INTEL® ACTIVE MANAGEMENT TECHNOLOGY

August 2018

How To Purchase and Install GoDaddy* Certificates for Intel® AMT Remote Setup and Configuration

Legal Disclaimer

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com/AMT.

Cost reduction scenarios described are intended as examples of how a given Intel-based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.

Intel® Active Management Technology requires activation and a system with a corporate network connection, an Intel Active Management Technology-enabled chipset, and network hardware and software. For notebooks, Intel Active Management Technology may be unavailable or limited over a host OS-based VPN, when connecting wirelessly, on battery power, sleeping, hibernating, or powered off. Results dependent upon hardware, setup, and configuration. For more information, visit intel.com/AMT.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

Contents

Revision History

Revision	Revision History	Date
1.0	First release.	August 17, 2012
1.1	Added steps to install intermediate certificate.	August 22, 2012
1.2	Added steps to verify thumbprint; clarified the multi-domain certificates; changed recommendation for key length to only 2048 bits.	September 17, 2012
1.3	Added section on how to verify the certificate.	September 19, 2012
1.4	Include SHA2 support	March 10, 2015
2.0	Updated screens for Standard SSL Certificate	August 3, 2018

1   Preface

Intel® Active Management Technology (Intel® AMT) must be setup and configured before you can use the remote manageability and security features. One method is to install Intel® Setup and Configuration Software (Intel® SCS) and then use *remote configuration*. Remote configuration uses Transport Layer Security (TLS) between the Intel SCS Remote Configuration Server (RCS) and the remote PCs with Intel AMT firmware. The Intel AMT firmware is pre-loaded with TLS certificate thumbprints from six different certificate vendors so all you need to do is install a third-party certificate on the Remote Configuration Server. This document includes step-by-step instructions on how to purchase and install a GoDaddy* certificate that will match the pre-installed GoDaddy thumbprint and allow you to use remote configuration and maintenance using Intel SCS.

1.1   Document Scope

This document does not include specific steps to install the GoDaddy certificate on other management consoles. For consoles that do not use Intel SCS, please refer to the vendor's documentation for installing the certificate. The steps used to purchase the certificate are the same for all management consoles.

1.2   Supported Intel® AMT Versions

The GoDaddy* Secure CA certificates are supported in the following versions of Intel AMT:

- 6.x and later

GoDaddy* certificates are not supported on the following AMT versions:

- 5.x and below

1.3   Intended Audience

This document is intended for Information Technology (IT) professionals who will be purchasing and installing the TLS certificates.

Readers should have a basic understanding of their IT infrastructure, especially Microsoft* Internet Information Service, the Microsoft Mangement Console, and a basic familiarity with TLS certificates.

1.4   Prerequisites

The Intel SCS User Guide provides information on the prerequisites for using the Remote Configuration Service (RCS). Before starting this process, you should have the following:

- Intel SCS Remote Configuration Service (RCS) installed on a supported Microsoft* operating system
- One or more domain names for your network (Microsoft* Workgroups are not supported)
- Microsoft* Internet Information Service (IIS) running on the server that is hosting the Remote Configuration Service
- Account permissions to install the certificate

2 Purchase a GoDaddy* Certificate

The following instructions were captured using Microsoft* Internet Information Services (IIS) for Windows* Server 2016.
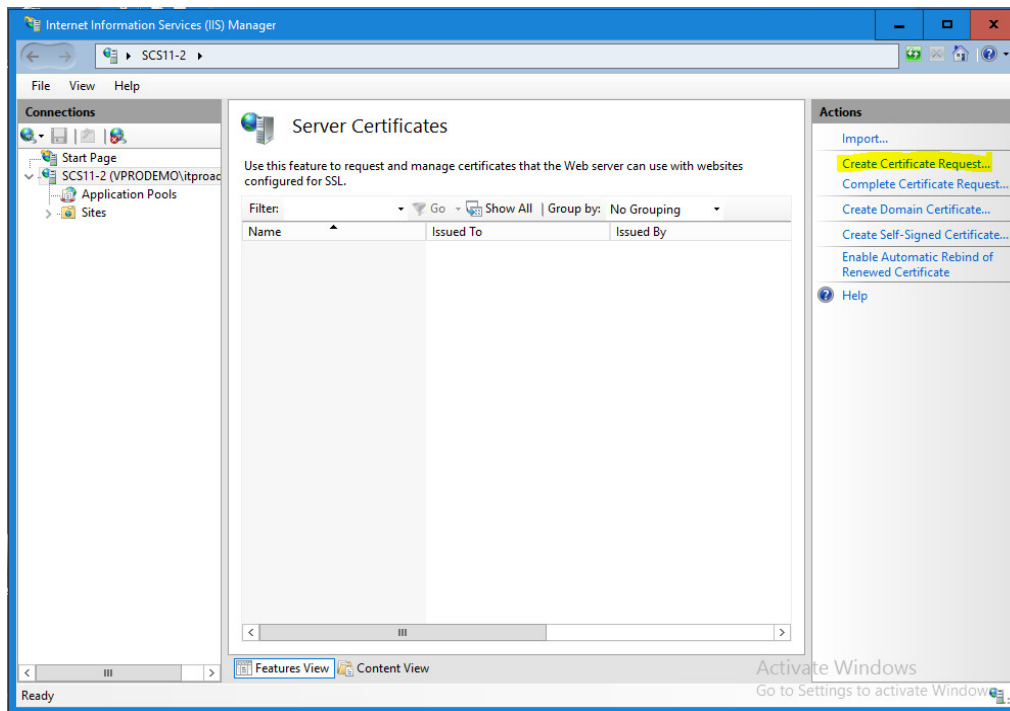
2.1 Create a Certificate Signing Request (CSR)

1. On your Intel SCS Remote Configuration Server (RCS), open **Programs->Administrative Tools→Internet Information Services (IIS) Manager**.
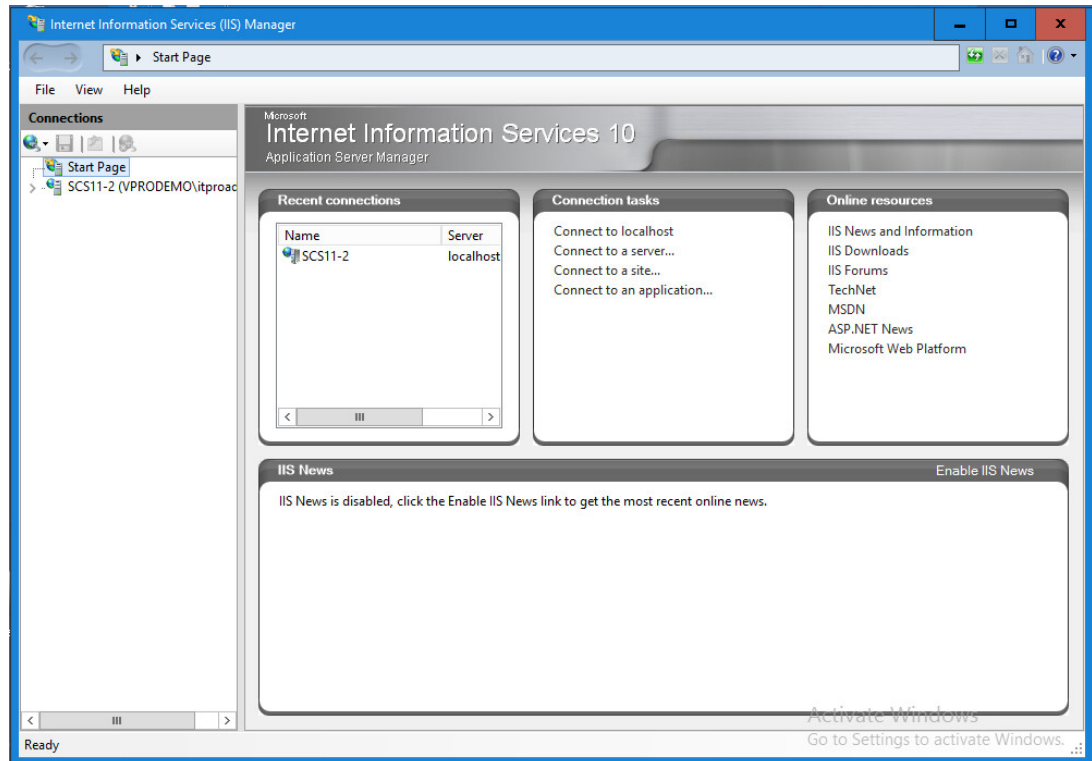
2. In the Internet Information Services (IIS) Manager, open the **Server Certificate** icon.
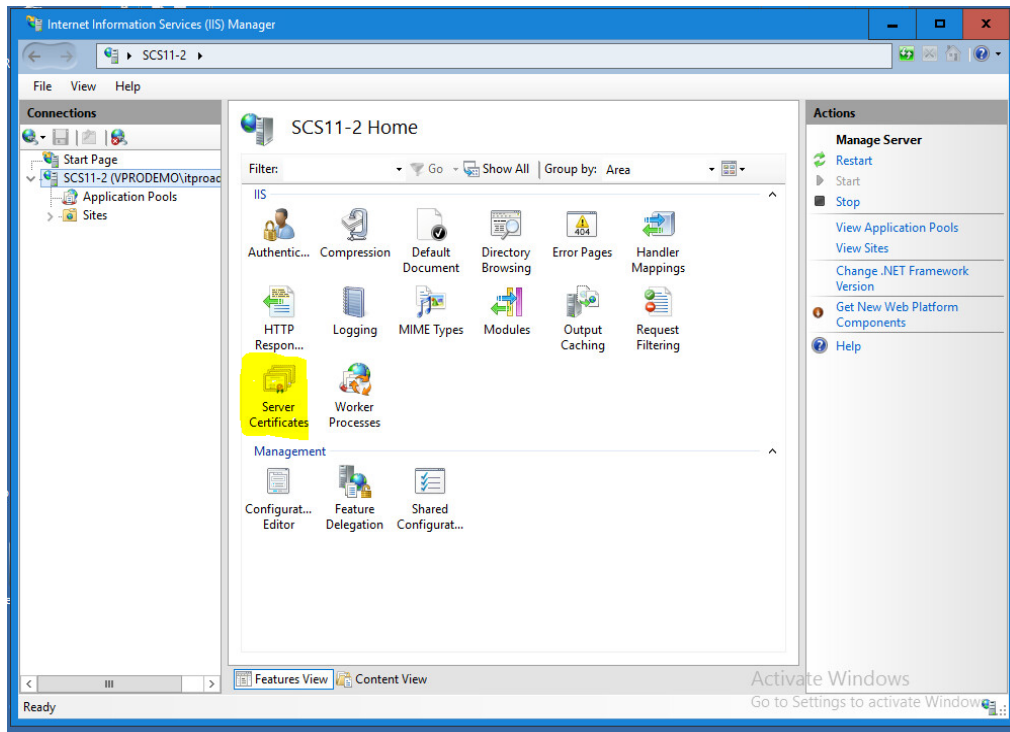
3. From the Actions menu, select Create Certificate Request.

4. Fill in the **Distinguished Name Properties** form as follows:

Common Name: The common name, or CN, for standard certificates, is the RCS server hostname plus a domain suffix. To determine if the certificate is valid, the client compares the domain portion of the Common Name to the value returned by DHCP option 15, or, if set, to the Secure DNS Suffix or Provisioning Server FQDN value set in the client's Intel® Management Engine BIOS Extension (Intel® MEBX). For help in understanding the rules for determining if the two values match, and support for second- and third-level domains in each version of Intel AMT, refer to the _Domain Suffix Guide for Intel® AMT Remote Configuration Process_. If you are purchasing a wildcard certificate then you can use one certificate to span different branches in the domain forest. For wildcard certificates, use an asterisk followed by a domain suffix in the CN.

Example 1 (CN=RCS Server FQDN):

In this example, assume that the DHCP Option 15 has been set to "vprodemo.com," and that you did not set the Secure DNS Suffix or the Provision Server FQDN values in the client's Intel MEBX.

Then, if your Remote Configuration Service (RCS) is running on scs10.vprodemo.com, set CN=scs10.vprodemo.com.

You can verify the DHCP Option 15 setting by running the SCSDiscovery utility (provided with Intel SCS) on the client. The DHCP Option 15 setting is called the OSSpecificDNSSuffix.

Example 2 (CN=RCS server host with client DNS Suffix)

In this example, the DHCP option 15 value has been set to "vprodemo.edu" for the environment. If your Remote Configuration Service is running on myRCS.vprodemo.com, set the certificate CN=myRCS.vprodemo.edu.

Organization: The name of the organization that is requesting the certificate and owns the domain

Organizational Unit: (not used by GoDaddy)

City: The requesting organization's city

State: The requesting organization's state

Country: The requesting organization's country code

5. Click **Next.**

6. Leave the Cryptographic Service Provider set to **Microsoft RSA SChannel Cryptographic Provider** and select **2048** as your key Bit length.

7. Click **Next**, and in the next panel, click the browse (**...**) button to select a location. Enter a file name to store the certificate request and then choose **Submit**.
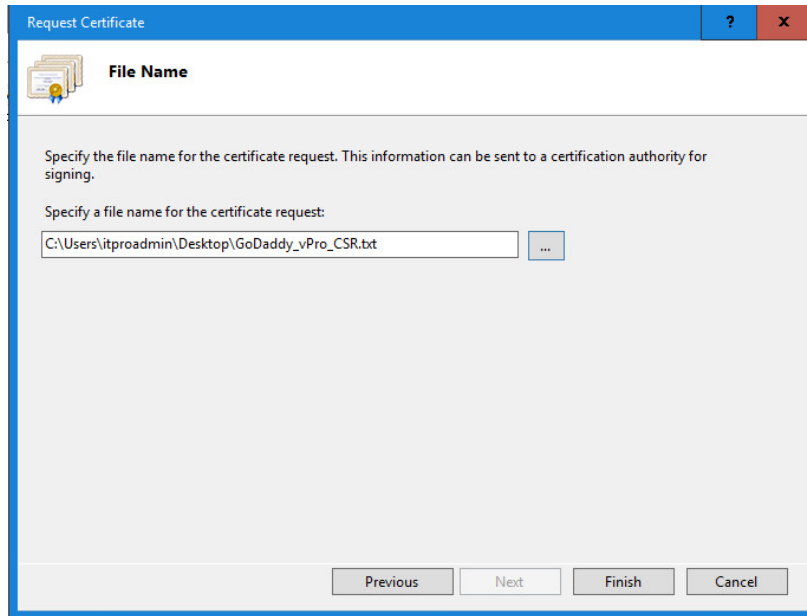
8. Click **Finish**.

    The file you created, named GoDaddy_vPro_CSR in our example, will be used to submit your request to GoDaddy for an Intel AMT Setup and Configuration certificate. You can open the file in Notepad to view the encrypted certificate request.
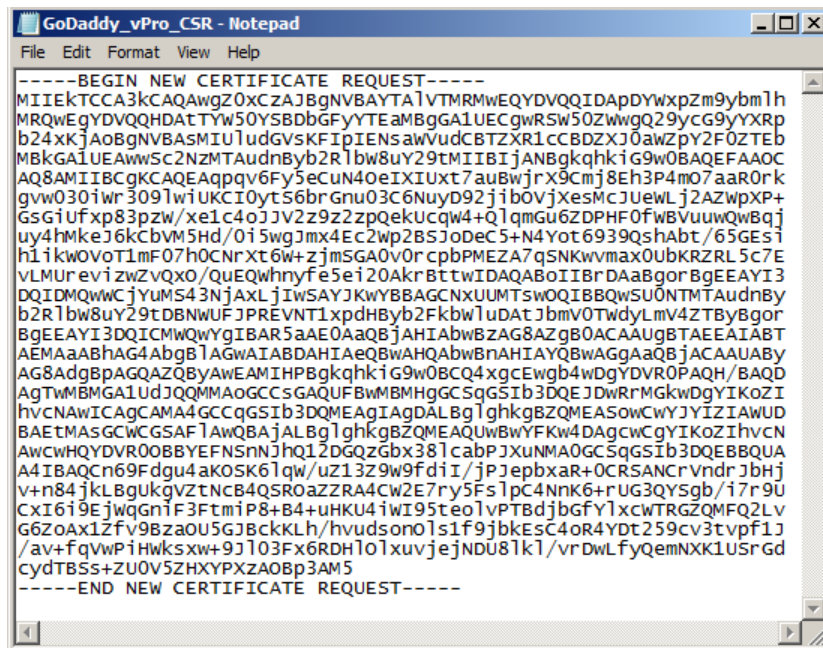
3   Send the Certificate Request to GoDaddy*

1. Set up a GoDaddy* account (link).

2. Go to the GoDaddy web site: www.godaddy.com

3. Login to your GoDaddy* account. Go to the home page and select **Web Security**.
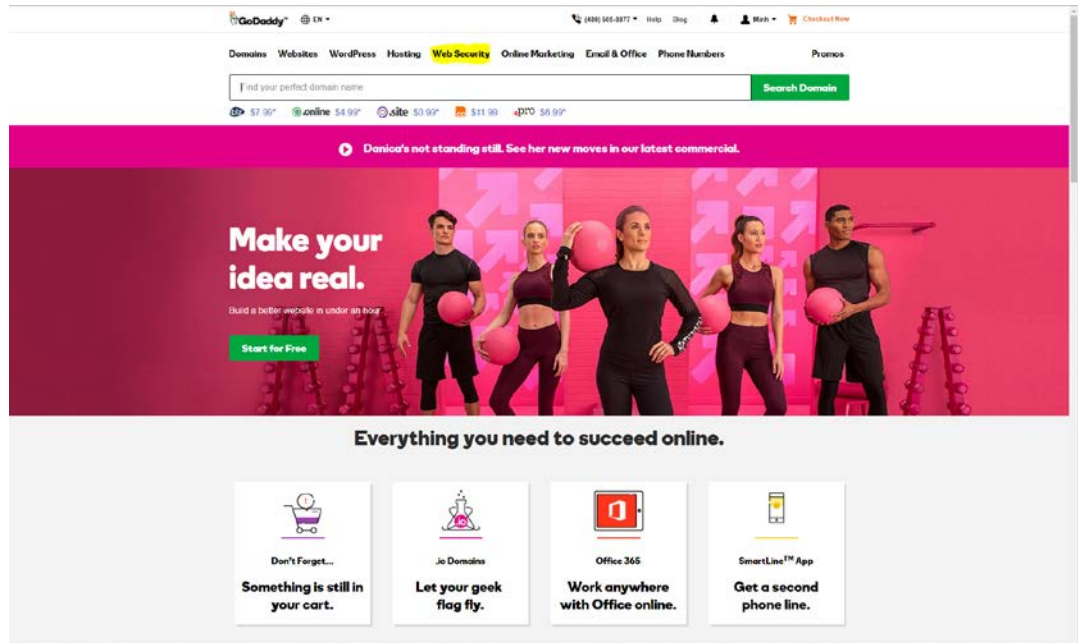
4. From the All Products menu, choose **SSL Certificates**.

5. From the SSL Certificates, choose **Protect one website** and then click **Add to Cart**.

   Note: The certificate it will *not* have the OU of "Intel(R) Client Setup Certificate". It will be issued with the supported OID 2.16.840.1.113741.1.2.3 (this is the unique Intel AMT OID).

6. Choose the **Deluxe SSL OV** and select how long you would like this certificate to be valid before having to renew this certificate. Click **Continue**.

7. Fill in the appropriate payment information and click **Complete Purchase.**

8. You will now see the Order Details. Choose **Go to My Account**.

9. Under **SSL Certificates** section, choose **Set Up** for the certificate you just purchased.

10. Paste your CSR into the available window. Under the Advanced Options, select "This certificate is for Intel® vPro," then click **Next**.

11. Fill out the **Type** page with company information and click **Finished**.

DBA or Legally Registered Assumed Name

Business Registration Jurisdiction Level

State / Province / Territory ▼

Jurisdiction Country/Region

United States ▼

Jurisdiction State/Province/Territory

Oregon ▼

Contact & Organization Address Information

☐ Organizational contact is the same as customer account contact.

First name *

Last name *

Company phone *

Job / Title *

Email *

Phone number *

Country / Region *

United States ▼

Physical Address (Not Mailing / PO Box) *

5200 NE Elam Young Parkway

Address 2

City / Locality *

Hillsboro

State / Province / Territory *

Oregon

Zip / Postal code

97124

☑ I agree to the terms and conditions of the Subscriber Agreement.

Cancel   **Back**   **Finished**

12. On the "Pending Requests" page, and before the certificate is issued, there will be a sequence of verifications, Domain name, Corporation, and Final Phone Call.
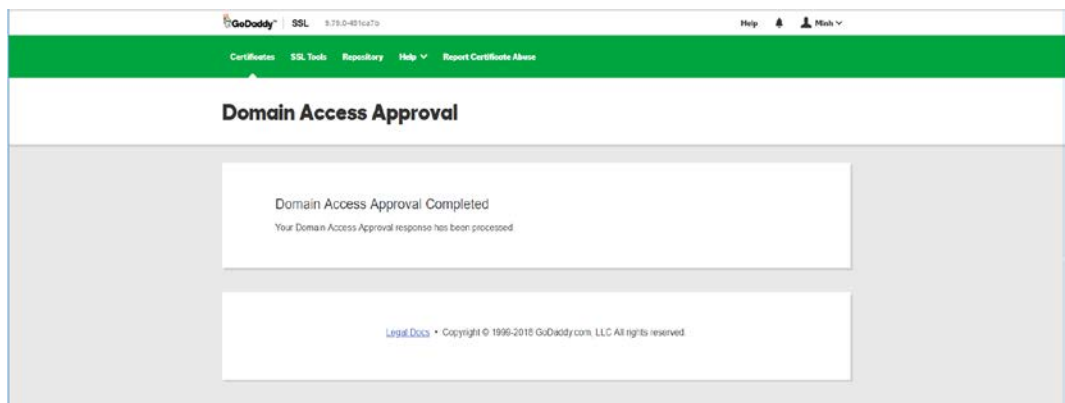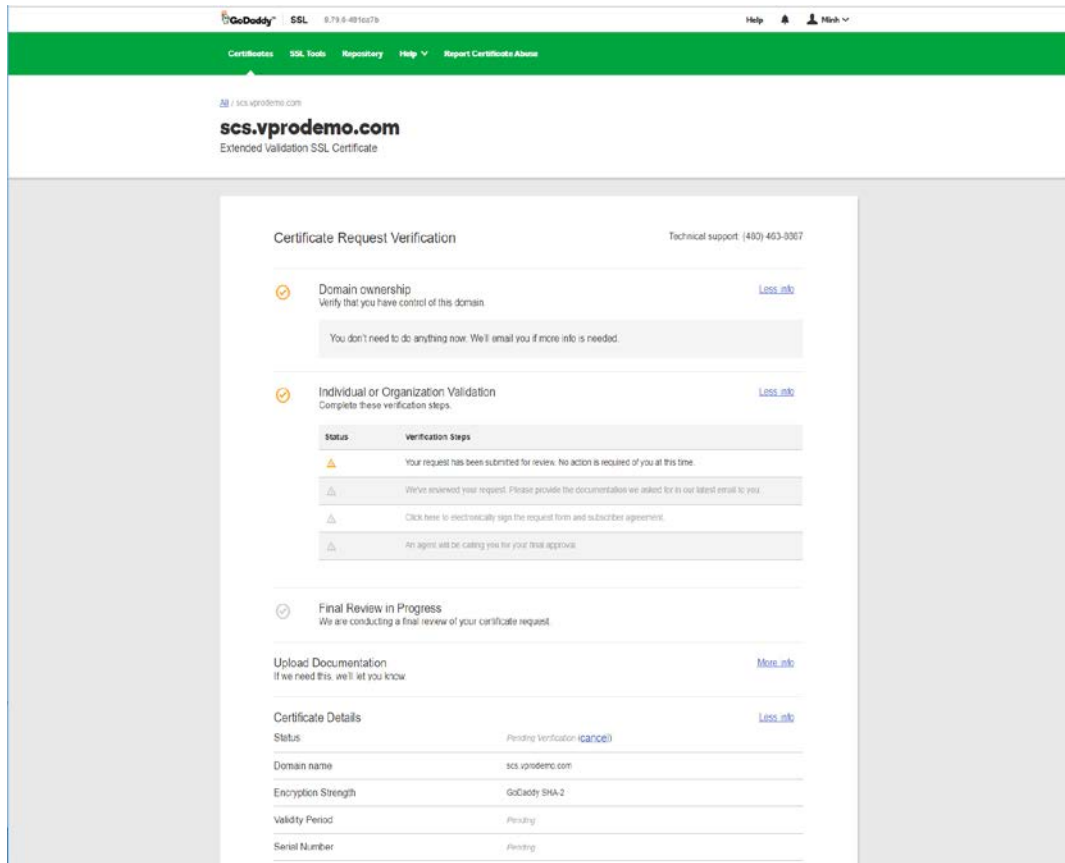
13. Choose **My Account**, choose **Manage** for the certificate you just purchased.

14. From the Certificate Management Options, select **Download**.

15. From the drop down list, **select server type** (IIS MUST be selected to appropriately complete the CSR in later step below), and then choose **Download Zip File**.

16. Save the Zip file on your Remote Configuration Service (RCS) server so you can complete the re-keying of the certificate with the server that generated the CSR.

    In this example, the zip file contains two files:
    - 76dc39f61e43eb9.crt
    - gd-g2_iis_intermidiates.p7b

4   Prepare the Certificate

1. Once you receive the certificate from GoDaddy*, select the **Complete Certificate Request.**
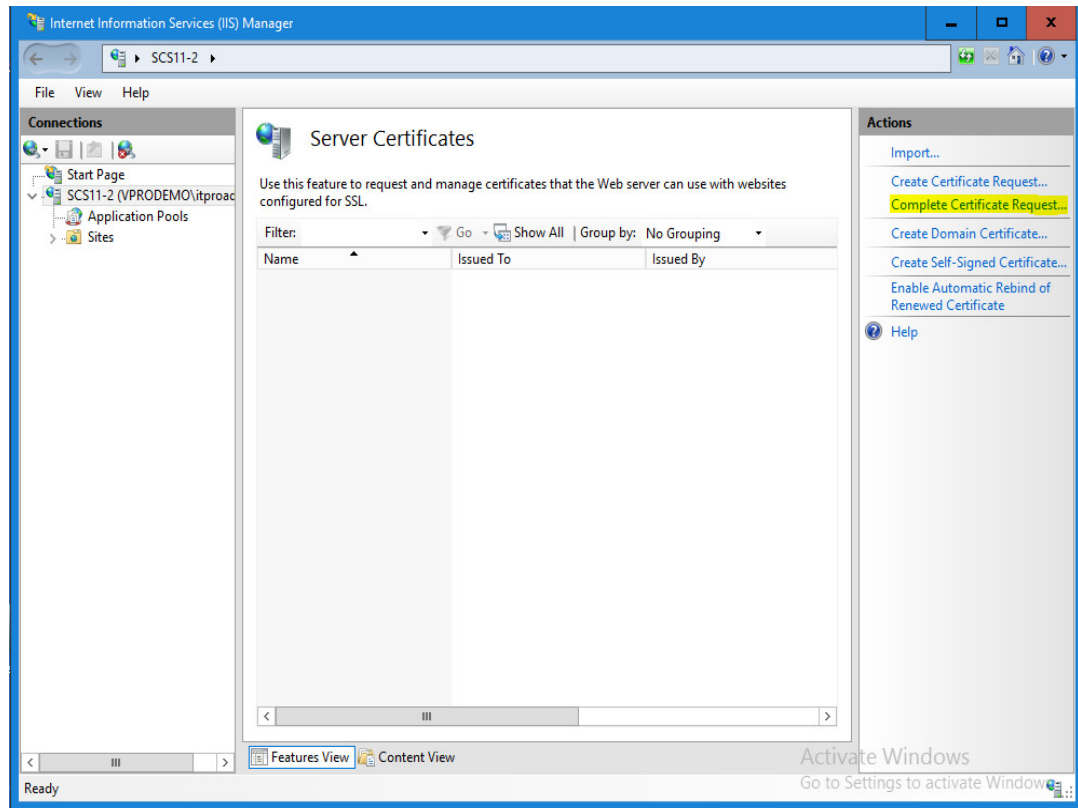
2. Locate the certificate file you received, enter a Friendly name, select Personal and click **OK.**
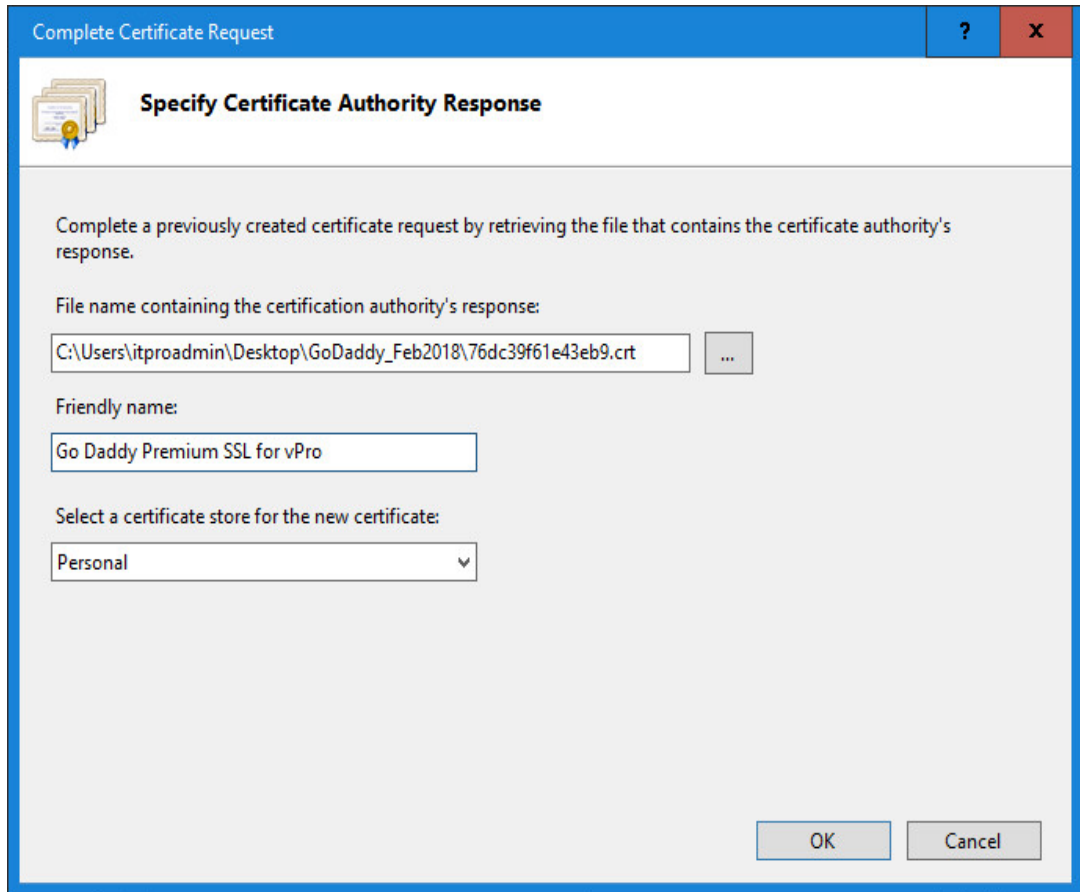
3. You will now see the Intel AMT Setup and Configuration Certificate in your IIS Server. Highlight this certificate and choose **Export...** in the Actions menu.
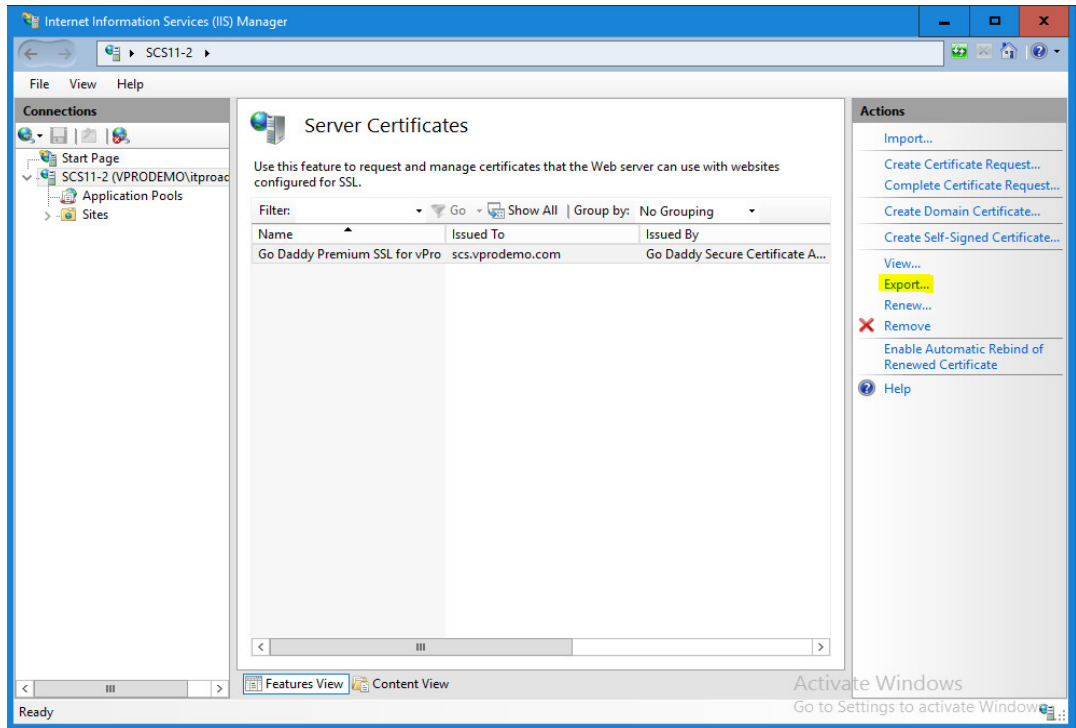
4. Choose a location to export to, name the file, then enter a strong password. (This password will protect the private key.) Re-enter the password to confirm the password.
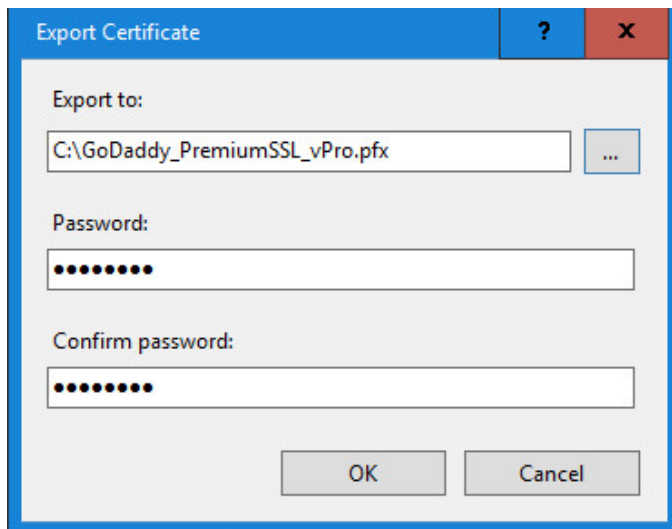
5. Click **OK**.

5 Install the Certificate

This section will show you how to do the following:

- Install the intermediate certificates (the intermediate certificate forms part of the chain from the certificate that you purchased to the root certificate).
- Install the certificate that you purchased
- Verify that the certificate is installed correctly

5.1 Install the Intermediate Certificate

The first step is to import the intermediate certificate into the Current User Intermediate Certificate Authorities Store of the service account for the RCS server.

1. Log on as the service account for the RCS server.

2. Right-click the **gd-g2_iis_intermediates.p7b** file where you saved it. Choose **Install Certificate.**

3. Use the default settings and then choose **Next**.
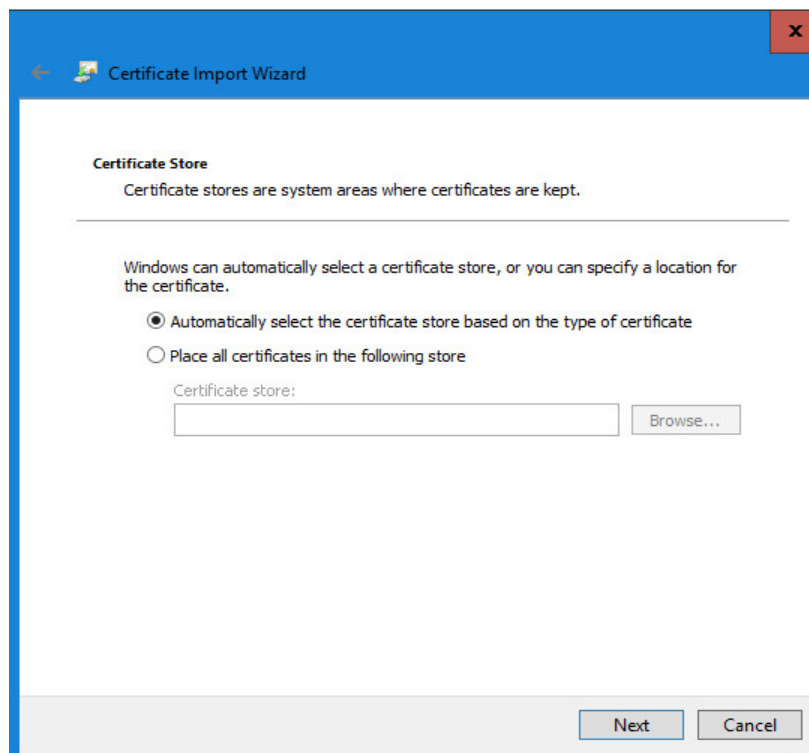
The certificate is now installed in the Intermediate Certificate Authorities store.

4. Download the GoDaddy Class 2 Certificate Authority Root Certificate from https://certs.godaddy.com/repository.

5. Choose the DER format.

⊖ GoDaddy Certificate Chain

Name	File	Certificate Thumbprint (sha256)
GoDaddy Class 2 Certification Authority Root Certificate	gd-class2-root.crt (pem) gd-class2-root.cer (der)	C3 84 6B F2 4B 9E 93 CA 64 27 4C 0E C6 7C 1E CC 5E 02 4F FC AC D2 D7 40 19 35 0E 81 FE 54 6A E4

6. Right-click the gd-class2-root.cer file. Choose **Install Certificate**.

7. Place the certificate in the Trusted Root Certificate Authorities store and then click **Next**.
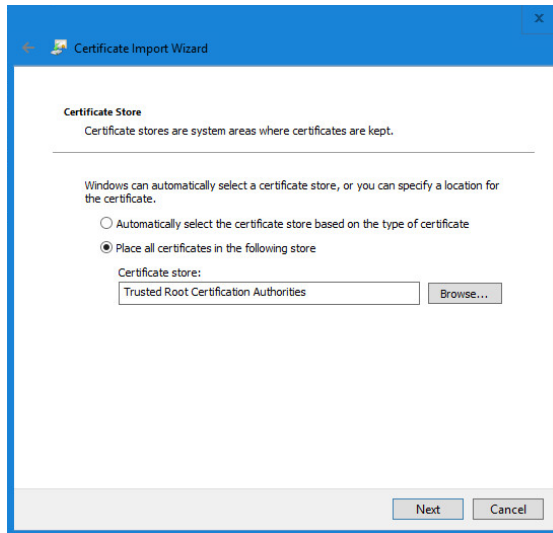
8. Click **Finish**. The certificate is now installed in the Trusted Root Certificate Authorities store.
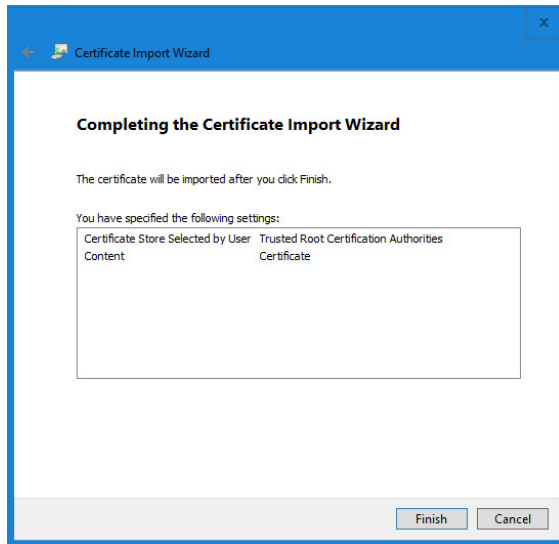
5.2 Install the PFX Certificate

Next, the PFX certificate created earlier will be installed and chained to the intermediate certificate that you installed in the previous step. The .pfx certificate will be imported into the **Current User Personal Certificate Store**.

1. Double-click on the .pfx file where you saved it. Click **Next**.
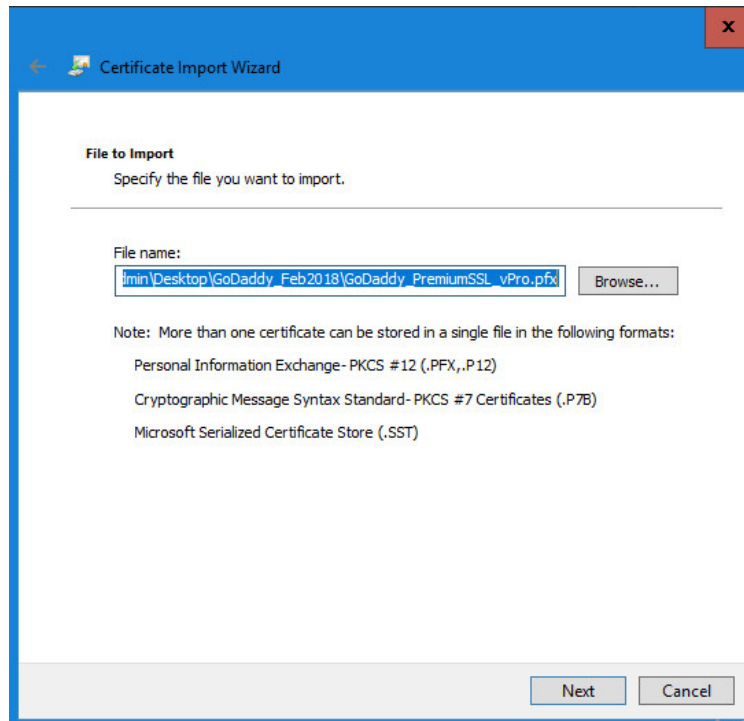
2. Enter in the password and select the **Mark Key as exportable**, and **Include all extended properties** check boxes.
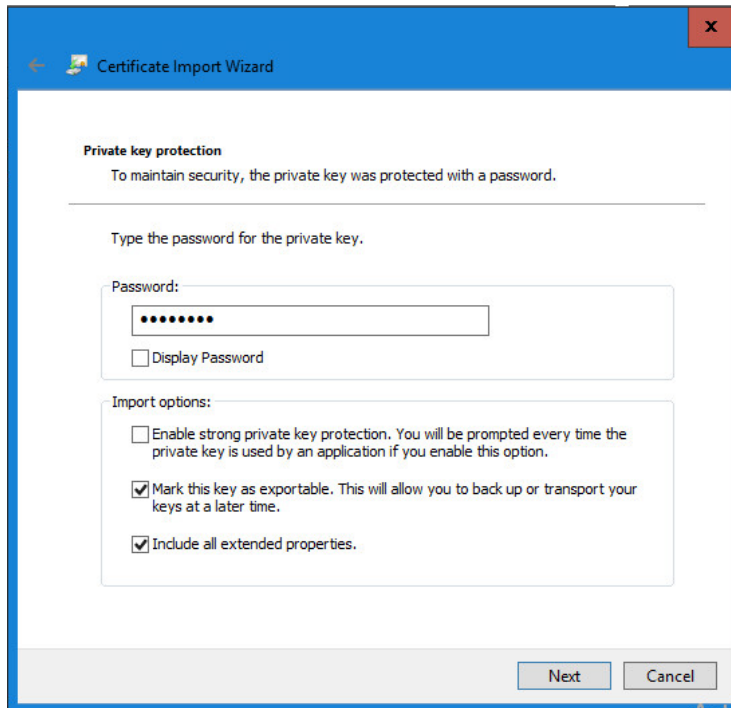
3. Leave the default setting, to automatically select the certificate store. Click **Next**.

4. Click **Finish**.

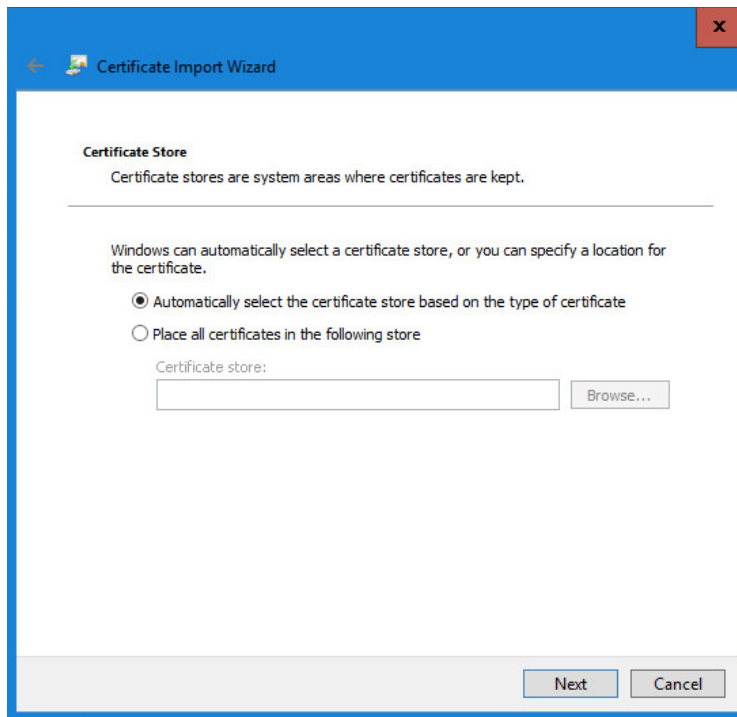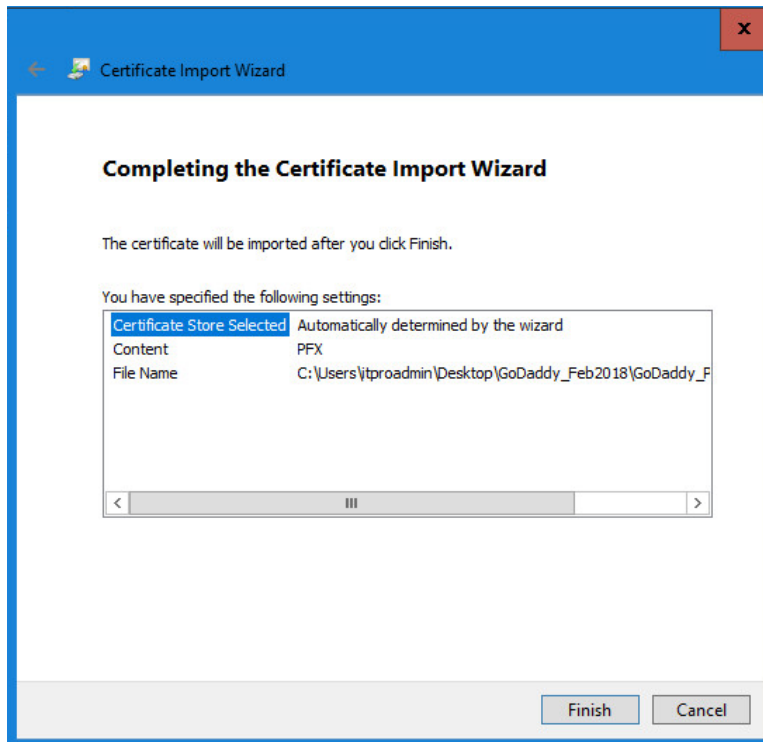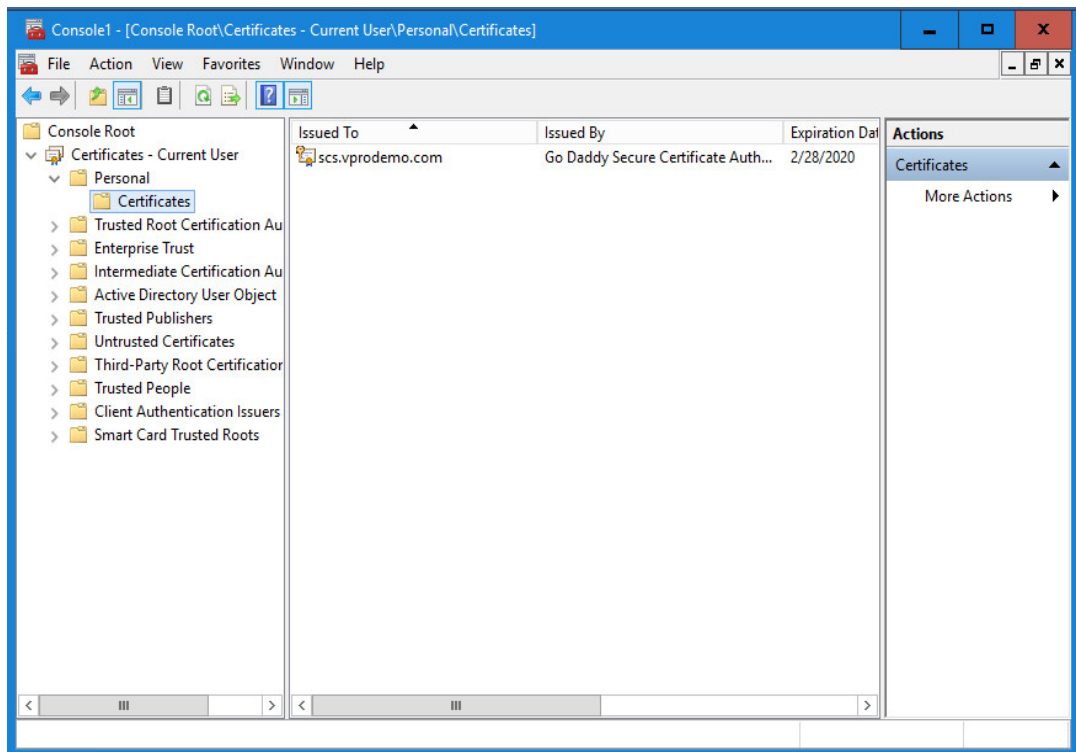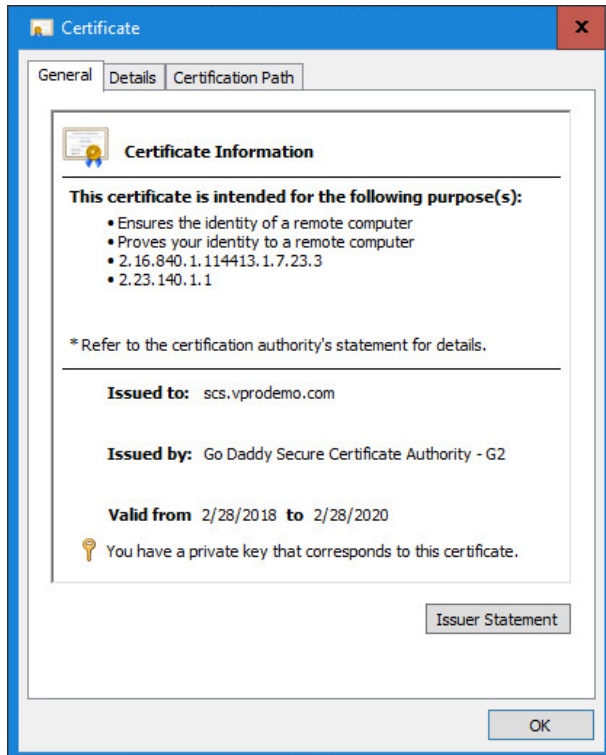The certificate is now installed in the current user's Personal Certificates store.

5.3 Verify the Certificate Chain
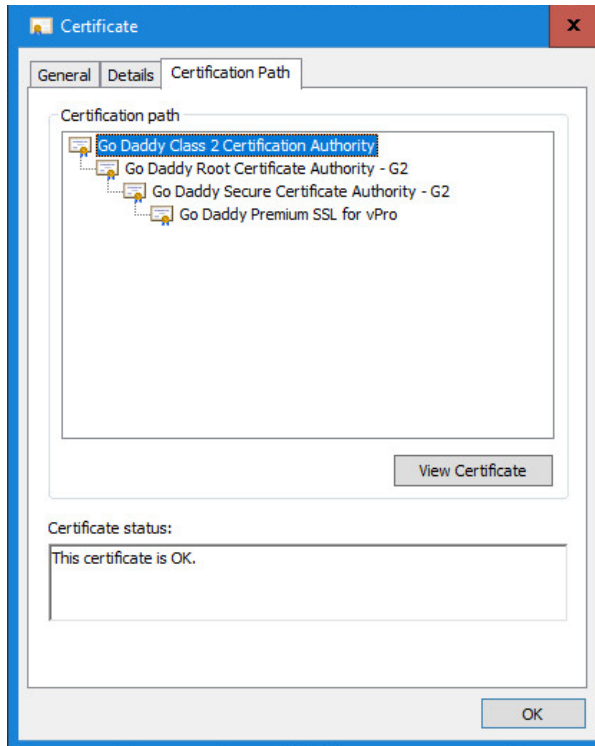
1. To verify the chain, double click **SCS.vprodemo.com**.

2. In the Certificate Information menu, confirm there are no errors. Check that the private key corresponds to the certificate. Click the **Certificate Path** tab.
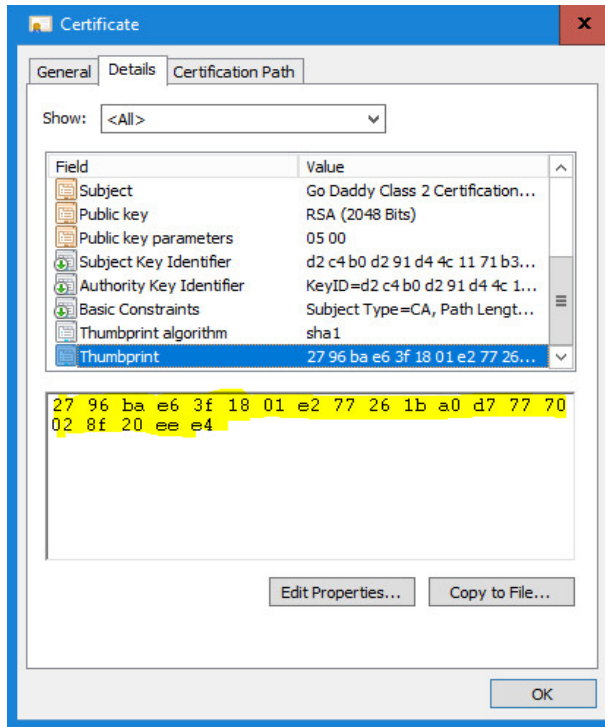
3. Check that the certificate is mapped to the intermediate Certificate Authorities as shown. Double click on the root cert **GoDaddy Class 2 Certificate Authority**.

4. Verify there are no errors with the root certificate and click the **Details tab**.
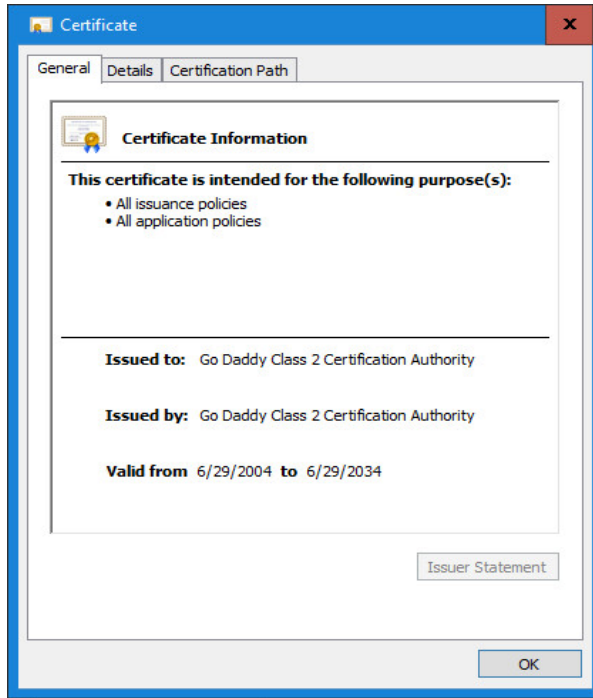
5. In the **Details** tab, scroll down and highlight the **Thumbprint** field. The number must match what is shown below.

This Intel AMT setup and configuration certificate can now be used with the Intel SCS remote configuration service (RCS) for remote configuration and maintenance of PCs with Intel AMT.

6 Verify that it Works

To verify that the certificate works in your environment, create a test environment with one or more Intel AMT capable PCs that have not previously been set up and configured. Follow the instruction in the Intel SCS documentation to try Remote Configuration in Admin Control mode. If successful, then your certificate is installed correctly.