

# 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](http://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](http://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.

© 2018 Intel Corporation. All rights reserved. Intel, the Intel logo, Intel Core, and Intel vPro are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

\* Other names and brands may be claimed as the property of others.

# Contents

<b>1</b>	<b>Preface</b> .....	<b>4</b>
1.1	Document Scope.....	4
1.2	Supported Intel® AMT Versions.....	4
1.3	Intended Audience.....	4
1.4	Prerequisites.....	4
<b>2</b>	<b>Purchase a GoDaddy* Certificate</b> .....	<b>5</b>
2.1	Create a Certificate Signing Request (CSR).....	5
<b>3</b>	<b>Send the Certificate Request to GoDaddy*</b> .....	<b>10</b>
<b>4</b>	<b>Prepare the Certificate</b> .....	<b>23</b>
<b>5</b>	<b>Install the Certificate</b> .....	<b>26</b>
5.1	Install the Intermediate Certificate.....	26
5.2	Install the PFX Certificate.....	29
5.3	Verify the Certificate Chain.....	33
<b>6</b>	<b>Verify that it Works</b> .....	<b>38</b>

## 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 Management 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:

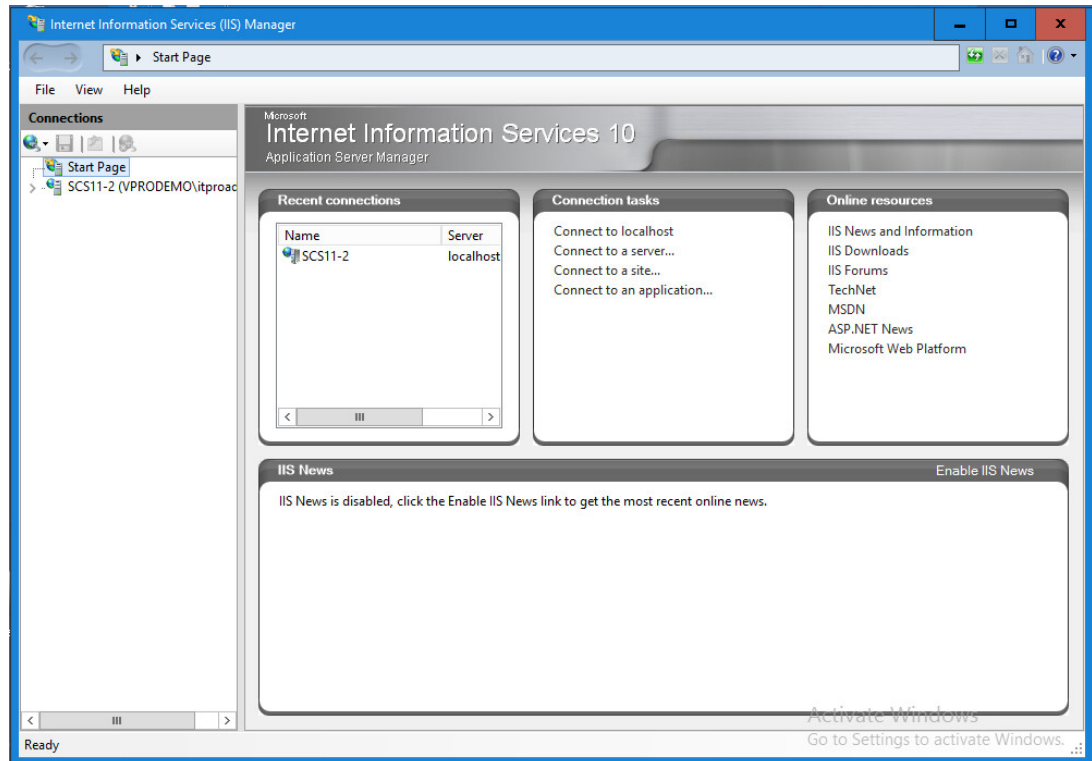
- Intel SCS Remote Configuration Service (RCS) installed on a supported Microsoft\* operating system
- One or more domain names for your network (Microsoft\* Workgroups are not supported)
- Microsoft\* Internet Information Service (IIS) running on the server that is hosting the Remote Configuration Service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

## 2 Purchase a GoDaddy\* Certificate

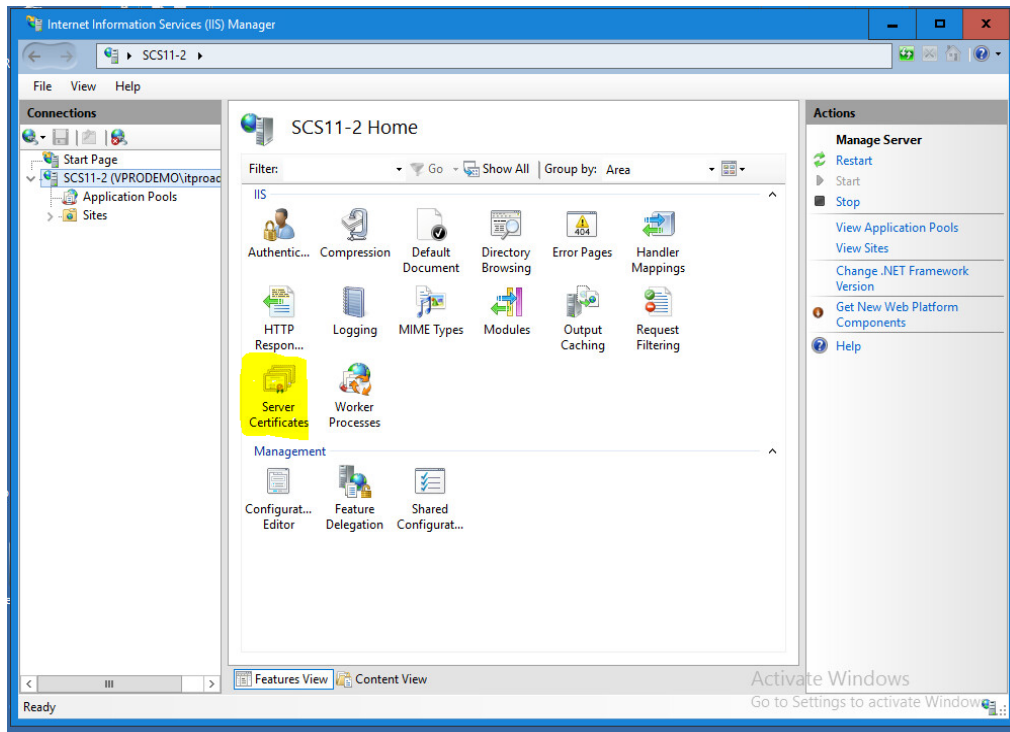
The following instructions were captured using Microsoft\* Internet Information Services (IIS) for Windows\* Server 2016.

### 2.1 Create a Certificate Signing Request (CSR)

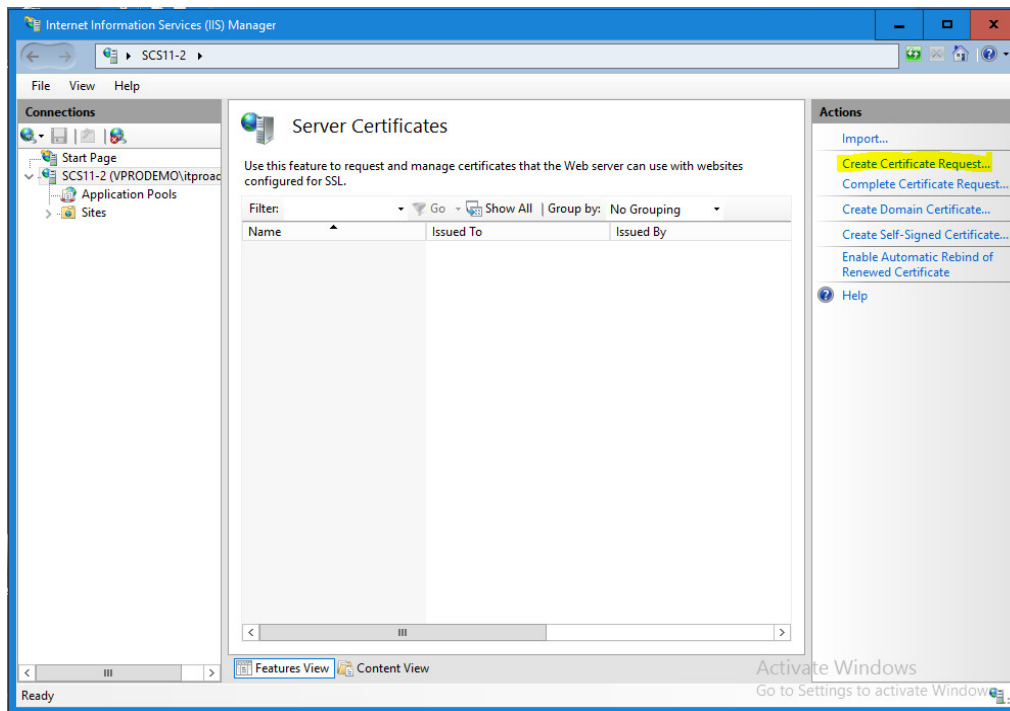
1. On your Intel SCS Remote Configuration Server (RCS), open **Programs->Administrative Tools->Internet Information Services (IIS) Manager**.



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**.

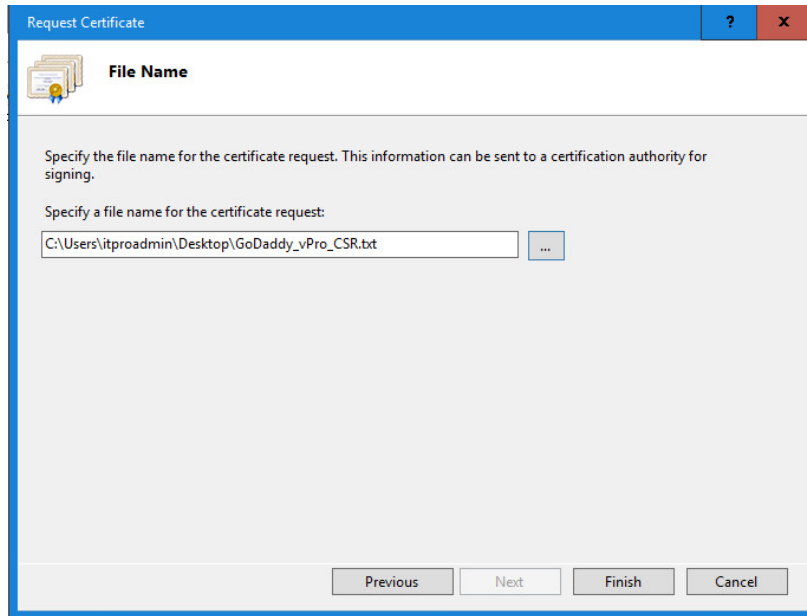
The screenshot shows the 'Request Certificate' dialog box with the 'Distinguished Name Properties' tab selected. The dialog has a blue title bar with a question mark and a close button. Below the title bar is a header area with a certificate icon and the title 'Distinguished Name Properties'. The main area contains a text box with the instruction: 'Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.' Below this are several input fields: 'Common name' (scs.vprodemo.com), 'Organization' (Intel Corporation), 'Organizational unit' (Intel), 'City/locality' (Santa Clara), 'State/province' (California), and 'Country/region' (US). At the bottom are four buttons: 'Previous', 'Next', 'Finish', and 'Cancel'.

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

The screenshot shows the 'Request Certificate' dialog box with the 'Cryptographic Service Provider Properties' tab selected. The dialog has a blue title bar with a question mark and a close button. Below the title bar is a header area with a certificate icon and the title 'Cryptographic Service Provider Properties'. The main area contains a text box with the instruction: 'Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.' Below this are two dropdown menus: 'Cryptographic service provider' (Microsoft RSA SChannel Cryptographic Provider) and 'Bit length' (2048). At the bottom are four buttons: 'Previous', 'Next', 'Finish', and 'Cancel'.

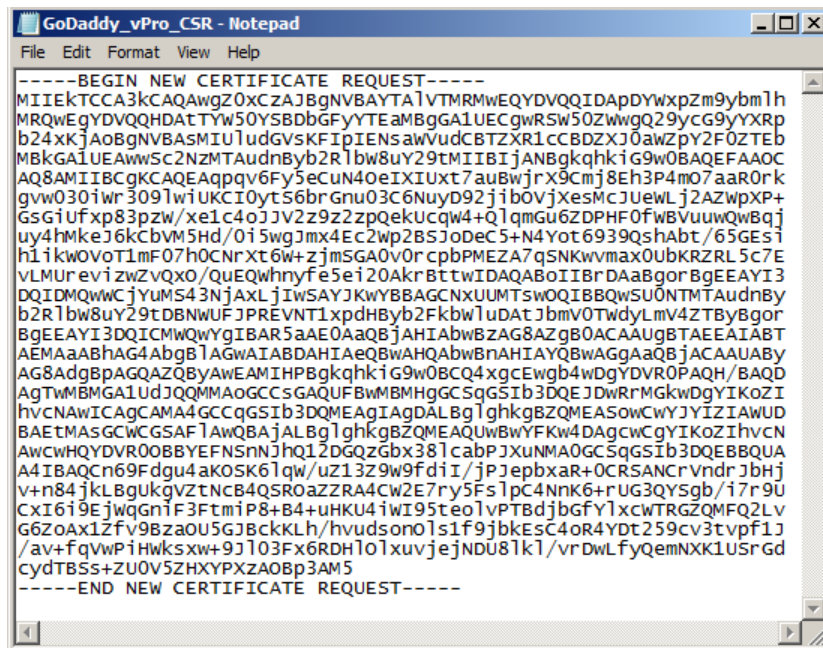


- Click **Next**, and in the next panel, click the browse (...) button to select a location. Enter a file name to store the certificate request and then choose **Submit**.



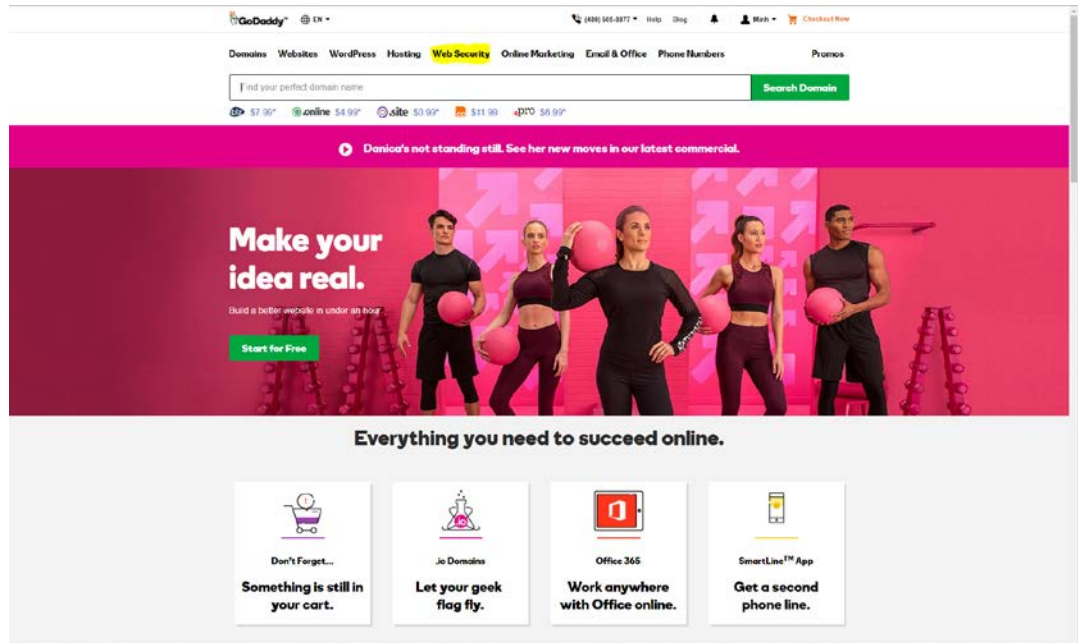
- Click **Finish**.

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](http://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**.

The screenshot shows the GoDaddy website's navigation and product categories. The top navigation bar includes 'GoDaddy', 'EN', 'Contact Us 24/7', 'Help', 'Blog', 'Minh', and 'Checkout Now'. Below this is a secondary navigation bar with 'Domains', 'Websites', 'WordPress', 'Hosting', 'Web Security', 'Online Marketing', 'Email & Office', 'Phone Numbers', and 'Promos'. The 'Web Security' section is highlighted in green and contains the following text: 'Web Security', 'For your business to succeed, customers need to trust that you'll protect them from viruses, hackers and identity thieves. Count on our security products to keep your website secure, your visitors safe and your business growing.', and a 'Learn More' button. To the right of this text is a list of SSL Certificate types: 'SSL Certificates - On Sale' (circled in red), 'Extended Validation SSL Certificates', 'Organizational Validation SSL Certificates', 'SAN SSL Certificate', 'Wildcard SSL Certificates', and 'Code Signing Certificate'. Further right is a 'Website Protection' section with 'Website Security', 'Website Backup - New', and 'Express Malware Removal - Fix Hacked Sites'. Below the green section is a yellow banner with the text 'No credit card required.' and an image of a person. At the bottom, there are four promotional cards: 'Don't Forget... Something is still in your cart.', 'Web Hosting Trust the world's #1 web host.', 'Office 365 Work anywhere with Office online.', and '.info Sale! Now \$2.99\*/1st yr Show the world what you know.'. A blue button at the bottom right says 'Get Online in 3 Steps'.

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).

GoDaddy EN

Contact Us 24/7 Help Blog

Domains Websites WordPress Hosting Web Security Online Marketing Email & Office Phone Numbers Promos

SSL Certificates SSL Certificates Extended Validation SSL Certificates Organizational Validation SSL Certificates SAN SSL Certificate Wildcard SSL Certificates Code Signing Certificate

Find out more about Google's *Not-Secure* initiative and [why it matters to you](#).

SSL Certificates

**Saving the internet, one green lock at a time.**

If you don't have the little green lock from a trusted SSL certificate, Google Chrome will tag your site as *Not Secure*.

Protect one website	Protect multiple websites	Protect all subdomains
UCC/SAN SSL	UCC/SAN SSL	Wildcard SSL
As low as <b>\$59.99/yr</b> On sale - <b>Save 20%</b> \$74.99/yr when you renew <sup>4</sup>	As low as <b>\$135.99/yr</b> On sale - <b>Save 20%</b> \$169.99/yr when you renew <sup>4</sup>	As low as <b>\$279.99/yr</b> On sale - <b>Save 20%</b> \$349.99/yr when you renew <sup>4</sup>
<b>Add to Cart</b>	<b>Add to Cart</b>	<b>Add to Cart</b>
Secures one website Strong SHA2 & 2048-bit encryption Available in DV, OV and EV SSL Certificates EV SSL turns browser bar green Boosts your site's Google ranking McAfee SECURE trustmark	Secures up to five websites Strong SHA2 & 2048-bit encryption Available in DV, OV and EV SSL Certificates EV SSL turns browser bar green Boosts your site's Google ranking McAfee SECURE trustmark	Secures one website and all its subdomains Strong SHA2 & 2048-bit encryption Available in DV and OV SSL Certificates Boosts your site's Google ranking McAfee SECURE trustmark

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**.

GoDaddy

Contact Us 24/7 • Help • Blog • • • Checkout Now

Domains Websites WordPress Hosting Web Security Online Marketing Email & Office Phone Numbers Promos

You've selected to Protect One Website

Select your certificate

Standard SSL DV **\$74.99/yr**

- Best for blogs and social websites
- Validates domain ownership
- USD \$100,000 warranty

Deluxe SSL OV **\$129.99/yr**

- Best for businesses and organizations
- Validates domain ownership and organization
- USD \$250,000 warranty

Premium SSL EV **\$149.99/yr**  
~~\$199.99/yr~~  
On Sale (Save 25%)

- Best for eCommerce websites
- Validates domain ownership and highest level of organization authentication
- High-assurance green address bar:  
 [GoDaddy, Inc. | US | https://](https://www.godaddy.com)
- USD \$1,000,000 warranty

Select Term Length

Lock in your savings with a multi-year term.

1 year **\$129.99/yr**

2 years **\$103.99/yr**  
~~\$129.99/yr~~  
On Sale (Save 20%)

Secure your site

Add malware scan and removal **\$6.99/mo**

Defend your site against hackers and malware with automatic daily scans and guaranteed cleanup.

**Continue**

Order summary

Protect 1 Website	\$129.99
Deluxe SSL OV	1 year
<b>Total</b>	<b>\$129.99</b>

Subtotal does not include applicable taxes.  
Term lengths adjustable prior to checkout.

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

The screenshot shows the GoDaddy checkout process. At the top, there's a navigation bar with the GoDaddy logo, language settings (EN), and links for Contact Us, Help, Blog, and a shopping cart icon. Below this is a secondary navigation bar with categories like Domains, Websites, WordPress, etc. A progress bar indicates four steps: Sign In, Payment, Billing Information, and Complete. The 'Payment' section shows a card ending in 2084 and a PayPal option. The 'Billing Information' section lists the user as Minh Pham from Intel Corporation. The 'Your Items' section displays a 'Deluxe (OV) SSL' certificate for \$129.99. A summary table shows a subtotal of \$129.99, taxes of \$0.00, and a total of \$129.99. A large green 'Complete Purchase' button is prominent. Below it, a disclaimer states that clicking 'Complete Purchase' implies agreement to GoDaddy's Terms & Conditions and Privacy Policy. A 'Chat Now' button is also visible. On the left, there are 'Recommended for you' sections for 'Search Engine Visibility' and 'Add Domain'.

**GoDaddy** EN Contact Us 24/7 Help Blog 1 Minh Checkout Now

Domains Websites WordPress Hosting Web Security Online Marketing Email & Office Phone Numbers Promos

**Purchase** ✓ Sign In ✓ Payment ✓ Billing Information 4 Complete

**Payment**

Ending with 2084

[+ Add payment](#) or [PayPal](#)

Your payment is being processed in United States.

**Billing Information**

Minh Pham  
Intel Corporation  
2200 Mission College Blvd, Santa Clara, California 95054, United States [Edit](#)

**Your Items**

Deluxe (OV) SSL \$129.99  
Quantity: 1 Certificate  
1 Year  
Renews at \$129.99/yr

[View offer disclaimers](#) [Empty Cart](#)

Subtotal \$129.99  
**Taxes & Fees** \$0.00  
Round up for charity? (optional) [Add](#)

**Total** \$129.99

[Have a promo code?](#)

**Complete Purchase**

By clicking "Complete Purchase" you agree to GoDaddy's [Terms & Conditions](#) and [Privacy Policy](#), and consent to enroll your product(s) in our automatic renewal service, which can be cancelled at any time via the Renewals and Billing page. Automatic renewals are billed to your default payment method until cancelled.

[Chat Now](#)

**Recommended for you**

**Search Engine Visibility** \$1.99/mo  
~~\$6.99/mo~~  
• Improve your search engine ranking  
• Increase visitors and sales  
• Simple one-click site submission [Add](#)

**Add Domain**  
Find your perfect domain [Search](#)

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

The screenshot displays the GoDaddy website interface. At the top, there is a navigation bar with the GoDaddy logo, a phone number (480) 505-8877, and links for Help, Blog, and a user profile. Below this is a secondary navigation menu with categories: Domains, Websites, WordPress, Hosting, Web Security, Online Marketing, Email & Office, Phone Numbers, and Promos.

The main content area is titled "Receipt" and includes the text: "A copy of your receipt below has been sent to minh.t.pham@intel.com". It features a table with order details:

Order	
Date	February 21, 2018
Number	1287614299
Payment	Ending with 2034
<hr/>	
TOTAL	\$199.98

Below the table is a "Print receipt" link. To the right of the receipt, there is a "Manage Products" section with the text: "All your purchased products are available in 'My Account'", followed by a green "Go to My Account" button. Below that is a "Want to keep shopping?" section with a green "Keep Shopping" button. At the bottom of this section is a "Need help?" link and the text "24/7 Support: (480) 505-8877".

A green banner below the receipt area contains the text: "Need help? Call our award-winning support team 24/7 at (480) 505-8877".

The footer is dark and contains several columns of links:

- About GoDaddy:** About Us, Contact Us, Newsroom, Investor Relations, Careers, Corporate Responsibility, GoDaddy Store, Legal, GoDaddy Blog.
- Support:** Product Support, Compliance, Report Abuse.
- Resources:** Webmail, WHOIS, ICANN Certification, Tools for Pros, Redem. Code, Product Catalog, Site Map.
- Partner Programs:** Affiliates, Reseller Programs, GoDaddy Pin.
- Account:** My Account, My Renewals, Create Account.
- Shopping:** Domains, Websites, WordPress, Hosting, Web Security, Online Marketing, Email & Office, Phone Numbers, Promos.

At the bottom of the footer, there is a sign-up form for news and special offers with an "Email Address" input field and a "Submit" button. To the right, there are social media icons for Facebook, Twitter, and YouTube, and a "Follow Us" link. The footer also includes "United States - English" and "USD" indicators.

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

The screenshot shows the GoDaddy My Account dashboard. At the top, there is a green header with the GoDaddy logo and 'My Account'. Below the header, there are navigation links for 'My Products' and 'Account Settings'. A red notification banner at the top states: 'One or more of your products failed billing. Resolve.' with an 'Update' button. The main content area is divided into sections. The 'Domains' section shows 'mpham.us' with an 'Add domain' button and a search bar. The 'SSL Certificates' section lists several certificates. The first certificate is 'Deluxe (OV) SSL' for 'vprodomain.vprodemo.com', which is expired on 5/12/2018 and has 'Options' and 'Manage' buttons. The second certificate is 'Deluxe (OV) SSL' for 'vprodemo.com', also with 'Options' and 'Manage' buttons. The third certificate is 'Standard SSL' with 'Options' and 'Set up' buttons. The fourth certificate is 'Standard SSL' with 'Options' and 'Set up' buttons. The fifth certificate is 'Standard SSL' with 'Options' and 'Set up' buttons. The sixth certificate is 'Deluxe (OV) SSL' for 'unite3.vprodemo.com' with 'Options' and 'Manage' buttons. The seventh certificate is 'Deluxe (OV) SSL' with 'Options' and 'Set up' buttons, where the 'Set up' button is circled in red. The eighth certificate is 'Premium (EV) SSL' with 'Options' and 'Set up' buttons. Below the SSL Certificates section is an 'Additional Products' section.



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

1 Choose Website 2 Organization Info 3 You're Done!

### Choose website

**Provide a certificate signing request (CSR)**  
Certificate Signing Request (CSR) [Learn more](#)

```
-----BEGIN CERTIFICATE REQUEST-----
4WU2q1VYQhmwF7oVFczXlw1DrwHvjB8gWnZGVzwKKoAEJlcyO
iowxpm
-----END NEW CERTIFICATE REQUEST-----
```

Domain Name (based on CSR):  
scs.vprodemo.com

### Domain ownership

We'll send an email with a unique code to your address on file. Follow its instructions to verify you have website or DNS control over the selected domain. [More info](#)

AND

We can send domain ownership instructional emails to one or both of the following:

- Contacts listed in the domain's public WHOIS database record
- Email addresses: admin@[domain], administrator@[domain], hostmaster@[domain], postmaster@[domain], and webmaster@[domain]

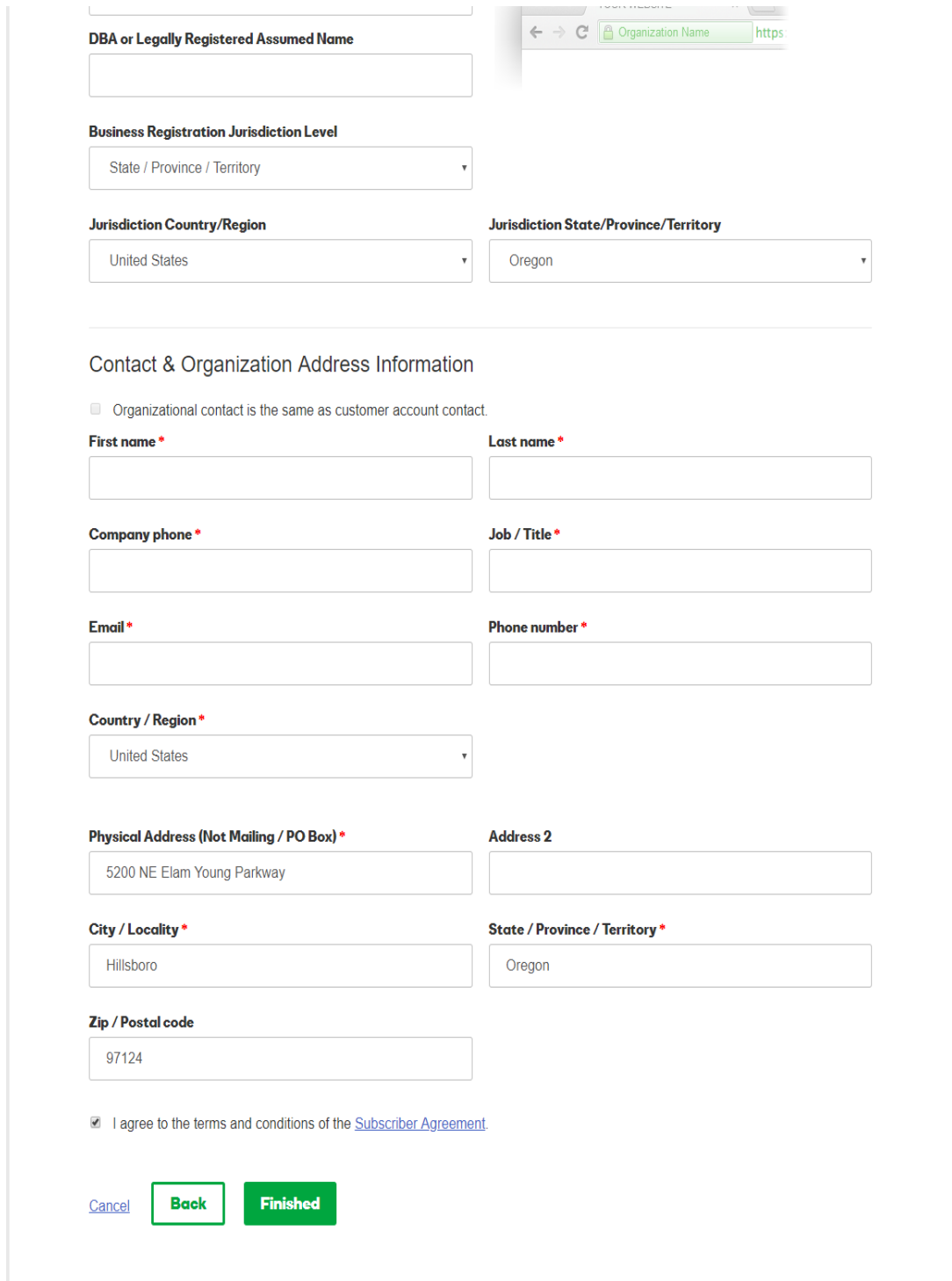
[Hide advanced options](#)

Signature Algorithm [Learn more](#)  
GoDaddy SHA-2

This certificate is for Intel® vPro [Learn more](#)

Cancel **Next**

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



DBA or Legally Registered Assumed Name

Business Registration Jurisdiction Level

Jurisdiction Country/Region

Jurisdiction State/Province/Territory

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 \*

Physical Address (Not Mailing / PO Box) \*

Address 2

City / Locality \*

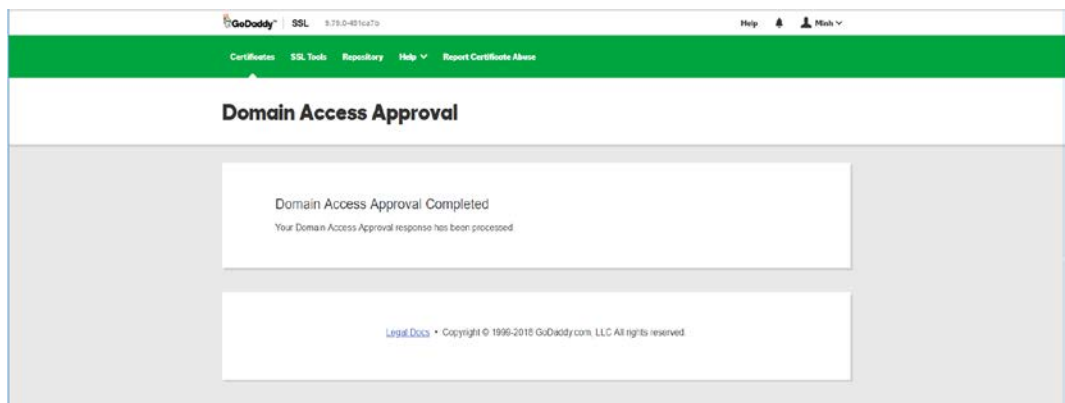
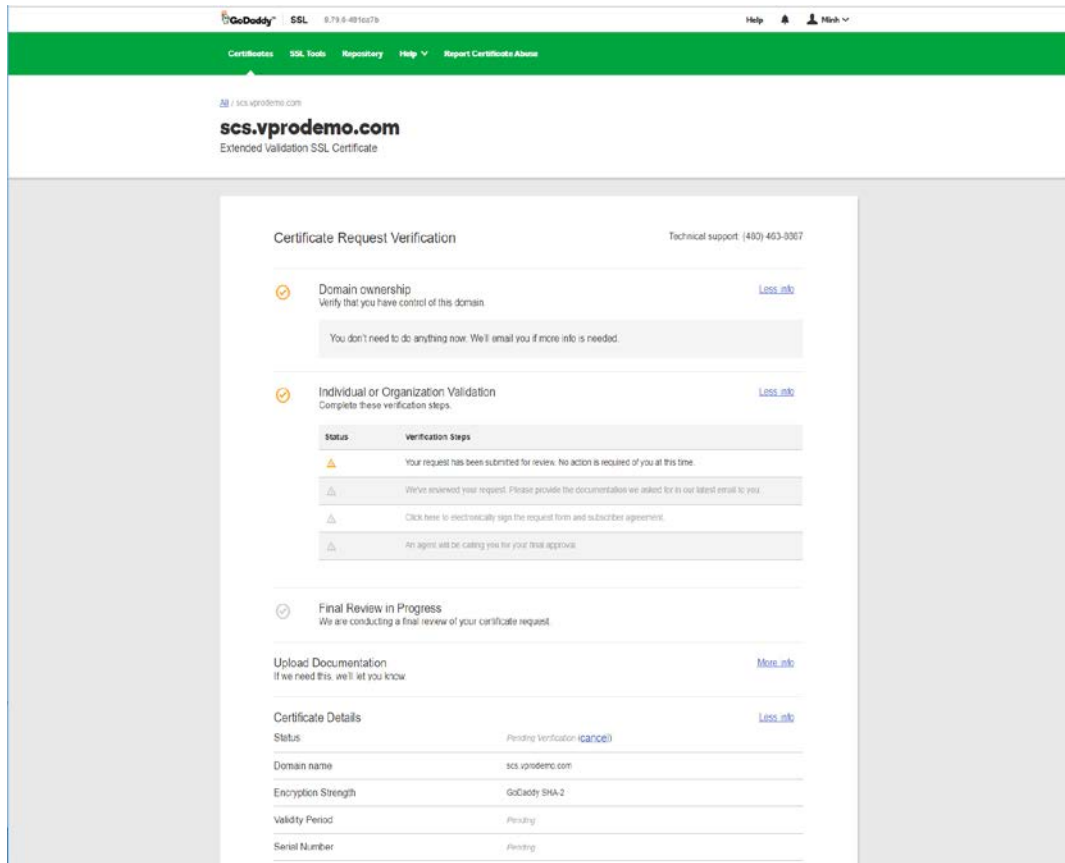
State / Province / Territory \*

Zip / Postal code

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.

The screenshot shows the GoDaddy 'My Account' dashboard. At the top, there is a green navigation bar with 'My Products' and 'Account Settings' on the left, and '24/7 Support (480) 505-8877' on the right. Below this, the 'Domains' section is visible, featuring a search bar for 'minhpham.us' and a search input field. The main content area is titled 'SSL Certificates' and lists four certificates:

- Deluxe (OV) SSL** for vprodomain.vprodemo.com, with an expiration date of 5/11/2018. Buttons for 'Options' and 'Manage' are present.
- Deluxe (OV) SSL** for vprodemo.com, with buttons for 'Options' and 'Manage'.
- Standard SSL**, with buttons for 'Options' and 'Set up'.
- Deluxe (OV) SSL** for scs.vprodemo.com, with buttons for 'Options' and 'Manage'. The 'Manage' button is circled in red.

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

The screenshot shows the GoDaddy SSL management interface for the domain **scs.vprodemo.com**. At the top, there is a green navigation bar with links for Certificates, SSL Tools, Repository, Help, and Report Certificate Abuse. Below this, the domain name and 'Deluxe SSL Certificate' are displayed. A purple banner at the top of the main content area promotes the McAfee SECURE trustmark. Below the banner are three main action buttons: **Download** (circled in red), **Rekey & Manage**, and **History**. The **Download** button features a download icon. To the right of these buttons is a section titled 'Display your SSL Certificate security seal', which includes a dropdown menu for 'Type' (set to McAfee), a 'Preview' section showing the McAfee SECURE logo, and a 'Code' section with an 'Activate' link. Below the buttons is a 'Certificate Details' table with the following information:

Certificate Details <a href="#">Less info</a>	
Status	Certificate issued ( <a href="#">Revoke</a> )
Domain name	scs.vprodemo.com
Encryption Strength	GoDaddy SHA-2
Validity Period	2/28/2018 - 2/28/2020
Serial Number	07:6d:c3:9f:61:e4:3e:b9

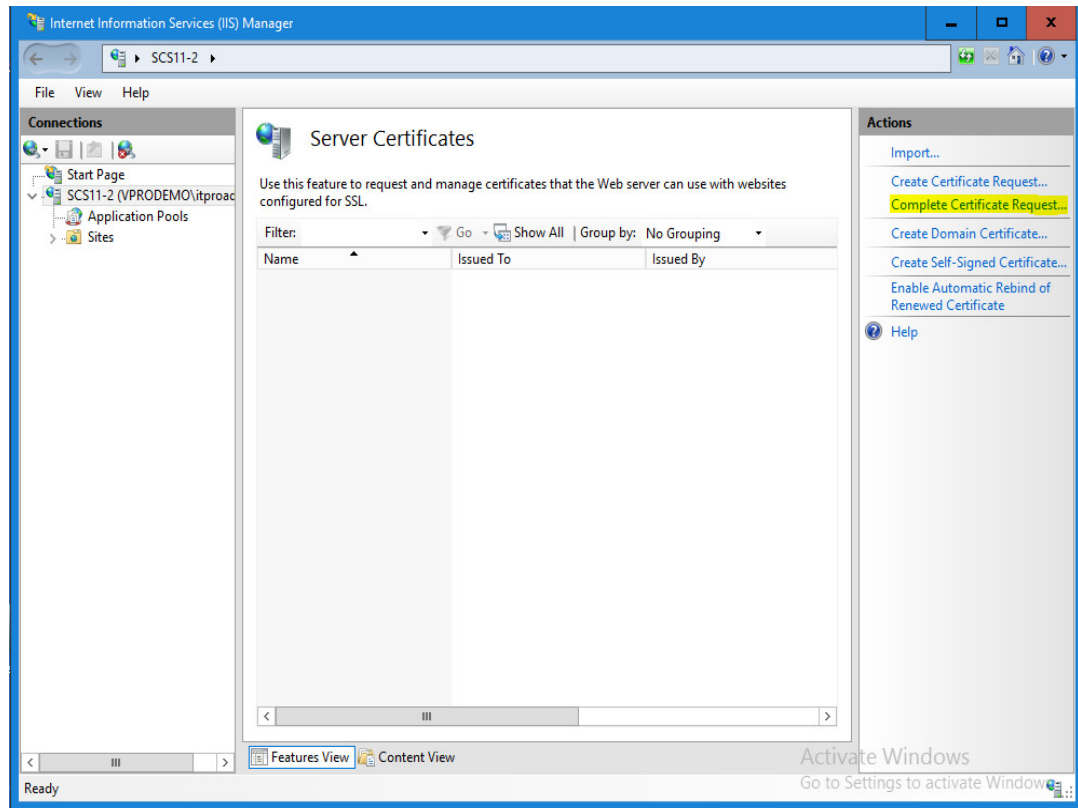
15. From the drop down list, **select server type (IIS MUST be selected to appropriately complete the CSR in later step below)**, and then choose **Download Zip File**.

The screenshot shows the GoDaddy SSL management interface. At the top, there is a navigation bar with 'Certificates', 'SSL Tools', 'Repository', 'Help', and 'Report Certificate Abuse'. Below this, the domain 'scs.vprodemo.com' is displayed with the text 'Deluxe SSL Certificate'. A purple banner at the top of the main content area contains a message about McAfee SECURE. The main content is divided into two columns. The left column is titled 'Download Certificate' and contains instructions on how to download and install the certificate. Below the instructions is a 'Server type' dropdown menu with 'IIS' selected, and a green 'Download Zip File' button. The right column is titled 'Display your SSL Certificate security seal' and contains instructions on how to display the seal. It features a 'Type' dropdown menu with 'McAfee' selected, a preview of the McAfee SECURE seal, and a 'Code' field with an 'Activate' link.

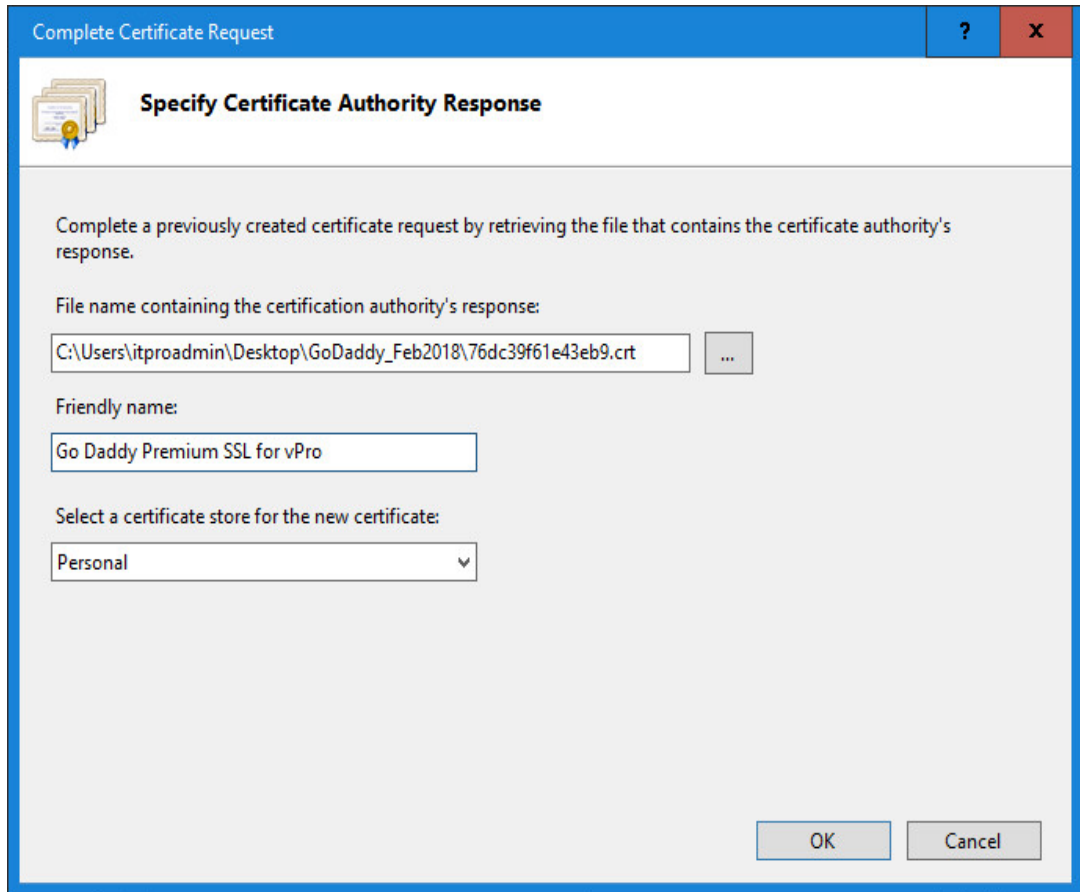
16. Save the Zip file on your Remote Configuration Service (RCS) server so you can complete the re-keying of the certificate with the server that generated the CSR.
- In this example, the zip file contains two files:
- 76dc39f61e43eb9.crt
  - gd-g2\_iis\_intermediates.p7b

## 4 Prepare the Certificate

1. Once you receive the certificate from GoDaddy\*, select the **Complete Certificate Request**.

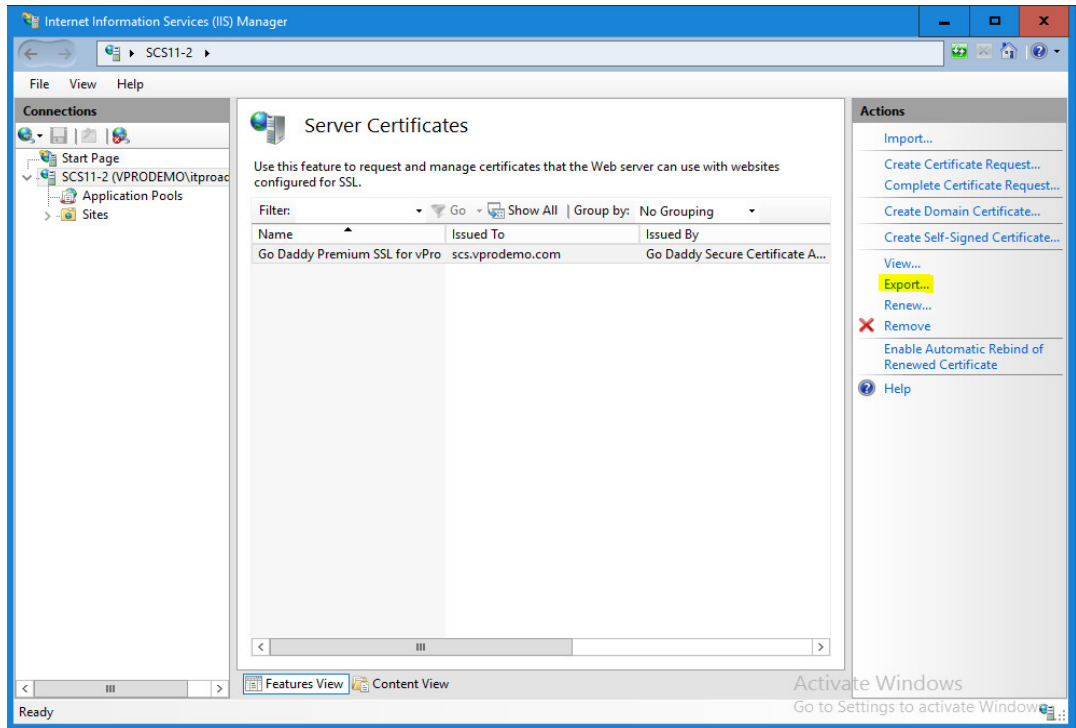


2. Locate the certificate file you received, enter a Friendly name, select Personal and click **OK**.

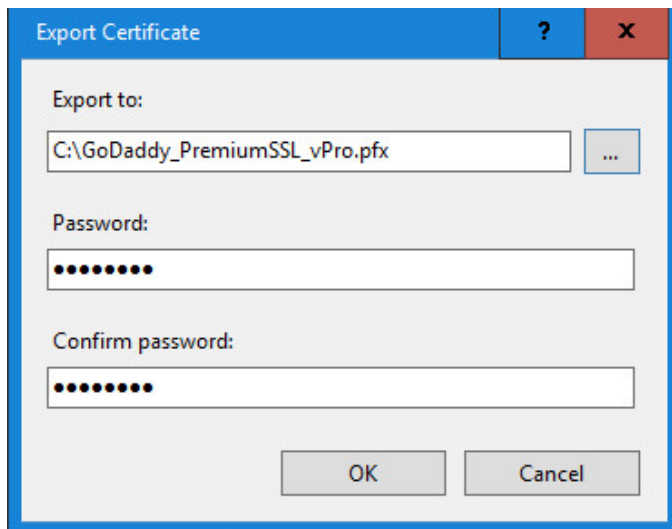




3. You will now see the Intel AMT Setup and Configuration Certificate in your IIS Server. Highlight this certificate and choose **Export...** in the Actions menu.



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

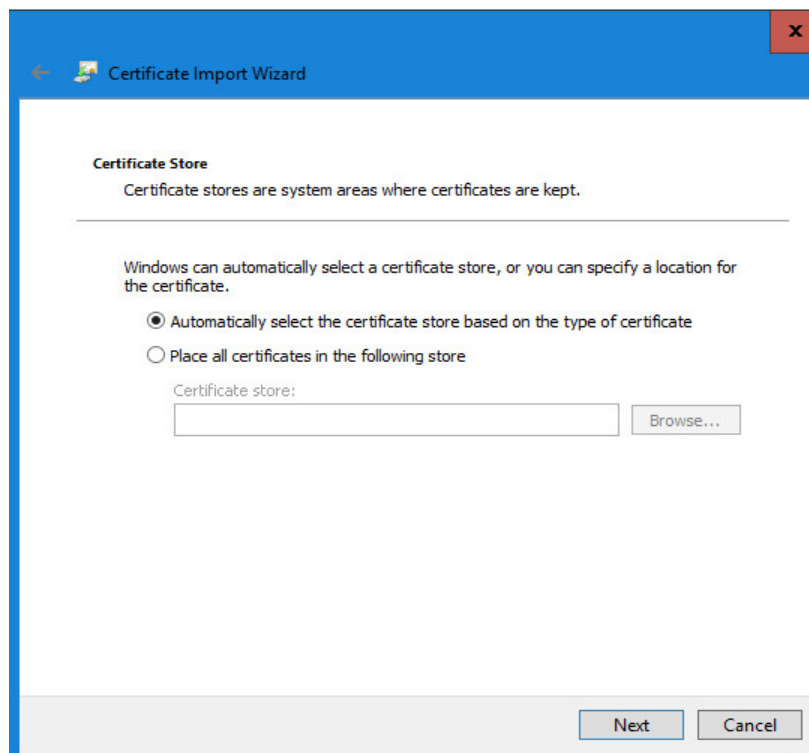
This section will show you how to do the following:

- 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**.



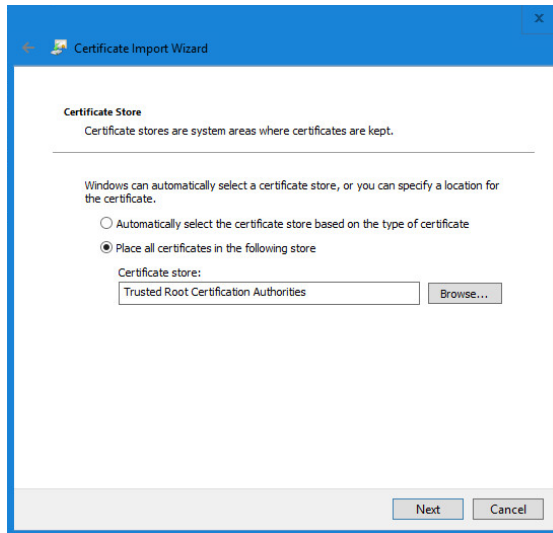
The certificate is now installed in the Intermediate Certificate Authorities store.

4. Download the GoDaddy Class 2 Certificate Authority Root Certificate from <https://certs.godaddy.com/repository>.
5. Choose the DER format.

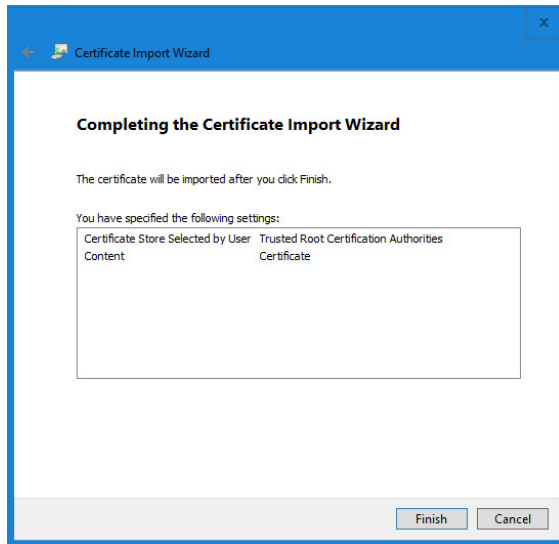
#### GoDaddy Certificate Chain

Name	File	Certificate Thumbprint (sha256)
GoDaddy Class 2 Certification Authority Root Certificate	<a href="#">gd-class2-root.crt (pem)</a> <a href="#">gd-class2-root.cer (der)</a>	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**.



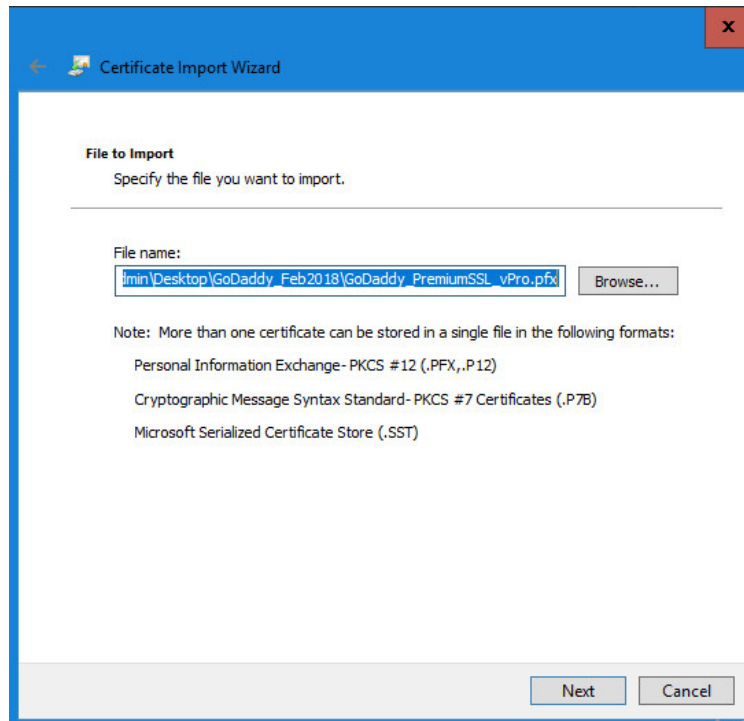
8. Click **Finish**. The certificate is now installed in the Trusted Root Certificate Authorities store.



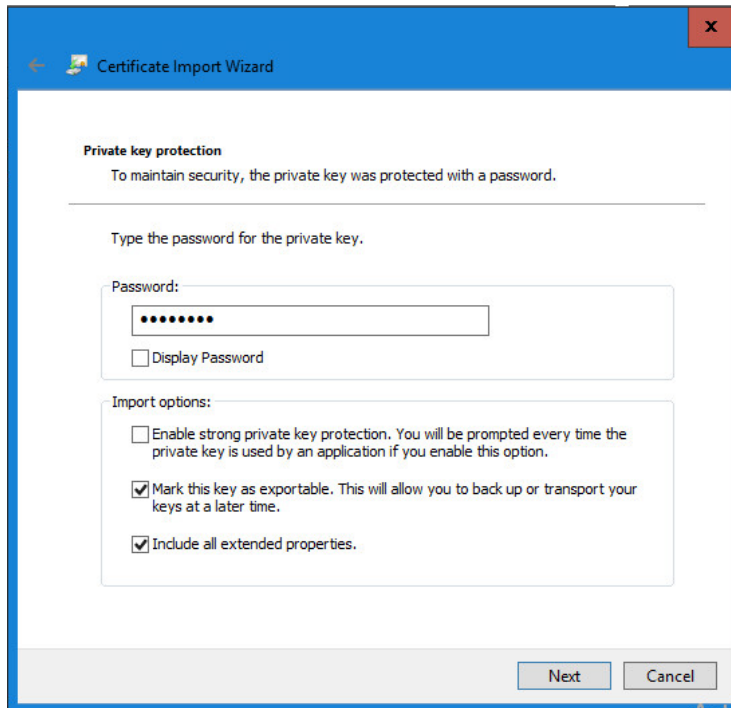
## 5.2 Install the PFX Certificate

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**.

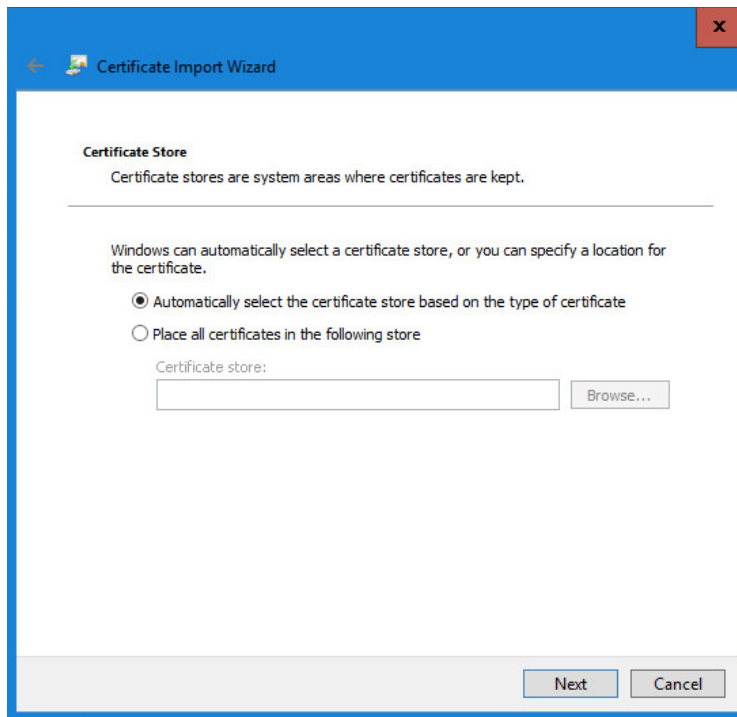
1. Double-click on the .pfx file where you saved it. Click **Next**.



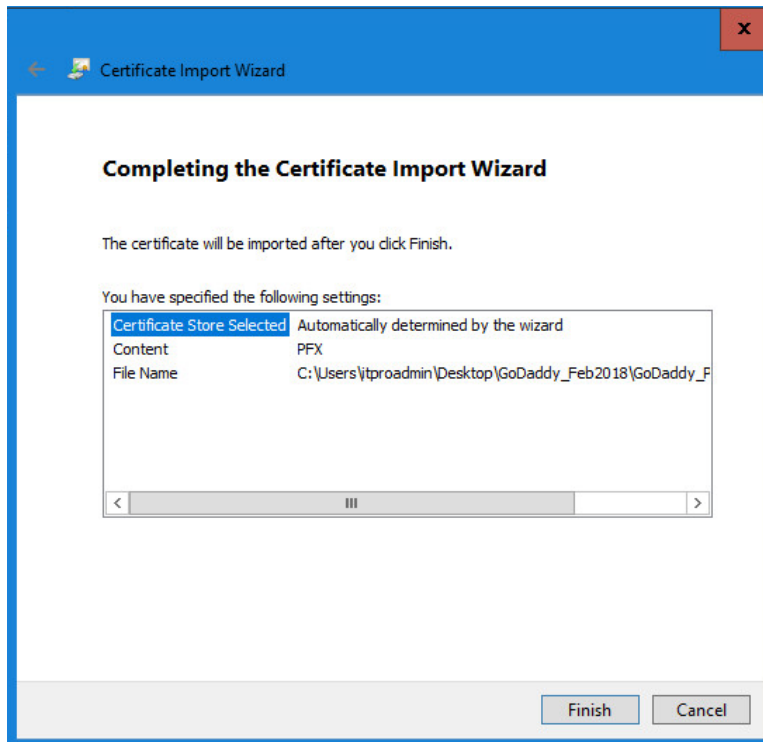
2. Enter in the password and select the **Mark Key as exportable**, and **Include all extended properties** check boxes.



3. Leave the default setting, to automatically select the certificate store. Click **Next**.



4. Click **Finish**.

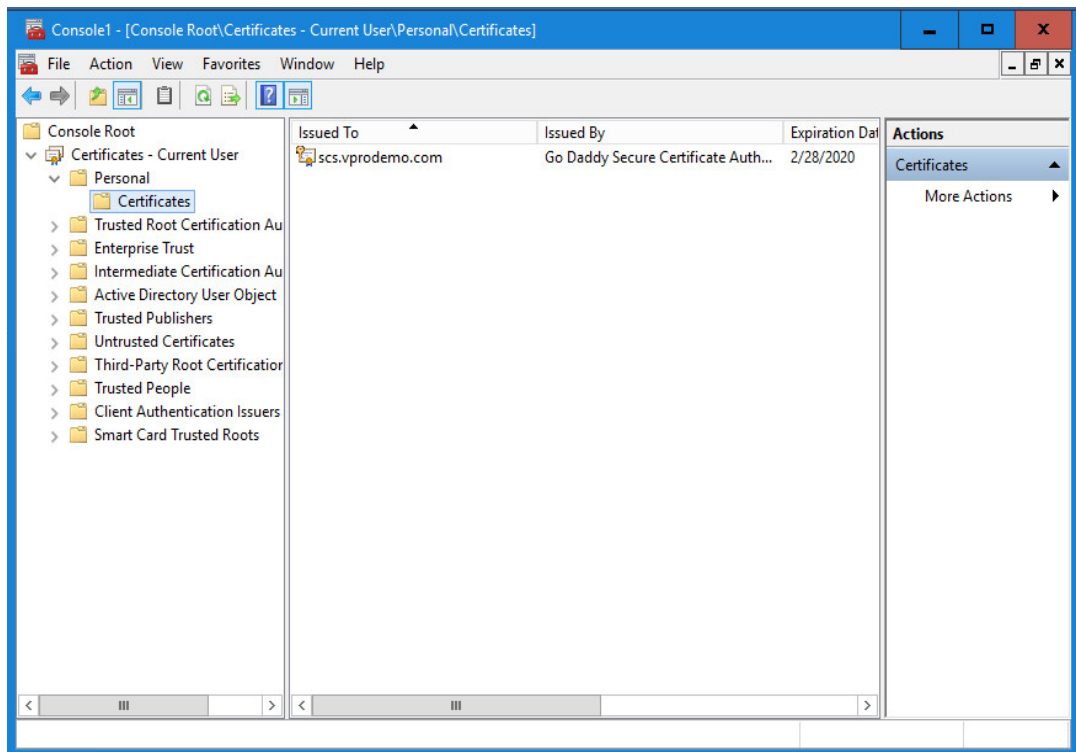


The certificate is now installed in the current user's Personal Certificates store.

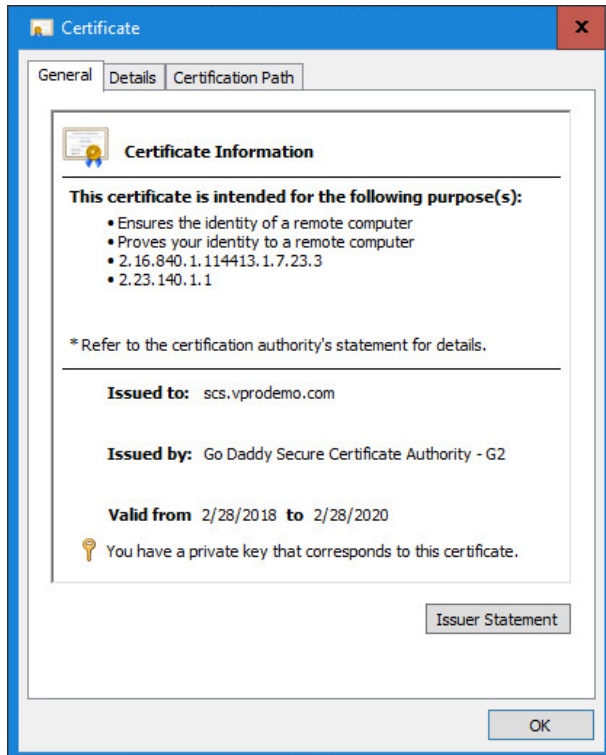


## 5.3 Verify the Certificate Chain

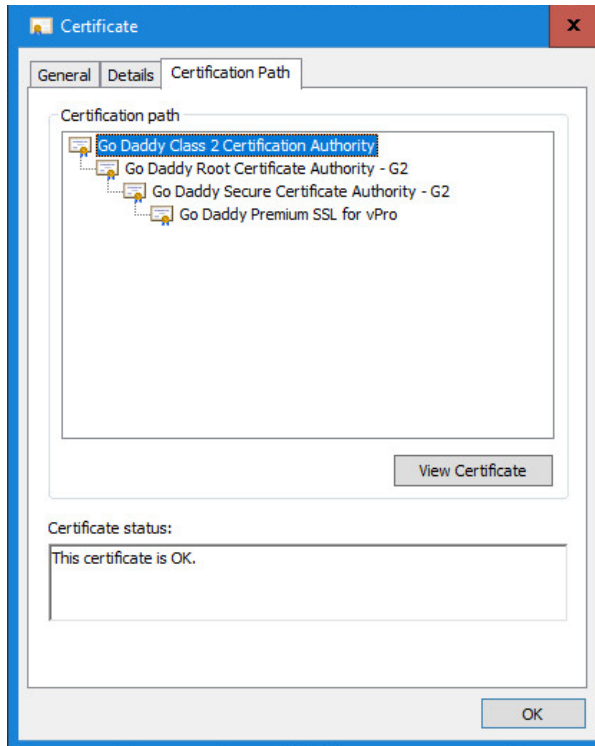
1. To verify the chain, double click **SCS.vprodemo.com**.



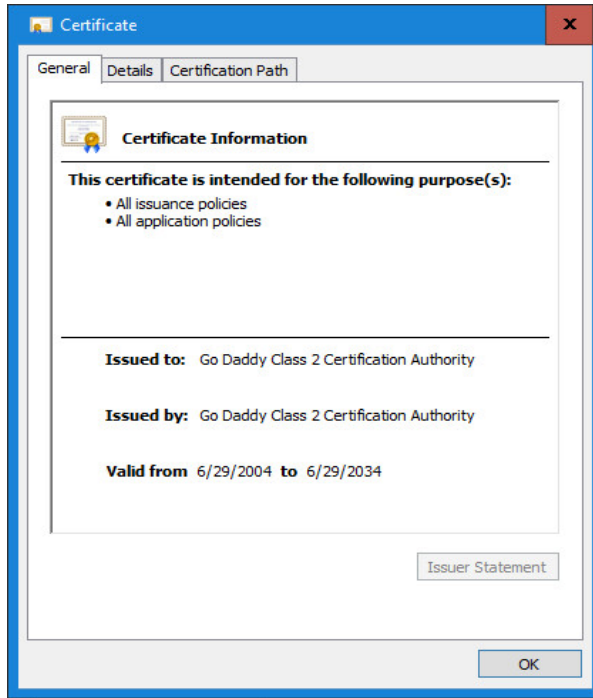
2. In the Certificate Information menu, confirm there are no errors. Check that the private key corresponds to the certificate. Click the **Certificate Path** tab.



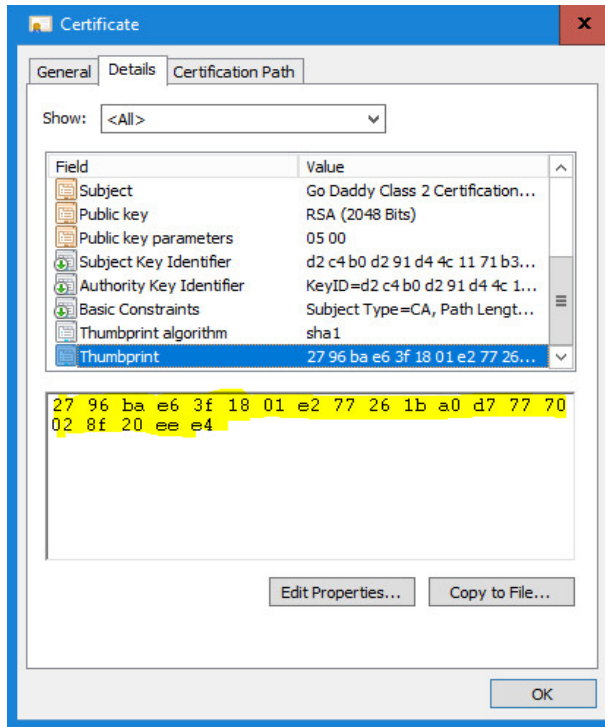
3. Check that the certificate is mapped to the intermediate Certificate Authorities as shown. Double click on the root cert **GoDaddy Class 2 Certification Authority**.



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.