Intel vPro® Technology

How To Purchase and Install Sectigo* Certificates for Intel® AMT

Revision 1.2

September 9, 2021

Revision History

Revision	Revision History	Date
1.0	First release.	May 31, 2013
1.1	Second release	Feb 23, 2021
1.2	Third release	Sep 9,2021

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

The products and services described may contain defects or errors known as errata which may cause deviations from published specifications. Current characterized errata are available on request. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses. Check with your system manufacturer or retailer or learn more at http://www.intel.com/technology/vpro.

Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

Microsoft Windows* operating system screenshots used with permission from Microsoft.

Sectigo* web screenshots used with permission from Sectigo.

Contents

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) or Intel® Endpoint Management Assistance (Intel® EMA) and then use *remote configuration*. Remote configuration uses Transport Layer Security (TLS) between the Intel SCS, Intel EMA Remote Configuration Servers, 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 Sectigo* certificate that will match the pre-installed Sectigo thumbprint and allow you to use remote configuration and maintenance using Intel SCS or Intel EMA.

1.1 Document Scope

This document does not include specific steps to install the Sectigo certificate on other management consoles. For consoles that do not use Intel SCS or Intel EMA, 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 Sectigo AAA CA certificates are supported in the following versions of Intel AMT:

- 6.x and later

Sectigo certificates are not supported on the following Intel 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 or Intel EMA User Guides provides information on the prerequisites for using the remote configuration service. Before starting this process, you should have the following:

- Intel SCS or Intel EMA installed on a supported Microsoft operating system
- One or more domain names for your network (Microsoft Workgroups are not supported)

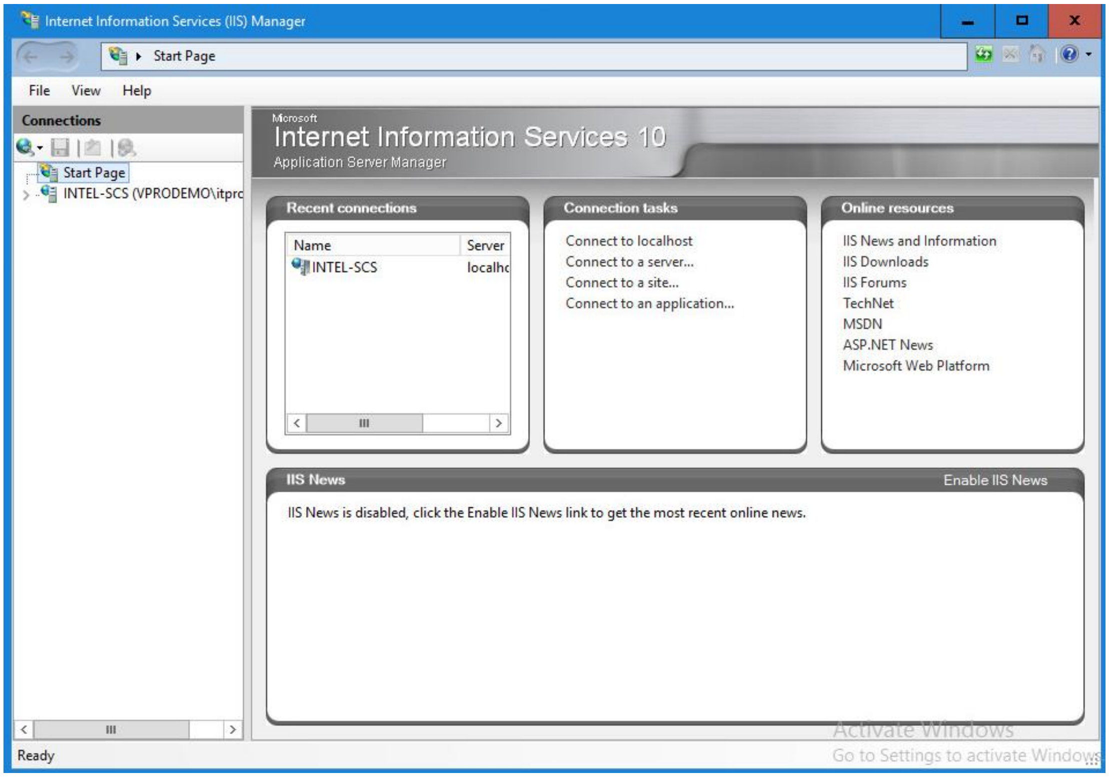
- Microsoft Internet Information Service (IIS) running on the server that is hosting the remote configuration service
- Account permissions to install the certificate

2 Purchase a Sectigo* Certificate

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

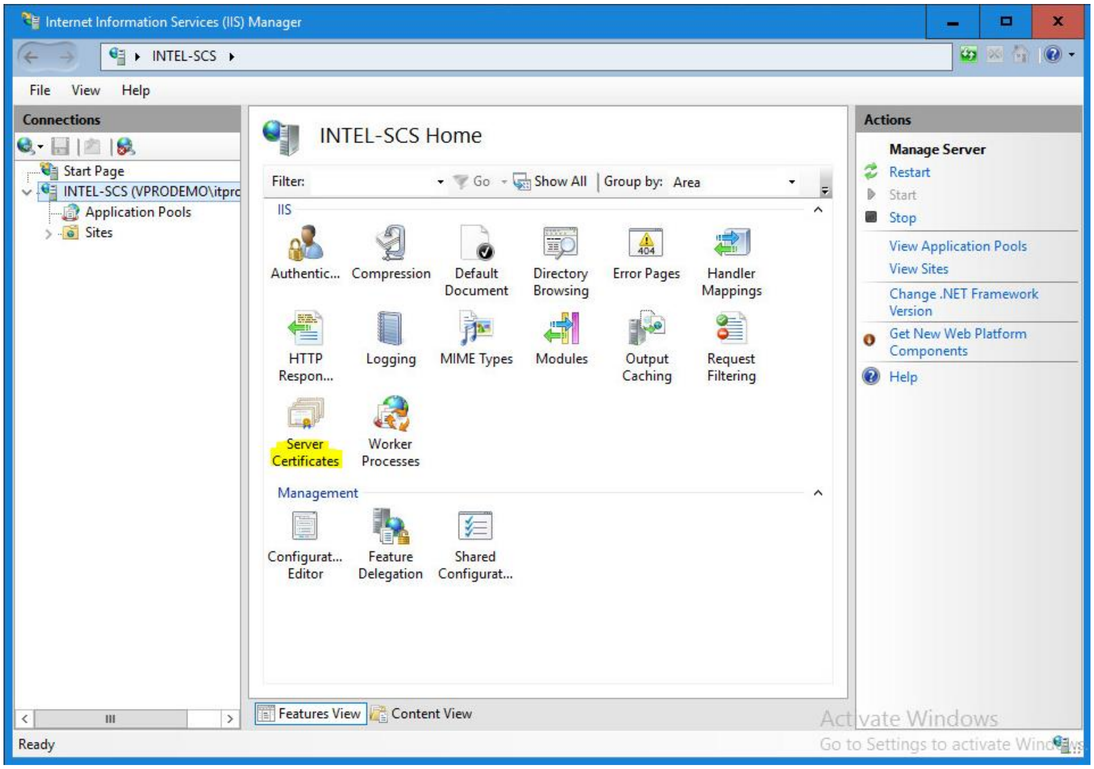
2.1 Create Certificate Signing Request (CSR)

1. On your Intel SCS remote configuration server, open Programs→Administrative Tools→**Internet Information Services (IIS) Manager**.

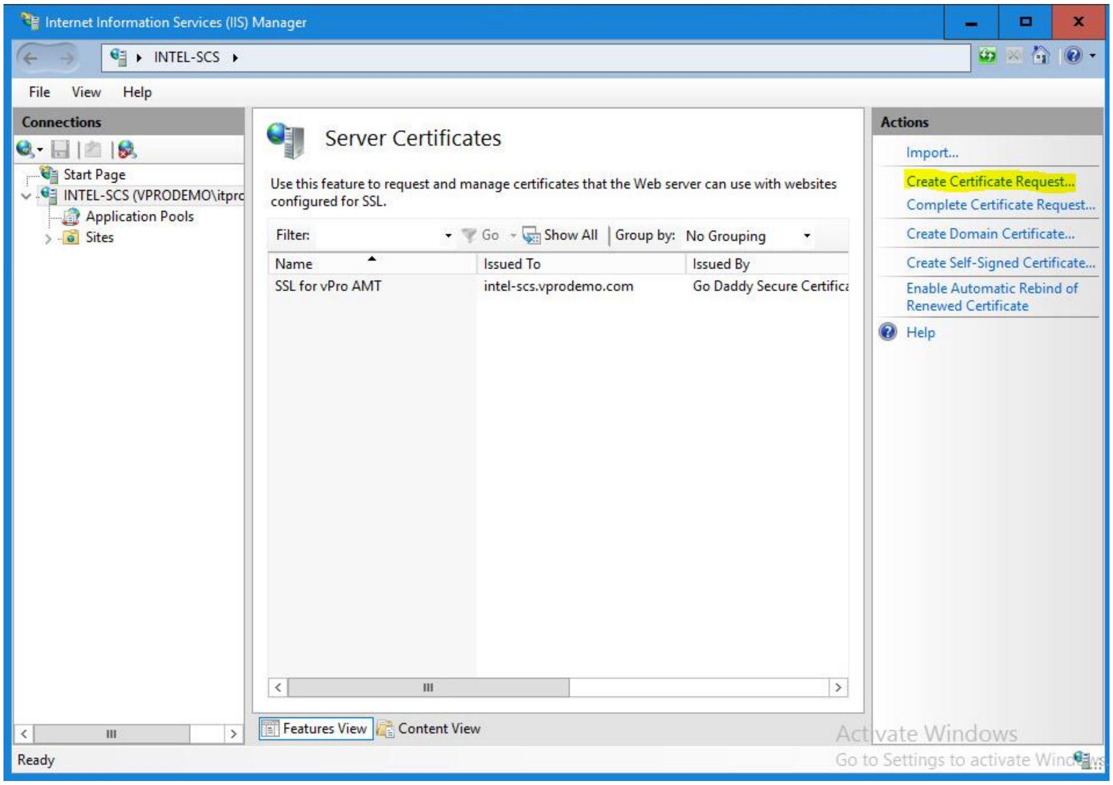


IIS News is disabled, click the Enable IIS News link to get the most recent online news.

2. In the Internet Information Services (IIS) Manager, open the **Server Certificate** icon.



3. Select **Create Certificate Request...** from the Actions menu.


Internet Information Services (IIS) Manager
INTEL-SCS
File
View
Help
Connections
Start Page
INTEL-SCS (VPRODEMO\itprc
Application Pools
Sites
Server Certificates
Filter:
Go
Show All
Group by:
No Grouping
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help
Features View
Content View
Ready
Activate Windows
Go to Settings to activate Windows

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Name	Issued To	Issued By
SSL for vPro AMT	intel-scs.vprodemo.com	Go Daddy Secure Certifica

4. Fill-in the **Distinguished Name Properties** form:
   - **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® MEBX. For help in understanding the rules for determining if the two values match, and support for 2nd and 3rd 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 intel.vprodemo.com, set CN=intel.vprodemo.com.

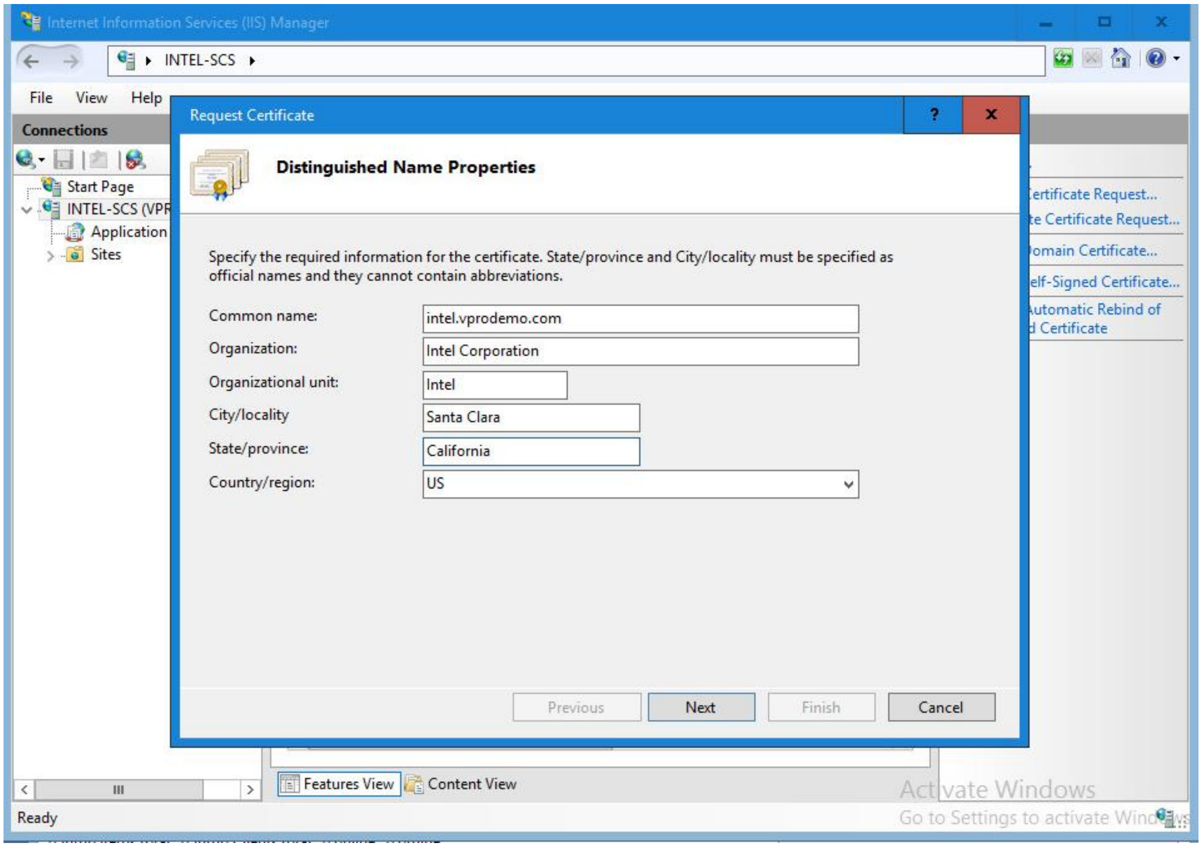
You can verify the DHCP Option 15 setting by running the SCSDiscovery utility (provided with Intel SCS) on the client. The DHCP Option 15 setting is called the OSSpecificDNSSuffix.

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

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

- **Organization**: The name of the organization that is requesting the certificate and owns the domain
- **Organizational Unit**: (not used by Sectigo)
- **City**: The requesting organization's city
- **State**: The requesting organization's state (spell it out)
- **Country**: The requesting organization's two letter country code

Click **Next.**

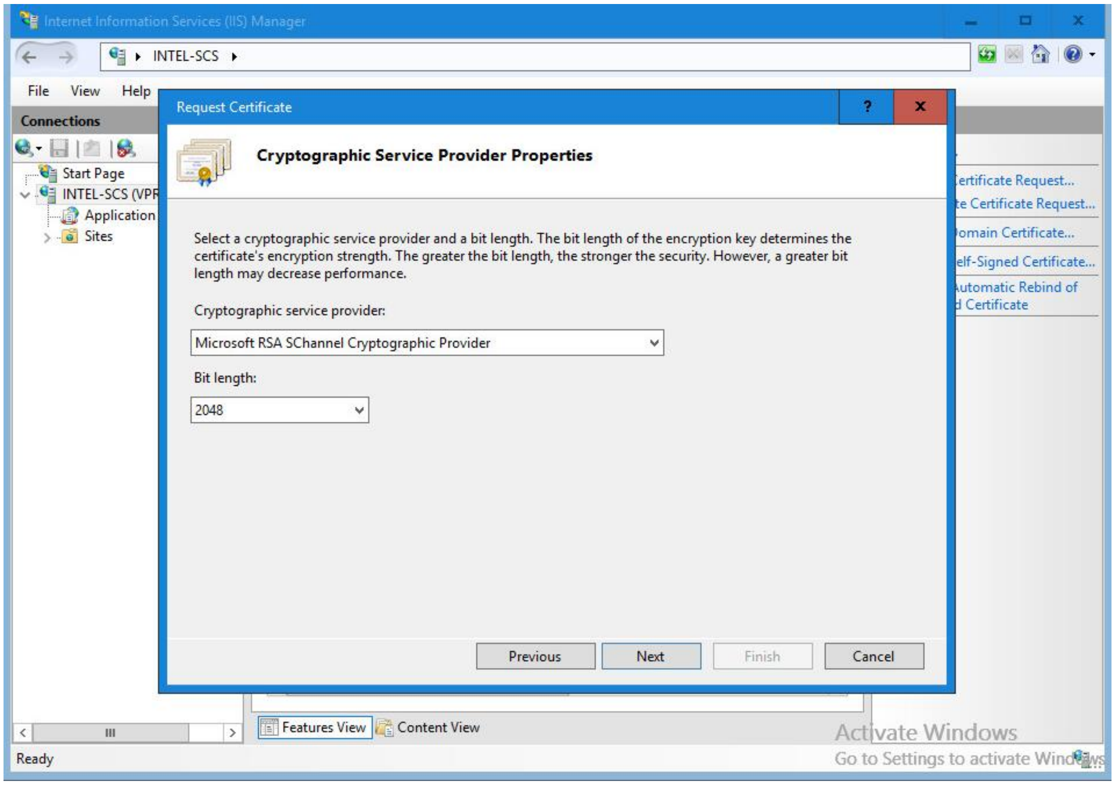


Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:	intel.vprodemo.com
Organization:	Intel Corporation
Organizational unit:	Intel
City/locality	Santa Clara
State/province:	California
Country/region:	US

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



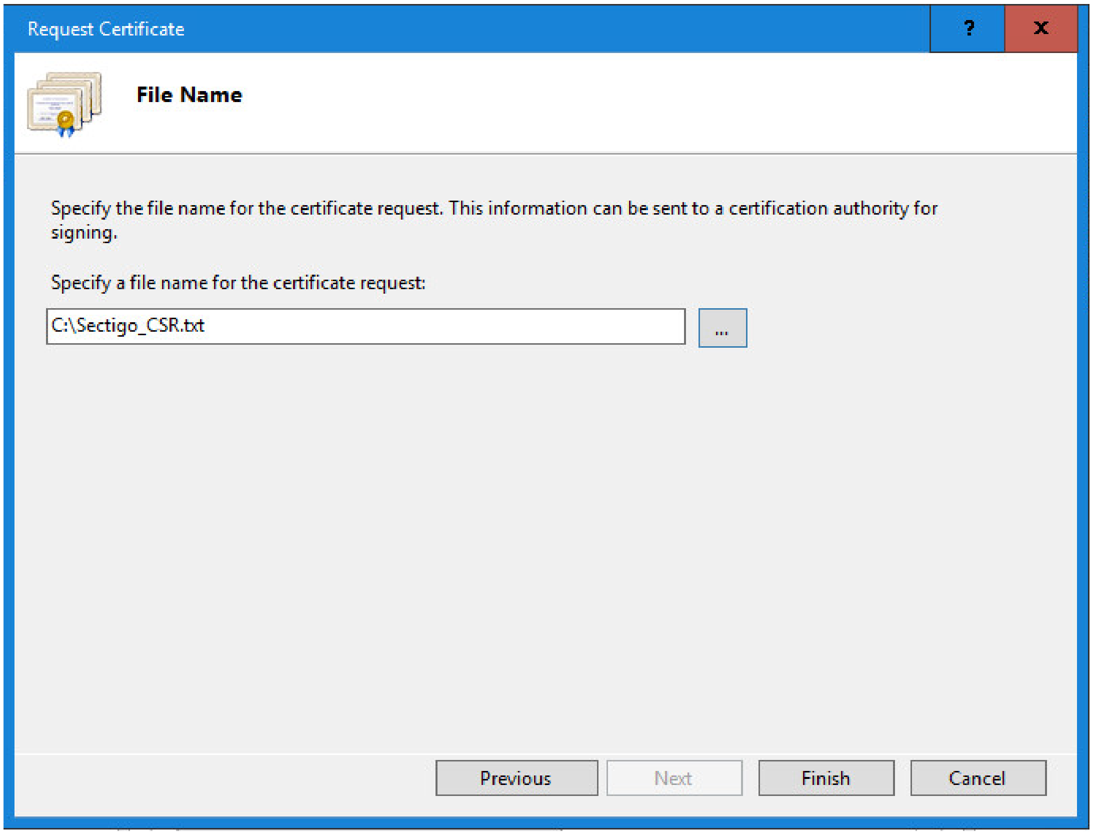
Cryptographic Service Provider Properties

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.

Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider

Bit length: 2048

6. Click the "…" button to select a location. Enter a file name to store the certificate request and then click **Submit**. Click **Finish.**

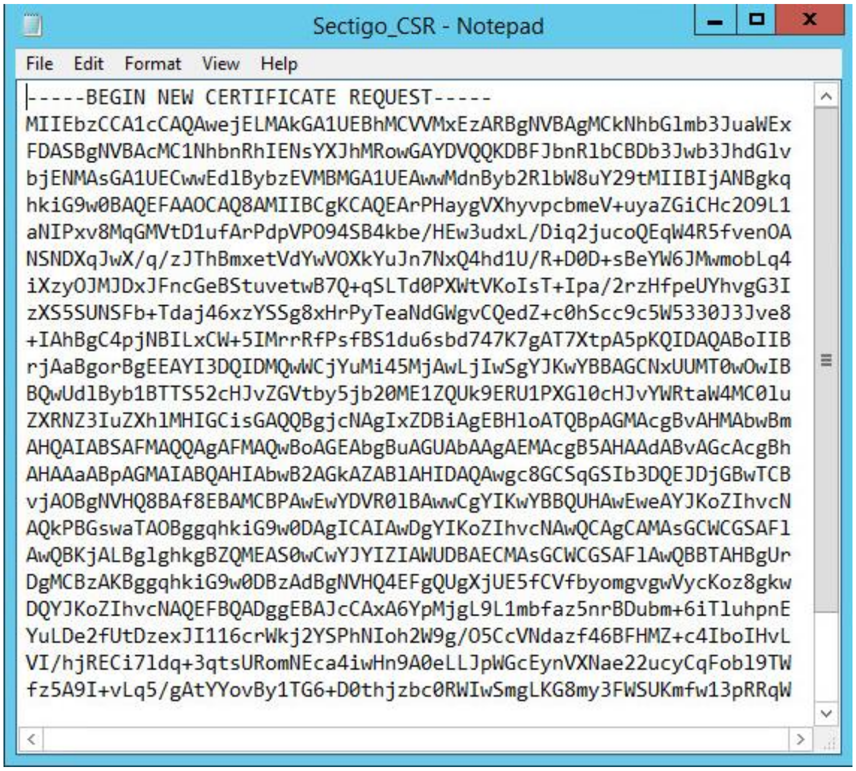


Specify the file name for the certificate request. This information can be sent to a certification authority for signing.

Specify a file name for the certificate request:

C:\Sectigo_CSR.txt

7. This file, Sectigo_CSR.txt in our example, will be used to submit your request to Sectigo for an Intel vPro AMT certificate. You can open the file in Notepad to view encrypted certificate request.

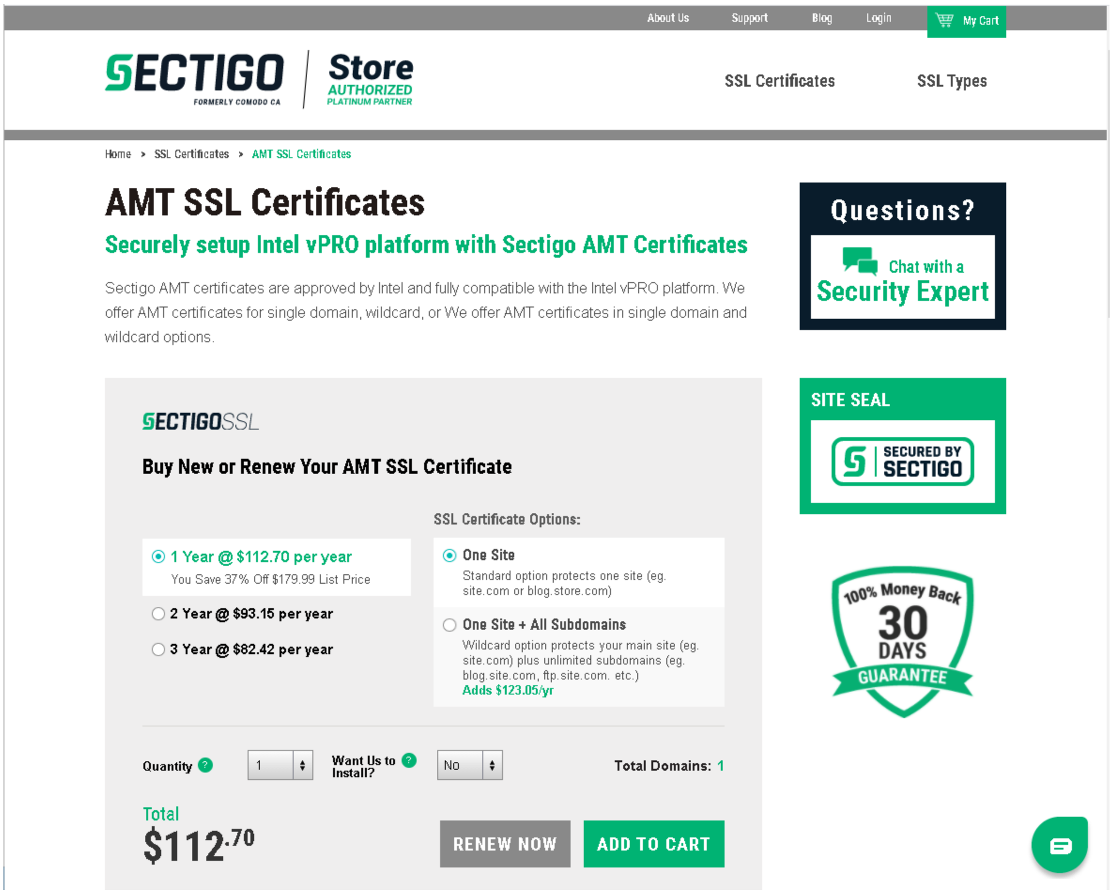


```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIEbzCCA1cCAQAwejELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWEx
FDASBgNVBAcMC1NhbnRhIENsYXJhMRowGAYDVQQKDBFJbnRlbCBDb3Jwb3JhdGlv
bjENMAsGA1UECwwEdlBybzEVMBMGA1UEAwwMdnByb2RlbW8uY29tMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArPHaygVXhyvpcbmeV+uyaZGiCHc2O9L1
aNIPxv8MqGMVtD1ufArPdpVPO94SB4kbe/HEw3udxL/Diq2jucoQEqW4R5fvenOA
NSNDXqJwX/q/zJThBmxetVdYwVOXkYuJn7NxQ4hd1U/R+D0D+sBeYW6JMwmobLq4
iXzyOJMJDxJFncGeBStuvetwB7Q+qSLTd0PXWtVKoIsT+Ipa/2rzHfpeUYhvgG3I
zXS5SUNSFb+Tdaj46xzYSSg8xHrPyTeaNdGWgvCQedZ+c0hScc9c5W5330J3Jve8
+IAhBgC4pjNBILxCW+5IMrrRfPsfBS1du6sbd747K7gAT7XtpA5pKQIDAQABoIIB
rjAaBgorBgEEAYI3DQIDMQwWCjYuMi45MjAwLjIwSgYJKwYBBAGCNxUUMT0wOwIB
BQwUdlByb1BTTS52cHJvZGVtby5jb20ME1ZQUk9ERU1PXG10cHJvYWRtaW4MC0lu
ZXRNZ3IuZXhlMHIGCisGAQQBgjcNAgIxZDBiAgEBHloATQBpAGMAcgBvAHMAbwBm
AHQAIABSAFMAQQAgAFMAQwBoAGEAbgBuAGUAbAAgAEMAcgB5AHAAdABvAGcAcgBh
AHAAaABpAGMAIABQAHIAbwB2AGkAZABlAHIDAQAwgc8GCSqGSIb3DQEJDjGBwTCB
vjAOBgNVHQ8BAf8EBAMCBPAwEwYDVR0lBAwwCgYIKwYBBQUHAwEweAYJKoZIhvcN
AQkPBGswaTAOBggqhkiG9w0DAgICAIAwDgYIKoZIhvcNAwQCAgCAMAsGCWCGSAFl
AwQBKjALBglghkgBZQMEAS0wCwYJYIZIAWUDBAECMAsGCWCGSAFlAwQBBTAHBgUr
DgMCBzAKBggqhkiG9w0DBzAdBgNVHQ4EFgQUgXjUE5fCVfbyomgvgwVycKoz8gkw
DQYJKoZIhvcNAQEFBQADggEBAJcCAxA6YpMjgL9L1mbfaz5nrBDubm+6iTluhpnE
YuLDe2fUtDzexJI116crWkj2YSPhNIoh2W9g/O5CcVNdazf46BFHMZ+c4IboIHvL
VI/hjRECi7ldq+3qtsURomNEca4iwHn9A0eLLJpWGcEynVXNae22ucyCqFobl9TW
fz5A9I+vLq5/gAtYYovBy1TG6+D0thjzbc0RWIwSmgLKG8my3FWSUKmfw13pRRqW
```

3 Send the Certificate Request to Sectigo*

1. Go to the Sectigo web site: https://sectigostore.com/ssl-certificates/amt-certificate

2. At the **AMT SSL Certificate** menu, select how long you would like this certificate to be valid before having to renew this certificate. Note that the cost of the certificate goes up with the length of the validity period. The example shows a **1-year validity period** selected. Click **Add To Cart**.



AMT SSL Certificates

Securely setup Intel vPRO platform with Sectigo AMT Certificates

Sectigo AMT certificates are approved by Intel and fully compatible with the Intel vPRO platform. We offer AMT certificates for single domain, wildcard, or We offer AMT certificates in single domain and wildcard options.

Buy New or Renew Your AMT SSL Certificate

● 1 Year @ $112.70 per year
You Save 37% Off $179.99 List Price

○ 2 Year @ $93.15 per year

○ 3 Year @ $82.42 per year

SSL Certificate Options:

● One Site
Standard option protects one site (eg. site.com or blog.store.com)

○ One Site + All Subdomains
Wildcard option protects your main site (eg. site.com) plus unlimited subdomains (eg. blog.site.com, ftp.site.com. etc.)
Adds $123.05/yr

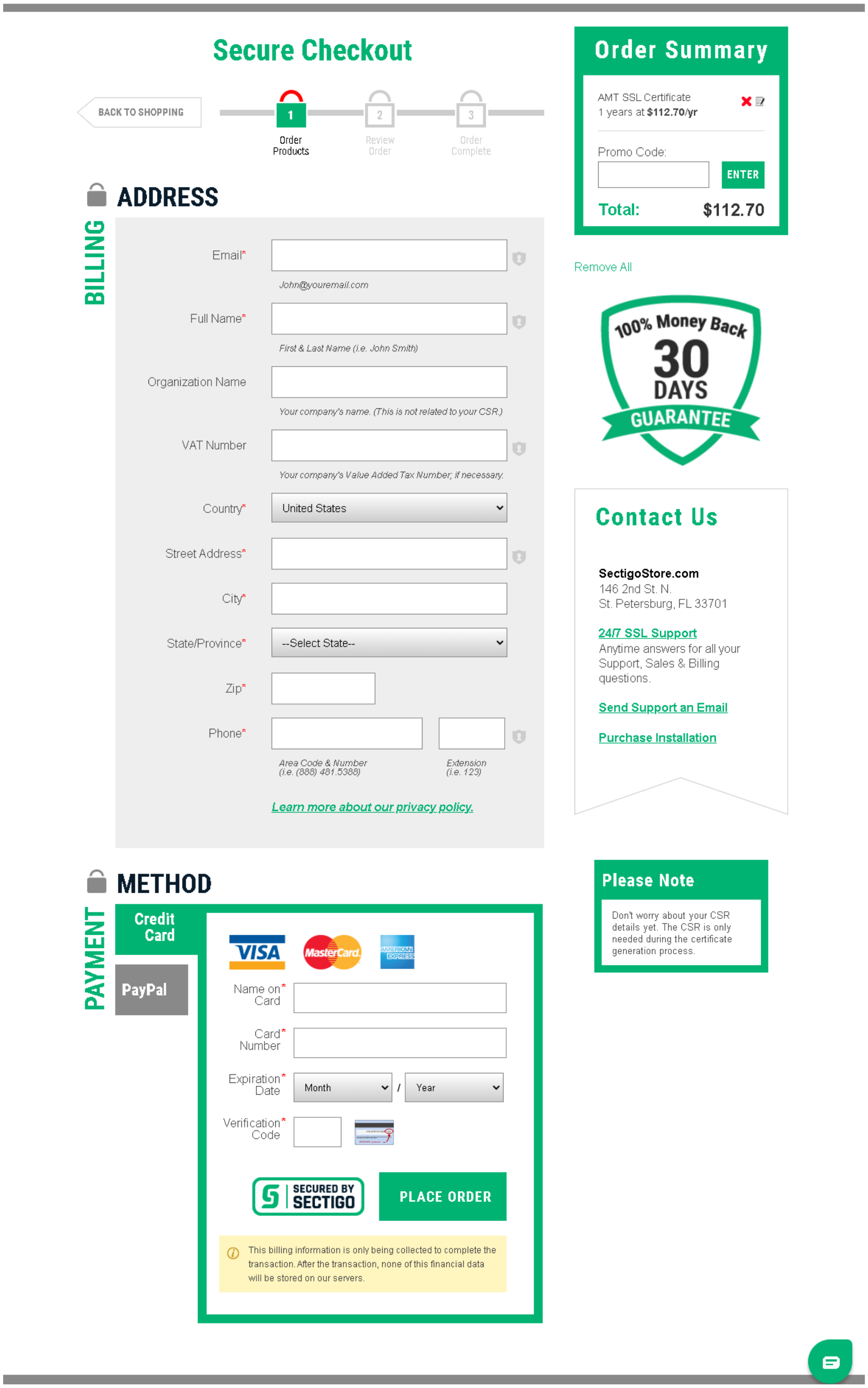
Quantity ? 1

Want Us to Install? ? No

Total Domains: 1

Total
$112.70

3. At the Secure Checkout menu, enter your billing and payment information. Click **Place Order.**



Secure Checkout

BILLING

ADDRESS

Email*
John@youremail.com

Full Name*
First & Last Name (i.e. John Smith)

Organization Name
Your company's name. (This is not related to your CSR.)

VAT Number
Your company's Value Added Tax Number; if necessary.

Country* United States

Street Address*

City*

State/Province* --Select State--

Zip*

Phone*
Area Code & Number (i.e. (888) 481.5388)
Extension (i.e. 123)

Learn more about our privacy policy.

PAYMENT

METHOD

Name on* Card

Card* Number

Expiration* Date Month / Year

Verification* Code

This billing information is only being collected to complete the transaction. After the transaction, none of this financial data will be stored on our servers.

Order Summary

AMT SSL Certificate
1 years at $112.70/yr

Promo Code:

Total: $112.70

Contact Us

SectigoStore.com
146 2nd St. N.
St. Petersburg, FL 33701

24/7 SSL Support
Anytime answers for all your Support, Sales & Billing questions.

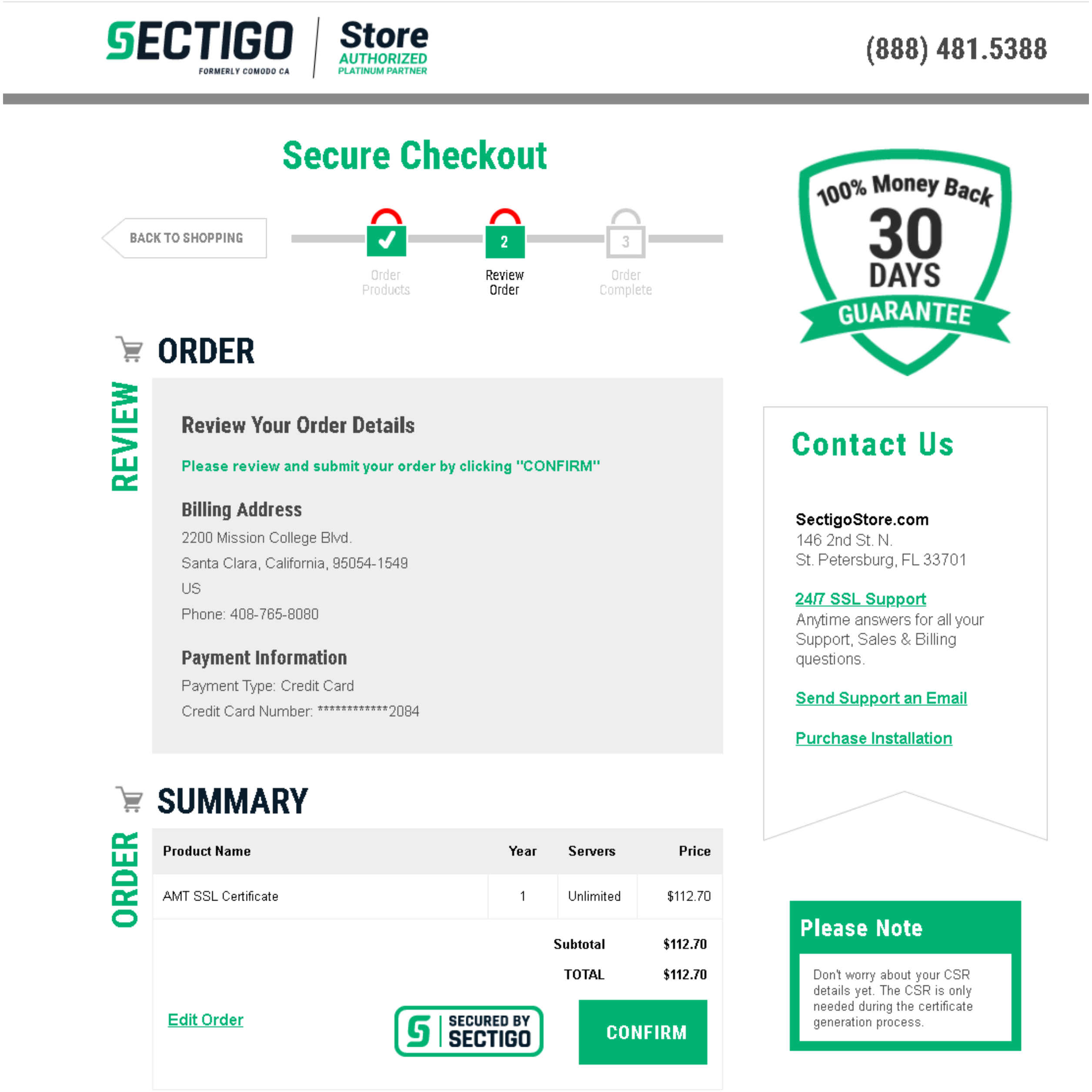
Send Support an Email

Purchase Installation

Please Note

Don't worry about your CSR details yet. The CSR is only needed during the certificate generation process.

4. Review the order details and click **Confirm**.



Review Your Order Details

Please review and submit your order by clicking "CONFIRM"

Billing Address
2200 Mission College Blvd.
Santa Clara, California, 95054-1549
US
Phone: 408-765-8080

Payment Information
Payment Type: Credit Card
Credit Card Number: ************2084

Product Name	Year	Servers	Price
AMT SSL Certificate	1	Unlimited	$112.70
		Subtotal	$112.70
		TOTAL	$112.70

Contact Us

SectigoStore.com
146 2nd St. N.
St. Petersburg, FL 33701

24/7 SSL Support
Anytime answers for all your Support, Sales & Billing questions.

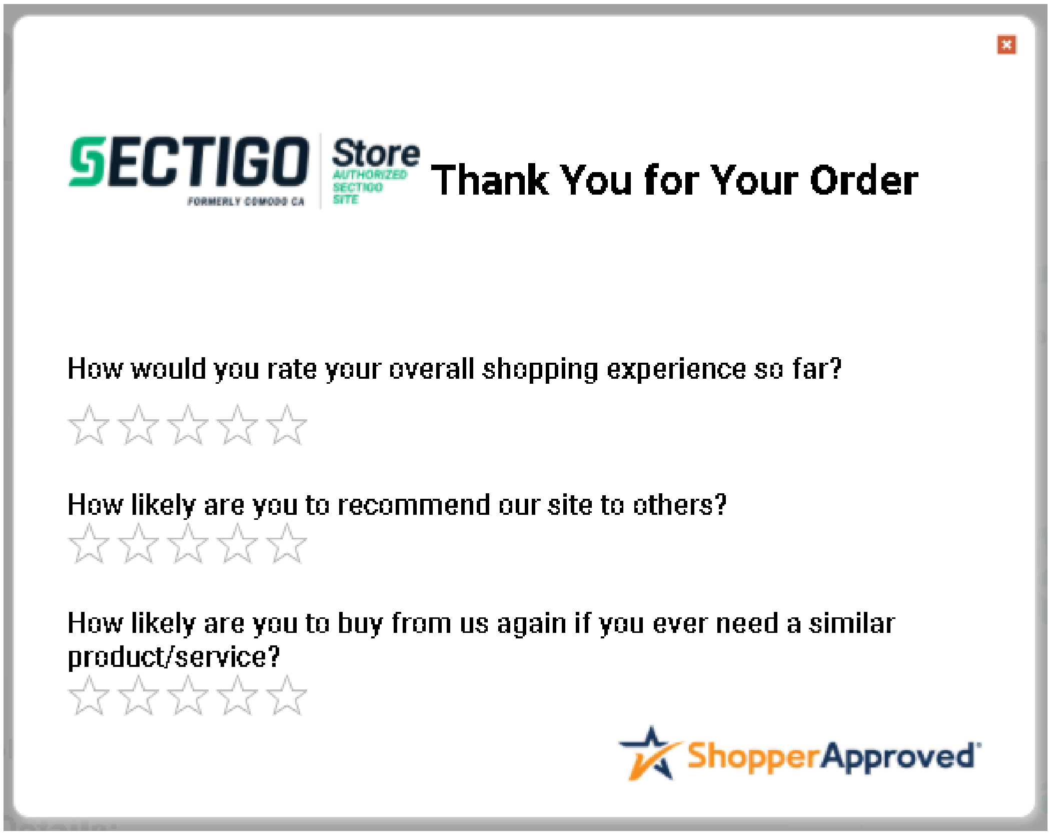
Send Support an Email

Purchase Installation

Please Note

Don't worry about your CSR details yet. The CSR is only needed during the certificate generation process.

5. At the thank you and summary menu, click on **Generate.**



Thank You for Your Order

How would you rate your overall shopping experience so far?

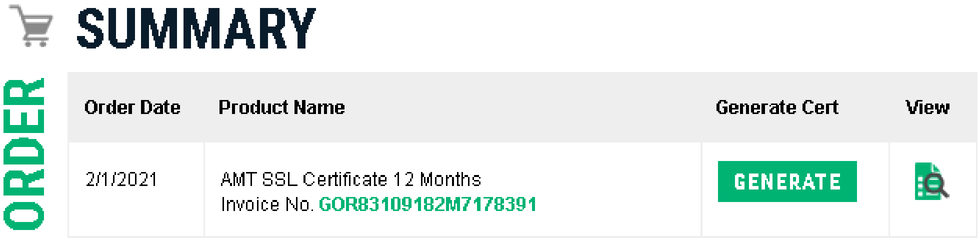
☆☆☆☆☆

How likely are you to recommend our site to others?

☆☆☆☆☆

How likely are you to buy from us again if you ever need a similar product/service?

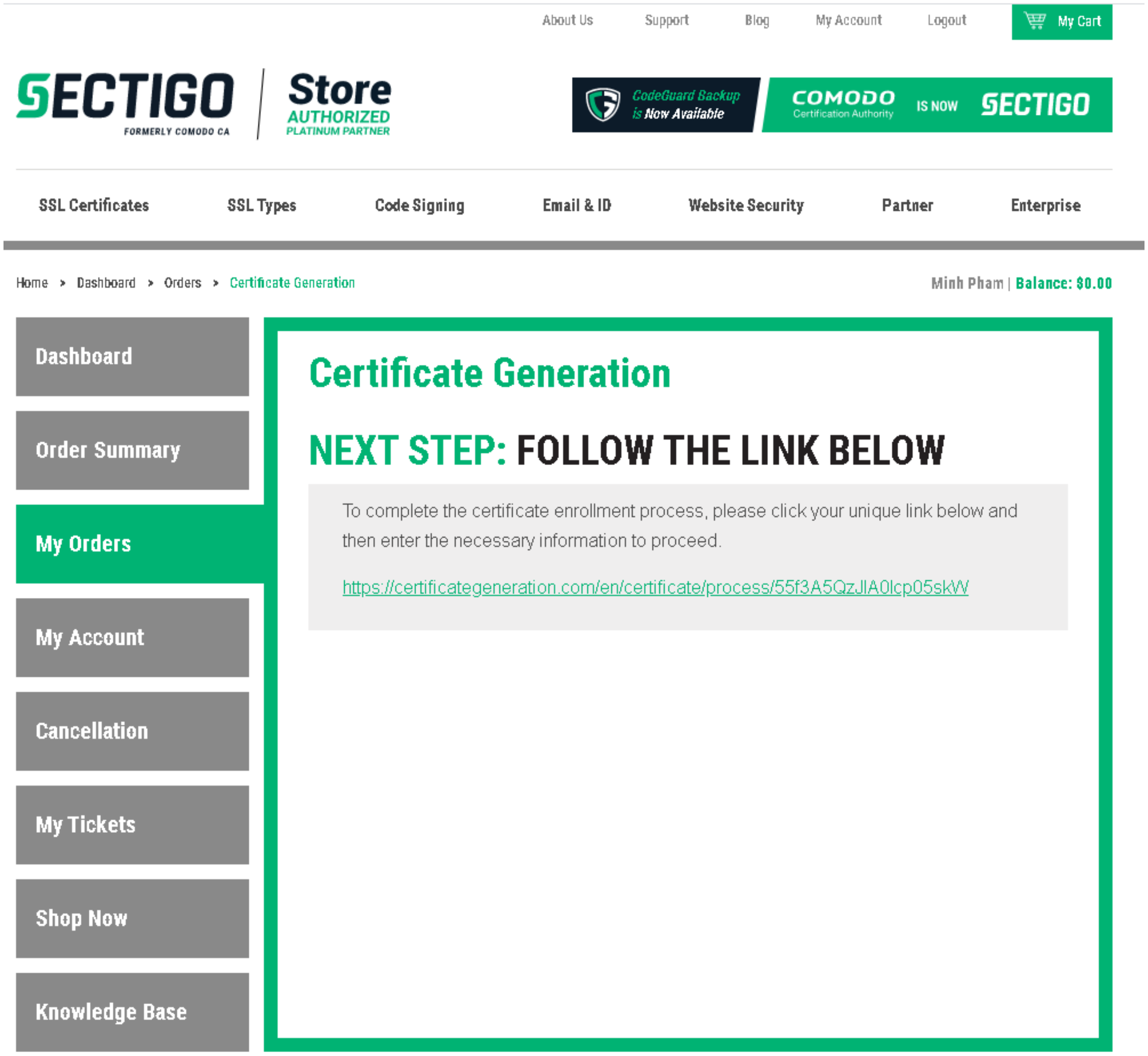
☆☆☆☆☆



SUMMARY

Order Date	Product Name	Generate Cert	View
2/1/2021	AMT SSL Certificate 12 Months Invoice No. GOR83109182M7178391	GENERATE	

6. Click on the link at the Certificate Generation menu.



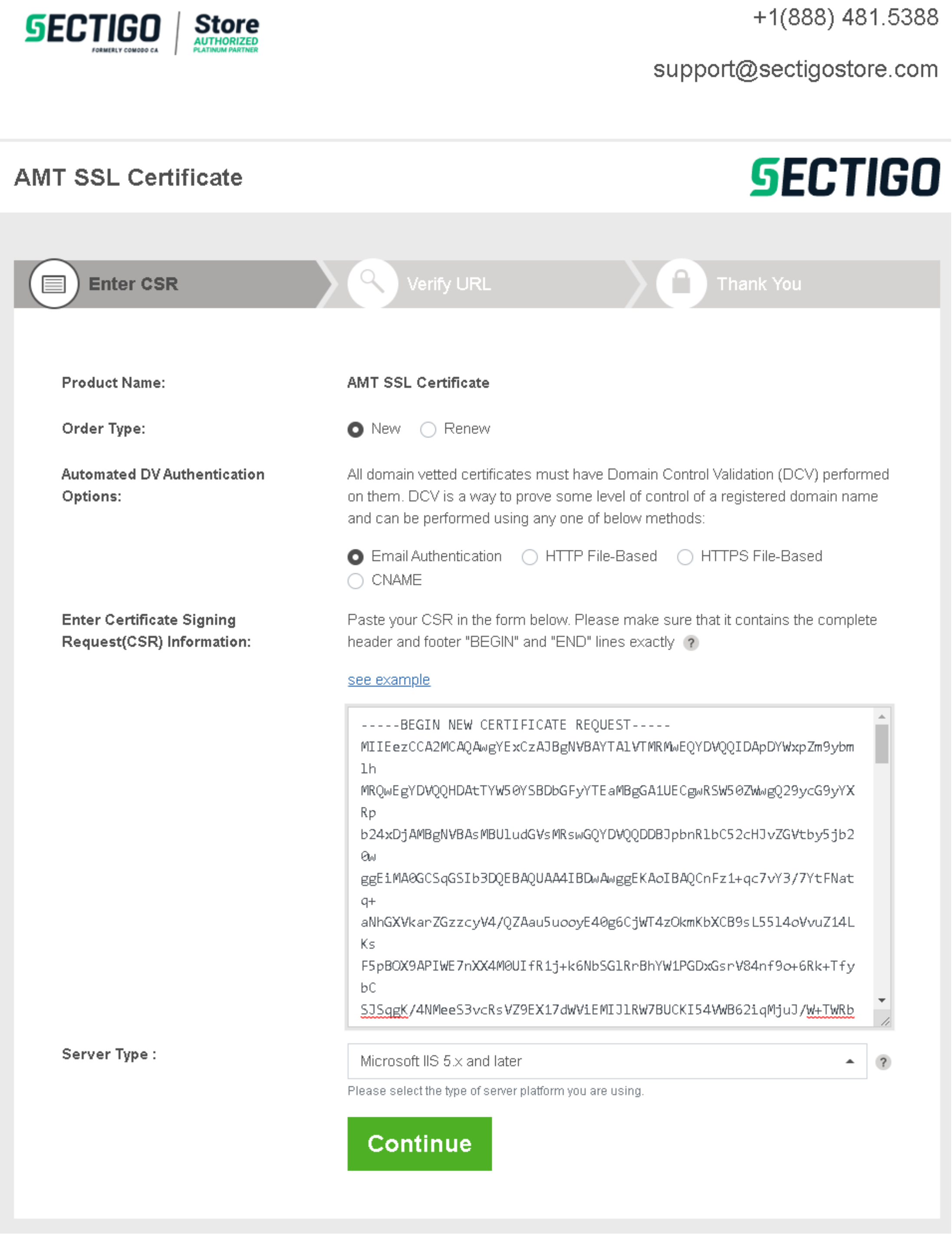
Certificate Generation

NEXT STEP: FOLLOW THE LINK BELOW

To complete the certificate enrollment process, please click your unique link below and then enter the necessary information to proceed.

https://certificategeneration.com/en/certificate/process/55f3A5QzJlA0lcp05skW

7. The next menu will require you to paste in the CSR information. Select **New** for Oder type, paste in the contents or your CSR like shown below, choose **Microsoft IIS 5.x and later** for the server type. Click **Continue**.



SECTIGO FORMERLY COMODO CA | Store AUTHORIZED PLATINUM PARTNER

+1(888) 481.5388

support@sectigostore.com

AMT SSL Certificate

Product Name: AMT SSL Certificate

Order Type: ● New ○ Renew

Automated DV Authentication Options: All domain vetted certificates must have Domain Control Validation (DCV) performed on them. DCV is a way to prove some level of control of a registered domain name and can be performed using any one of below methods:

● Email Authentication ○ HTTP File-Based ○ HTTPS File-Based ○ CNAME

Enter Certificate Signing Request(CSR) Information: Paste your CSR in the form below. Please make sure that it contains the complete header and footer "BEGIN" and "END" lines exactly ?

see example

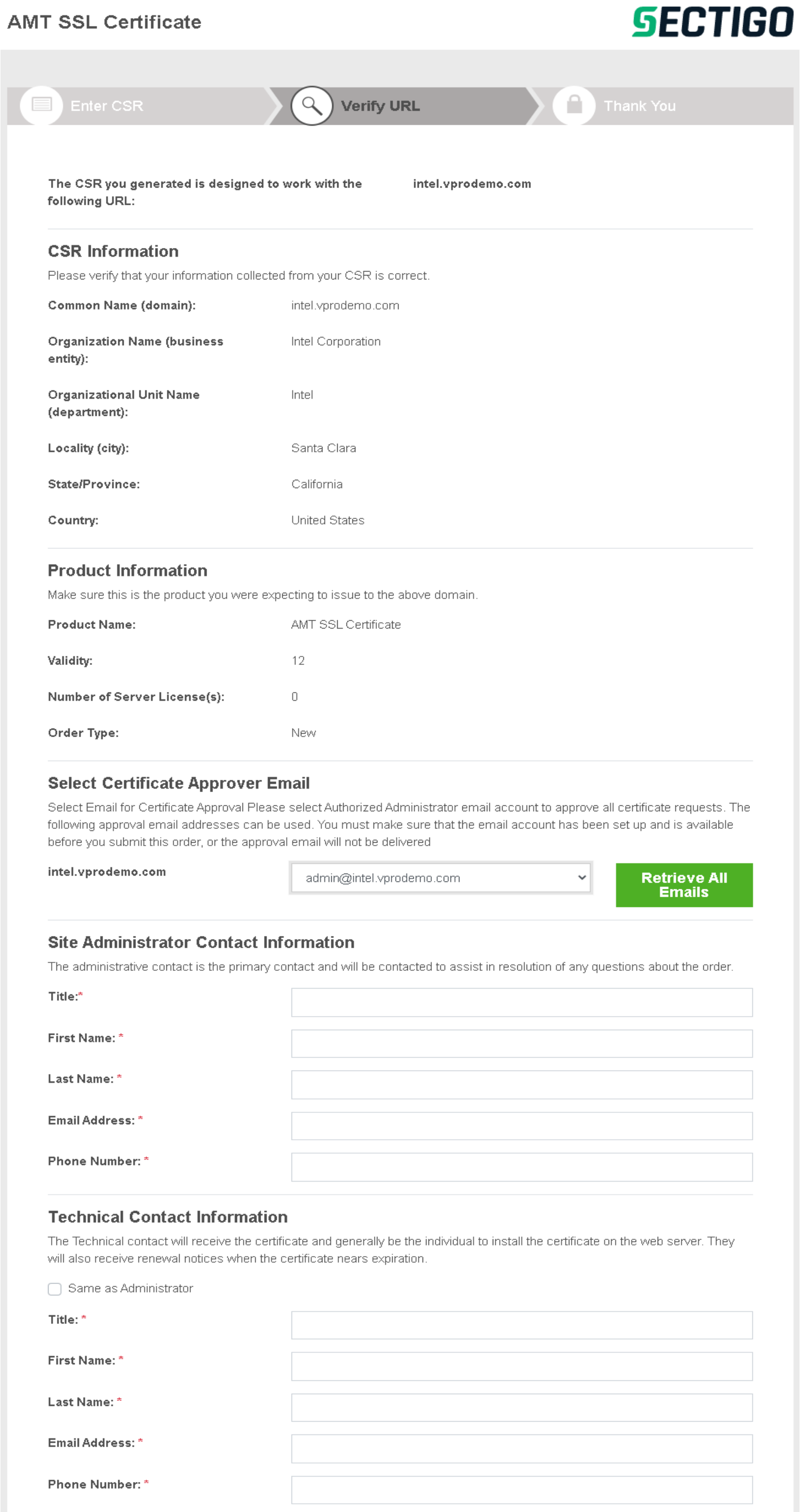
```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIEezCCA2MCAQAwgYExCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybm
lh
MRQwEgYDVQQHDAtTYW50YSBDbGFyYTEaMBgGA1UECgwRSW50ZWwgQ29ycG9yYX
Rp
b24xDjAMBgNVBAsMBUludGVsMRswGQYDVQQDDBJpbnRlbC52cHJvZGVtby5jb2
0w
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCnFz1+qc7vY3/7YtFNat
q+
aNhGXVkarZGzzcyV4/QZAau5uooyE40g6CjWT4zOkmKbXCB9sL5514oVvuZ14L
Ks
F5pBOX9APIWE7nXX4M0UIfR1j+k6NbSGlRrBhYW1PGDxGsrV84nf9o+6Rk+Tfy
bC
SJSqgK/4NMeeS3vcRsVZ9EX17dWViEMIJlRW7BUCKI54VWB62iqMjuJ/W+TWRb
```

Server Type : Microsoft IIS 5.x and later ?

Please select the type of server platform you are using.

Continue

8. Verify the URL information and enter the Site Administrator contact information. Click **Continue.**



AMT SSL Certificate

The CSR you generated is designed to work with the following URL: intel.vprodemo.com

CSR Information

Please verify that your information collected from your CSR is correct.

Common Name (domain):	intel.vprodemo.com
Organization Name (business entity):	Intel Corporation
Organizational Unit Name (department):	Intel
Locality (city):	Santa Clara
State/Province:	California
Country:	United States

Product Information

Make sure this is the product you were expecting to issue to the above domain.

Product Name:	AMT SSL Certificate
Validity:	12
Number of Server License(s):	0
Order Type:	New

Select Certificate Approver Email

Select Email for Certificate Approval Please select Authorized Administrator email account to approve all certificate requests. The following approval email addresses can be used. You must make sure that the email account has been set up and is available before you submit this order, or the approval email will not be delivered

intel.vprodemo.com: admin@intel.vprodemo.com

Site Administrator Contact Information

The administrative contact is the primary contact and will be contacted to assist in resolution of any questions about the order.

Title:*

First Name: *

Last Name: *

Email Address: *

Phone Number: *

Technical Contact Information

The Technical contact will receive the certificate and generally be the individual to install the certificate on the web server. They will also receive renewal notices when the certificate nears expiration.

□ Same as Administrator

Title: *

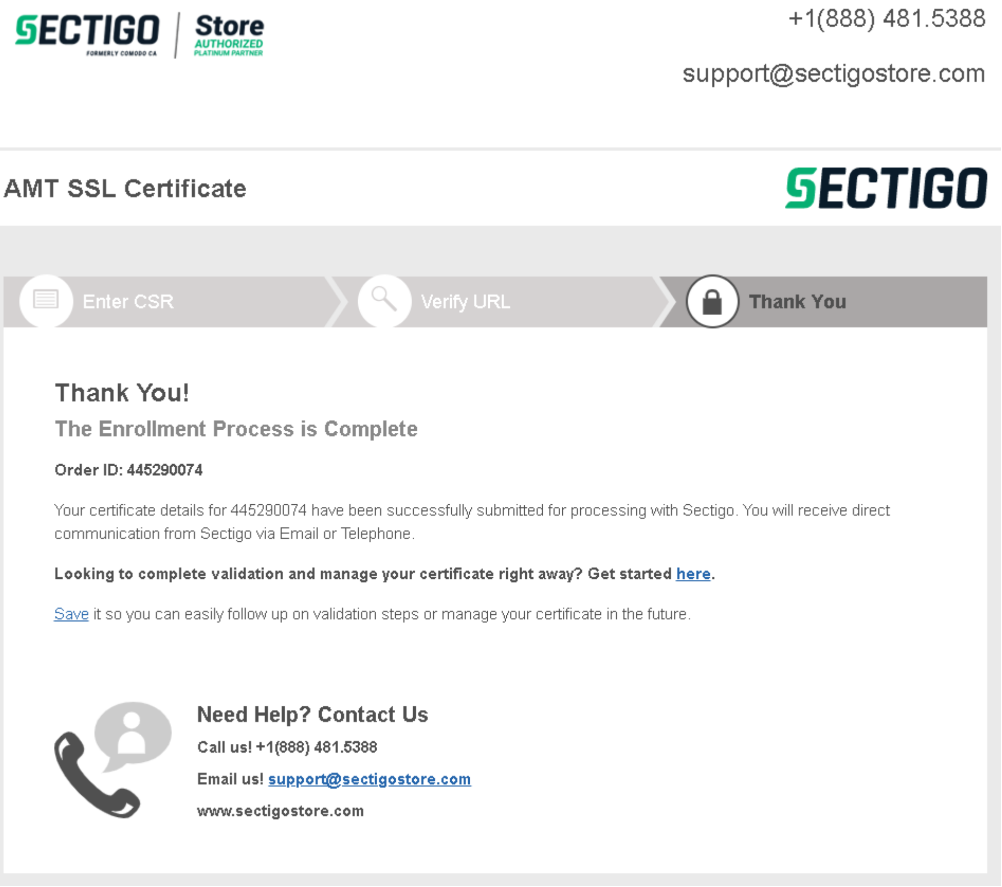
First Name: *

Last Name: *

Email Address: *

Phone Number: *

9. The Enrollment Process is complete.



Thank You!

The Enrollment Process is Complete

Order ID: 445290074

Your certificate details for 445290074 have been successfully submitted for processing with Sectigo. You will receive direct communication from Sectigo via Email or Telephone.

Looking to complete validation and manage your certificate right away? Get started here.

Save it so you can easily follow up on validation steps or manage your certificate in the future.

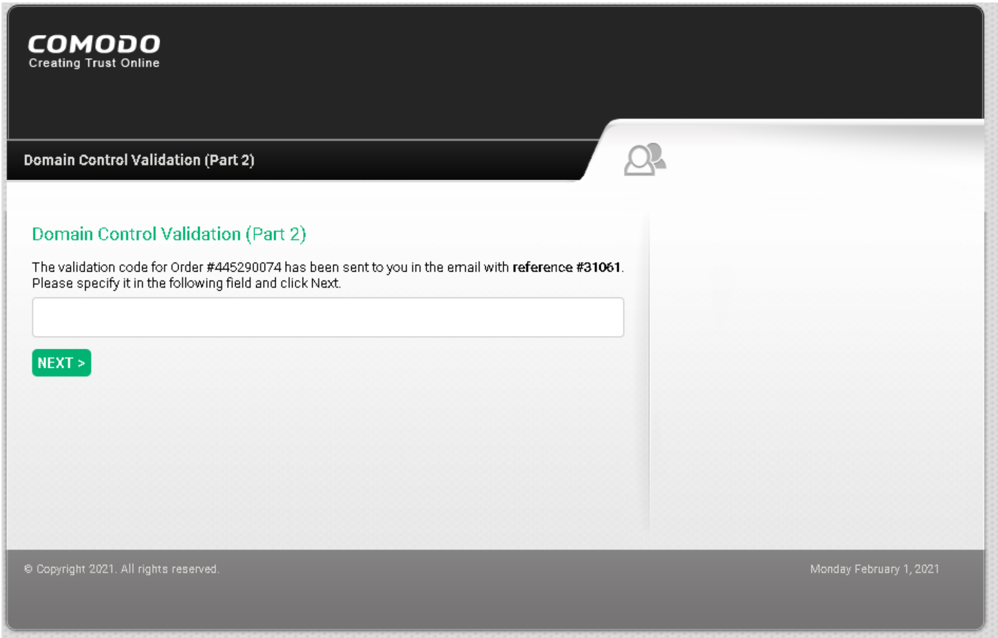
Need Help? Contact Us

Call us! +1(888) 481.5388

Email us! support@sectigostore.com

www.sectigostore.com

10. You will receive an email or telephone call from Sectigo with a validation code. Follow the links to enter in the code. Click **Next**.

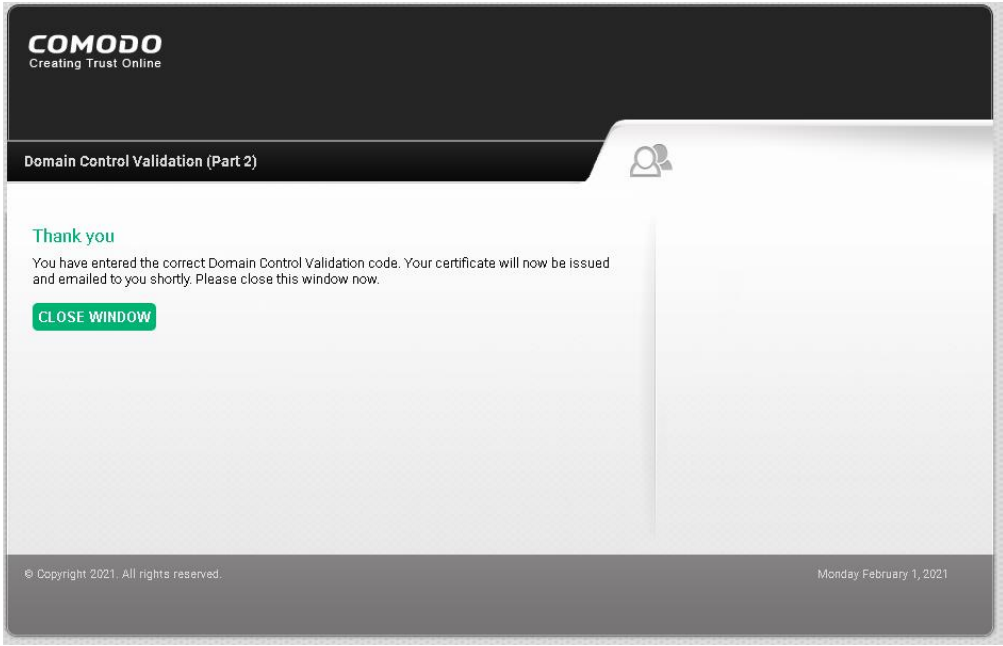

COMODO
Creating Trust Online
Domain Control Validation (Part 2)

Domain Control Validation (Part 2)

The validation code for Order #445290074 has been sent to you in the email with **reference #31061**. Please specify it in the following field and click Next.

NEXT >
© Copyright 2021. All rights reserved.
Monday February 1, 2021

11. You should see that the validation code is accepted. Click **Close Window**.


COMODO
Creating Trust Online
Domain Control Validation (Part 2)

Thank you

You have entered the correct Domain Control Validation code. Your certificate will now be issued and emailed to you shortly. Please close this window now.

CLOSE WINDOW
© Copyright 2021. All rights reserved.
Monday February 1, 2021

12. The Sectigo SSL Certificate for the domain will be issued and attached in email notification.

    Save the Zip file on your Intel SCS or EMA server so you can complete the re-keying of the certificate with the server that generated the CSR.

The zip file contains your Sectigo AMT SSL:

Intel_vprodemo_com.cer

Copy the chaining Root CA Certificate to the (RCS) - AAACertificateServices.crt

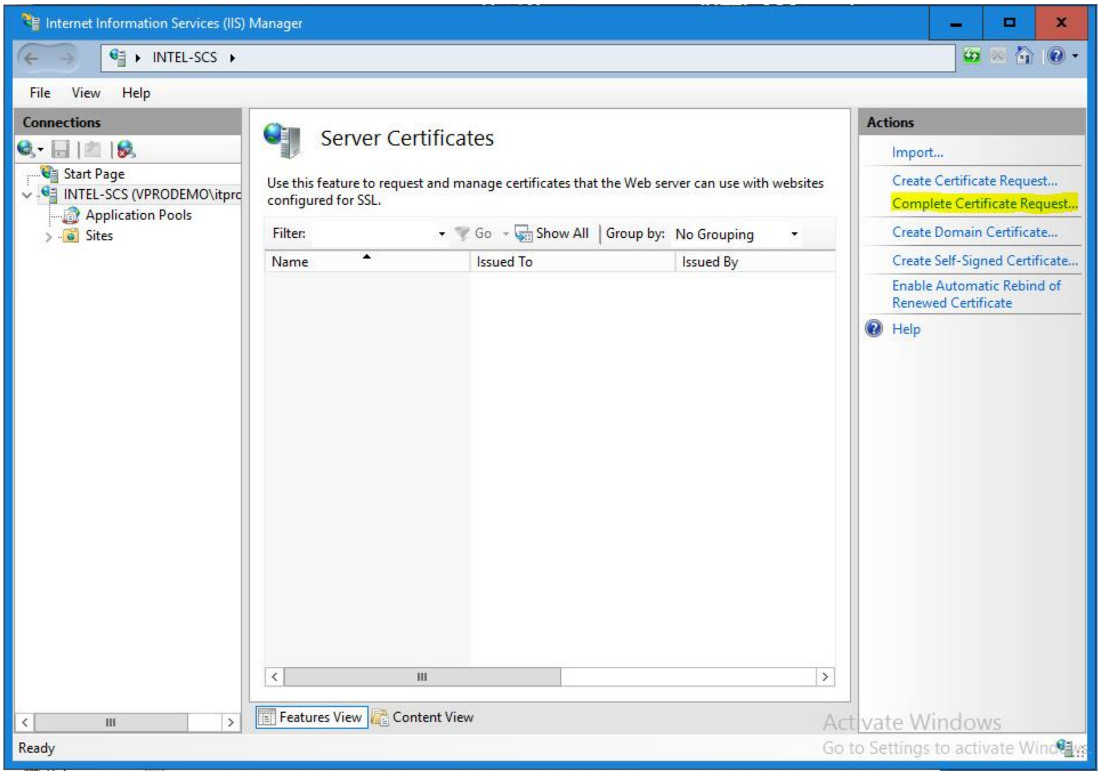
AAACertificateServices.crt

Copy the Chaining Intermediate CA Certificate to the (RCS) - COMODOProSeriesSecureServerCA.crt

COMODOProSeriesSecureServerCA.crt

4 Prepare the Certificate

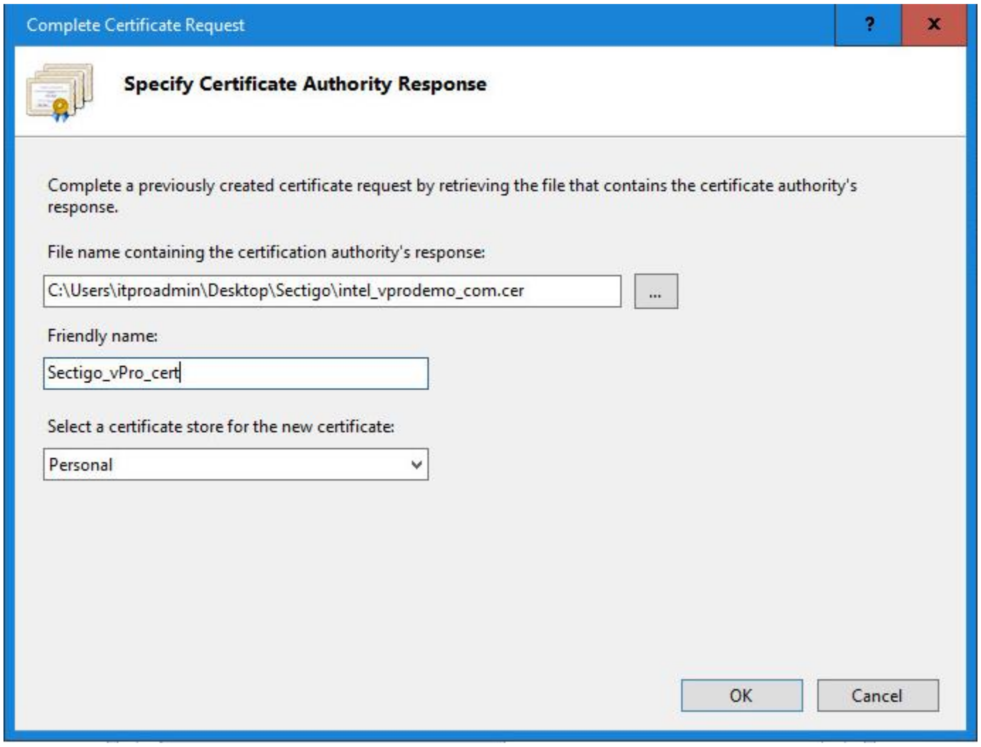
1. Once you receive the certificate from Sectigo, select the **Complete Certificate Request.**



Internet Information Services (IIS) Manager
INTEL-SCS
File
View
Help
Connections
Start Page
INTEL-SCS (VPRODEMO\itprc
Application Pools
Sites
Server Certificates
Filter:
Go
Show All
Group by:
No Grouping
Name
Issued To
Issued By
Features View
Content View
Ready
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help
Activate Windows
Go to Settings to activate Windows

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

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



Complete Certificate Request

Specify Certificate Authority Response

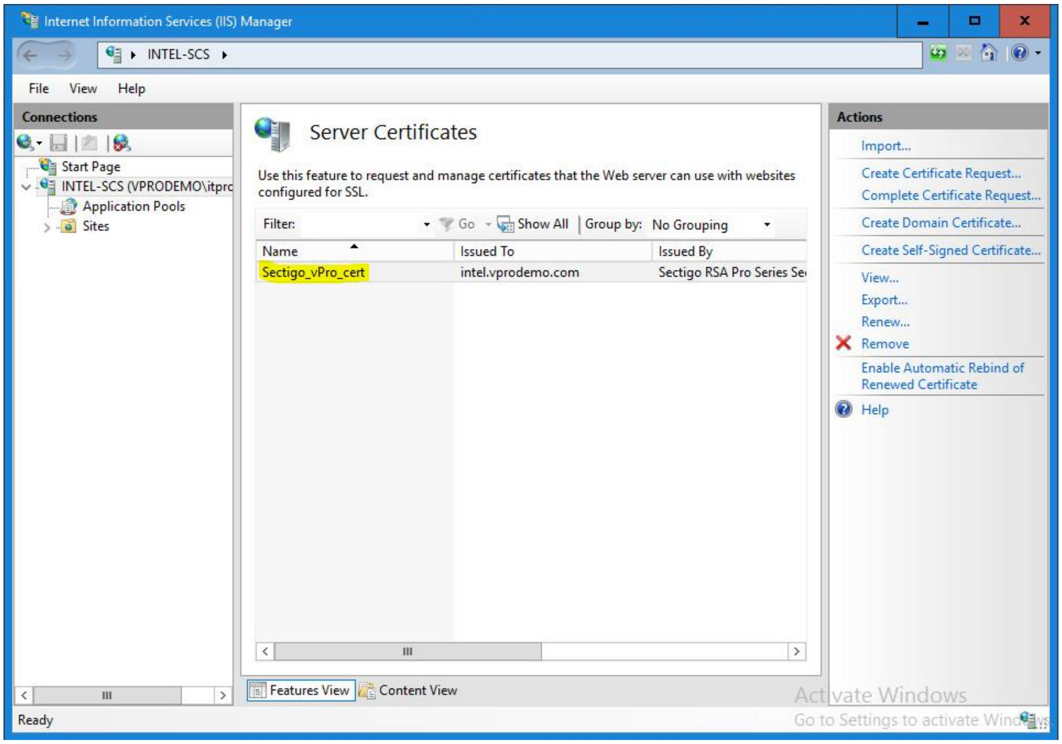
Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response: C:\Users\itproadmin\Desktop\Sectigo\intel_vprodemo_com.cer

Friendly name: Sectigo_vPro_cert

Select a certificate store for the new certificate: Personal

3. You should now see the Intel AMT Setup and Configuration Certificate in your IIS Server. Select this certificate and click **Export…** in the Actions menu.



Internet Information Services (IIS) Manager

Server Certificates

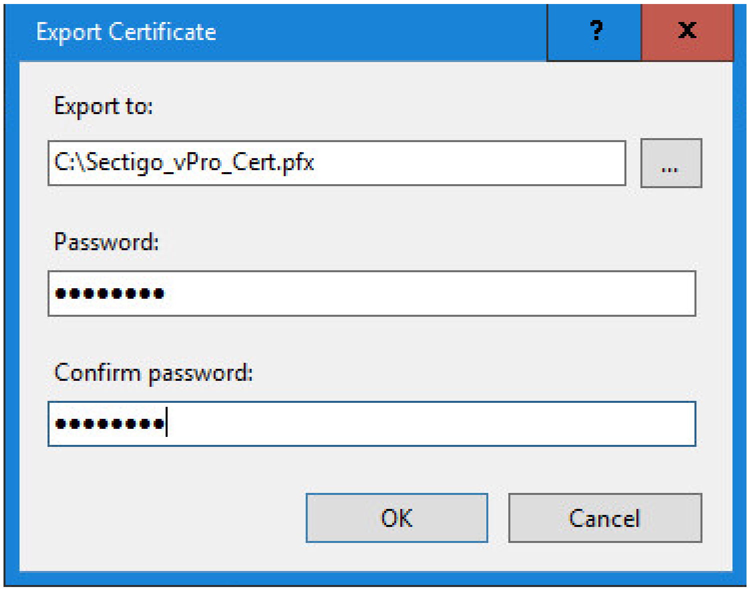
Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Filter: Go Show All | Group by: No Grouping

Name	Issued To	Issued By
Sectigo_vPro_cert	intel.vprodemo.com	Sectigo RSA Pro Series Se

INTEL-SCS
File
View
Help
Connections
Start Page
INTEL-SCS (VPRODEMO\itpro
Application Pools
Sites
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Renew...
Remove
Enable Automatic Rebind of Renewed Certificate
Help
Features View
Content View
Ready
Activate Windows
Go to Settings to activate Windows.

4. Browse to an export location, then enter a strong password. (This password will protect the private key.) Re-enter the password to confirm.



Export Certificate

Export to: C:\Sectigo_vPro_Cert.pfx

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

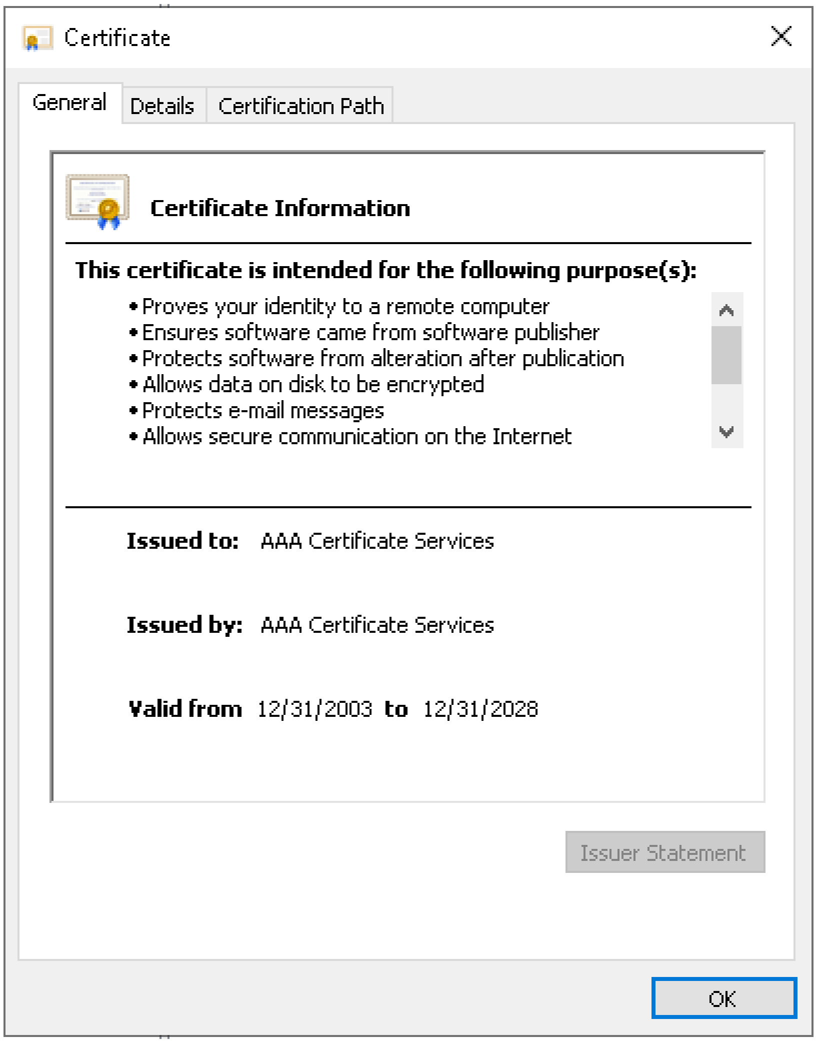
Click **OK**.

5 Install the Certificate

5.1 Install Root and Intermediate Certificates

Begin the installation by importing the root and intermediate certificates into the Current User Certificate Authorities Store of the service account for the RCS server.

1. Logon as the service account for the RCS server.
2. Double-click the **AAACertificateServices.crt** file where you saved it. Click **Install Certificate.**



Certificate Information

This certificate is intended for the following purpose(s):

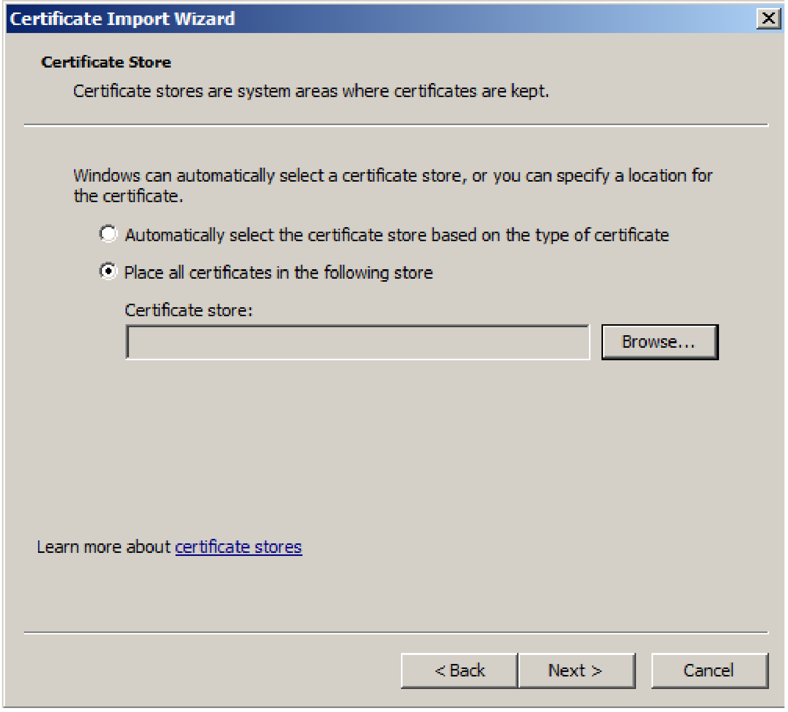
- Proves your identity to a remote computer
- Ensures software came from software publisher
- Protects software from alteration after publication
- Allows data on disk to be encrypted
- Protects e-mail messages
- Allows secure communication on the Internet

Issued to: AAA Certificate Services

Issued by: AAA Certificate Services

Valid from 12/31/2003 **to** 12/31/2028

3. Select **Place all certificates in the following store** and then click **Browse**.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

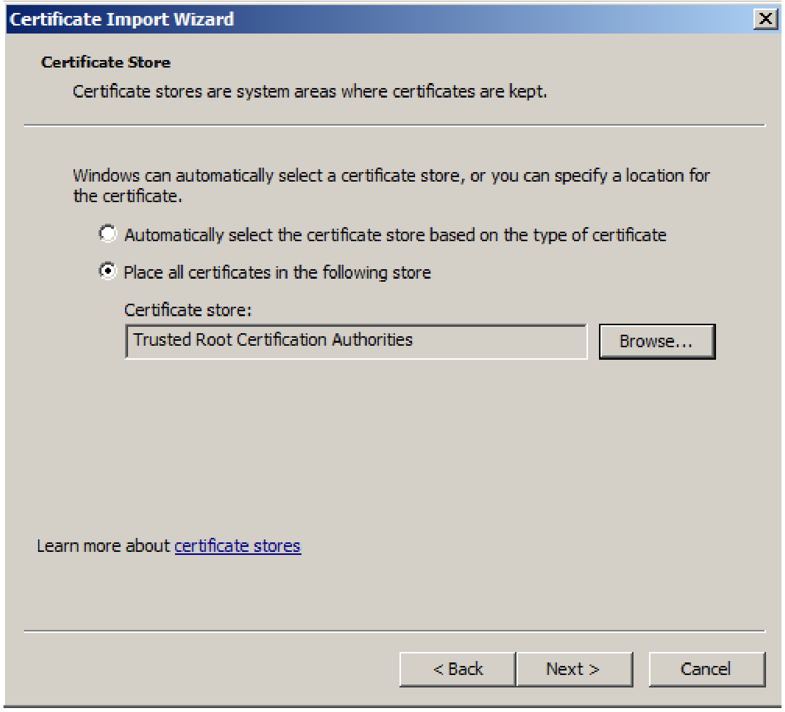
Windows can automatically select a certificate store, or you can specify a location for the certificate.

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

● Place all certificates in the following store

Certificate store:

Place the certificate in the Trusted Root Certificate Authorities. Click **Next**.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

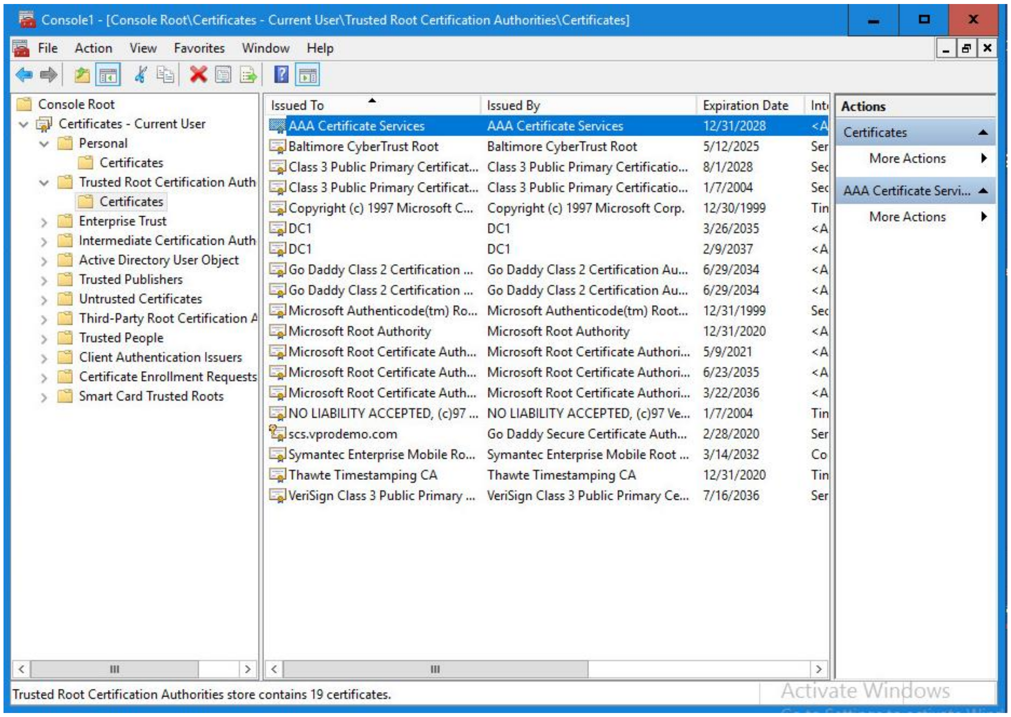
Windows can automatically select a certificate store, or you can specify a location for the certificate.

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

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

The certificate is now installed in the Trusted Root Certificate Authorities store.

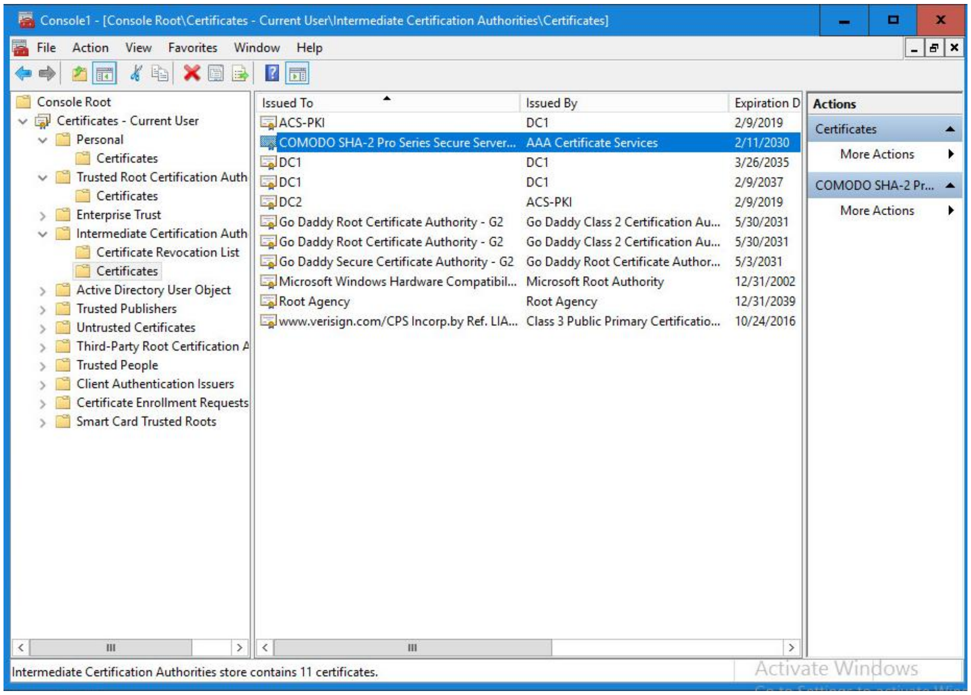


Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]

Issued To	Issued By	Expiration Date	Int
AAA Certificate Services	AAA Certificate Services	12/31/2028	<A
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Ser
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Sec
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	1/7/2004	Sec
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Tin
DC1	DC1	3/26/2035	<A
DC1	DC1	2/9/2037	<A
Go Daddy Class 2 Certification ...	Go Daddy Class 2 Certification Au...	6/29/2034	<A
Go Daddy Class 2 Certification ...	Go Daddy Class 2 Certification Au...	6/29/2034	<A
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999	Sec
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<A
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021	<A
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	6/23/2035	<A
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	3/22/2036	<A
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 Ve...	1/7/2004	Tin
scs.vprodemo.com	Go Daddy Secure Certificate Auth...	2/28/2020	Ser
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root ...	3/14/2032	Co
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Tin
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	7/16/2036	Ser

Trusted Root Certification Authorities store contains 19 certificates.

4. Repeat steps to install the **COMODOProSeriesSecureServerCA.crt** in the Intermediate Certificate Authorities store.



Console1 - [Console Root\Certificates - Current User\Intermediate Certification Authorities\Certificates]

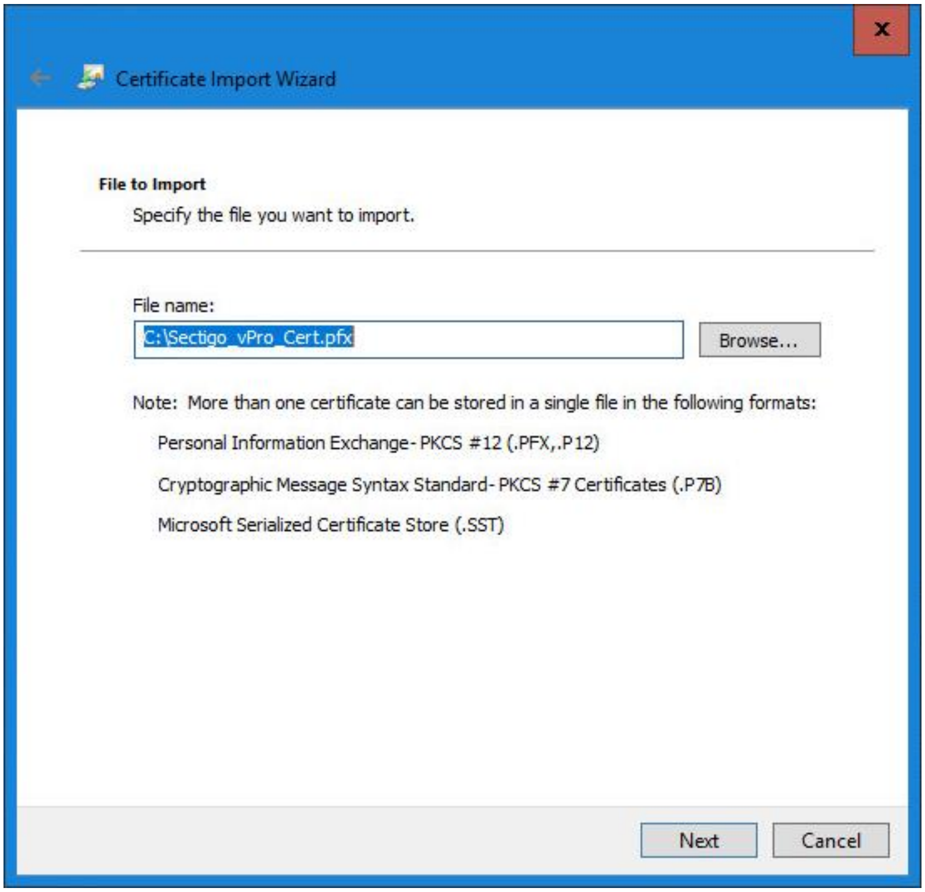
Issued To	Issued By	Expiration D
ACS-PKI	DC1	2/9/2019
COMODO SHA-2 Pro Series Secure Server...	AAA Certificate Services	2/11/2030
DC1	DC1	3/26/2035
DC1	DC1	2/9/2037
DC2	ACS-PKI	2/9/2019
Go Daddy Root Certificate Authority - G2	Go Daddy Class 2 Certification Au...	5/30/2031
Go Daddy Root Certificate Authority - G2	Go Daddy Class 2 Certification Au...	5/30/2031
Go Daddy Secure Certificate Authority - G2	Go Daddy Root Certificate Author...	5/3/2031
Microsoft Windows Hardware Compatibil...	Microsoft Root Authority	12/31/2002
Root Agency	Root Agency	12/31/2039
www.verisign.com/CPS Incorp.by Ref. LIA...	Class 3 Public Primary Certificatio...	10/24/2016

Intermediate Certification Authorities store contains 11 certificates.

5.2 Install and Chain PFX Certificate

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

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



File to Import

Specify the file you want to import.

File name: C:\Sectigo_vPro_Cert.pfx

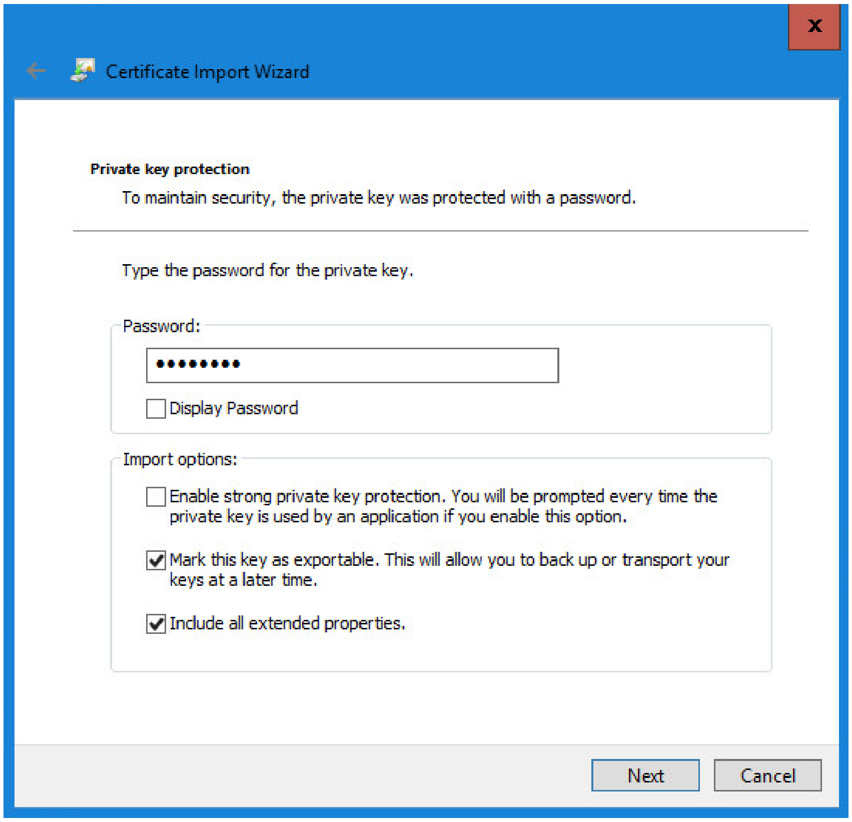
Note: More than one certificate can be stored in a single file in the following formats:

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

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

Microsoft Serialized Certificate Store (.SST)

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



Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

••••••••

□ Display Password

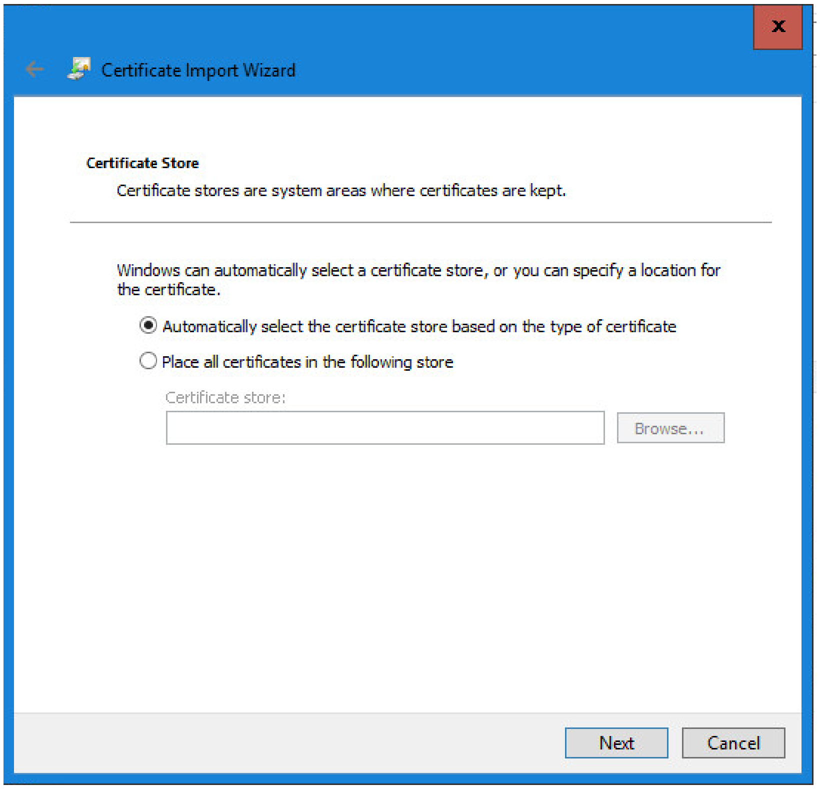
Import options:

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☑ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

3. Leave the default to place automatically in certificate store. Click **Next**.



Certificate Store

Certificate stores are system areas where certificates are kept.

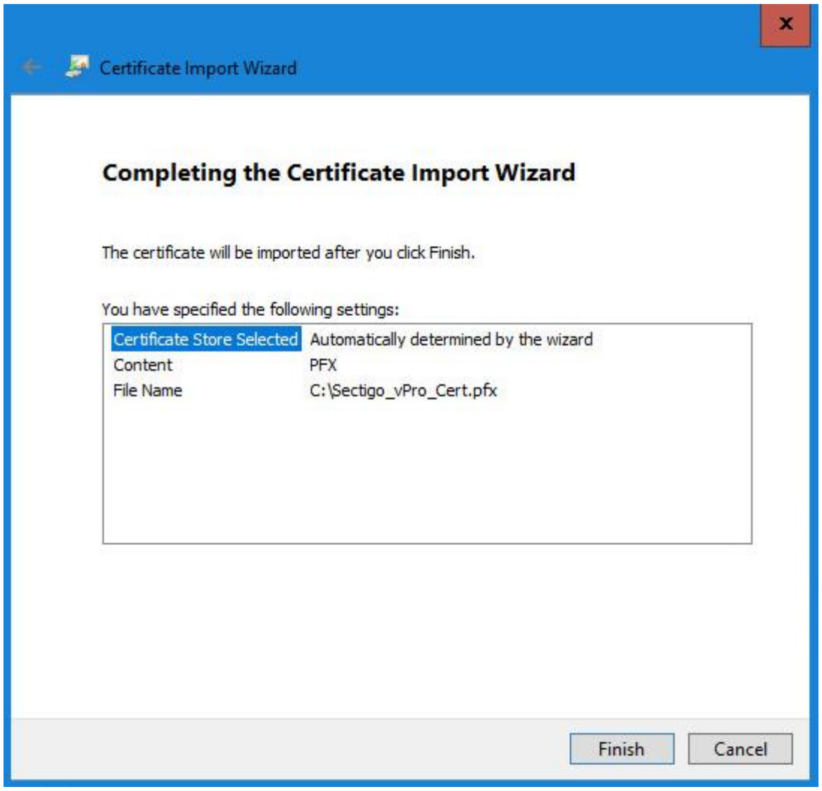
Windows can automatically select a certificate store, or you can specify a location for the certificate.

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

○ Place all certificates in the following store

Certificate store:

4. Click **Finish.**



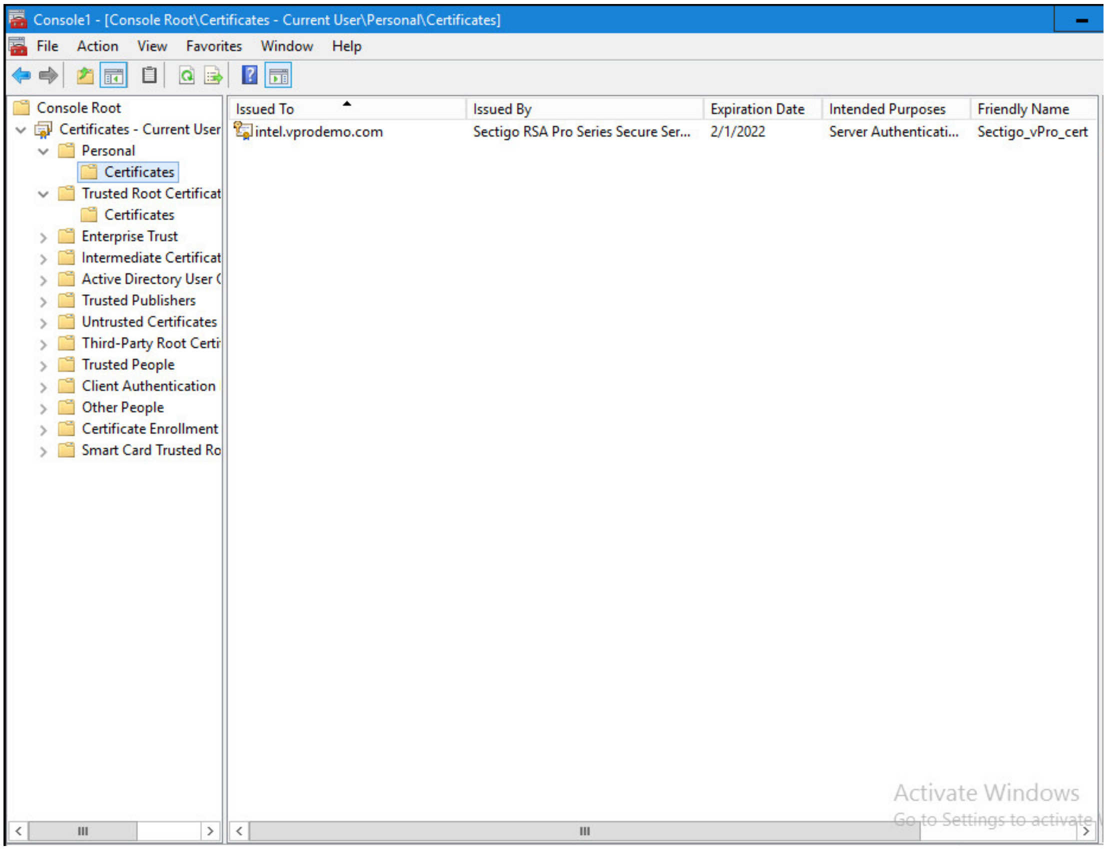
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

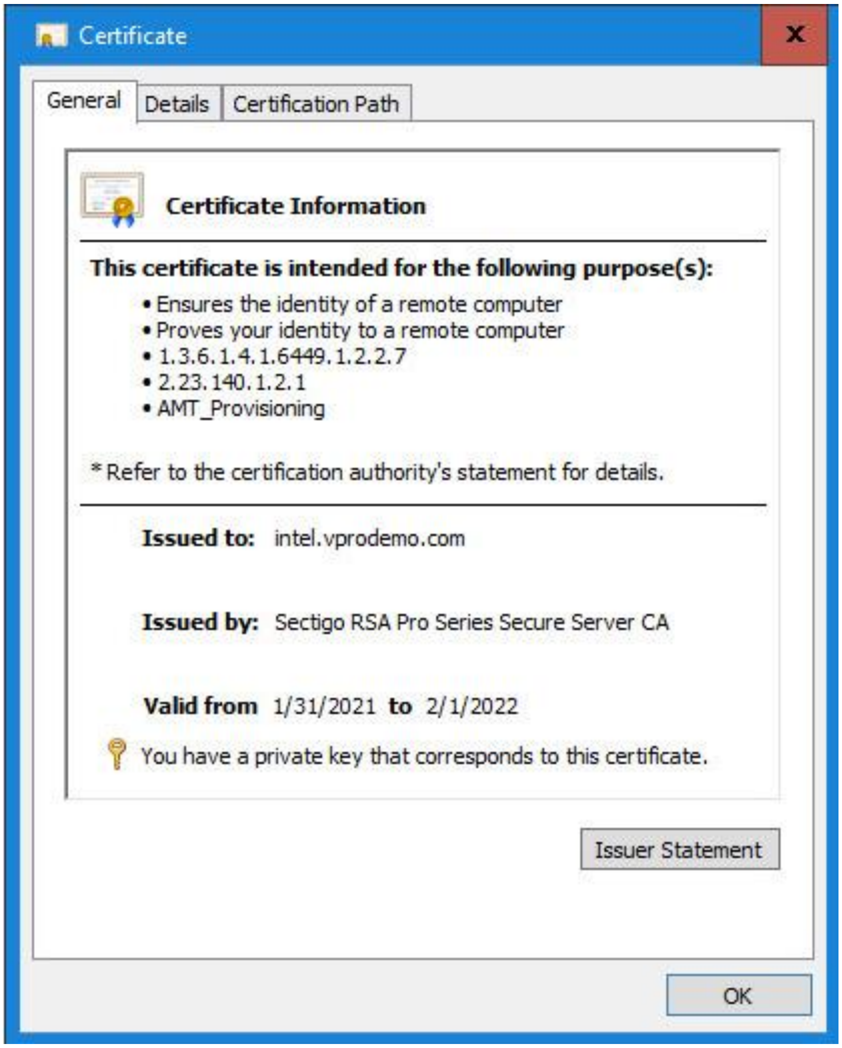
Certificate Store Selected	Automatically determined by the wizard
Content	PFX
File Name	C:\Sectigo_vPro_Cert.pfx

5. The certificate is now installed in the Current User Personal Certificates store. To verify the chain, double click **intel.vprodemo.com**.



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
intel.vprodemo.com	Sectigo RSA Pro Series Secure Ser...	2/1/2022	Server Authenticati...	Sectigo_vPro_cert

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



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 1.3.6.1.4.1.6449.1.2.2.7
- 2.23.140.1.2.1
- AMT_Provisioning

* Refer to the certification authority's statement for details.

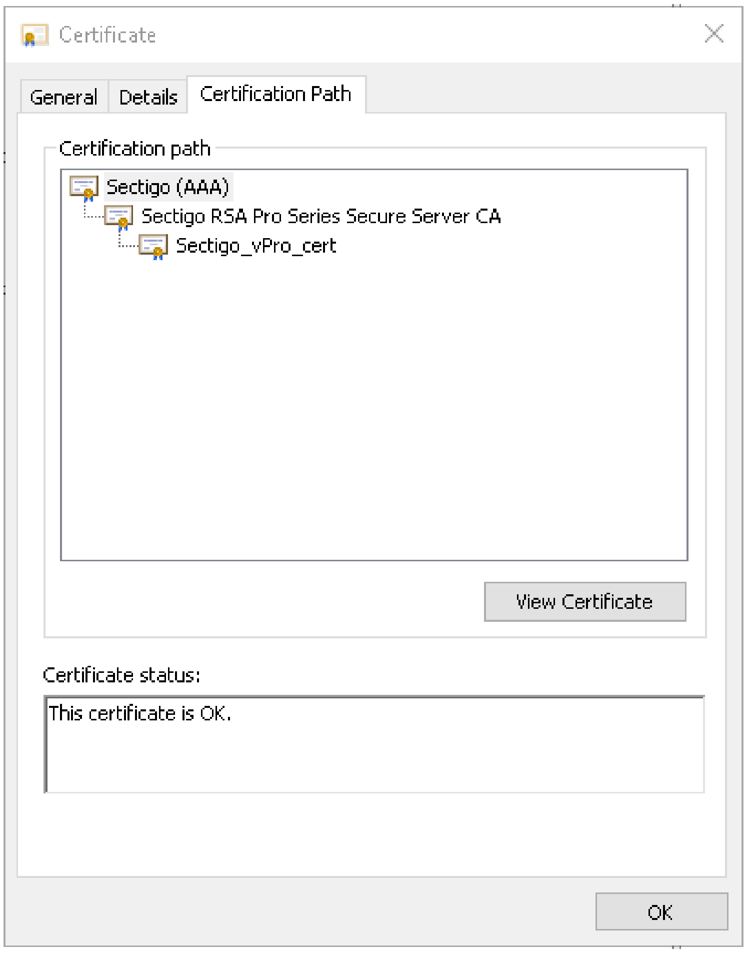
Issued to: intel.vprodemo.com

Issued by: Sectigo RSA Pro Series Secure Server CA

Valid from 1/31/2021 **to** 2/1/2022

You have a private key that corresponds to this certificate.

7. Check that the certificate is mapped to the Root Certificate Authorities as shown. Double-click on the root cert **Sectigo (AAA)** or **AAA Certificate Services**.

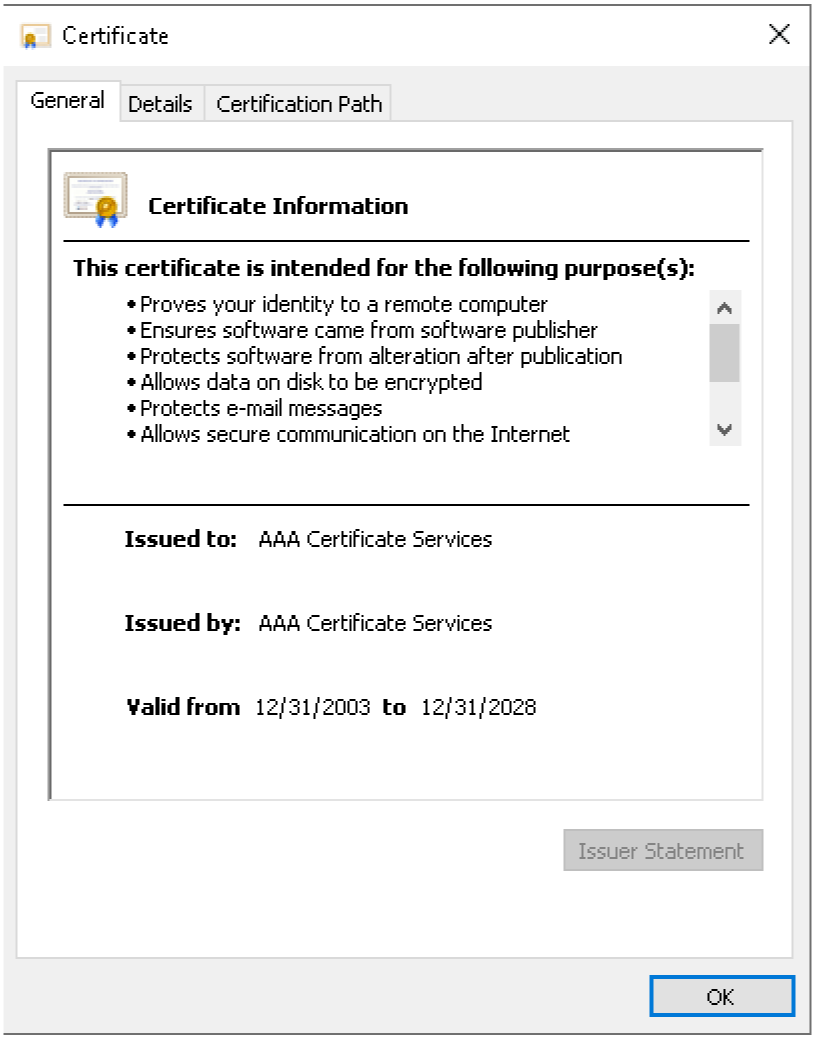


Sectigo (AAA)
Sectigo RSA Pro Series Secure Server CA
Sectigo_vPro_cert

Certificate status:

This certificate is OK.

8. Verify there are no errors with the root certificate, then click the **Details** tab.



Certificate Information

This certificate is intended for the following purpose(s):

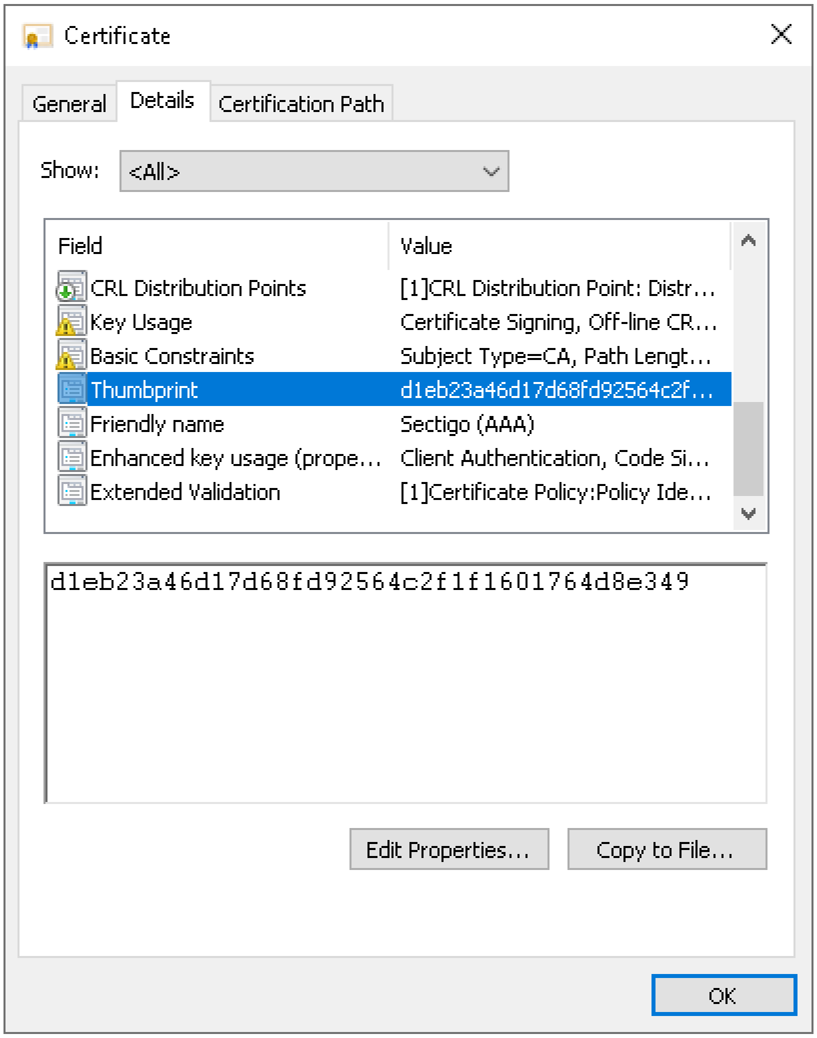
- Proves your identity to a remote computer
- Ensures software came from software publisher
- Protects software from alteration after publication
- Allows data on disk to be encrypted
- Protects e-mail messages
- Allows secure communication on the Internet

Issued to: AAA Certificate Services

Issued by: AAA Certificate Services

Valid from 12/31/2003 **to** 12/31/2028

9. On the Details tab, scroll down and select **Thumbprint**. The number must match what is shown below.



Show: <All>

Field	Value
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Key Usage	Certificate Signing, Off-line CR...
Basic Constraints	Subject Type=CA, Path Lengt...
Thumbprint	d1eb23a46d17d68fd92564c2f...
Friendly name	Sectigo (AAA)
Enhanced key usage (prope...	Client Authentication, Code Si...
Extended Validation	[1]Certificate Policy:Policy Ide...

```
d1eb23a46d17d68fd92564c2f1f1601764d8e349
```

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

6 Verify Successful Installation

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 or EMA documentation to try Remote Based Configuration in Admin Control mode. If successful, then your certificate is installed correctly.