Certificate Store Manager
Application Guide

These instructions do not purport to cover all details or variations in equipment, nor to provide for every possible contingency to be met during installation, operation, and maintenance. The information is supplied for informational purposes only, and GE makes no warranty as to the accuracy of the information included herein. Changes, modifications, and/or improvements to equipment and specifications are made periodically and these changes may or may not be reflected herein. It is understood that GE may make changes, modifications, or improvements to the equipment referenced herein or to the document itself at any time. This document is intended for trained personnel familiar with the GE products referenced herein.

Public Information *– This document contains non-sensitive information approved for public disclosure.*

GE may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not provide any license whatsoever to any of these patents.

GE provides the following document and the information included therein as is and without warranty of any kind, expressed or implied, including but not limited to any implied statutory warranty of merchantability or fitness for particular purpose.

For further assistance or technical information, contact the nearest GE Sales or Service Office, or an authorized GE Sales Representative.

Issued: Sept 2015

We would appreciate your feedback about our documentation.
Please send comments or suggestions to controls.doc@ge.com

Contents

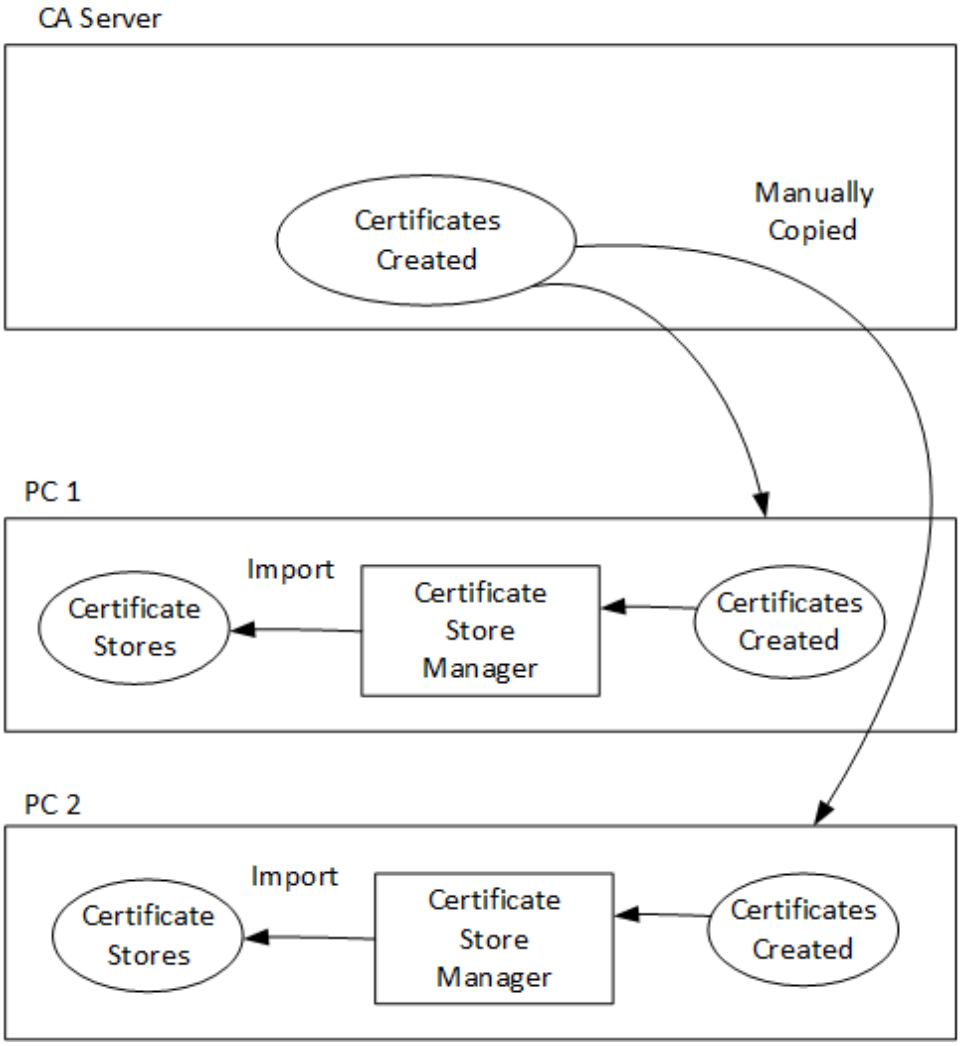
1 Overview

The ControlST* Software Suite V06.00 includes the Certificate Store Manager application, which provides the user the ability to manage X509 certificates for use in the ToolboxST* application when configuring a secure system. The user can view all of their certificate stores, and import and delete certificates in specific stores.

Note For advanced operations, use the *mmc.exe* tool (execute from the command line) or the MMC *snapin CertMgr.msc* for the current user.

2 Data Flow

The following diagram illustrates the overall process of certificate creation and installation to the local computer's stores.



Data Flow Diagram

3 Guidelines

The guidelines for using the Certificate Store Manager in a security system include:

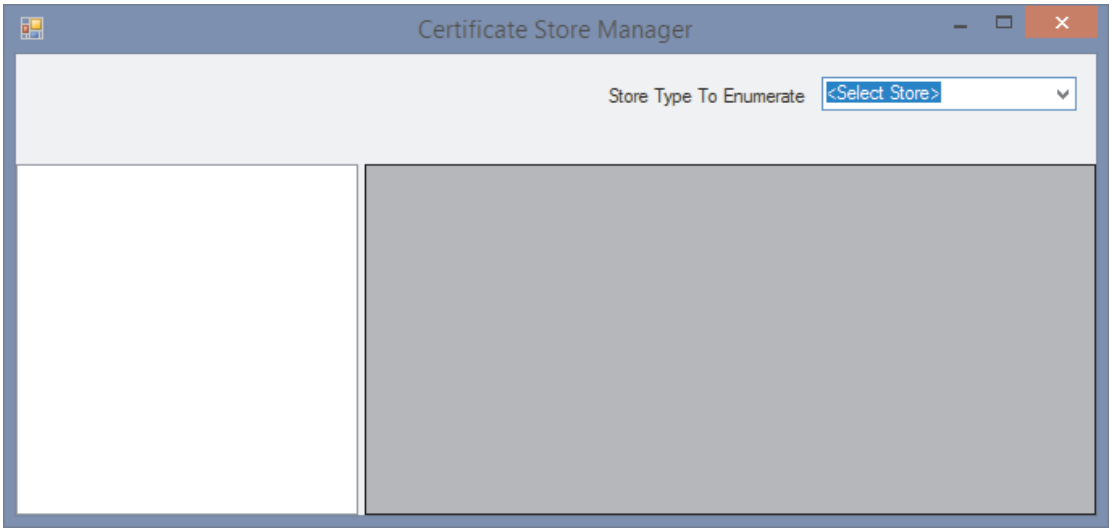
- Certificates to be imported must be created, copied to each computer, then imported using the Certificate Store Manager application.
- The user launching the Certificate Store Manager must be an Administrator, must be using Windows 7 or later, and the Certificate Store Manager application must be started using the Windows Explorer File menu, Run as Administrator option.
- The password assigned to the certificate when it was created must be known. A prompt displays when a certificate is imported to a store and the import will fail if the password entry does not match the password assigned to the certificate.
- Certificates can only be imported to the following stores: *CurrentUser/My* and *LocalMachine/My stores*. All other stores are Read-only.
- Only certificates with the file extension *.pfx* can be imported.
- The *CurrentUser/My* store only displays the certificates for the current Windows user. To import certificates for a specific user, that user must be logged on to the computer.

4 Operation

When the Certificate Store Manager application is opened, the Certificate Store Manager window prompts the user to select a Store Type.

The available Store Types are:

- CurrentUser
- LocalMachine



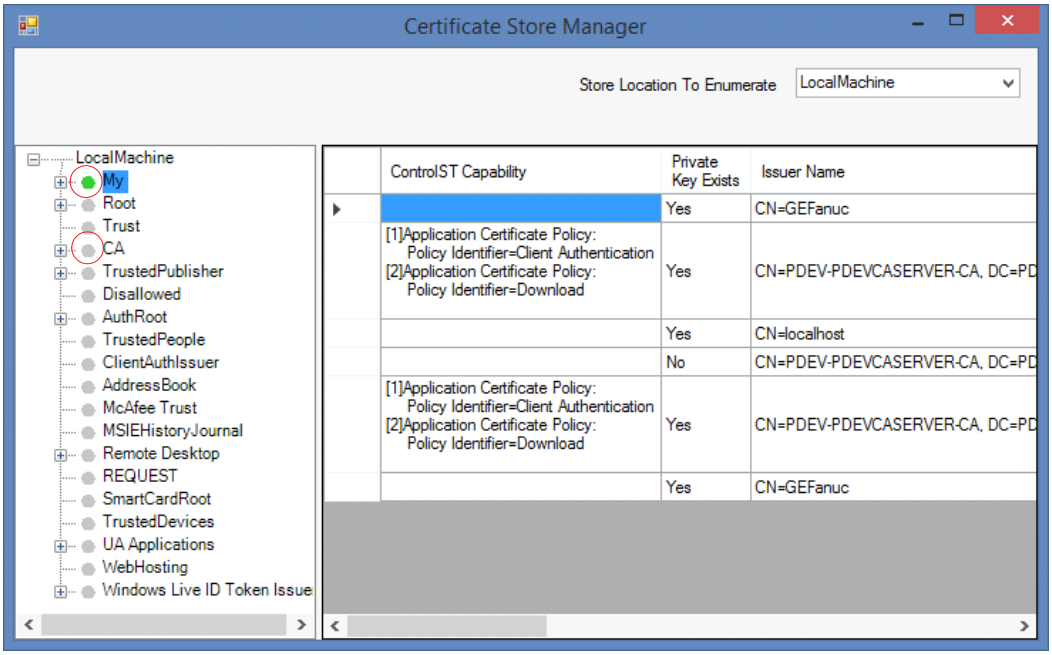
Certificate Store Manager Launch Window

When a item is selected from the Tree view, the certificate details for all certificates are displayed in the right window.

When the Tree view is expanded, an individual certificate may be selected.

A **green** icon indicates that importing and deletion of certificates is allowed.

A **gray** icon indicates Read-only.

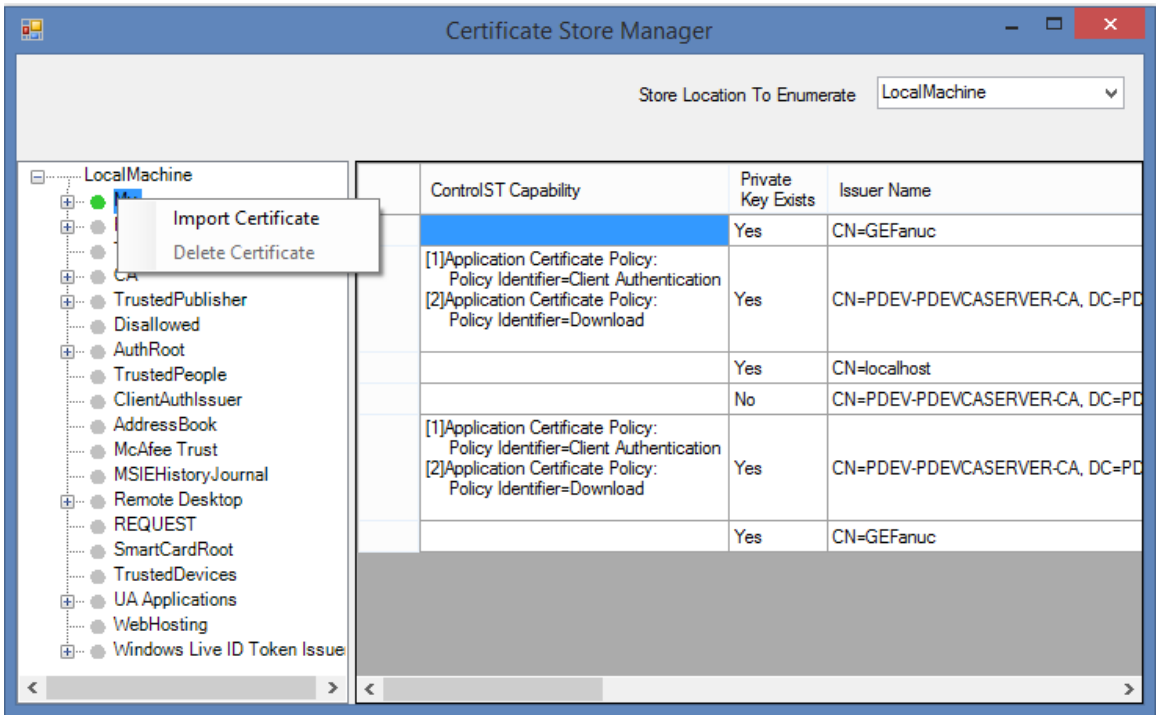


Example of LocalMachine Store Type, My Store, and Certificate Details

➢ To import a certificate

1. Select the store location to which to import a certificate.

From the **Tree** View, expand **LocalMachine**, right-click **My** location, and select **Import Certificate**.



Example of Import Certificate Feature Enabled

Note In this example, only *Import Certificate* is enabled. *Delete Certificate* is enabled when a Tree View item is expanded and a single certificate is selected. Other stores and store locations function the same way.

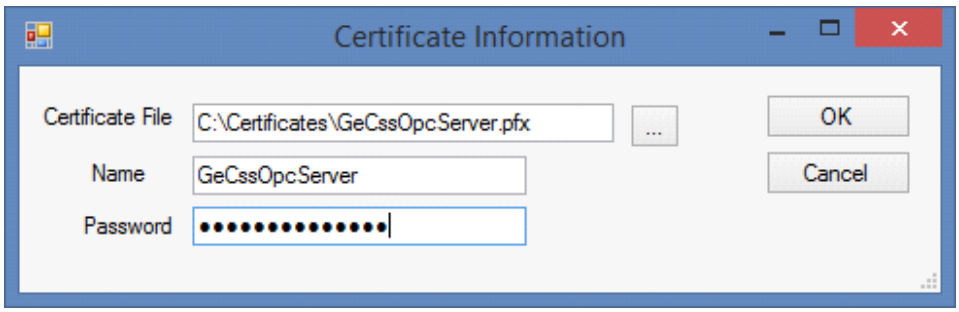
---

2. Enter the details for the certificate being imported.

Enter or click browse (…) to select the **Certificate File** location. This is the fully qualified *.pfx* certificate file to be imported.

Enter the certificate **Name**. This must be the name assigned to the certificate when created.

Enter the **Password** assigned when the certificate was created.



Example of Importing the GeCssOpcServer Certificate

Note For the OPC DA server in the WorkstationST application, the name must be *GeCssOpcServer*.

For the Device Manager Gateway feature in the WorkstationST application, the name must be *GeCssDeviceManagerGateway*.

The name of the certificate used within the WorkstationST application is the same as the process name of the running feature.

---

5 Command Line Support

To assist in managing certificates more efficiently, a number of command line options are supported for importing certificates to the stores.

The following is script the output of the command line help:

CertificateStoreManager [/?] | [/<Location> / PfxFile:<file name> /Password: <password>] [/V]

Line Item	Description
/?	Displays the supported command line options
/<Location>:<Store>	<Location> is the certificate Store Location. Valid value is *LocalMachine*.
	<Store> is the certificate store within the specified Location. Valid store name is *My*.
/PfxFile:<filename>	Fully qualified name of the certificate .pfx file to import. If the filename path has spaces, you must use quotation marks (“ “).
/Password:<password>	Password assigned when the certificate was created
/V	Verbose mode

An example of importing the Device Manager Gateway certificate into the LocalMachine location, *My* store is as follows:
CertificateStoreManager.exe /LocalMachine:My /PfxFile:C:\Certificates \GeCssDeviceManagerGateway.pfx /Password:thepassword

Note If the certificate already exists in the store, it is replaced with the new certificate.