How to Install SSL Certificates on Microsoft Servers

Realtime publishers

Dan Sullivan

Copyright Statement

Chapter 2: Understanding the Microsoft Certificate Store

One of the things we quickly realize when we start to work with SSL certificates is how many we need to manage. We can have SSL certificates for Web servers, mail servers, various kinds of application servers, and individual users can have servers, too. And those are just the servers we generate or acquire for internal purposes. We also need to manage certificates for trusted third parties, like Microsoft or security vendors that provide SSL certificates. Certificates from these trusted sources are kept on our computers so that we can determine the authenticity of certificates signed by these parties. Clearly, we need a way to keep track of all the digital certificates. This is where a certificate store comes in.

In this, the second chapter of *How to Install SSL Certificates for on Microsoft Servers,* we will examine some of the basic tasks associated with managing and maintaining SSL certificates. Before we jump into various certificate operations, we need to understand a bit about the certificate store and tools for working with that store.

The chapter is organized into three main sections:

- Overview of the purpose of the certificate store
- How to manage certificates with the Microsoft Management Console (MMC)
- Maintenance tasks associated with SSL certificates

The object of this chapter is to familiarize you with how the Windows operating systems (OSs) manage certificates and what you need to do to before taking the next step of deploying SSL certificates in your Web servers, email servers, database servers, and other enterprise applications.

Purpose of the Certificate Store

The certificate store is part of Windows OSs and is a persistent storage service for digital certificates. The interface to the certificate store is the MMC. The MMC is a general systems management tool that provides for different plug-ins that offer a variety of systems management capabilities. Some you may be familiar with include:

- Authorization manager for setting role-based permissions
- Computer management and related system tools
- Device manager for listing devices

- Event viewer for monitoring and troubleshooting
- Security templates for editing security template files
- Task scheduler for setting up and running tasks automatically

The MMC is something of a Swiss Army knife for systems administrators. One of the especially important features, at least from a usability perspective, is that you can install only the capabilities you need. These capabilities are delivered in the form of modules called snap-ins. Systems administrators get to choose which snap-ins they need. This lets us work in a relatively clean MMC environment without extraneous clutter. For the purpose of this chapter, we are primarily concerned with the Certificates snap-in and will focus on that.

Getting Started with the MMC

If you are not familiar with the MMC, it will not take long to get started. In spite of what could be construed as an ominous sounding tool, it is pretty straightforward to work with. You can start the MMC from either the Start Menu (see Figure 2.1a) or the command line (see Figure 2.1b).

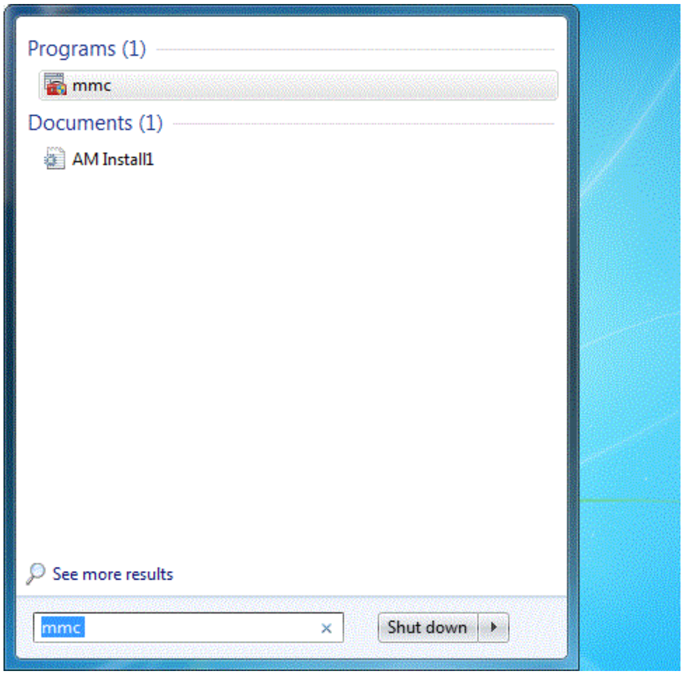
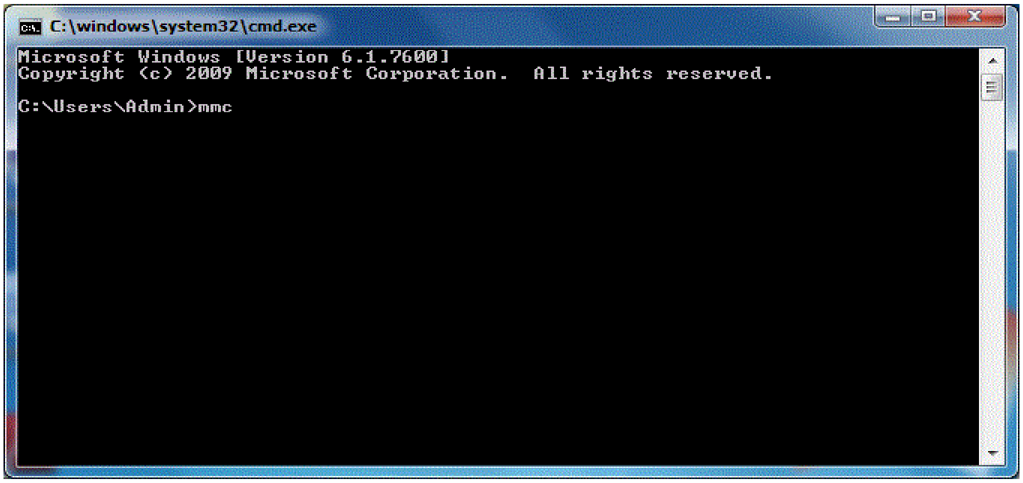


Figure 2.1a. Starting the MMC from the Start Menu.

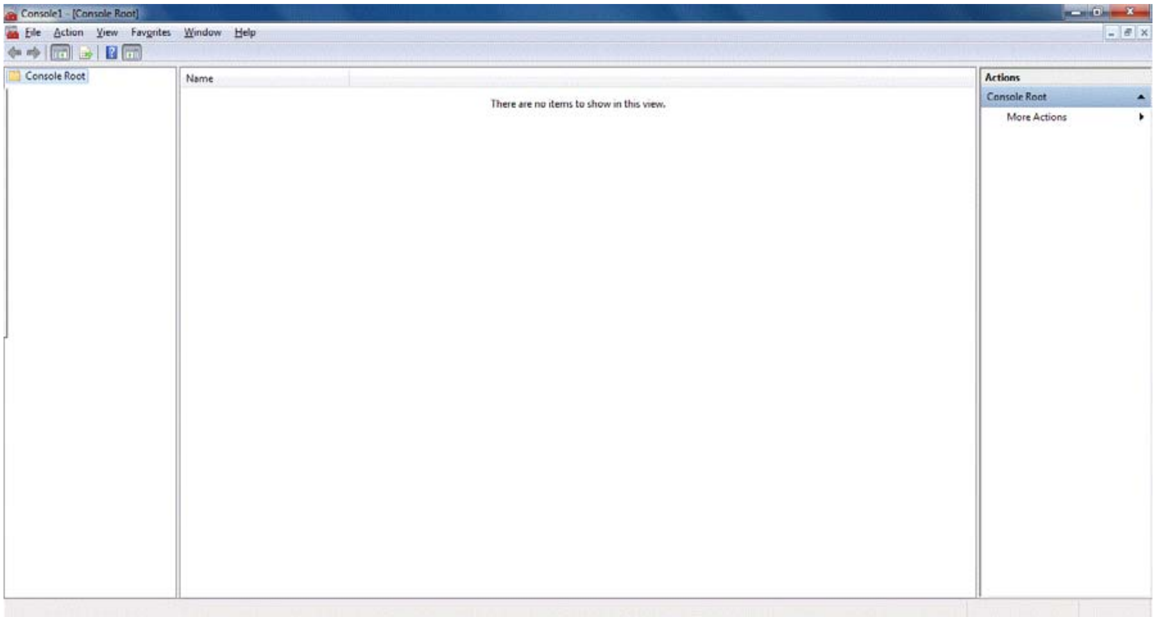


```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Admin>mmc
```

Figure 2.1b: Entering the command 'mmc' at the command line is an alternative way of starting the MMC.

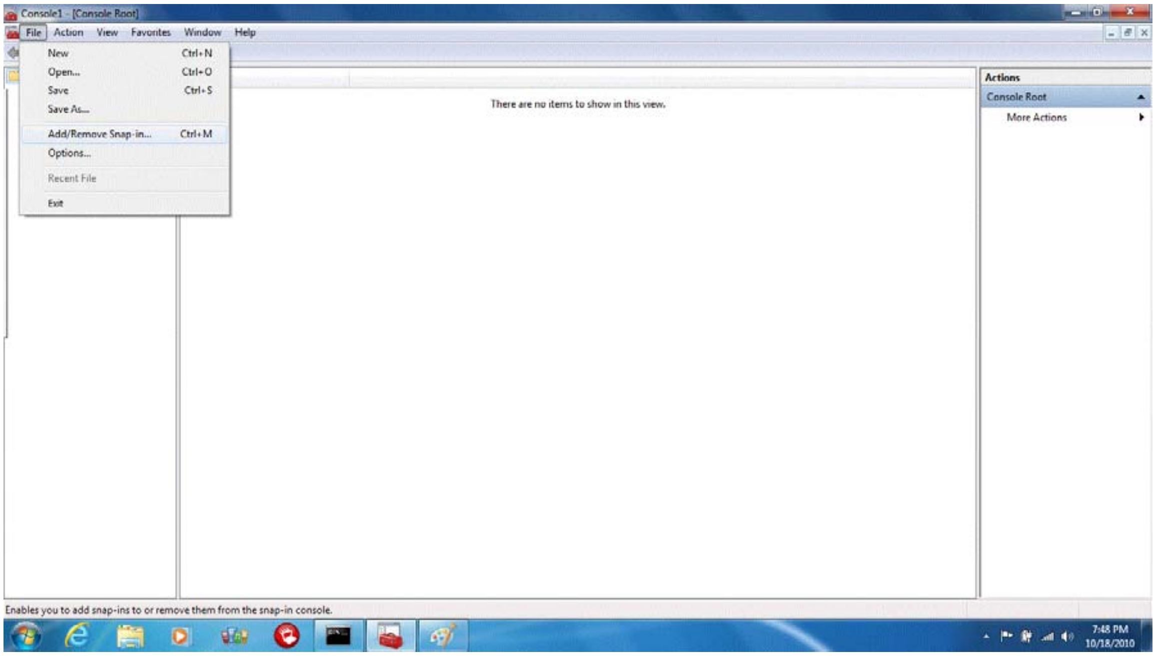
Systems administrators are free to configure the MMC as they like, so the first time you start the tool it will look pretty bare (see Figure 2.2).



There are no items to show in this view.

Figure 2.2: Starting the MMC for the first time brings it up in the starting configuration without snap-ins.

The first thing we want to do is to get the snap in to manage SSL certificates. To do this, navigate to the File menu, and select the Add/Remove Snap-in option (see Figure 2.3) or type Ctrl-M.

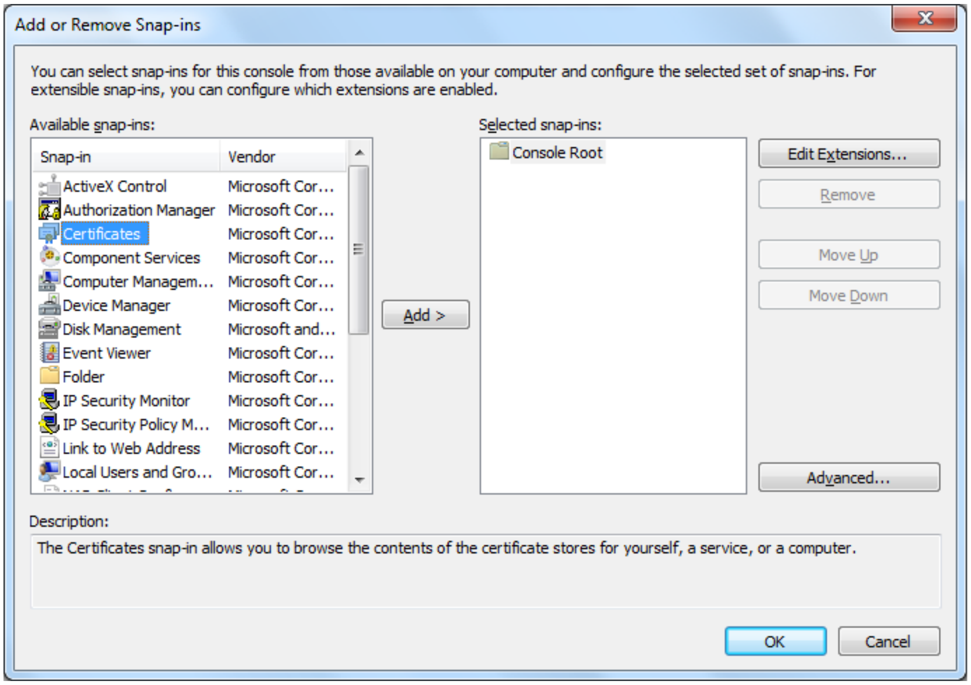


There are no items to show in this view.

Enables you to add snap-ins to or remove them from the snap-in console.

Figure 2.3: Adding snap-ins to the MMC.

Both methods of adding a snap-in to the MMC will bring up the dialog box Figure 2.4 shows.


Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...
Local Users and Gro...	Microsoft Cor...

Selected snap-ins:

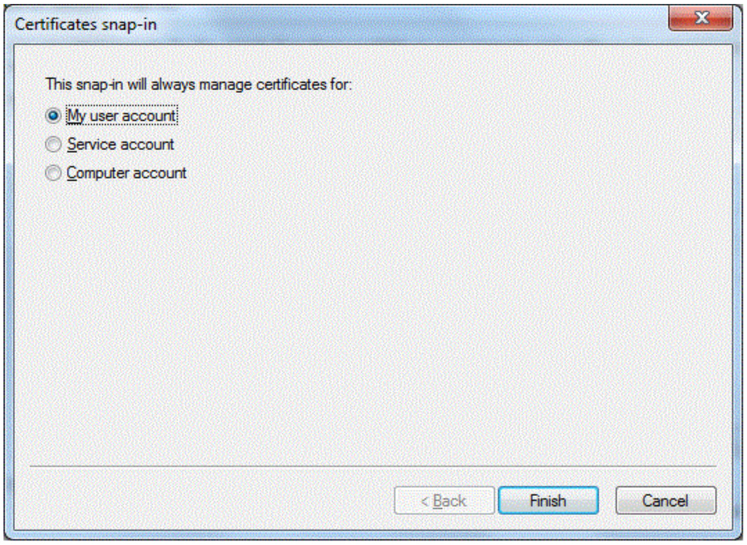
Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Figure 2.4: The Add or Remove Snap-ins dialog box allows systems administrators to choose the capabilities to be deployed in the MMC.

After clicking Add, a couple of dialog boxes will appear to enable you to further customize how the Certificate snap-in works. The first option is for determining the scope of management, which could be for an account, as service, or a computer (see Figure 2.5).



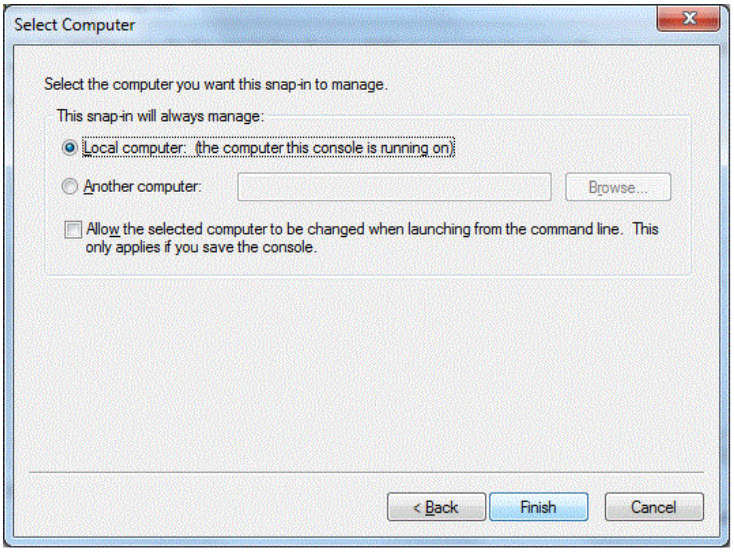
This snap-in will always manage certificates for:

● My user account
○ Service account
○ Computer account

Figure 2.5: Determining the scope of management for the snap-in.

When adding the snap-in, we have the choice of managing for just a single user account, a service account, or the computer account. Choose the computer account option. If a user is not an administrator, she can only manage for her user account.

The second dialog box is for selecting the computer to manage; the default is the local computer (see Figure 2.6).



Select the computer you want this snap-in to manage.

This snap-in will always manage:

● Local computer: (the computer this console is running on)
○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

Figure 2.6: The Certificate snap-in allows for remotely managing certificates on another computer.

Once these dialog boxes are completed, the Certificates snap-in will be installed. Once the installation is done, the MMC will appear as in Figure 2.7. Of course, if you have already installed other snap-ins, your interface will be slightly different.

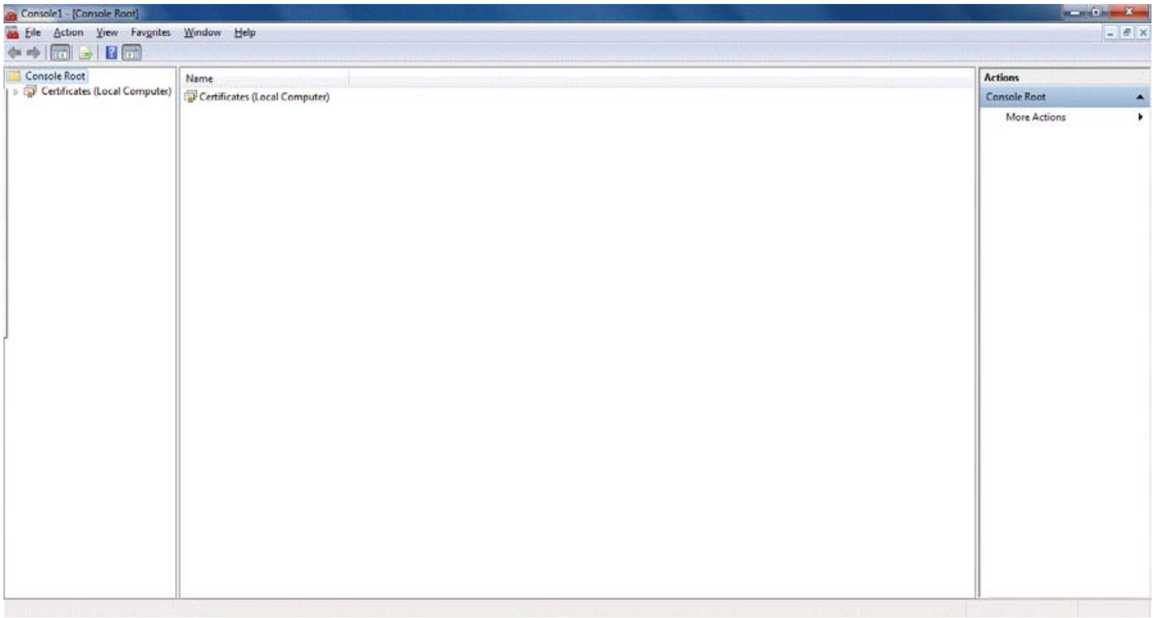
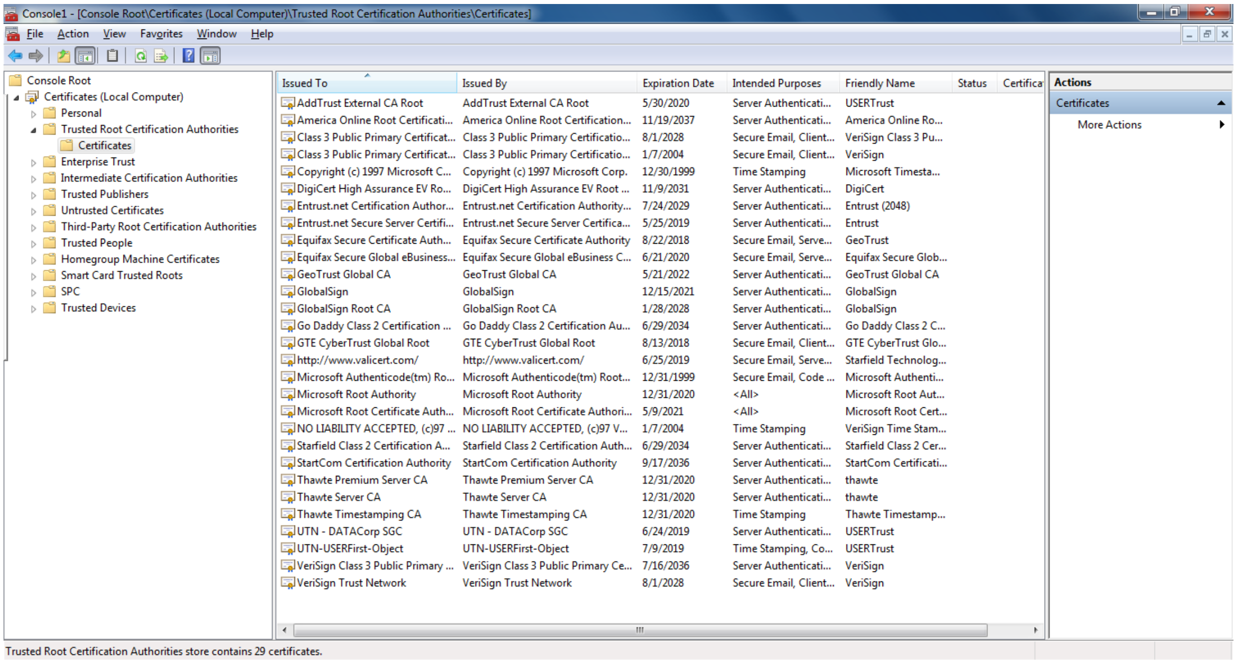

Console1 - [Console Root]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Name
Certificates (Local Computer)
Actions
Console Root
More Actions

Figure 2.7: Once the Certificates snap-in is installed, the MMC will display it in the main panel of the interface.

Before moving on to specific SSL certificate operations, we will review basic features of the Certificates snap-in.

Certificates Snap-in Features

The Certificates snap-in allows systems administrators to easily view and manage SSL certificates. One of the first things you may notice with the Certificates snap-in is the number of different certificates that are already installed in the Windows OS. For example, if you were to open the Certificates snap-in and expand the list of certificate types and then select Trusted Root Certificate Authorities, you would see a list something like that shown in Figure 2.8.


Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Homegroup Machine Certificates
Smart Card Trusted Roots
SPC
Trusted Devices
Actions
Certificates
More Actions

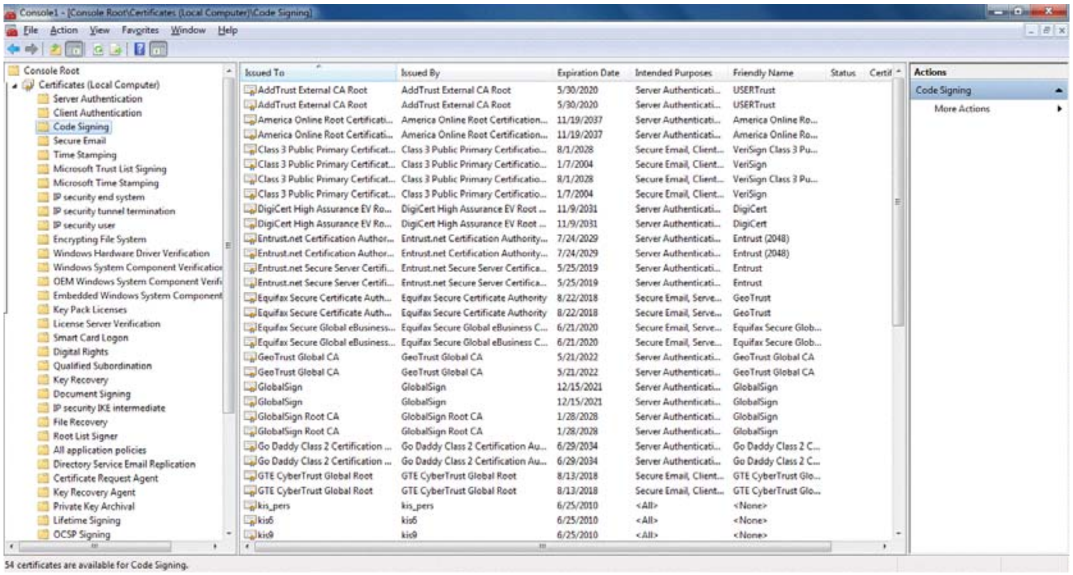
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certifica
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenticati...	USERTrust		
America Online Root Certificati...	America Online Root Certification...	11/19/2037	Server Authenticati...	America Online Ro...		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Secure Email, Client...	VeriSign Class 3 Pu...		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	1/7/2004	Secure Email, Client...	VeriSign		
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timesta...		
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/9/2031	Server Authenticati...	DigiCert		
Entrust.net Certification Author...	Entrust.net Certification Authority...	7/24/2029	Server Authenticati...	Entrust (2048)		
Entrust.net Secure Server Certifi...	Entrust.net Secure Server Certifica...	5/25/2019	Server Authenticati...	Entrust		
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Serve...	GeoTrust		
Equifax Secure Global eBusiness...	Equifax Secure Global eBusiness C...	6/21/2020	Secure Email, Serve...	Equifax Secure Glob...		
GeoTrust Global CA	GeoTrust Global CA	5/21/2022	Server Authenticati...	GeoTrust Global CA		
GlobalSign	GlobalSign	12/15/2021	Server Authenticati...	GlobalSign		
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Server Authenticati...	GlobalSign		
Go Daddy Class 2 Certification ...	Go Daddy Class 2 Certification Au...	6/29/2034	Server Authenticati...	Go Daddy Class 2 C...		
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/13/2018	Secure Email, Client...	GTE CyberTrust Glo...		
http://www.valicert.com/	http://www.valicert.com/	6/25/2019	Secure Email, Serve...	Starfield Technolog...		
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, Code ...	Microsoft Authenti...		
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021	<All>	Microsoft Root Cert...		
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...	1/7/2004	Time Stamping	VeriSign Time Stam...		
Starfield Class 2 Certification A...	Starfield Class 2 Certification Auth...	6/29/2034	Server Authenticati...	Starfield Class 2 Cer...		
StartCom Certification Authority	StartCom Certification Authority	9/17/2036	Server Authenticati...	StartCom Certificati...		
Thawte Premium Server CA	Thawte Premium Server CA	12/31/2020	Server Authenticati...	thawte		
Thawte Server CA	Thawte Server CA	12/31/2020	Server Authenticati...	thawte		
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Thawte Timestamp...		
UTN - DATACorp SGC	UTN - DATACorp SGC	6/24/2019	Server Authenticati...	USERTrust		
UTN-USERFirst-Object	UTN-USERFirst-Object	7/9/2019	Time Stamping, Co...	USERTrust		
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	7/16/2036	Server Authenticati...	VeriSign		
VeriSign Trust Network	VeriSign Trust Network	8/1/2028	Secure Email, Client...	VeriSign		

Trusted Root Certification Authorities store contains 29 certificates.

Figure 2.8: The list of Trusted Root Certification Authorities certificates includes those certificate providers trusted by default by the Windows OS.

This list of trusted authorities is quite useful. It prevents us from having to manually specify that we trust each of the major certification authorities.

The list presented in Figure 2.8 is what is known as the logical view of the list of certificates. We can also view certificates by their function, such as server authentication, client authentication, code signing, IP security, digital rights, BitLocker encryption, and a large number of other purposes (see Figure 2.9).



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certif
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenticati...	USERTrust		
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenticati...	USERTrust		
America Online Root Certificati...	America Online Root Certification...	11/19/2037	Server Authenticati...	America Online Ro...		
America Online Root Certificati...	America Online Root Certification...	11/19/2037	Server Authenticati...	America Online Ro...		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Secure Email, Client...	VeriSign Class 3 Pu...		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	1/7/2004	Secure Email, Client...	VeriSign		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Secure Email, Client...	VeriSign Class 3 Pu...		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	1/7/2004	Secure Email, Client...	VeriSign		
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/9/2031	Server Authenticati...	DigiCert		
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/9/2031	Server Authenticati...	DigiCert		
Entrust.net Certification Author...	Entrust.net Certification Authority...	7/24/2029	Server Authenticati...	Entrust (2048)		
Entrust.net Certification Author...	Entrust.net Certification Authority...	7/24/2029	Server Authenticati...	Entrust (2048)		
Entrust.net Secure Server Certifi...	Entrust.net Secure Server Certifica...	5/25/2019	Server Authenticati...	Entrust		
Entrust.net Secure Server Certifi...	Entrust.net Secure Server Certifica...	5/25/2019	Server Authenticati...	Entrust		
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Serve...	GeoTrust		
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Serve...	GeoTrust		
Equifax Secure Global eBusiness...	Equifax Secure Global eBusiness C...	6/21/2020	Secure Email, Serve...	Equifax Secure Glob...		
Equifax Secure Global eBusiness...	Equifax Secure Global eBusiness C...	6/21/2020	Secure Email, Serve...	Equifax Secure Glob...		
GeoTrust Global CA	GeoTrust Global CA	5/21/2022	Server Authenticati...	GeoTrust Global CA		
GeoTrust Global CA	GeoTrust Global CA	5/21/2022	Server Authenticati...	GeoTrust Global CA		
GlobalSign	GlobalSign	12/15/2021	Server Authenticati...	GlobalSign		
GlobalSign	GlobalSign	12/15/2021	Server Authenticati...	GlobalSign		
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Server Authenticati...	GlobalSign		
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Server Authenticati...	GlobalSign		
Go Daddy Class 2 Certification ...	Go Daddy Class 2 Certification Au...	6/29/2034	Server Authenticati...	Go Daddy Class 2 C...		
Go Daddy Class 2 Certification ...	Go Daddy Class 2 Certification Au...	6/29/2034	Server Authenticati...	Go Daddy Class 2 C...		
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/13/2018	Secure Email, Client...	GTE CyberTrust Glo...		
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/13/2018	Secure Email, Client...	GTE CyberTrust Glo...		
kis_pers	kis_pers	6/25/2010	<All>	<None>		
kis6	kis6	6/25/2010	<All>	<None>		
kis9	kis9	6/25/2010	<All>	<None>		

54 certificates are available for Code Signing.

Figure 2.9: The Certificate Purpose list is useful for viewing certificates according to how they are used by the OS.

To view certificates by purpose, right-click Certificates, then select View and then Options in the left-most panel, as show in Figure 2.10.

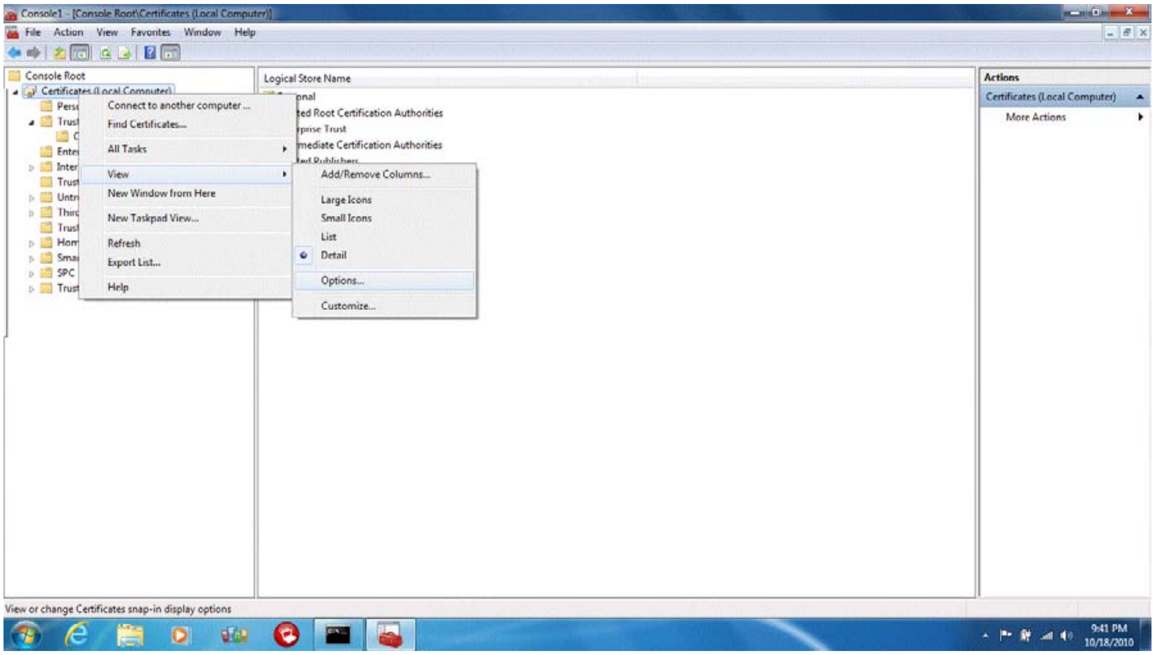
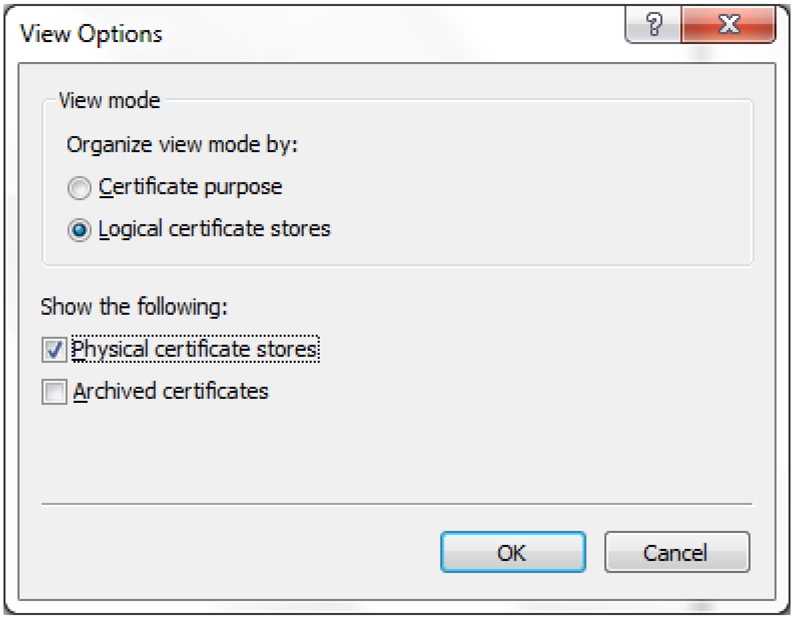


Figure 2.10: Right-clicking the certificates under the Console Root, and selecting View followed by Options allows MMC users to change the way certificate categories are displayed.

After selecting the Options item, a View Options dialog box appears that allows the user to select either the logical view mode (the default) or the view by certificate purpose mode.


View Options

View mode

Organize view mode by:

○ Certificate purpose

● Logical certificate stores

Show the following:

☑ Physical certificate stores

☐ Archived certificates

Figure 2.11: By default, the Certificates snap-in displays certificates in logical order. The View Options dialog box allows users to change to a purpose-oriented display.

As you can imagine, as the number of certificates grows, it becomes more difficult to find certificates by browsing and scanning lists. Fortunately, the Certificates snap-in provides a search functionality for narrowing the range of certificates displayed.

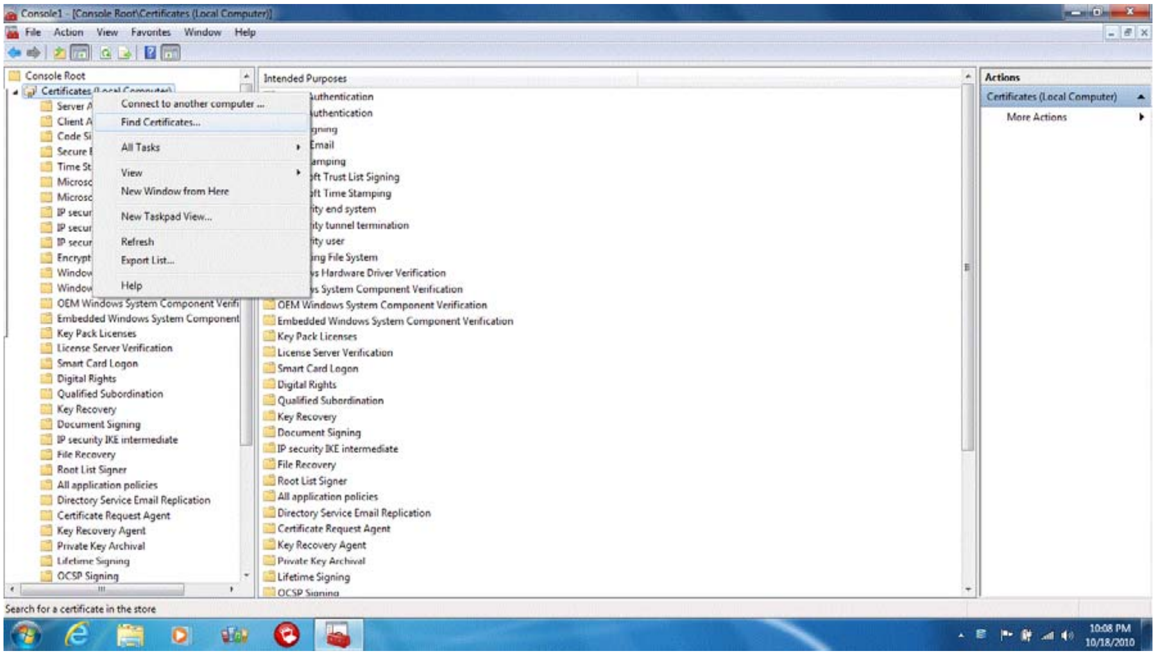
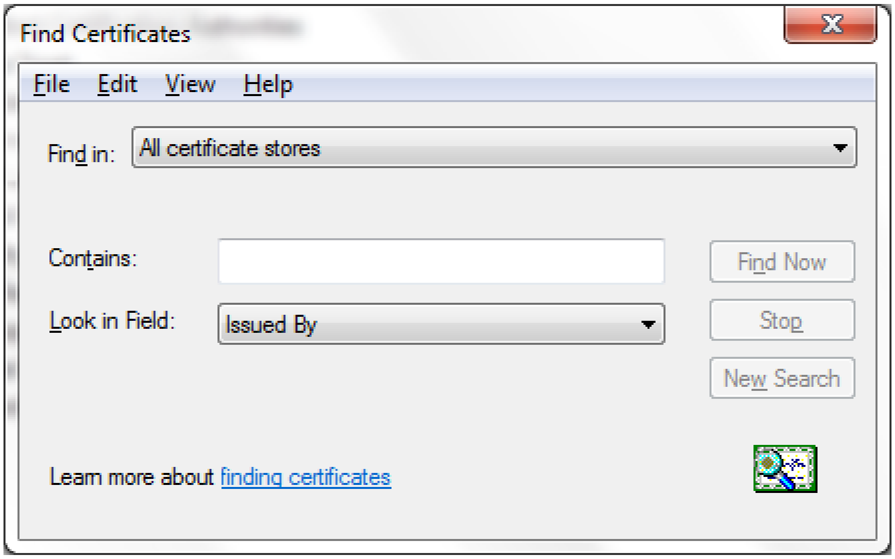

Console1 - [Console Root\Certificates (Local Computer)]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Connect to another computer ...
Find Certificates...
All Tasks
View
New Window from Here
New Taskpad View...
Refresh
Export List...
Help
Intended Purposes
OEM Windows System Component Verification
Embedded Windows System Component Verification
Key Pack Licenses
License Server Verification
Smart Card Logon
Digital Rights
Qualified Subordination
Key Recovery
Document Signing
IP security IKE intermediate
File Recovery
Root List Signer
All application policies
Directory Service Email Replication
Certificate Request Agent
Key Recovery Agent
Private Key Archival
Lifetime Signing
OCSP Signing
Actions
Certificates (Local Computer)
More Actions
Search for a certificate in the store
10:08 PM
10/18/2010

Figure 2.12: Right-clicking Certificates in the Console Root list displays a list of options, including Find.

Selecting the Find option displays a dialog box for finding certificates by searching for strings of text.



Find in: All certificate stores

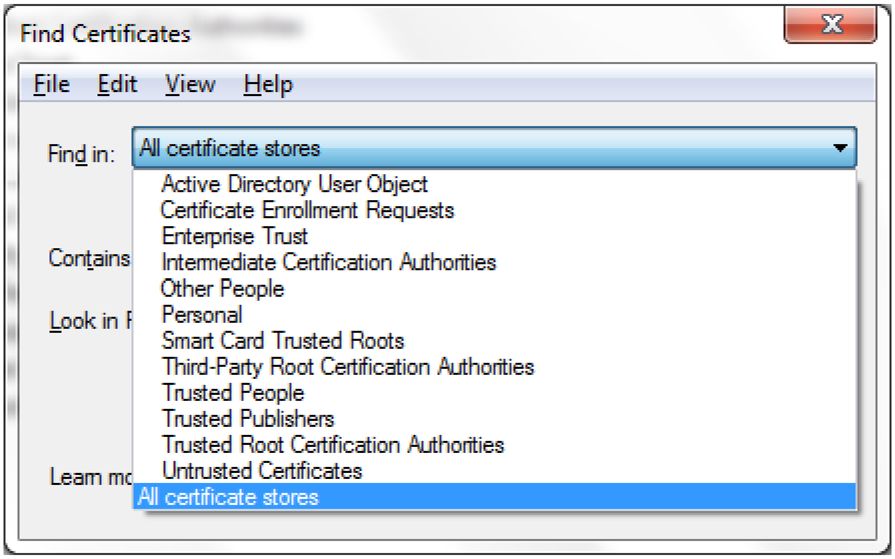
Contains:

Look in Field: Issued By

Learn more about finding certificates

Figure 2.13: The Find Certificates dialog box searches for strings of text in certificates.

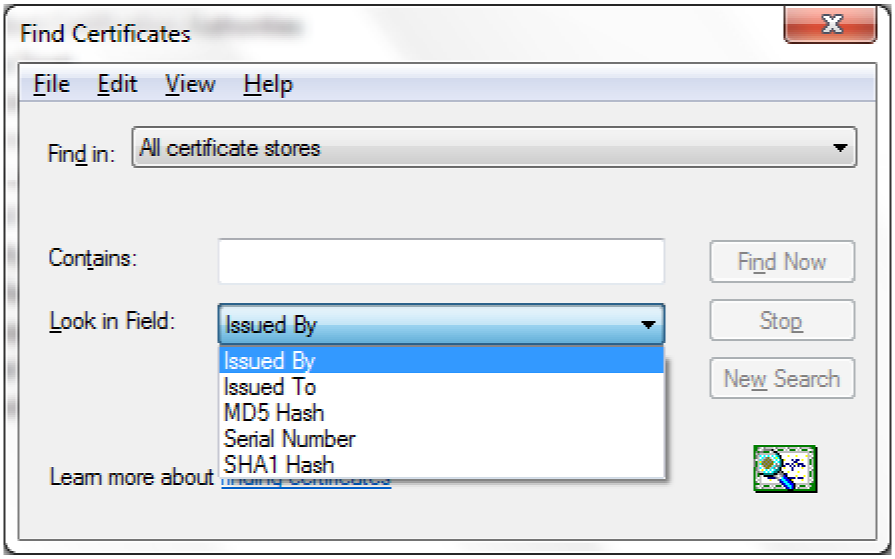
One of the options in the dialog box allows you to narrow your search by location within the Certificate store.



Find in: All certificate stores

Figure 2.14: You can search for particular types of certificates.

Search can be also constrained by looking in a handful of certificate fields, such as the Issued To field.



Find in: All certificate stores

Contains:

Look in Field: Issued By

Figure 2.15: The Find certificates features allows users to search several attributes of SSL certificates.

Now that we have covered the basics of installing the Certificates snap-in and browsing and searching the certificate store, we can move on to some basic certificate operations.

Managing Certificates with MMC

Sometimes it helps to think of SSL certificates at a logical level; that is, as an abstract data structure that has components such as cryptography keys, issuer information, an expiration date, and so on. Other times, it is more helpful to think of digital certificates in terms of their implementation, which is as a file. Certificate files are like other files: we can download, copy, store, and delete them. When it comes to basic operations on the certificate store, we'll tend to refer to SSL certificates in terms of their implementation as a file.

The basic operations on the certificate store we will cover are:

- Adding an SSL certificate
- Removing an SSL certificate
- Exporting certificates
- Updating properties
- Renewing certificates

Not surprisingly, many of these operations will involve familiar file manipulation steps.

Adding an SSL Certificate to the Certificate Store

If you want to use a certificate for client or server authentication, code signing, or any of the other uses of SSL certificates, you will need to add the SSL certificate file to the certificate store. We'll use the Certificates MMC snap-in to do so.

> **Note**
>
> At this point, we will just assume you have received or created an SSL certificate file. In the next chapter, we will describe in detail how to acquire an SSL certificate from third-party providers as well as how to create self-signed certificates.

We begin the process of adding a certificate by selecting the Action menu, then selecting All Tasks. This displays a submenu with the Import option (see Figure 2.16).

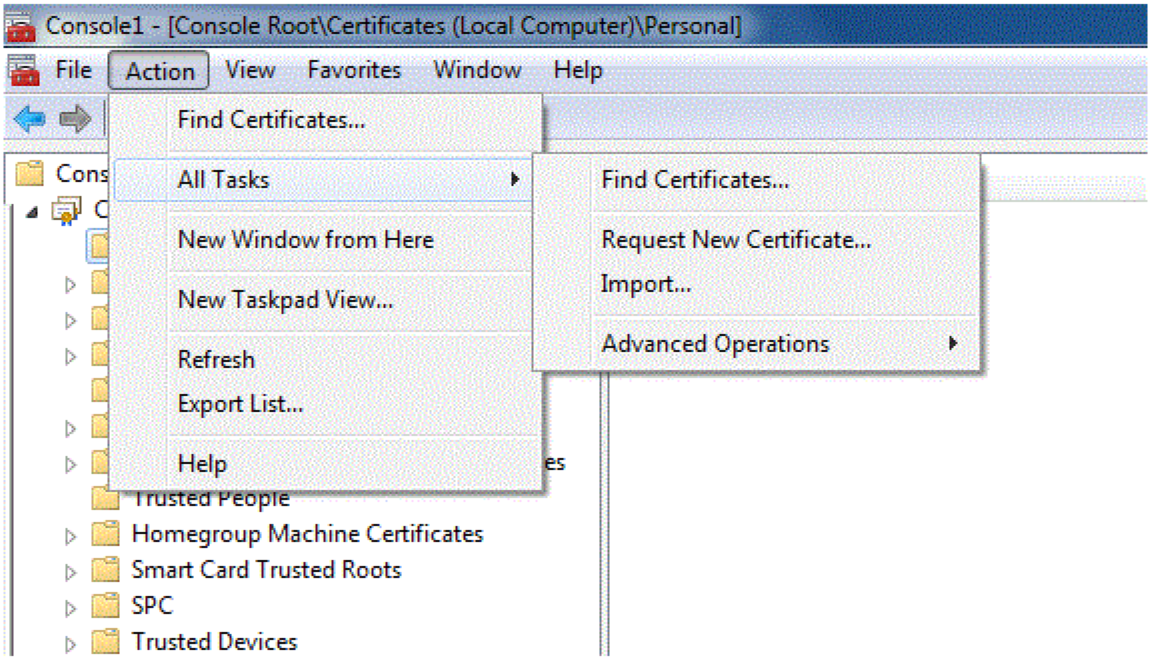
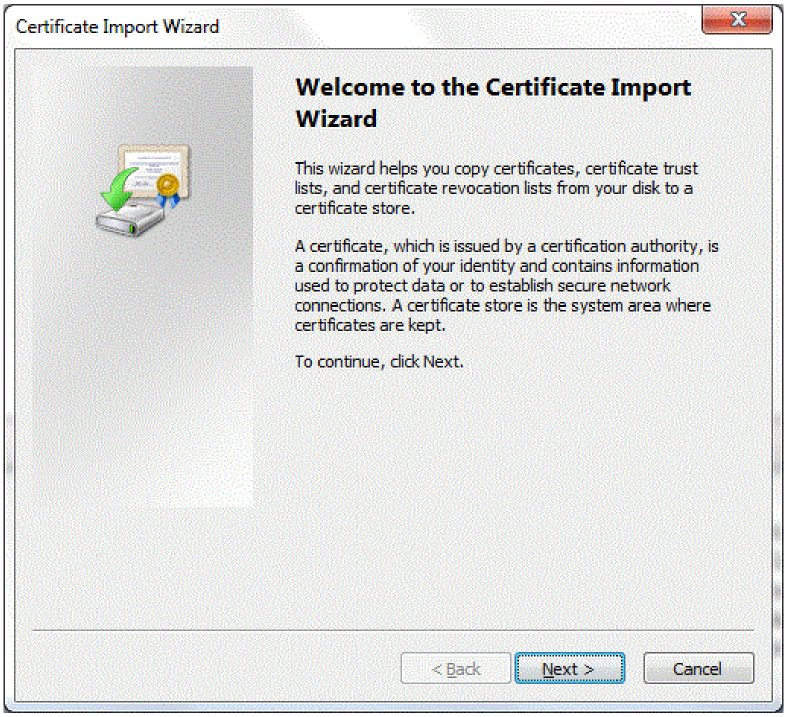


Figure 2.16: The Import Wizard is launched from the Actions menu and the All Tasks submenu.

Selecting Import starts the Import Wizard and displays the first of several dialog boxes. The first dialog box contains a description of the wizard's function (see Figure 2.17).



Certificate Import Wizard

Welcome to the Certificate Import Wizard

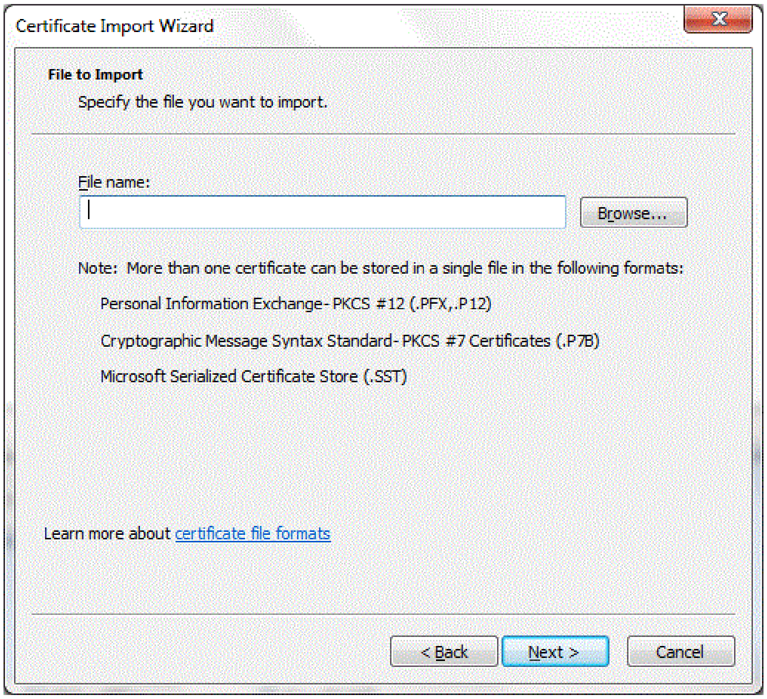
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Figure 2.17: The first dialog box in the Certificate Import Wizard describes the purpose of the wizard.

The next dialog box prompts for the file name containing the certificate to import. You can use the browse button to invoke a file dialog box to find the certificate file.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

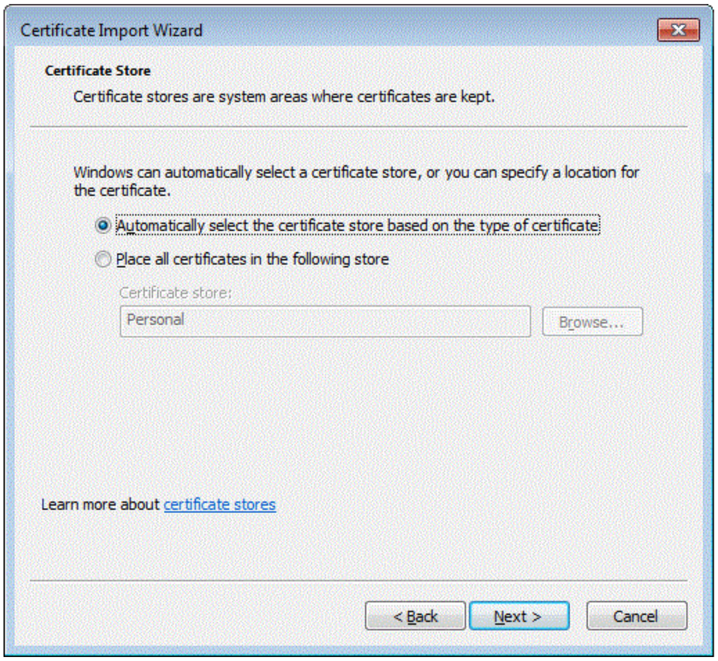
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

Figure 2.18: Select the file to import using this dialog box.

After the certificate file is specified, you will be prompted about where to place the certificate in the certificate store. Your options are to allow the wizard to automatically determine the location of the certificate or to specify which of the logical folders in the certificate store to import the file. If you choose to manually select where to store the file, you can click Browse to show a hiearchical display of certificate locations.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

● Automatically select the certificate store based on the type of certificate

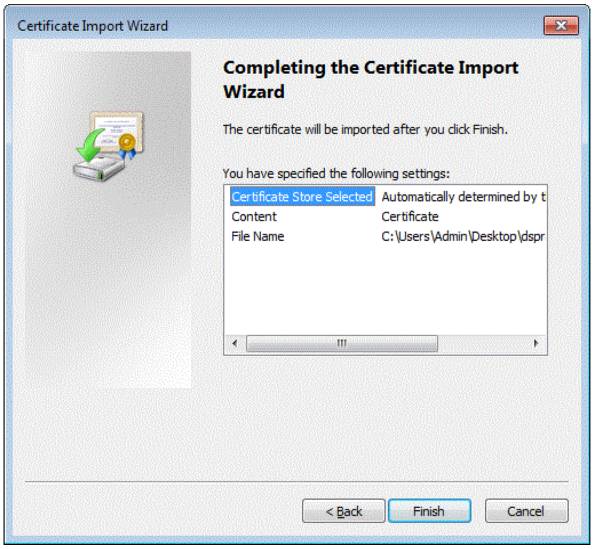
○ Place all certificates in the following store

Certificate store: Personal

Learn more about certificate stores

Figure 2.19: You can select where to store the certificate or have the wizard select for you.

In the last step of the process, the Certificate Import Wizard displays the parameters specified for the import operation. Click Finish to complete the import operation.



Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	Certificate
File Name	C:\Users\Admin\Desktop\dspr

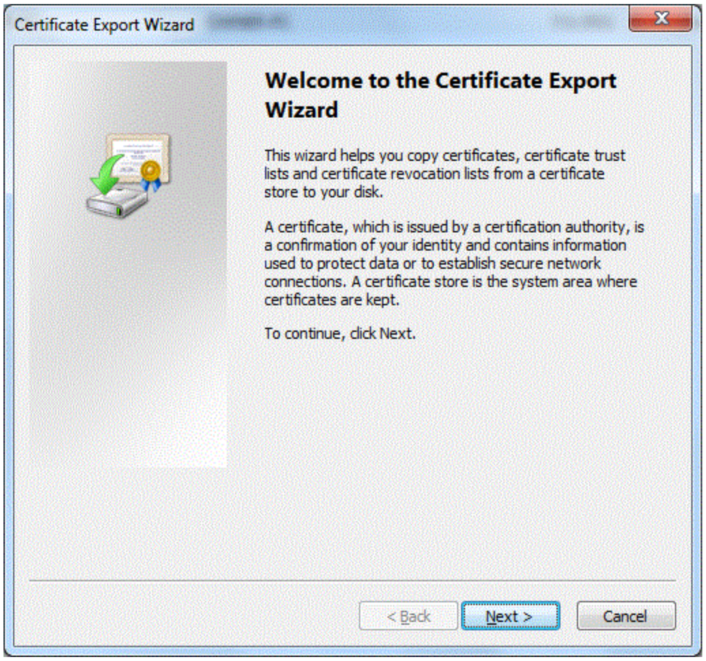
Figure 2.20: The last step of the Certificate Import Wizard shows the parameters of the import operation.

Removing an SSL Certificate from the Certificate Store

Removing a certificate is a simple task. Select the certificate from the main panel of the Certificates snap-in interface. Right-click the certificate. From the list of options, select Delete. You will be prompted to confirm you actually want to delete this certificate. Select Yes to remove the certificate. If you are unsure whether you should delete the certificate or if you think it might be needed in the future, you can export the certificate before deleting.

Exporting an SSL Certificate from the Certificate Store

SSL certificates are exported by running the Certificate Export Wizard from within the MMC. You start the export process by selecting a certificate in the Certificates snap-in, then either right-clicking the selection or clicking the Actions menu. Either operation will bring up a list of options that includes All Tasks. Select the All Tasks option, then select Export. The first dialog box of the Certificate Export Wizard will appear (see Figure 2.21).



Welcome to the Certificate Export Wizard

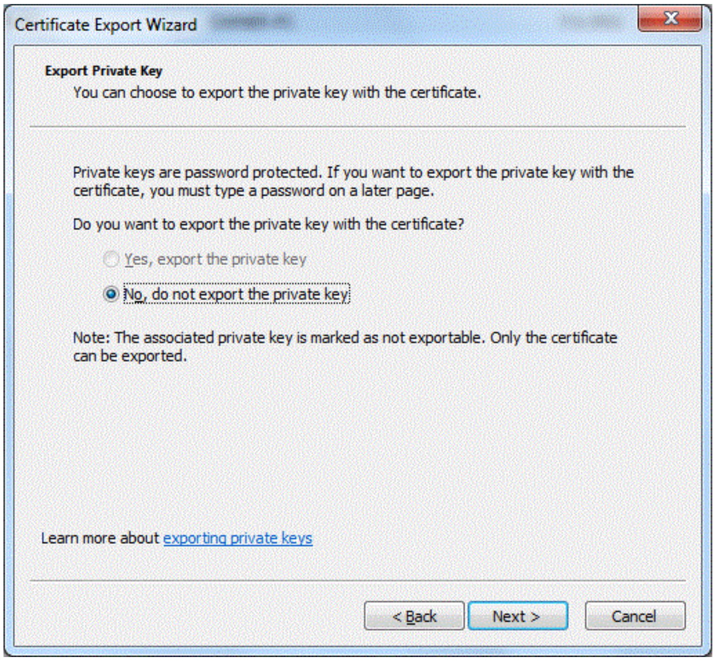
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Figure 2.21: The first dialog box of the Certificate Export Wizard describes the purpose of this task.

Proceed with the wizard by selecting Next. A dialog box will appear that will allow you to choose whether to export the private key associated with the certificate. In some cases, such as trusted third-party root certificates, you will not have the option of exporting the private key (see Figure 2.22). In general, it is more secure to not export the private key. Private keys must not be disclosed in order to maintain the security of operations using public key cryptography.



Certificate Export Wizard

Export Private Key
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

○ Yes, export the private key

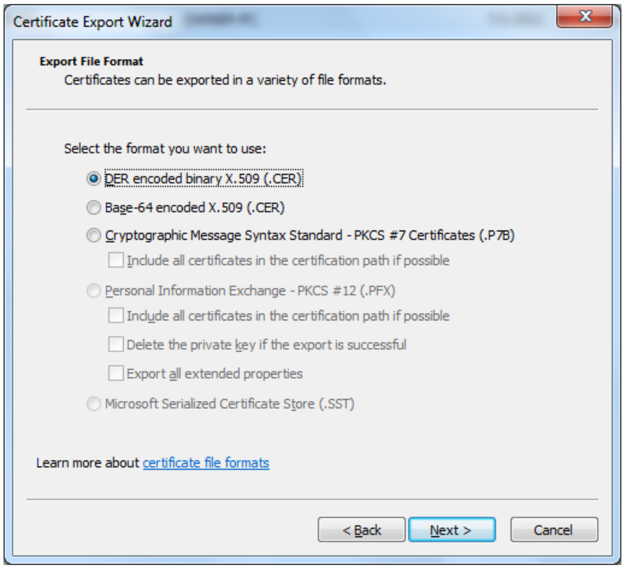
● No, do not export the private key

Note: The associated private key is marked as not exportable. Only the certificate can be exported.

Learn more about exporting private keys

Figure 2.22: If you have access to the private key associated with a certificate, you will be prompted to choose whether to export it.

The next dialog box prompts for a file format. There are several options. The DER or Distinguished Encoding Rules and the Base64-encoded X.509 are formats that support a single certificate but do not support the storage of private keys. The PKCS #7 format allows for all certificates in a certification path to be exported together. The PKCS #12, also known as the Personal Information Exchange, format supports the most features. It allows for exporting private keys and for storing all certificates in a certification path.



Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

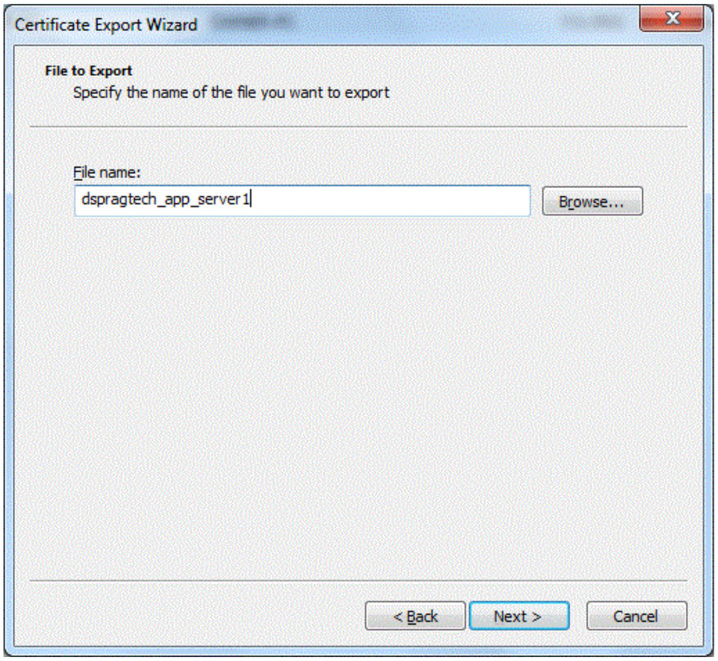
□ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

Figure 2.23: Select a file format appropriate for the number and attributes of a certificate to export. DER encoding is suitable for a single certificate in which the private key is not exported.

The certificate will be physically stored as a file, so we next need to specify a path and filename to store the certificate (see Figure 2.24).



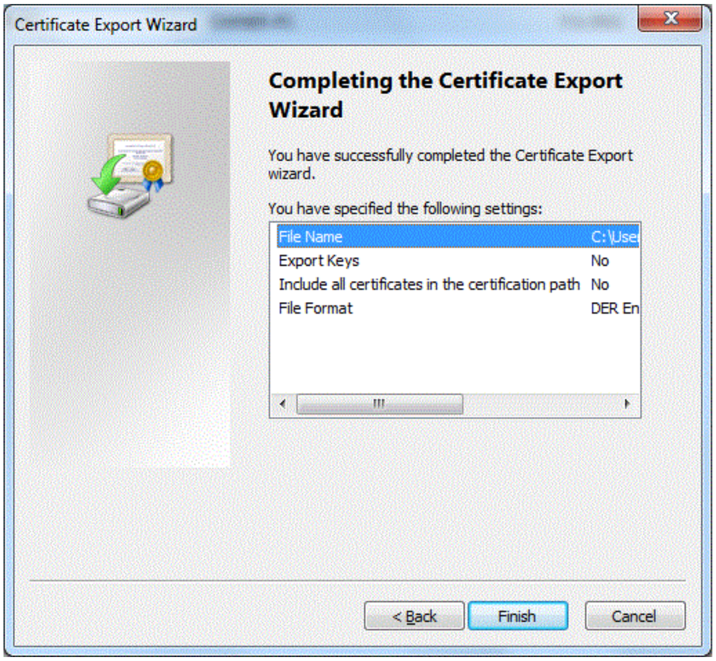
File to Export

Specify the name of the file you want to export

File name: dspragtech_app_server1

Figure 2.24: A filename and path are required to store the exported certificate.

The final dialog box of the Certificate Export Wizard displays the parameters of the export operation. Click Finish to complete the export.



Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

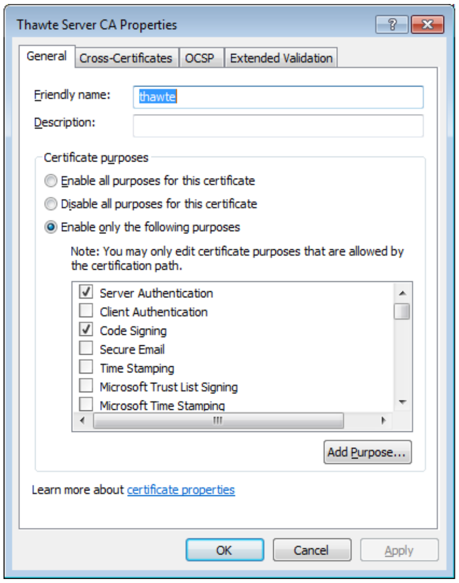
You have specified the following settings:

File Name	C:\Use
Export Keys	No
Include all certificates in the certification path	No
File Format	DER En

Figure 2.25: The final step of the Certificate Export Wizard displays the parameters of the export operation.

Updating Properties of a Certificate

When you are dealing with a large number of certificates, it helps to be able to add your own description and a more administration-friendly name. This is done by selecting a certificate in the main pane of the Certificates snap-in interface by right-clicking and selecting Properties from the menu (see the resulting dialog box in Figure 2.26).



Thawte Server CA Properties

Friendly name: thawte

Description:

Certificate purposes

○ Enable all purposes for this certificate

○ Disable all purposes for this certificate

● Enable only the following purposes

Note: You may only edit certificate purposes that are allowed by the certification path.

☑ Server Authentication

□ Client Authentication

☑ Code Signing

□ Secure Email

□ Time Stamping

□ Microsoft Trust List Signing

□ Microsoft Time Stamping

Learn more about certificate properties

Figure 2.26: The Properties dialog box allows administrators to specify more informative names and add descriptions to certificates.

Renewing SSL Certificates

SSL certificates are issued for a specific period of time after which they are no longer valid. At the end of a certificate's lifespan, or near the end, you should renew the certificate if it is still needed. The Certificates snap-in provides a couple of wizards for this. Selecting a certificate, right-clicking, then displaying the All Tasks menu will show two options when the certificate can be renewed: the Renew a Certificate with a New Key and the Renew a Certificate with the Same Key options.

When renewing with the same key, you have the option of taking the default parameters for the certificate or you can select the Details option followed by clicking Properties to specify alternative settings. When renewing with a new key, you also have the option of specifying new parameters, but this is recommended only for advanced users.

When working with SSL certificates in the MMC, we are often performing file-oriented operations such as importing, exporting, and updating properties. In addition to these certificate-oriented operations, there are a couple of maintenance tasks that should be addressed.

Maintenance Tasks

It is hard to imagine a systems administration responsibility that does not have a significant maintenance element to it. Managing SSL certificates is no different. As systems administrators, we need be able to restore an OS if it fails or if we make some kind of mistake in our day-to-day activities. Accidently deleting a needed SSL certificate falls into that category. Fortunately, the MMC makes it easy to export certificates so that backups can be made. Be sure to store copies of certificates on different storage devices than the originals. Storage locations should be secure, especially if private keys have been exported.

It does not take long to get an SSL certificate, but as a general rule, we do not want to be rushing to get one because our certificate has expired and customers are seeing warning messages in their browsers every time they initiate a secure communications with our site. The MMC Certificates snap-in displays certificate expiration dates in a date-sortable list so that it is relatively easy to track upcoming expiration dates.

Summary

The Microsoft Certificate Store and the MMC Certificates snap-in provide the basic tools we need as systems administrators to install, update, and remove SSL certificates as necessary. In the next chapter, we will discuss how to acquire SSL certificates, generate our own for test and development purposes, and how to install them in the IIS Web server.

Download Additional Books from Realtime Nexus!