Reference

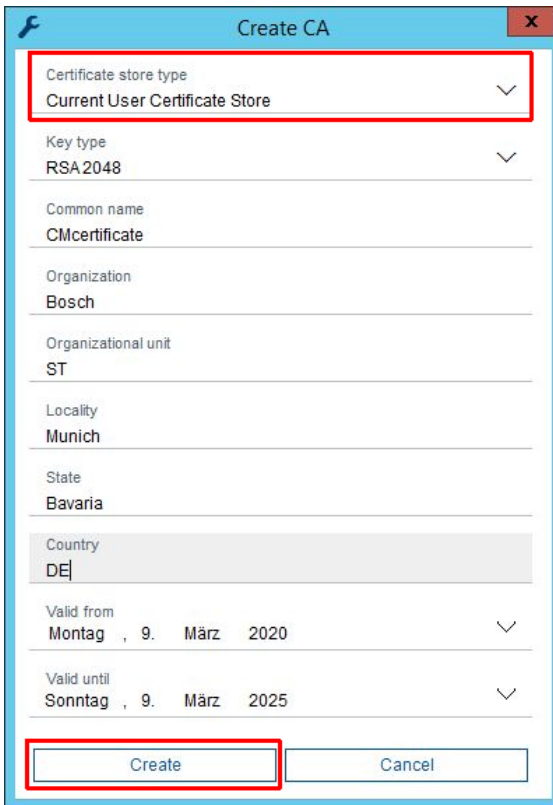
Tel

Report

Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

3. Select **Current User Certificate Store** as **Certificate store type**, enter the rest of the data in the dialog and press **Create** button:



The screenshot shows a 'Create CA' dialog box with the following fields and values:

- Certificate store type: Current User Certificate Store
- Key type: RSA 2048
- Common name: CMcertificate
- Organization: Bosch
- Organizational unit: ST
- Locality: Munich
- State: Bavaria
- Country: DE
- Valid from: Montag, 9. März 2020
- Valid until: Sonntag, 9. März 2025

The 'Create' button at the bottom left is highlighted with a red box.

Once a root certificate was created, it appears in the CM under **Preferences / Security**. The certificate is now available on the computer and it can be loaded from the Current User Certificate Store again in case it was deleted from CM configuration.

2.2.2 MicroCA certificate on USB stick

The CM own MicroCA certificate on the USB stick can be configured in a following way:

1. CM can be installed on any PC that fulfills the requirements from its release letter.
2. Insert and unlock an encrypted USB to the computer where CM is installed.

From
BT-SC/ESB

Our Reference

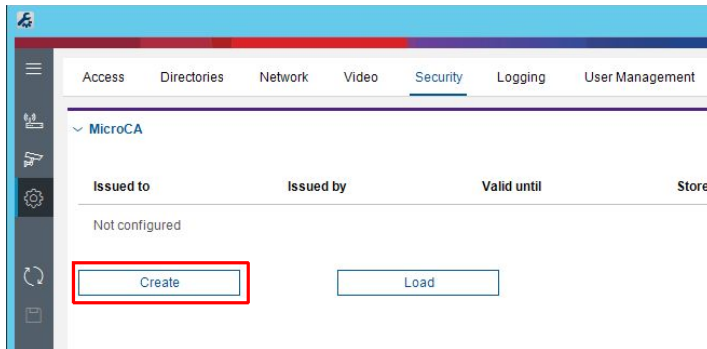
Tel

Report

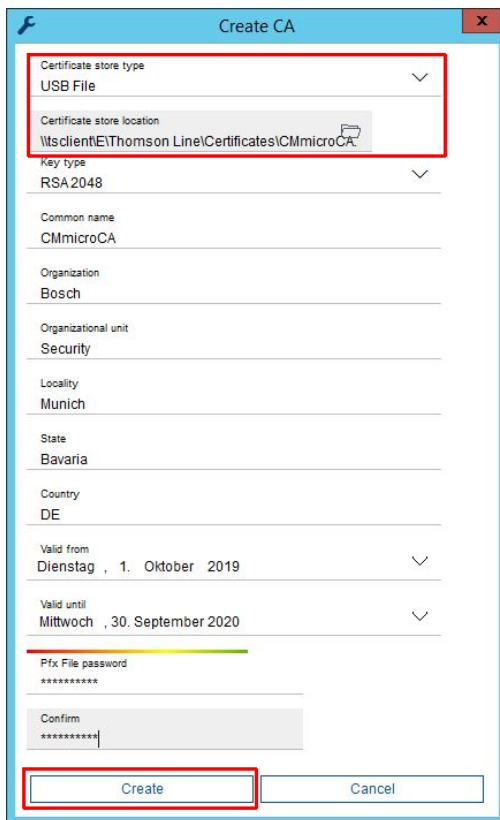
Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

3. In the CM go to **Preferences / Security** and click **Create** button:



4. Select **USB File** as **Certificate store type** and location in the encrypted USB stick as **Certificate store location**, enter the rest of the data in the dialog and press **Create** button:



From
BT-SC/ESB

Our Reference

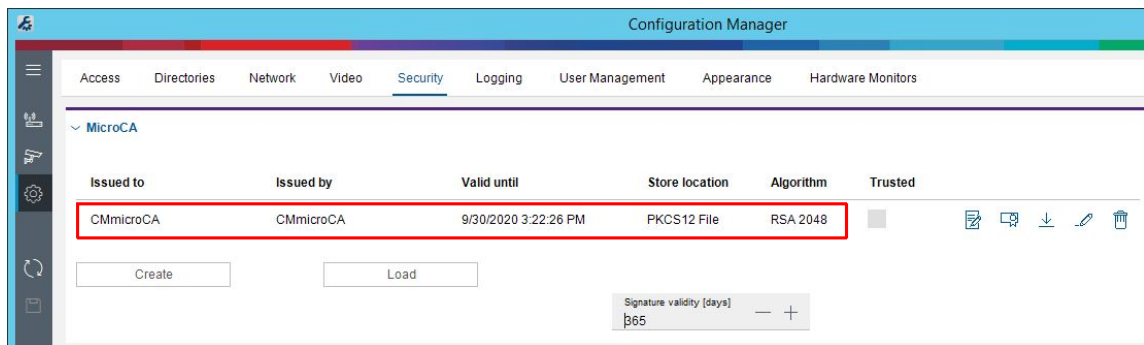
Tel

Report

Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

Once a root certificate was created, it appears in the CM under **Preferences / Security**. CM saves the link to the file with certificate, but not the certificate itself. Once the USB stick is removed no signing with the new created certificate is possible.

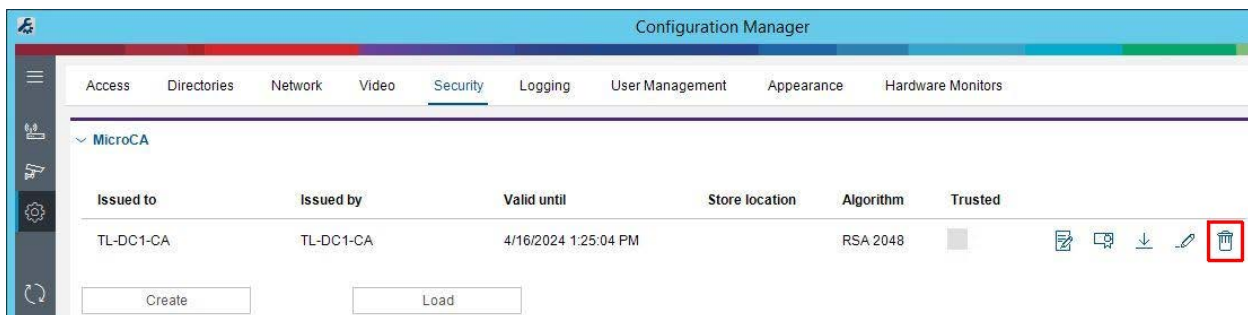


5. Create a security copy of the USB stick in order to avoid losing the CA certificate in case the original USB stick gets damaged. For this action no additional steps in CM are needed. Simply copy the content from one USB stick to the other.

2.3 Replacing CA certificates in Configuration Manager

CM can use multiple CA certificates for signing, however it is possible to use 1 CA certificate at once. Even though only 1 certificate is used, it has to be replaced regularly once its validity period has expired.

In order to exchange a CA certificate the currently used one has to be deleted first. This can be done with **delete** button next to the certificate under **Preferences / Security**:



From
BT-SC/ESB

Our Reference

Tel

Report

Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

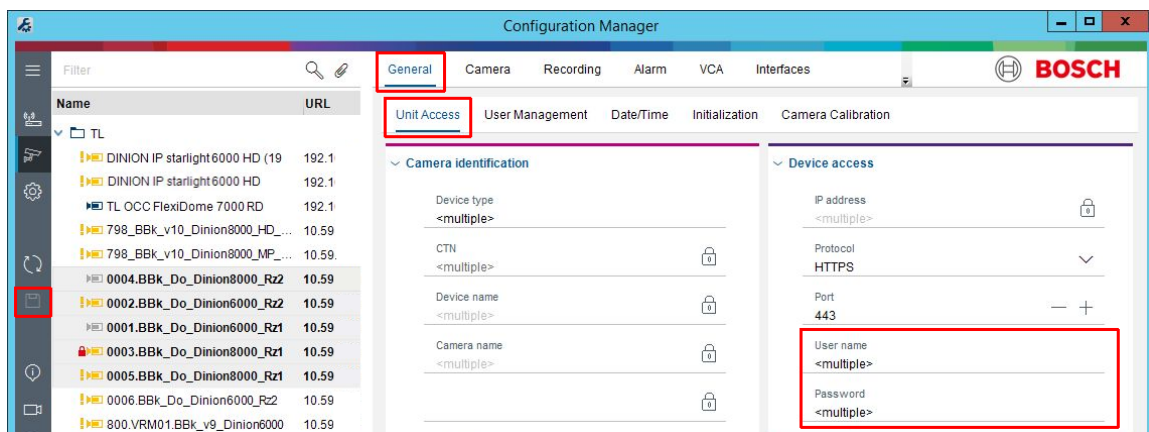
The next certificate can be uploaded or created with load or create buttons like explained in the chapters 2.1 and 2.2.

2.4 Bulk creation of camera certificates using Configuration Manager

Once CA certificate is available in CM configuration, bulk camera certificates can be created in a following way:

1. In case cameras are protected with passwords, it makes sense to save their passwords in CM configuration. For that reason cameras first should be added to CM My Devices tab by right clicking them and choosing **Add to System**. If multiple cameras have the same password, choose multiple cameras in My Devices tab and enter the service password on the right side under **General / Unit Access**. Press **save** button.

Note: If entire VRM is added to the CM My Devices tab, all the cameras in its configuration and their passwords are automatically included to CM. VRM can be added and authenticated in the same way like it is described for the cameras above.



From
BT-SC/ESB

Our Reference

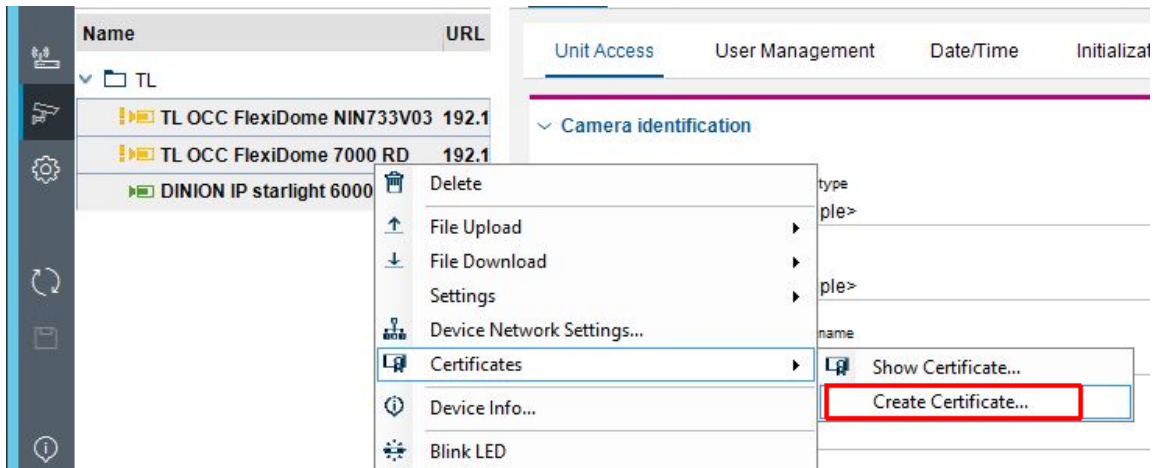
Tel

Report

Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

2. Select multiple cameras, right click on them and choose **Certificates / Create Certificate**:



3. Click on **New**:



From
BT-SC/ESB

Our Reference

Tel

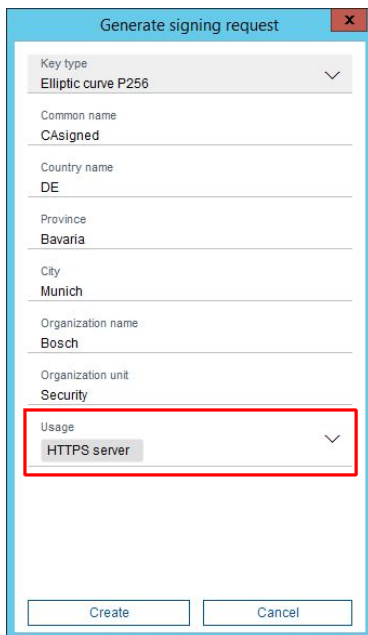
Grasbrunn
21 April 2020
No. 1.3

Report

Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

- In the signing request generation mask enter the **credentials**, choose **HTTPS server** as usage and press **Create** button. If nothing is entered as a *Common name*, the certificate's name will be its camera's IP address. Please be also aware of restrictions described in the chapter 4.

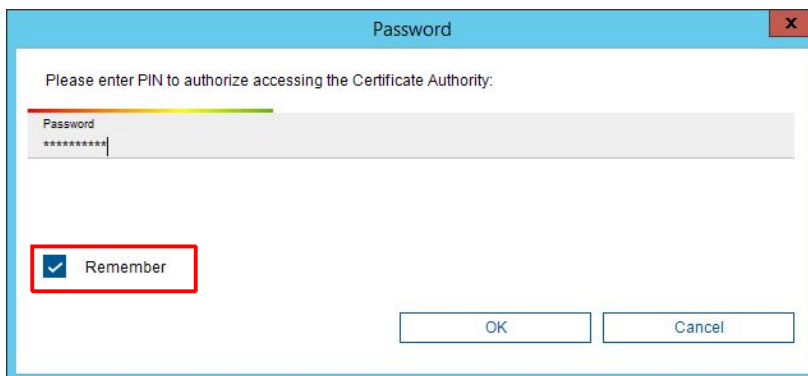


The screenshot shows a dialog box titled "Generate signing request" with a close button (X) in the top right corner. The dialog contains several input fields and a dropdown menu:

- Key type:** Elliptic curve P256 (dropdown)
- Common name:** CAssigned
- Country name:** DE
- Province:** Bavaria
- City:** Munich
- Organization name:** Bosch
- Organization unit:** Security
- Usage:** HTTPS server (dropdown, highlighted with a red box)

At the bottom of the dialog are two buttons: "Create" and "Cancel".

- In case a **CA certificate from USB stick** is used, CM will prompt to **enter the password** of the certificate file that was configured in the chapter 2.2.2 step 4. Select the check box **Remember** so that CM can use the password for signing the certificates of all the selected cameras. Otherwise CM will ask for a password for every camera separately. Press **OK** button to continue.



The screenshot shows a dialog box titled "Password" with a close button (X) in the top right corner. The dialog contains the following elements:

- Text: "Please enter PIN to authorize accessing the Certificate Authority:"
- Password:** A text input field containing "*****" (highlighted with a red box)
- Remember:** A checked checkbox (highlighted with a red box)

At the bottom of the dialog are two buttons: "OK" and "Cancel".

Grasbrunn
21 April 2020
No. 1.3

From
BT-SC/ESB

Our Reference

Tel

Report

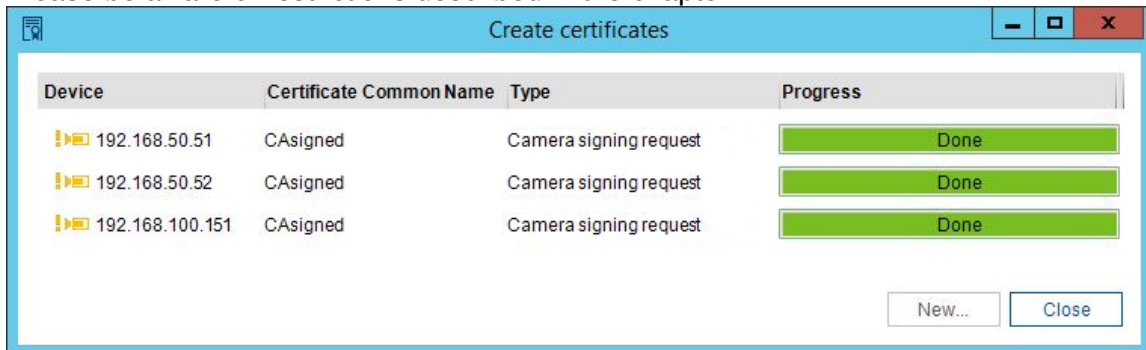
Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

- CM requests certificate signing requests from the cameras, signs them with CA certificate from its configuration and uploads the signed certificates back to the cameras. Operation status is shown in the progress bar for every camera separately. Please be aware that older cameras may take some minutes in order to generate a signing request.



Once the certification is done, the dialog window can be closed with the **close** button. Please be aware of restrictions described in the chapter 4.



From
BT-SC/ESB

Our Reference

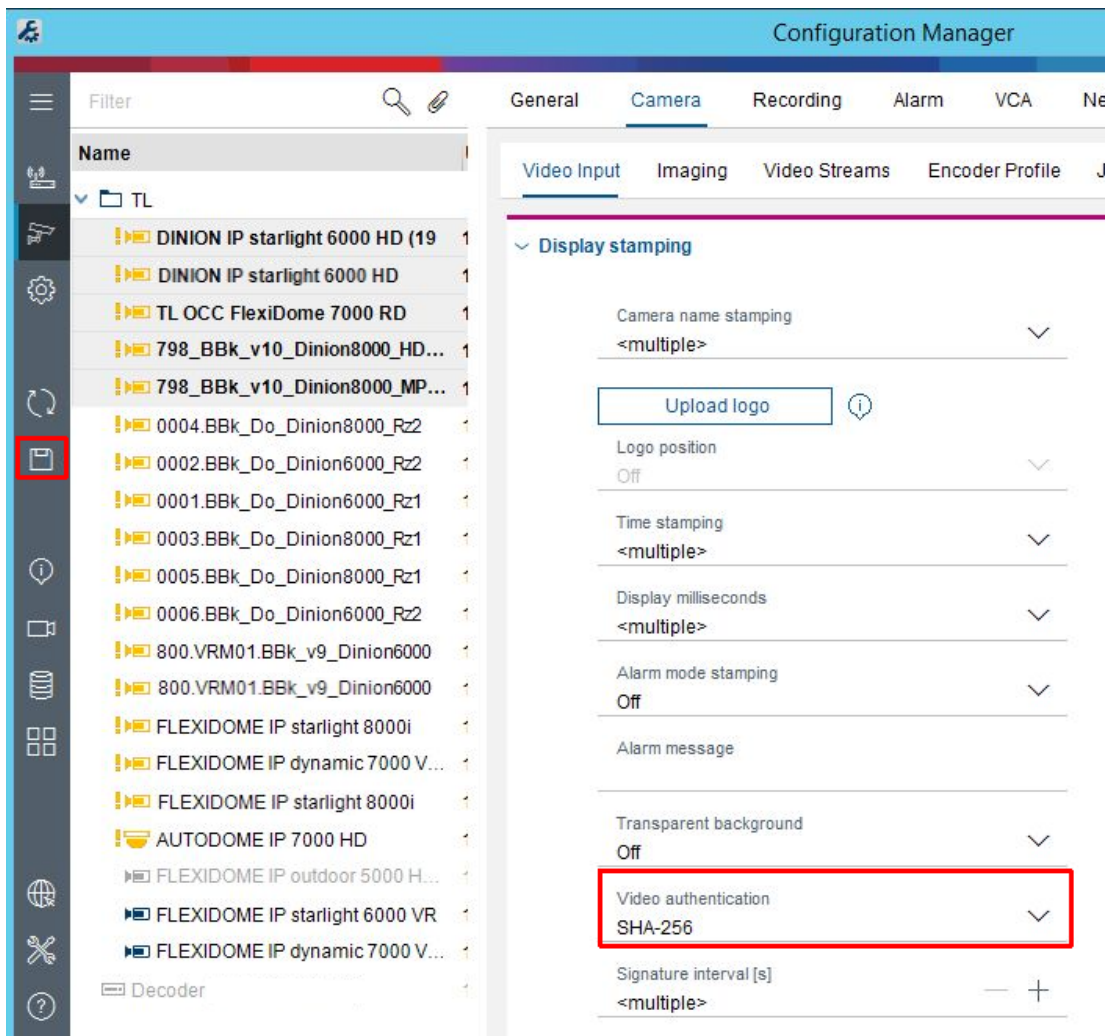
Tel

Report

Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

- 7. For video authentication feature in BVMS an authentication method has to be configured in the camera. The setting can be changed in CM under **Camera/Video Input** while multiple cameras are selected. **SHA-256** method is recommended. Once configured press **save** button.



From
BT-SC/ESB

Our Reference

Tel

Grasbrunn
21 April 2020
No. 1.3

Report

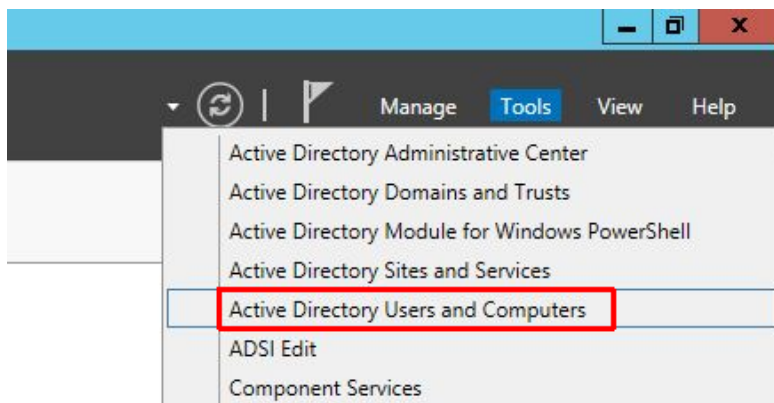
Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

3 Distribute CA certificates to BVMS Operator Client computers

3.1 Create AD computer group for BVMS Operator Client workstations

1. In the AD computer open the **Server Manager** and go to **Tools / Active Directory Users and Computers**:



From
BT-SC/ESB

Our Reference

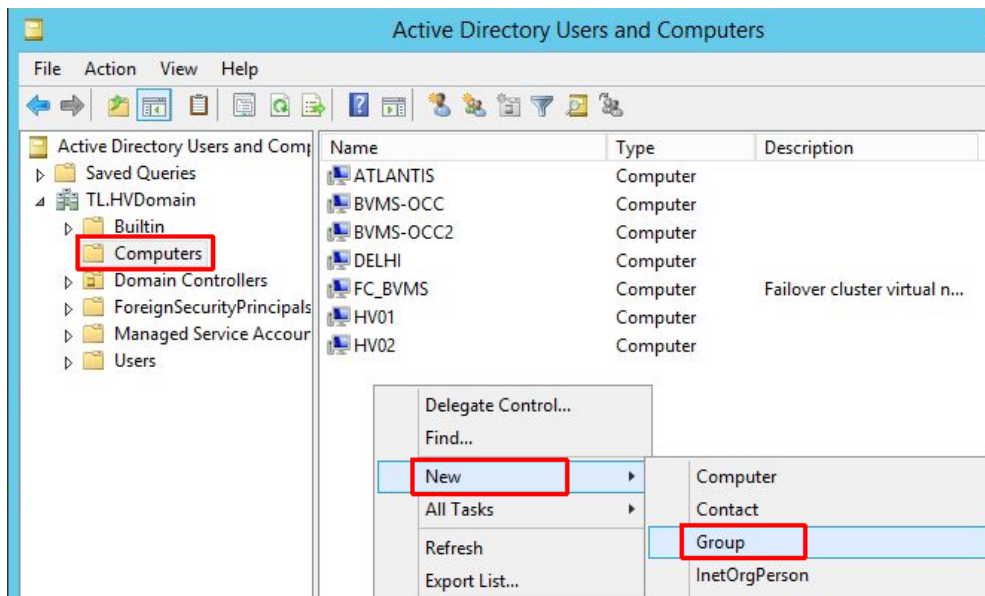
Tel

Report

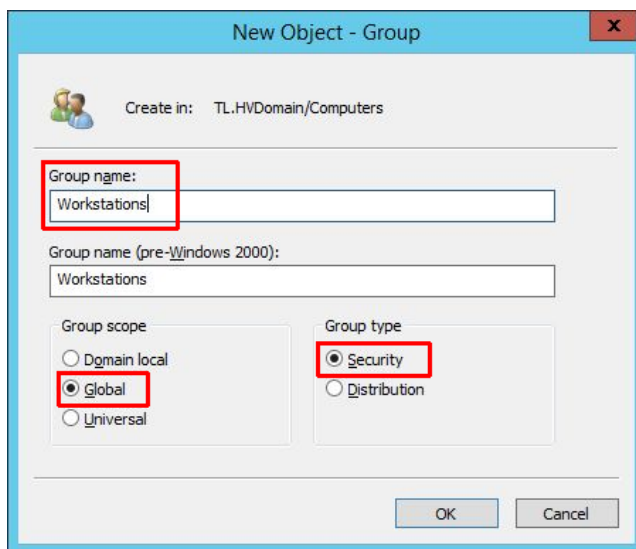
Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

- In the Active Directory Users and Computers navigate to **Computers** on the left side. On the right side **right click** and select **New / Group**:



- Enter the **group name** and select group scope **Global** and group type **Security**. Click **OK**.



From
BT-SC/ESB

Our Reference

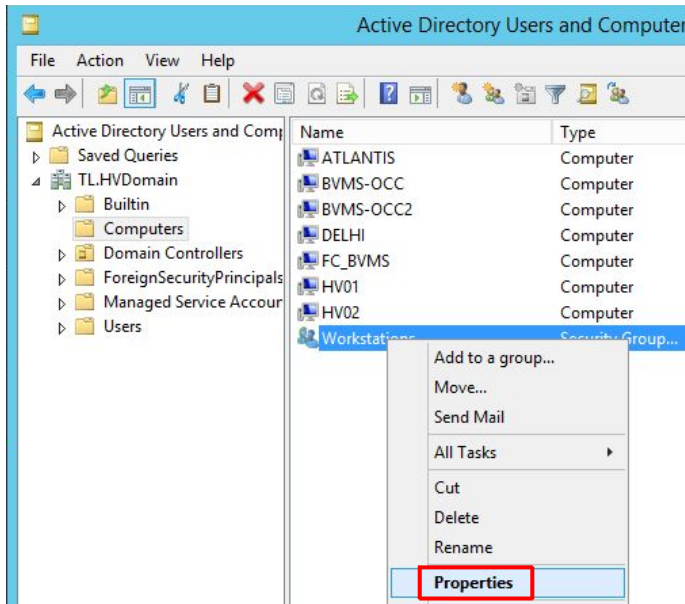
Tel

Report

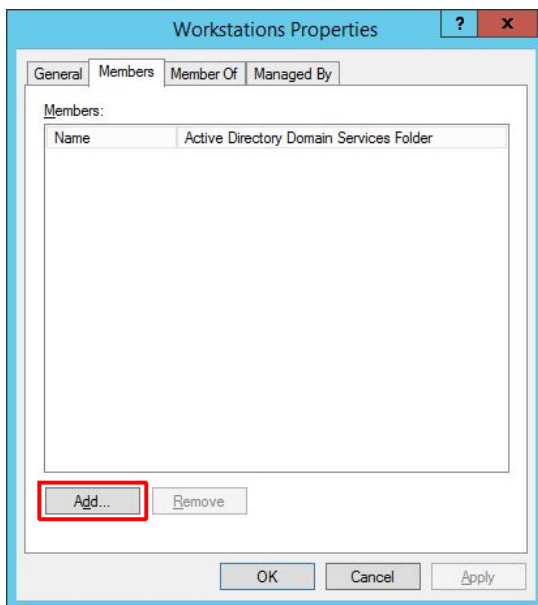
Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

4. **Right click** the new created computer group and select **Properties**:



5. Press **Add** button in order to add the BVMS Operator Client workstations to the group:



From
BT-SC/ESB

Our Reference

Tel

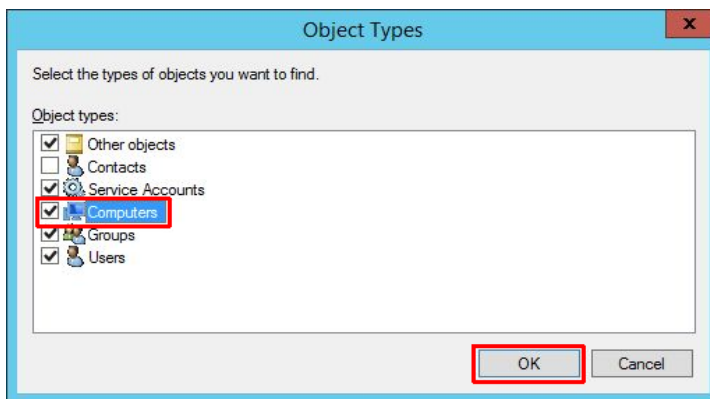
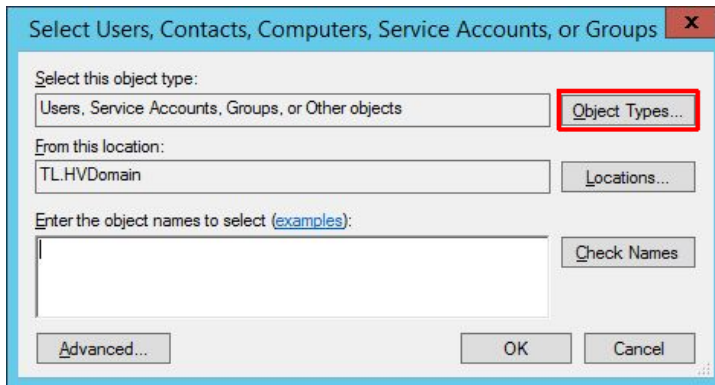
Grasbrunn
21 April 2020
No. 1.3

Report

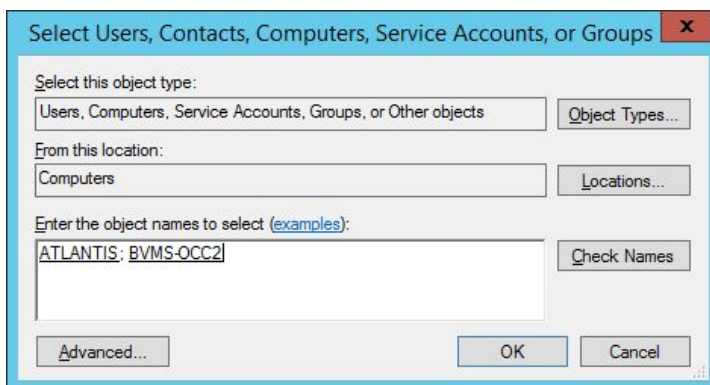
Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

- In the next dialog click on the **Object Types** and check **Computers** and press **OK** in order to be able to enter the workstations' host names.



- Enter **workstations' host names** and press **OK**:



From
BT-SC/ESB

Our Reference

Tel

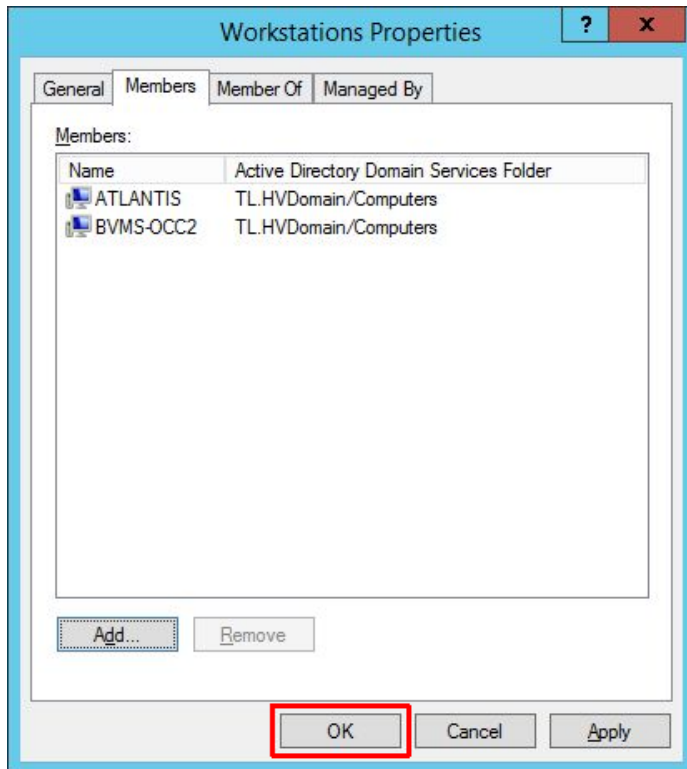
Grasbrunn
21 April 2020
No. 1.3

Report

Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

The workstations are now added as member computers to the group. Press **OK**:



8. **Reboot the added workstations** so that the AD changes take effect immediately.

From
BT-SC/ESB

Our Reference

Tel

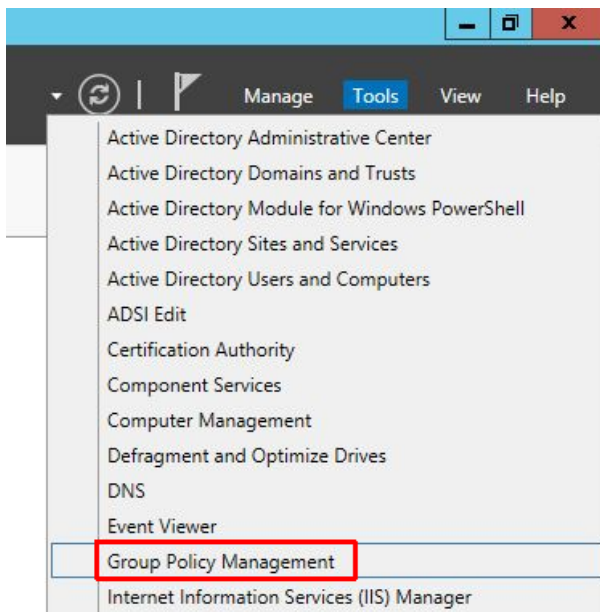
Report

Issue 1.3

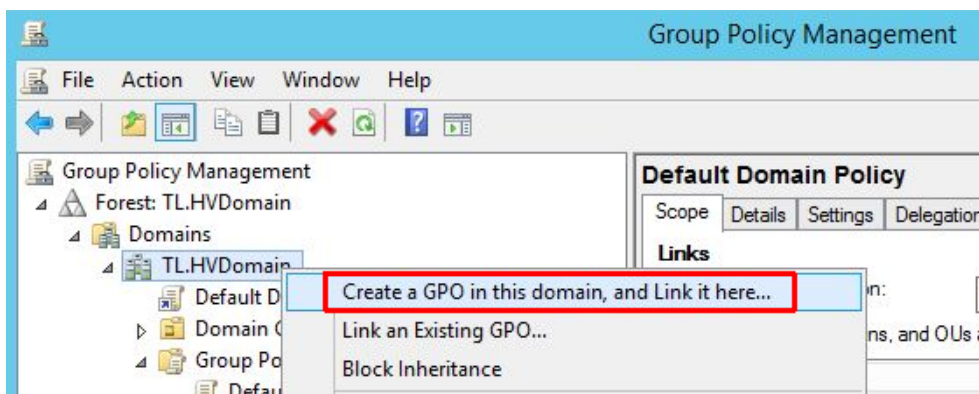
Topic Certificate distribution in the large system for BVMS recording authenticity feature

3.2 Configure a domain policy for workstations group

1. In the DC computer open the **Server Manager** and go to **Tools / Group Policy Management**:



2. **Right click** the **domain** and select **Create a GPO in this domain, and Link it here**:



From
BT-SC/ESB

Our Reference

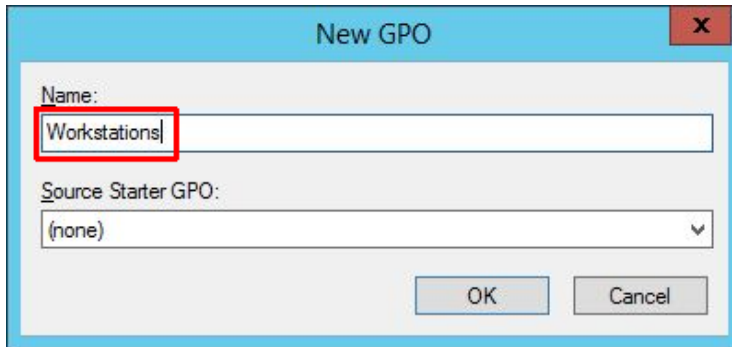
Tel

Report

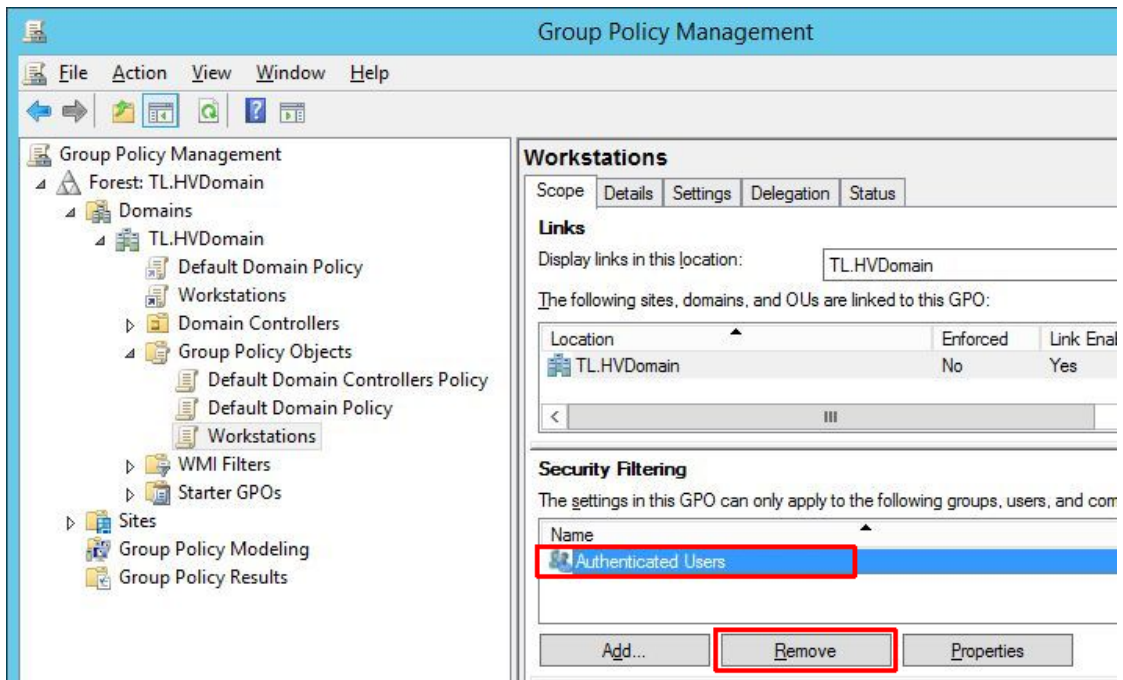
Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

3. Enter the group policie’s **name** and click **OK**:



4. Click on the new created group policy, select **Authenticated Users** on the right side and press **Remove** button. This is because certificates should be applied only on the workstations and not on all the members of domain.



From
BT-SC/ESB

Our Reference

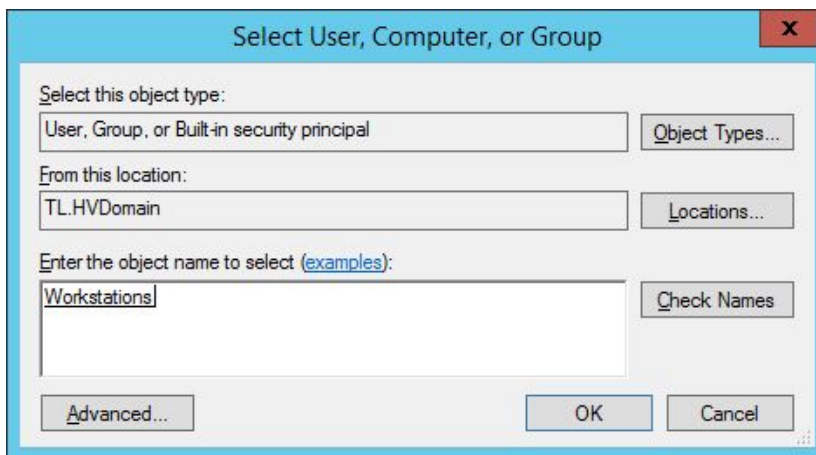
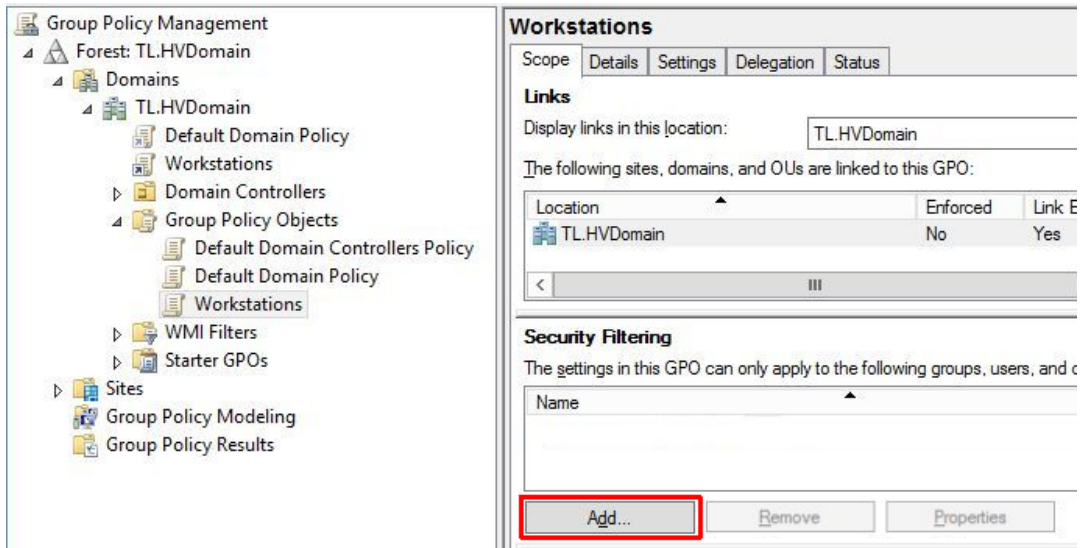
Tel

Report

Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

5. Click **Add** button and select the workstation computer group created in the chapter 3.1:



From
BT-SC/ESB

Our Reference

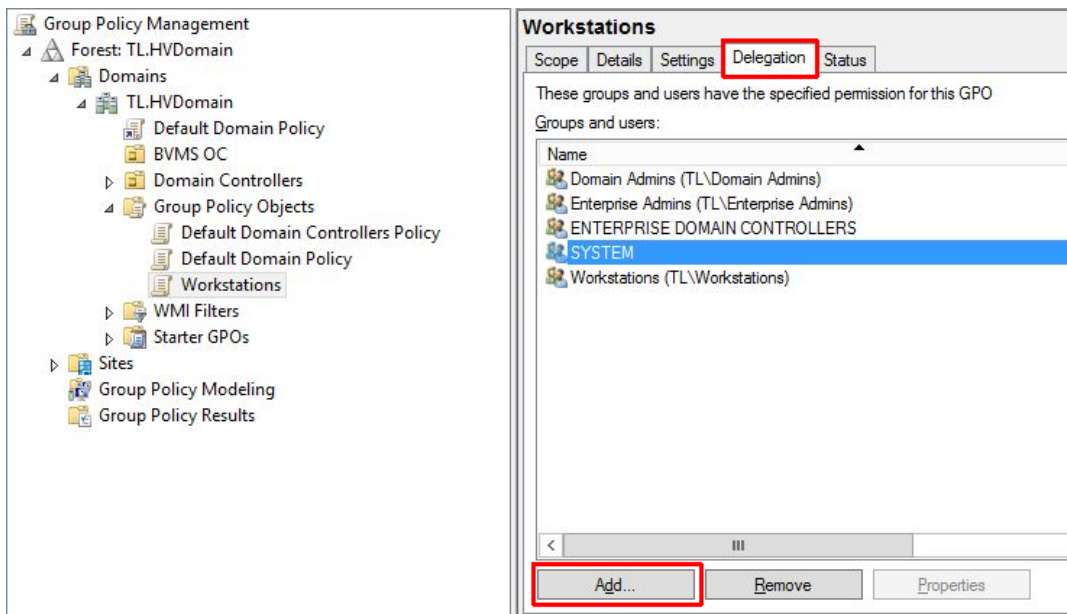
Tel

Report

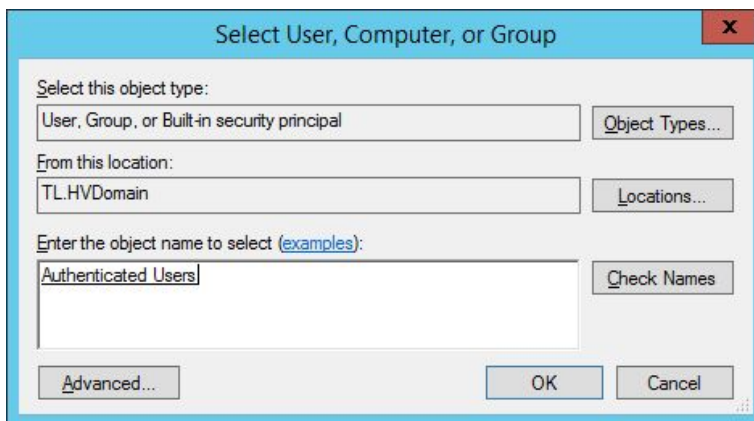
Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

6. Go to the **Delegation** tab, press **Add** button:



7. Enter the **Authenticated Users** and press **OK**. In the next dialog the permissions should be **Read**. Press **OK**.



From
BT-SC/ESB

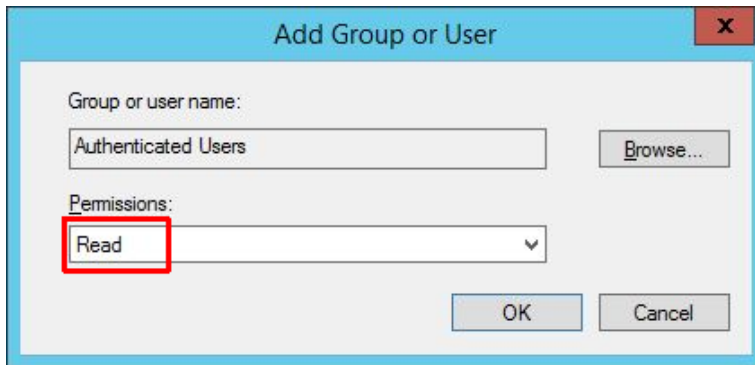
Our Reference

Tel

Report

Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

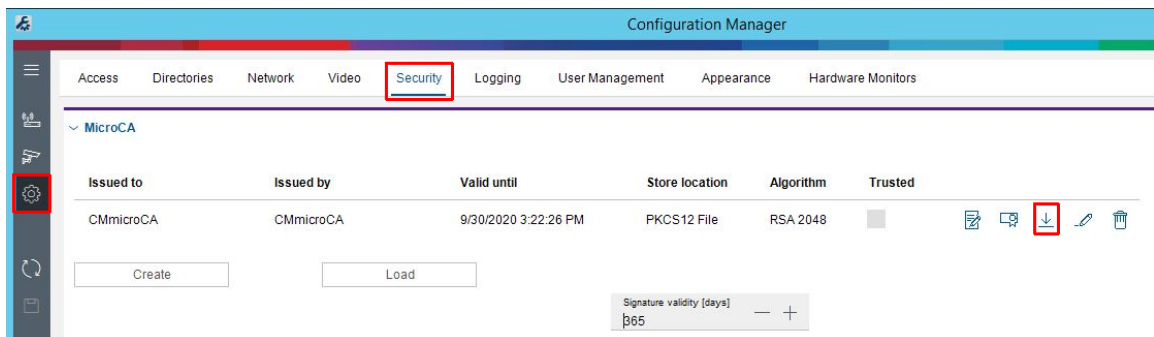


- It takes some minutes till group policies are applied to all computers by domain. In case an immediate effect is required force group policies manually by running the following command line on every workstation: `gpupdate /force`

```
C:\Users\Administrator.TL>gpupdate /force
```

3.3 Distribute CA certificate

- CA certificate with its public key can be exported using CM. Under **Preferences / Security** click on the **export** button:



From
BT-SC/ESB

Our Reference

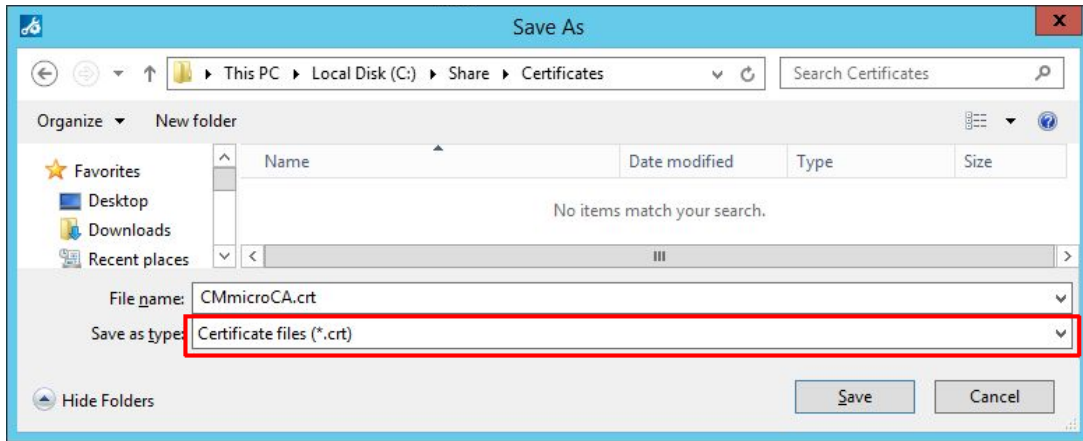
Tel

Report

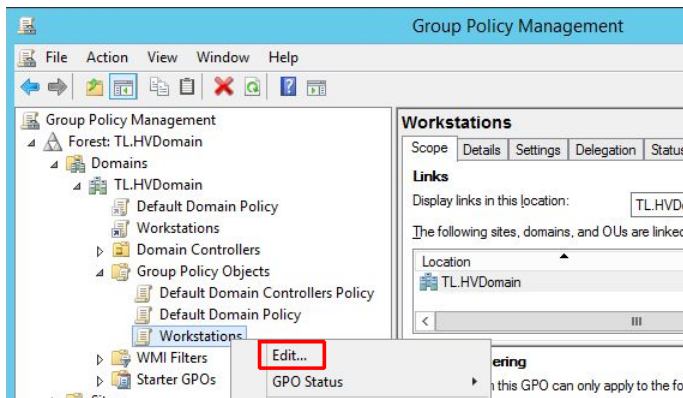
Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

2. Export certificate as .crt file:



3. Go to **Group Policy Management** like described in the chapter 3.2, **right click** the **Workstations Group Policy Object** created in the chapter 3.1 and select **Edit**:



From
BT-SC/ESB

Our Reference

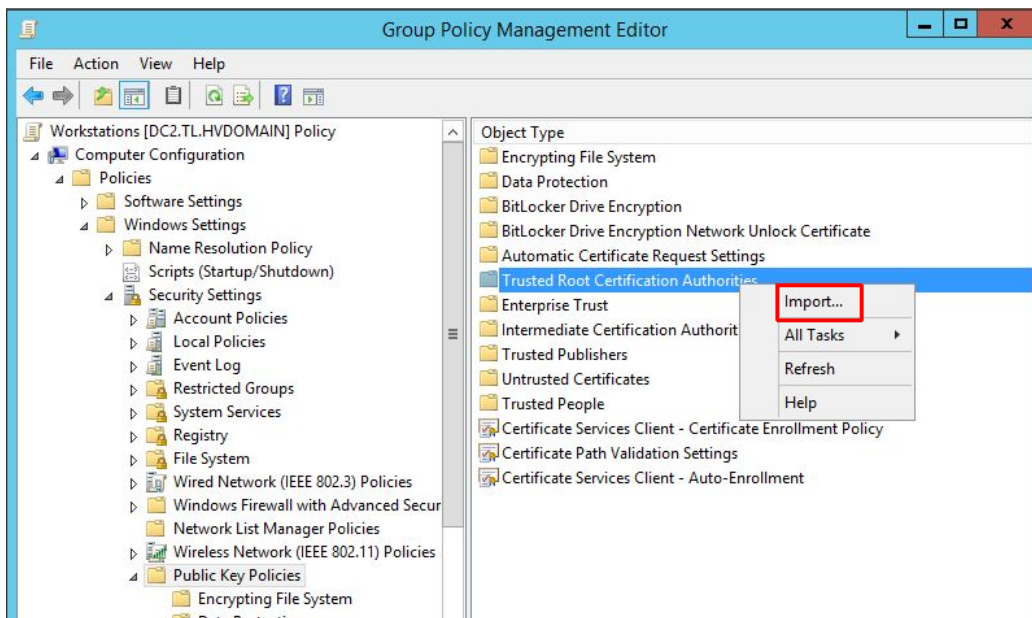
Tel

Report

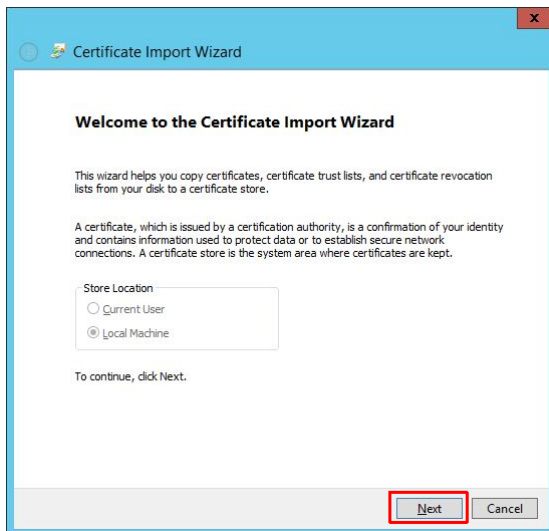
Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

- 4. In the newly opened window on the left side navigate to **Policies / Windows Settings / Security Settings / Public Key Policies**, right click on the **Trusted Root Certification Authorities** on the right side and select **Import**:



- 5. In the Certificate Import Wizard leave the default settings and click **Next**:



From
BT-SC/ESB

Our Reference

Tel

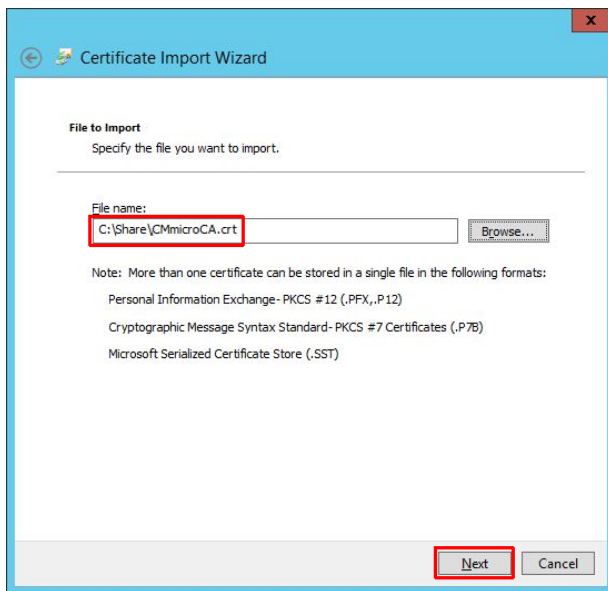
Grasbrunn
21 April 2020
No. 1.3

Report

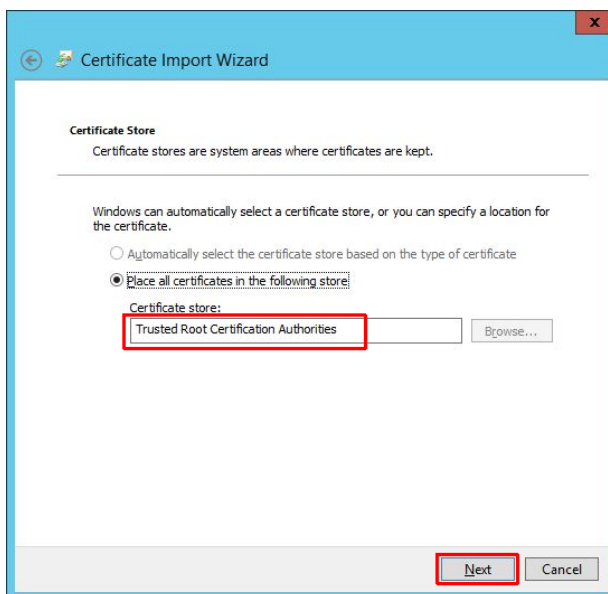
Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

6. Select the certificate exported in the step 2 and click Next:



7. Leave the default store to import the certificate – **Trusted Root Certification Authorities** – and click **Next**:



From
BT-SC/ESB

Our Reference

Tel

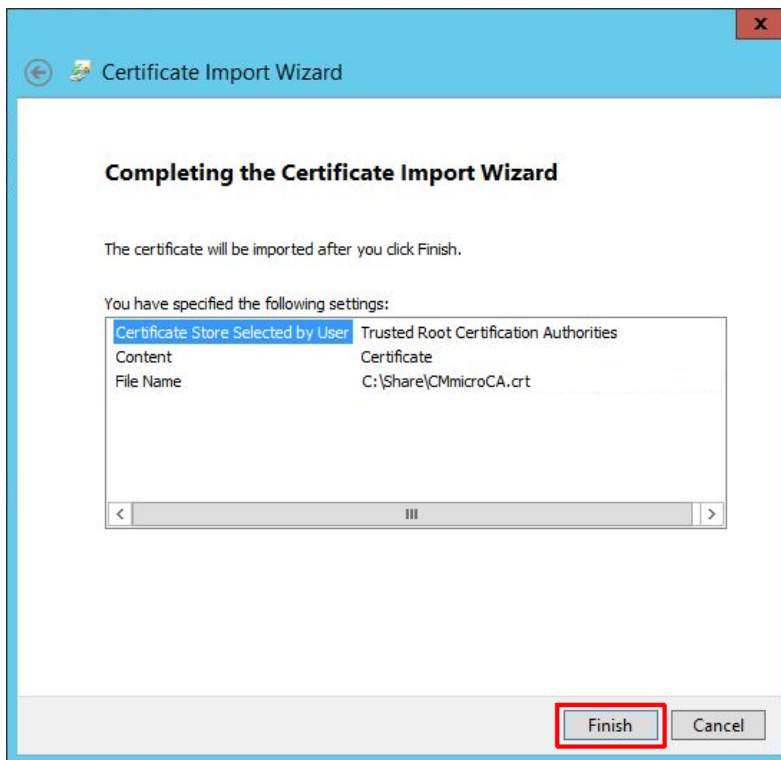
Grasbrunn
21 April 2020
No. 1.3

Report

Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

8. Review the selected options and click on Finish:



9. Once certificate was successfully imported it appears in the Group Policy Management Editor under **Policies / Windows Settings / Security Settings / Public Key Policies / Trusted Root Certification Authorities**:

Grasbrunn
21 April 2020
No. 1.3

From
BT-SC/ESB

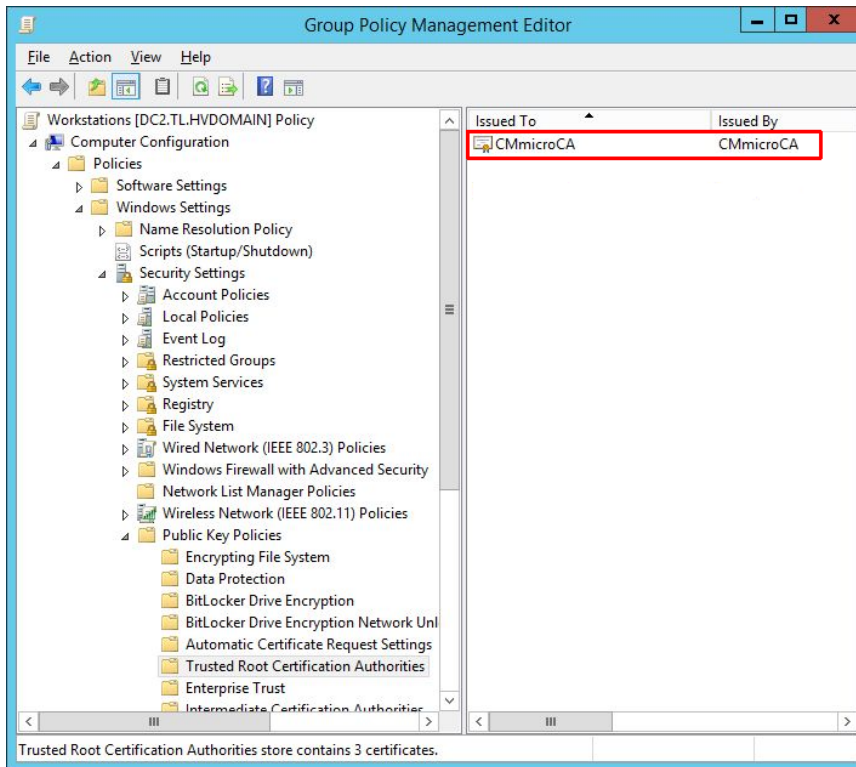
Our Reference

Tel

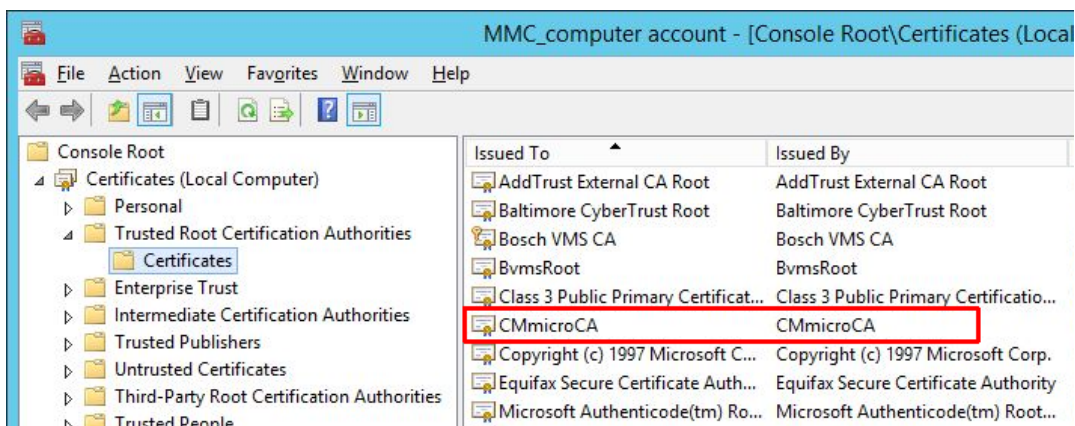
Report

Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature



It takes some minutes till group policies are applied to all computers by domain. The distributed certificates can be found on every computer that belongs to the group Workstations in MMC console under Certificates / Trusted Root Certification Authorities / Certificates:



From
BT-SC/ESB

Our Reference

Tel

Grasbrunn
21 April 2020
No. 1.3

Report

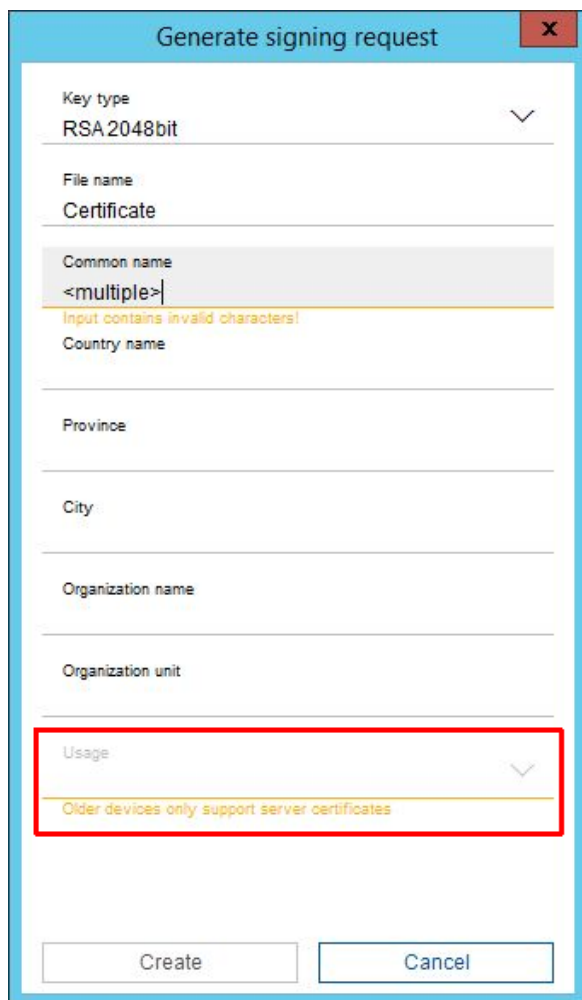
Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

4 Restrictions

CM was tested with camera firmware 5.70 and newer. Older firmware is not supported.

Older cameras like platform CPP3 do not provide a possibility to assign certificates to HTTPs server in the signing request dialog as these devices do not support different server types yet.



The screenshot shows a 'Generate signing request' dialog box with the following fields and values:

- Key type: RSA2048bit
- File name: Certificate
- Common name: <multiple> (highlighted in red with error message: 'Input contains invalid characters!')
- Country name: (empty)
- Province: (empty)
- City: (empty)
- Organization name: (empty)
- Organization unit: (empty)
- Usage: (empty, highlighted in red with error message: 'Older devices only support server certificates')

Buttons: Create, Cancel

From
BT-SC/ESB

Our Reference

Tel

Report

Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

In case multiple HTTPS server capable and 1 incapable device are selected, the usage selection is disabled for all of them. Therefore it is recommended to create certificates separately for these 2 groups in order to avoid additional steps. Nevertheless, older device certificates created without usage are utilized for HTTPS connections and video authentication by the camera.

By default certificate private key is created within a camera and CM is only downloading a signing request from the camera in order to create a CA signed certificate. Cameras with firmware version older than 6.50 handle certificates in a different way. In this case certificates with their private keys are created directly on the CM computer and uploaded to the camera over secured connection. Since handling of private keys on the local computer is considered to be not the safest way, the certificate type is indicated as “Locally created certificate” and the progress bar is colored yellow instead of green. A tool tip, when hovering with a mouse over the progress bar, advices to upgrade the firmware for more safety.



From
BT-SC/ESB

Our Reference

Tel

Grasbrunn
21 April 2020
No. 1.3

Report

Issue 1.3

Topic Certificate distribution in the large system for BVMS recording authenticity feature

5 Glossary

AD	Active Directory
BVMS	Bosch Video Recording System
CA	Certification Authority
CM	Configuration Client
CSR	Certificate Signing Request
DC	Domain Controller