

Intel® vPro™ Technology

How to Purchase and Install Entrust* Certificates for
Intel® AMT Remote Setup and Configuration

Revision History

Revision	Revision History	Date
1.0	First release.	Dec. 1, 2012

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: <http://www.intel.com/design/literature.htm%20>

Intel® vPro™ Technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software and IT environment. To learn more visit: <http://www.intel.com/technology/vpro>.

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

Intel, the Intel logo, Intel® AMT, and Intel® vPro are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.
 Microsoft Windows* operating system screenshots used with permission from Microsoft.
 Entrust* web screenshots used with permission from Entrust.

Copyright © 2012 Intel Corporation. All rights reserved.

Contents

1	Preface	1
1.1	Document Scope	1
1.2	Supported Intel® AMT Versions.....	1
1.3	Intended Audience.....	1
1.4	Prerequisites	1
2	Create a Certificate Signing Request	3
3	Send the Certificate Request to Entrust*	9
4	Prepare the Certificate	23
5	Install the Certificate	26
5.1	Install the Root Certificate	26
5.2	Install the Chain Certificate.....	28
5.3	Install the pfx Certificate	31
5.4	Verify the Certificate Chain	34
6	Verify that it Works	39

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 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 an Entrust* certificate that will match the pre-installed Entrust* 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 Entrust certificate on other management consoles. For consoles that do not use Intel SCS 8, 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 Entrust* certificates are supported in the following versions of Intel AMT:

- 7.0 and later

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. Before starting this process, you should have the following:

1. Intel SCS Remote Configuration Service installed on a supported Microsoft* operating system
2. One or more domain names for your network (Microsoft* Workgroups are not supported)

Purchasing Entrust* Certificates for Intel® AMT Remote Setup and Configuration

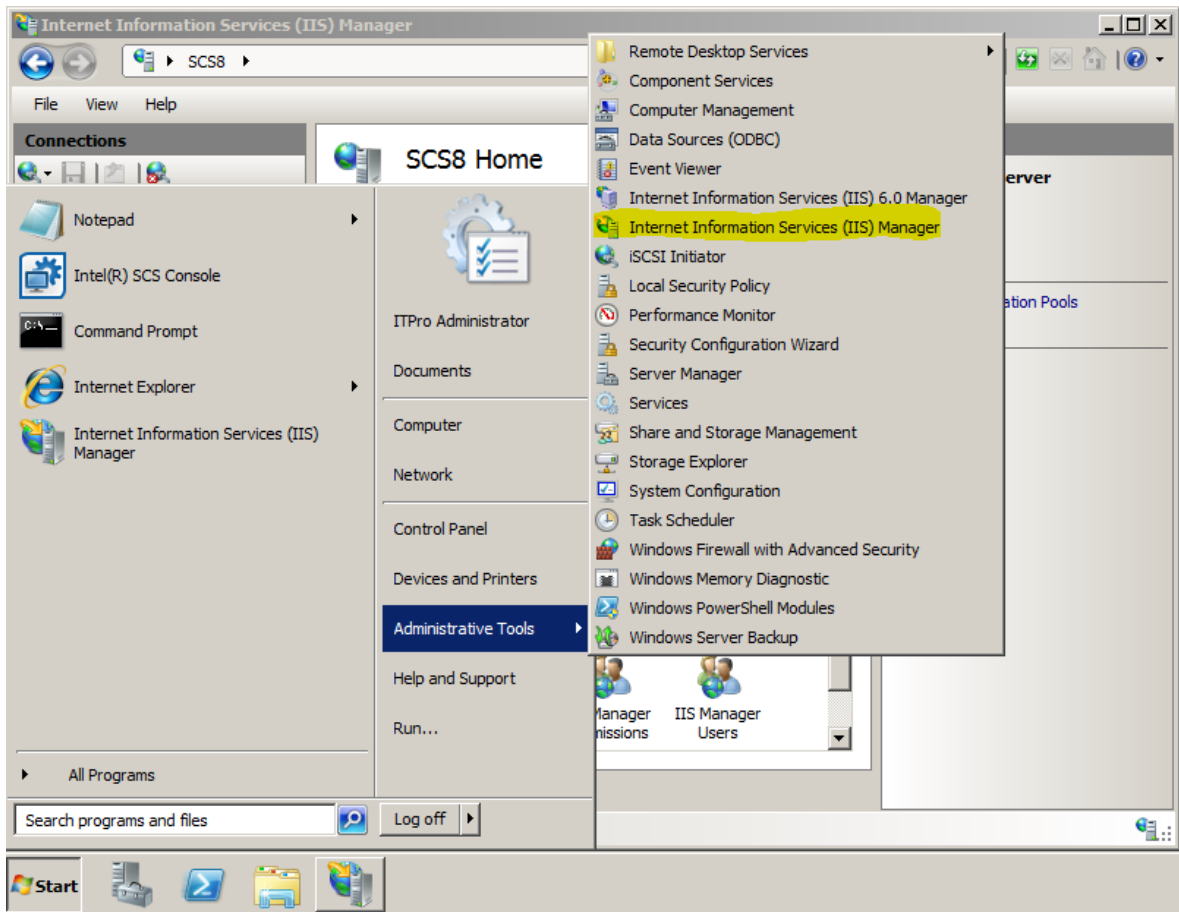
3. Microsoft* Internet Information Service (IIS) running on the server that is hosting the remote configuration service
4. Account permissions to install the certificate

2 Create a Certificate Signing Request

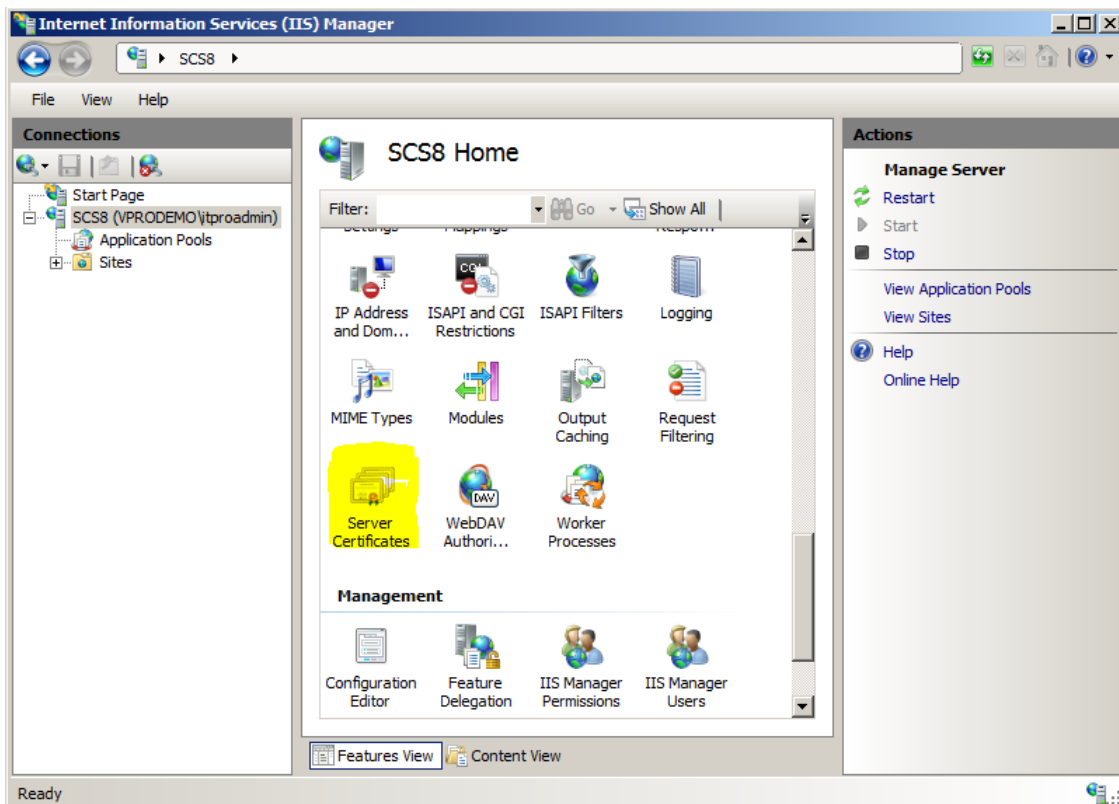
The following instructions were captured using Microsoft* Internet Information Services (IIS) for Windows* Server 2008 R2.

To create a Certificate Signing Request (CSR), do the following:

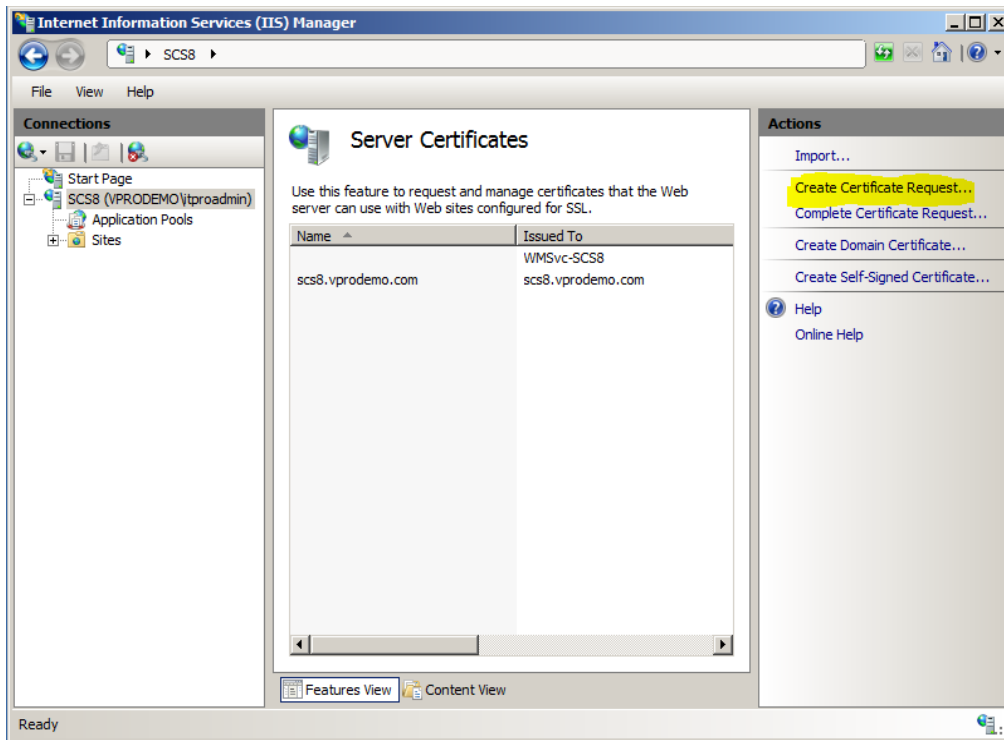
1. On your Intel SCS remote configuration server, open Programs→Administrative Tools→Internet Information Services (IIS) Manager.



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



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



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 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 MEBX.

Then, if your Remote Configuration Service (RCS) is running on SCS8.vprodemo.com, set CN=SCS8.vprodemo.com.

You can verify the DHCP Option 15 setting by running the SCSDiscovery utility (provided with Intel Setup and Configuration Software) 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:** Intel(R) Client Setup Certificate

Verify that the OU field is set to exactly "Intel(R) Client Setup Certificate" without the quote marks.

- **City:** The requesting organization's city
- **State:** The requesting organization's state
- **Country:** The requesting organization's country code

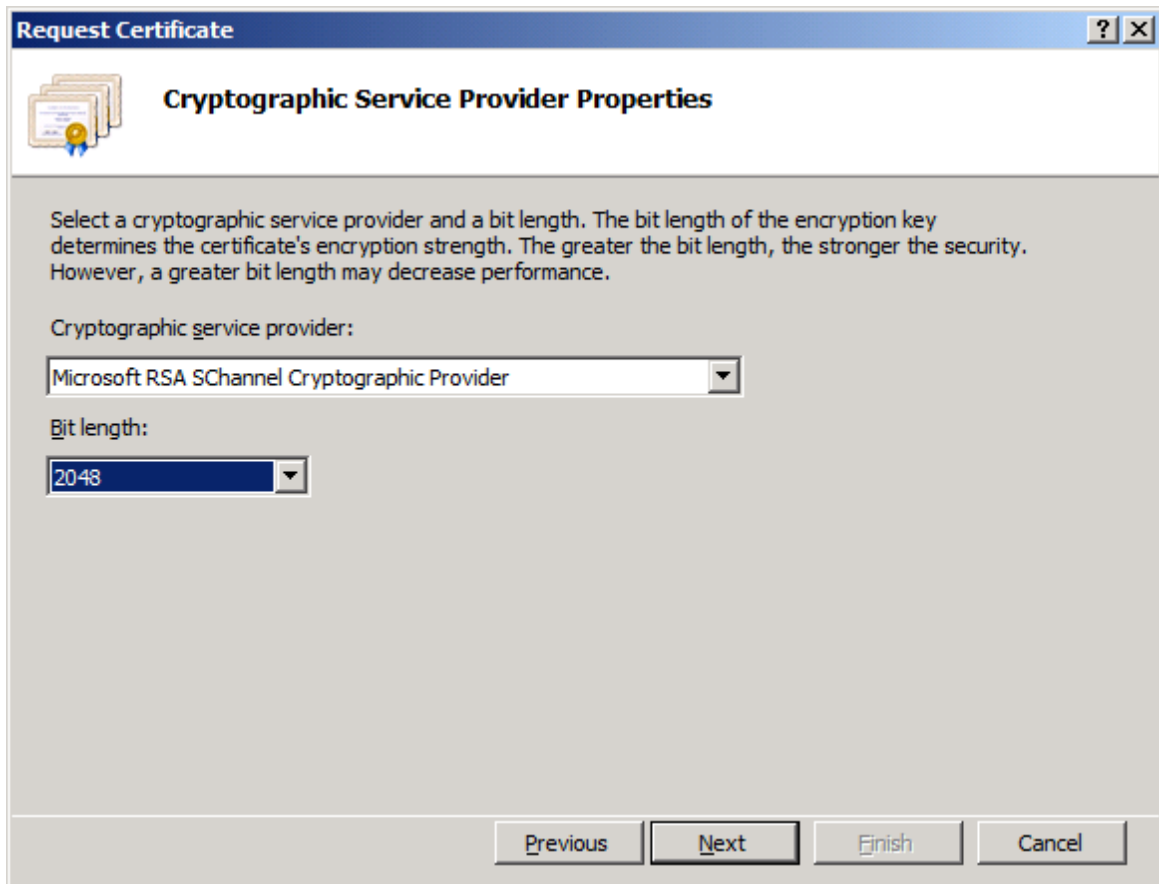
The screenshot shows a Windows dialog box titled "Request Certificate" with a sub-tab "Distinguished Name Properties". The dialog contains the following fields and values:

Field	Value
Common name:	SCS8.vprodemo.com
Organization:	Intel Corporation
Organizational unit:	Intel(R) Client Setup
City/locality:	Santa Clara
State/province:	California
Country/region:	US

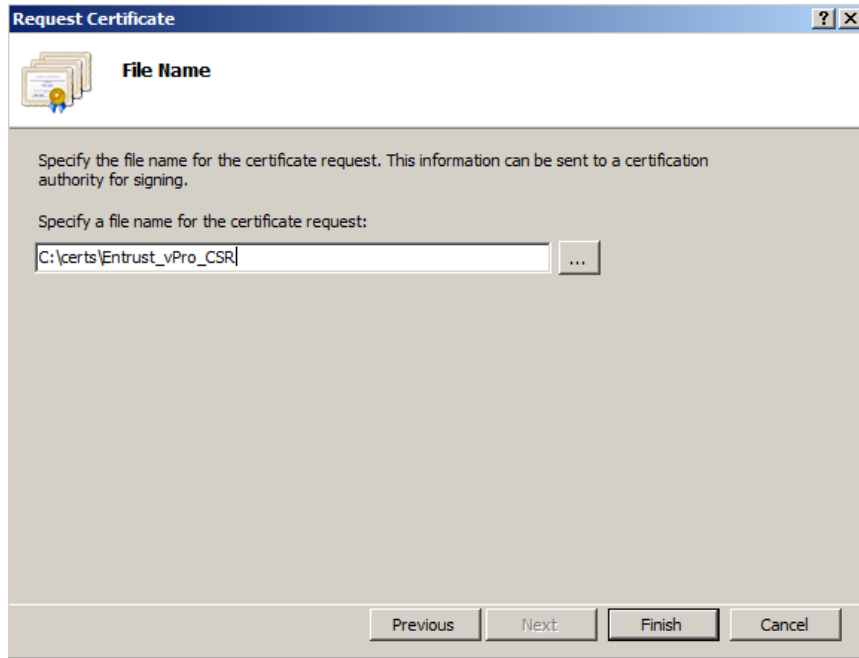
At the bottom of the dialog, there are four buttons: "Previous", "Next", "Finish", and "Cancel". The "Next" button is highlighted with a dark border.

Choose **Next**.

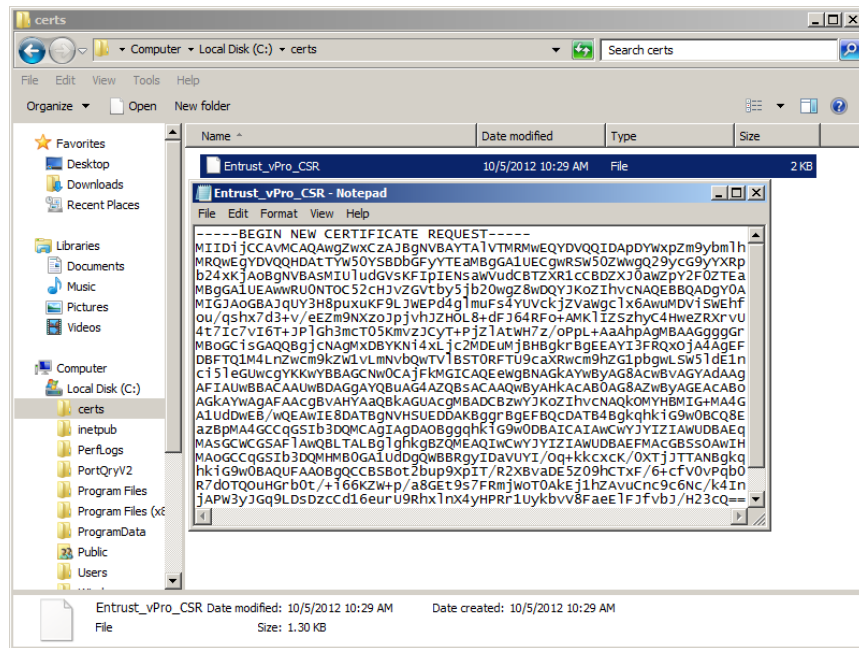
5. Leave the Cryptographic Service Provider set to **Microsoft RSA SChannel Cryptographic Provider** and select **2048** as your key Bit length. Choose **Next**.



- Choose the "...” button to select a location. Enter a file name to store the certificate request and then choose **submit**. Click **Finish**.



- This file, Entrust_vPro_CSR in our example, will be used to submit your request to Entrust for an Intel AMT Setup and Configuration certificate. You can open the file in Notepad to view encrypted certificate request.



3 Send the Certificate Request to Entrust*

1. Go to the Entrust* web site: <http://www.entrust.net/>
2. Intel® vPro™ Technology is supported on the following Entrust SSL certificates:
 - Advantage SSL Certificates
 - UC Multi-Domain SSL Certificates
 - Wildcard SSL Certificates

For this example, we will use **Advantage SSL Certificates**. From the Advantage SSL Certificates panel, choose **Buy Now**.

The screenshot displays the Entrust website interface. At the top, there is a navigation bar with links for Contact Us, Entrust.com, and a phone number (888-747-4086). A search bar is also present. The main banner features the Entrust logo and the text "SECURITY ON: SSL Entrust Discovery" with a sub-headline "Find, inventory and manage ALL certificates across ALL your systems and environments". Below the banner is a navigation menu with links for Why Entrust, Products, Support, Partners, About Us, and My Account. On the right side of the menu are icons for Chat, Phone, Blog, and Email. The main content area is divided into several sections:

- Go Wild!** New Wildcard SSL Certificates: From \$725/year. Includes a "Buy Now" button and a "Learn More" link.
- EV Multi-Domain SSL Certificates**: From \$373/year. Includes a "Buy Now" button and a "Learn More" link.
- UC Multi-Domain SSL Certificates**: From \$249/year. Includes a "Buy Now" button and a "Learn More" link.
- Advantage SSL Certificates**: From \$186/year. Includes a "Buy Now" button and a "Learn More" link.
- Standard SSL Certificates**: From \$155/year. Includes a "Buy Now" button and a "Learn More" link.

On the right side of the main content area, there is a list of services: Personal Secure Email, Enterprise Secure Email, Code Signing Certificates, Adobe CDS Signing Certificates, Certificate Management Service, and Certificate Discovery.

Below the main content area, there are two news items:

- Entrust Withdraws from CAB Forum**: CA/Browser Forum's Mandated Royalty-Free Intellectual Property Policy Change Requires Entrust to Withdraw from Organization it Co-Founded. Includes a "Learn More" link.
- Now Available — ECC Hybrid SSL Certificates**: Easily sign ECC keys via Entrust's proven RSA 2048-bit root for better performance and greater security. Includes a "Learn more" link.

At the bottom of the page, there is a footer with navigation links (Blog, Twitter, Site Map, Misuse Form, CPS, Privacy Policy, Legal), copyright information (© Copyright 2012 Entrust®, Inc. All rights reserved.), and the address (Entrust - Three Lincoln Centre - 5430 LBJ Freeway, Suite 1250 - Dallas Texas USA 75240). The Entrust logo and the Deloitte logo are also present.

- From the **Quote Order** menu, confirm **Advantage SSL** is chosen and choose **Buy Now**.

The screenshot shows the Entrust website interface for purchasing an SSL certificate. At the top, there is a navigation bar with links for 'Why Entrust', 'Products', 'Support', 'Partners', 'About Us', and 'My Account'. Below this is a progress indicator for the quote order process, with steps: Quote Order, Provide CSR, Provide Contact, Verify/Edit, Provide Payment, and Process Order. The 'Quote Order' step is currently active.

Below the progress indicator, there is a form asking 'Are you buying for a server outside of U.S., Great Britain or Canada?' with a checkbox and a 'Submit' button. To the right, there is a 'Promotional Code/Purchase Code' field with a 'Submit' button.

The main content area features a table with the following columns: Type, Lifetime, Quantity, Description, Renew Certificate Price, New Certificate Price, and Certificate Management Service Price. The table contains one row for 'Advantage SSL' with a quantity of 1. The 'Description' column lists features: 'Includes 2 domains', 'Server and client authentication support', and 'Unlimited re-issues'. The prices are: Renew Certificate Price: \$232.00, New Certificate Price: \$239.00, and Certificate Management Service Price: \$209.00. The total price is \$232.00. Below the table, there are buttons for 'Renew Now', 'Buy Now', and 'Buy Now'.

Below the table, there is a promotional banner that reads: 'Purchasing multiple SSL certificates? Save money. Increase efficiency. Rollover for more'. To the right of the banner is a padlock icon.

At the bottom of the page, there is a footer with links for 'Blog', 'Twitter', 'Site Map', 'Misuse Form', 'CPS', 'Privacy Policy', and 'Legal'. Below the links, there is a copyright notice: '© Copyright 2012 Entrust, Inc. All rights reserved.' and the address: 'Entrust - Three Lincoln Centre - 5430 LBJ Freeway, Suite 1250 - Dallas Texas USA 75240'. On the right side of the footer, there are logos for 'Entrust', 'WebTrust', and 'Deloitte'.

- At the **Provide CSR** menu, enter a secure passphrase and paste the CSR in the window. The passphrase will be used later in the process.

Confirm the following:

- Lifetime of the certificate
- Certificate Type
- Desired signing algorithm

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIEpzCCA3cCAQAwZm9ybmhm
IDApDYWxpZm9ybmhm
MRQwEgYDVQQHDATYwS0Y5SDBbGfYyTEaMBGGA1UECgwRS
W50ZWwgQ29ycG9yYXRp
b24xKjAoBgNVBAsMIUkudGVsKFp1EiE5aWVudCBTZXR1c2Vz
J0aWZpY2F0ZTEa
MBGGA1UEAwwRU0NTOC52CHvZGVtbysjb20wggEIMA0GCSq
GSIB3DQEBAAQUAA4IB
DwAwodEKAoIBAQDYaG7hkG7b5t1M10EmWFmpcM1hqNdlvB

Tracking ID | Type | Paste Certificate Signing Request (CSR), obtained from your server. CSR FAQ

1	Certificate Lifetime: 1 Year Certificate Type: Advantage SSL Signing Algorithm: SHA1	-----BEGIN NEW CERTIFICATE REQUEST----- MIIEpzCCA3cCAQAwZm9ybmhm IDApDYWxpZm9ybmhm MRQwEgYDVQQHDATYwS0Y5SDBbGfYyTEaMBGGA1UECgwRS W50ZWwgQ29ycG9yYXRp b24xKjAoBgNVBAsMIUkudGVsKFp1EiE5aWVudCBTZXR1c2Vz J0aWZpY2F0ZTEa MBGGA1UEAwwRU0NTOC52CHvZGVtbysjb20wggEIMA0GCSq GSIB3DQEBAAQUAA4IB DwAwodEKAoIBAQDYaG7hkG7b5t1M10EmWFmpcM1hqNdlvB
---	--	--

Previous Next
Cancel Order

Entrust Security Center
Certification Authorities
WebTrust
Deloitte

> Blog > Twitter > Site Map > Misuse Form > CPS > Privacy Policy > Legal
© Copyright 2012 Entrust®, Inc. All rights reserved.
Entrust - Three Lincoln Centre - 5430 LBJ Freeway, Suite 1250 - Dallas Texas USA 75240

Click **Next**.

5. Verify that the CSR fields are correct.

The screenshot shows the Entrust Security Center interface. At the top, there is a navigation menu with links for > Why Entrust, > Products, > Support, > Partners, > About Us, and > My Account. Below the menu is a progress bar with six steps: Quote Order, Provide CSR (current step), Provide Contact, Verify/Edit, Provide Payment, and Process Order. The main content area displays a table with the following data:

Certificate	Type	CSR Content	
1	1 Year Advantage SSL	SCS8.vprodemo.com UserDN=cn=SCS8.vprodemo.com, ou=Intel(R) Client Setup Certificate,o=Intel Corporation, l=Santa Clara, st=California, c=US Domain(s) Include All Remove All SCS8.vprodemo.com Default \$0.00 Add a new domain	Valid Replace

At the bottom right of the table area, there are buttons for **Previous**, **Next**, and [Cancel Order](#). The footer contains navigation links for > Blog, > Twitter, > Site Map, > Misuse Form, > CPS, > Privacy Policy, and > Legal. It also includes the Entrust logo, Certification Authorities logos (Entrust and WebTrust), and the Deloitte logo. Copyright information for 2012 Entrust, Inc. and the address 'Entrust - Three Lincoln Centre - 5430 LBJ Freeway, Suite 1250 - Dallas Texas USA 75240' are also present.

Choose **Next**.

- At the **Provide Contact** menu, enter the contact information for Billing, Authorization, and Technical.

[Contact Us](#) | [Entrust.com](#) | 877-661-5429 | | [Advanced Search](#)

[Why Entrust](#) | [Products](#) | [Support](#) | [Partners](#) | [About Us](#) | [My Account](#)

[Chat](#) | [Phone](#) | [Blog](#) | [Email](#)

Quote Order | Provide CSR | **Provide Contact** | Verify/Edit | Provide Payment | Process Order

[Returning Customer?](#)
 Enter an email address and passphrase from a previous order and we will pre-populate the contact information for you.

Contact Information

<input type="checkbox"/> Billing Contact Linda Harries	Required	[edit] [remove]
<input type="checkbox"/> Authorization Contact Minh Pham	Required	[edit] [remove]
<input type="checkbox"/> Technical Contact John Gardner	Required	[edit] [remove]

Note: Entrust requires you to provide different contacts for the authorization and technical contacts.

The information that you provide to Entrust in this form will be used to notify you of Entrust products and services that we think may be of interest to you.

If you do not want to receive such information please check this box.

[Previous](#) | [Next](#) | [Cancel Order](#)

[Blog](#) | [Twitter](#) | [Site Map](#) | [Misuse Form](#) | [CPS](#) | [Privacy Policy](#) | [Legal](#)

© Copyright 2012 Entrust, Inc. All rights reserved.
 Entrust - Three Lincoln Centre - 5430 LBJ Freeway, Suite 1250 - Dallas Texas USA 75240

Choose **Next**.

7. At the **Verify/Edit** menu, confirm all information are correct.

The screenshot shows the Entrust Security@Work web application interface. At the top, there is a navigation bar with the Entrust logo, a search bar, and links for Contact Us, Entrust.com, and a phone number. Below this is a secondary navigation bar with links for Why Entrust, Products, Support, Partners, About Us, and My Account, along with icons for Chat, Phone, Blog, and Email.

A progress indicator shows the current step as **Verify/Edit**, with other steps being Quote Order, Provide CSR, Provide Contact, Provide Payment, and Process Order.

The main content area displays a table of authorization contacts:

Contact Name	Status	Review	Edit
Billing Contact Linda Harries	Required	[review]	[edit]
Authorization Contact Minh Pham	Required	[review]	[edit]
Technical Contact John Gardner	Required	[review]	[edit]

Below the table is the **Authorization Contact** form, which includes fields for:

- First Name: Minh
- Last Name: [Redacted]
- Title/Position: vPro Support
- Email Address: [Redacted]
- Phone Number: [Redacted]
- Company Name: Intel Corporation
- Address: 200 Mission College Blvd
- City/Town: Santa Clara
- Country: United States
- State/Province: California
- Zip/Postal Code: 95054

Below the form is a table showing the Certificate details:

Certificate	Type	CSR Content	Action
1	1 Year Advantage SSL	SCSS.vprodemo.com UserDN=cn=SCSS.vprodemo.com, ou=Intel(R) Client Setup Certificate, o=Intel Corporation, l=Santa Clara, st=California, c=US Domain(s) SCSS.vprodemo.com	[Replace]

At the bottom, there is a **Subscription Agreement(s)** section with a scrollable text area containing the Entrust Certificate Services Subscription Agreement. Below the agreement is a checkbox for "By proceeding to the next step; I have read, understood and accept the Subscription Agreement." and buttons for **Previous**, **Next**, and **Cancel Order**.

Choose **Next**.

8. Fill in the appropriate payment information and then choose **Process Order**.

Entrust **SECURITYNOW** [Contact Us](#) [Entrust.com](#) 877-661-8429 [Advanced Search](#)

[Why Entrust](#) [Products](#) [Support](#) [Partners](#) [About Us](#) [My Account](#) [Chat](#) [Phone](#) [Blog](#) [Email](#)

Quote Order Provide CSR Provide Contact Verify/Edit **Provide Payment** Process Order

Quantity	Type	Unit Price	Total
1	1 Year Advantage SSL	\$239.00	\$239.00
		Subtotal	\$239.00
		GST	\$0.00
		PST	\$0.00
		Total Price	\$239.00

Entrust Limited
 1000 Innovation Drive Ottawa, Ontario, Canada K2K 3E7
 Phone: 1-877-369-7483 or 1-613-270-3769
 Fax: 1-877-839-3538 or 1-613-270-3280 [Email](#)

Payment Method

Card Type:	<input type="text" value="Select a credit card"/>
Card #:	<input type="text"/>
Expiry:	10 <input type="text"/> 2012 <input type="text"/>
Does the Billing Address of this card match the Billing Contact for the order?	<input type="radio"/> Yes <input type="radio"/> No

How Did You Hear About Us?

[Previous](#) [Process Order](#) [Cancel Order](#)

[Blog](#) [Twitter](#) [Site Map](#) [Misuse Form](#) [CPS](#) [Privacy Policy](#) [Legal](#)

© Copyright 2012 Entrust, Inc. All rights reserved.
 Entrust - Three Lincoln Centre - 5430 LBJ Freeway, Suite 1250 - Dallas Texas USA 75240

9. From the **Process Order** menu, you will see the order number.

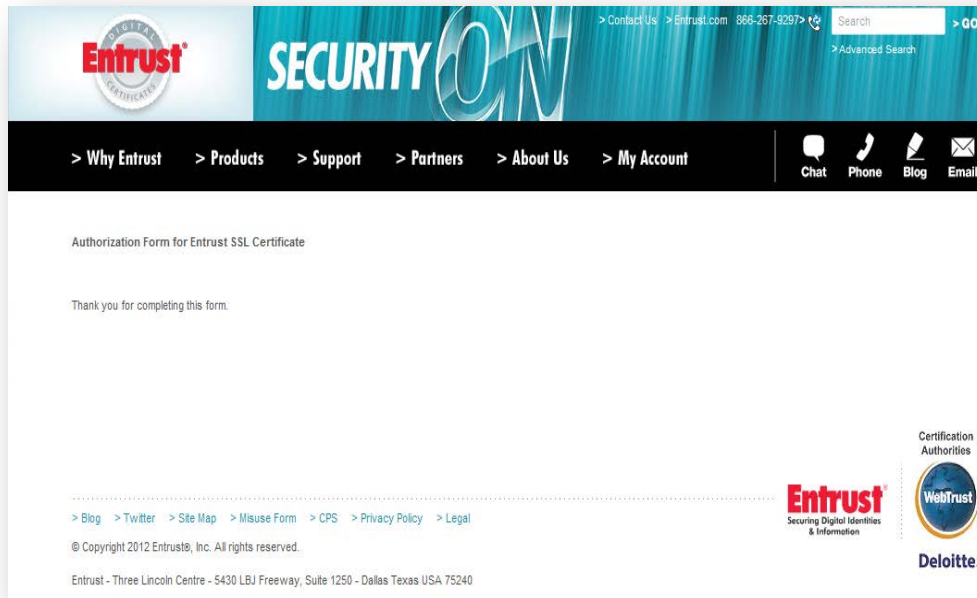
Securely store the order number along with the passphrase you supplied during the online enrollment process. Verification of the order will take 3 to 5 business days, after which time you will then be sent instructions for picking up and installing your Advantage SSL Certificate(s).

If you wish to know the status of your order at any time simply enter your order number into the form at:

http://www.entrust.net/customer/tracking_form.cfm

The screenshot shows the Entrust website's 'Thank you for your order' page. At the top, there is a navigation bar with the Entrust logo and 'SECURITY ON' text. Below the navigation bar, there are links for 'Why Entrust', 'Products', 'Support', 'Partners', 'About Us', and 'My Account'. A progress bar indicates the current step is 'Process Order'. The main content area features a 'Thank you for your order' heading, followed by the order number '12165084' and instructions for tracking the order. The footer includes a copyright notice for 2012 and logos for Entrust, WebTrust, and Deloitte.

10. A confirmation email is sent to the authorized contact. The authorized person is presented with a link to approve the consent form. Once approved, the process continues to the next phase: checking the Domain name, Corporation, and Final Phone Call.



11. Once the security verification process has been completed, a link to the certificate download page is provided with installation steps.

From the drop down list, **select server type** (IIS7 in our example), and then choose **Next**.

Entrust Digital Certificate

Installation Steps

Order ID: 12165084

[Installation Selection](#) > [Root Certificate](#) > [Chain Certificate](#) > [Server Certificate](#) > [Entrust Site Seal](#) > [Certificate Verification](#)

By stepping through this installation wizard, you will find your Entrust SSL certificate, the Entrust root/chain certificate(s) and the HTML code necessary to display the Entrust site seal on the web site protected by this certificate.

By installing these certificates onto your server, you will be able to provide seamless secure access to your site.

Please follow each step carefully to ensure that you have installed your certificate correctly.

Installation Selection

Select Certificate:

Select Server Type:

[Next >](#)

- From the **Root Certificate** menu, copy and paste the Root Certificate that is displayed into a text file. Save it as a .cer file. In this example, we named the file "Server_Certificate.cer".

Entrust DIGITAL CERTIFICATES

Installation Steps

Order ID: 12165084 Tracking ID: 153848
Installing Domain Name: SCS8.vprodemo.com Server Type: Microsoft IIS 7
> (Change)

Installation Selection > **Root Certificate** > Chain Certificate > Server Certificate > Entrust Site Seal > Certificate Verification

Instructions

- A root certificate is likely already installed on the server. If so, double check that it matches the one listed here.
- Copy the information from right or use button(s) to the right to create text file(s) on your hard drive.

Root Certificate

```
-----BEGIN CERTIFICATE-----  
MIIEKjCCAxKgAwIBAgIEOQPe+DANBgkqhkiG9w0BAQ  
UFADCBIDEUMBIGA1UEChMLRW50cnVzdC5u  
ZXQxQDA+BgNVBAsUN3d3dy5lbnRydXN0Lm5ldC9D  
UFNlMjA0OCBpbmNvcnAulGJ5HjZi4gKGrp  
bW0cyBsaWZlbnR5bW0zZDd3dy5lbnRydXN0Lm5ldC9D  
dHJ1c3QubmV0IEpibW0zZDd3dy5lbnRydXN0Lm5ldC9D  
BAMTKKvudHJ1c3QubmV0IENlcnRpZmljYXRpb24gCg
```

Root Cert File

< Previous **Next** >

FAQ

> Print FAQ

How is the Trusted Root Certificate installed on a Microsoft server?

Question:

How is the Trusted Root Certificate installed on Microsoft server?

NOTE: These instructions apply to the following server types:

- Microsoft IIS 6
- Microsoft IIS 7
- Microsoft Exchange 2007 (Windows Server 2008)
- Microsoft Exchange 2010
- Microsoft Office Communications Server 2010
- Microsoft Lync 2010
- Microsoft ISA
- Microsoft Forefront TMG

< Previous **Next** >

Choose **Next**.

- From the **Chain Certificates** menu, copy and paste the Chain Certificate that is displayed into a text file. Save it as a .cer file. In this example, we named the file "Chain_Certificate.cer".

Entrust DIGITAL CERTIFICATES

Installation Steps

Order ID: 12165084 Tracking ID: 153848
Installing Domain Name: SCS8.yprodemo.com Server Type: Microsoft IIS 7
> (Change)

Installation Selection > Root Certificate > **Chain Certificate** > Server Certificate > Entrust Site Seal > Certificate Verification

Instructions

1. Both a chain root and a chain certificate are being provided. Please note that both are needed.

Chain Certificate

```
-----BEGIN CERTIFICATE-----
MIIE9TCCA92gAwIBAgIETAE6MOTANBgkqhkiG9w0BAQ
UFADCBIDEUMBIGA1UEChML
RW50cmVzdC5uZXQxODAtBgNVBAsUN3d3dy5lbnRy
dXN0Lm5ldC9DUFNhY0QCBp
bmNvcnAulGJ5HJIZ4gKXpbWl0cyBsYW50Lm5ldC9DUFNhY0QCBp
gNVBAsTHChjKSAvOTk5
IEVudHJ1c3QubmV0IExpbnR0ZWQxMzAxBgNVBAMTK
```

Chain Cert File

< Previous **Next >**

FAQ > Print FAQ

How is the Chain Certificate installed on Microsoft IIS 7?

Question:
How is the Chain Certificate installed on Microsoft IIS 7?

NOTE: These instructions apply to the following server types:

- Microsoft IIS 7
- Microsoft Exchange 2007 (Windows Server 2008)
- Microsoft Exchange 2010
- Microsoft Office Communications Server 2010
- Microsoft Lync 2010
- Microsoft Forefront TMG

Answer:

< Previous **Next >**

Choose **Next**.

- From the **Server Certificates** menu, copy the Server Certificate that is displayed and then paste it into a text file. Save it as a .cer file. In this example, we named the file "Server_Certificate.cer".

Entrust DIGITAL CERTIFICATES

Installation Steps

Order ID: 12165084 Tracking ID: 153848
 Installing Domain Name: SCS8.vprodemo.com Server Type: Microsoft IIS 7
 > (Change)

Installation Selection > Root Certificate > Chain Certificate > **Server Certificate** > Entrust Site Seal > Certificate Verification

Instructions

- Your server certificate can be found in the box on the right.
- Copy the information from right or use button(s) to the right to create text file(s) on your hard drive.

Server Certificate

```
-----BEGIN CERTIFICATE-----
MIIFQDCCBgAwIBAgIETB4SKjANBgkqhkiG9w0BAQ
UFADCBsTELMAGGA1UE
BhMCVWmxFJAUBgNVBAoTDUUVudHJ1c3QsIEUyY4xO
TA3BgtNVBA5TMHd3dy5l
bnRydXNOLm5ldC9ycGEgaXMgaW5jb3Jwb3JhdGVk
GJ5IHUJ2mVjZW5jZTEf
MB0GA1UECzMMWKGmpDlwmDkgRW50cnVzdCwgSW
```

Server Cert File

< Previous **Next >**

FAQ > Print FAQ

How is the Server Certificate installed on IIS 7?

Question:
How is the Server Certificate installed on IIS 7?

Answer:
After you receive the secure certificate pickup link from Entrust, follow the instructions below to install your new certificate in IIS 7 and bind your new certificate with the Web site to be secured.

To install the SSL certificate in IIS 7:

- Pick up your Entrust Certificate through the secure pickup link that is sent to you. Copy and paste the certificate that is displayed into a text file.

The certificate should look like this:

```
-----BEGIN CERTIFICATE-----
MIIEITCCA2mgAwIBAgIESyDyZjANBgkqhkiG9w0BAQUFADCBsTELMAGGA1UE
```

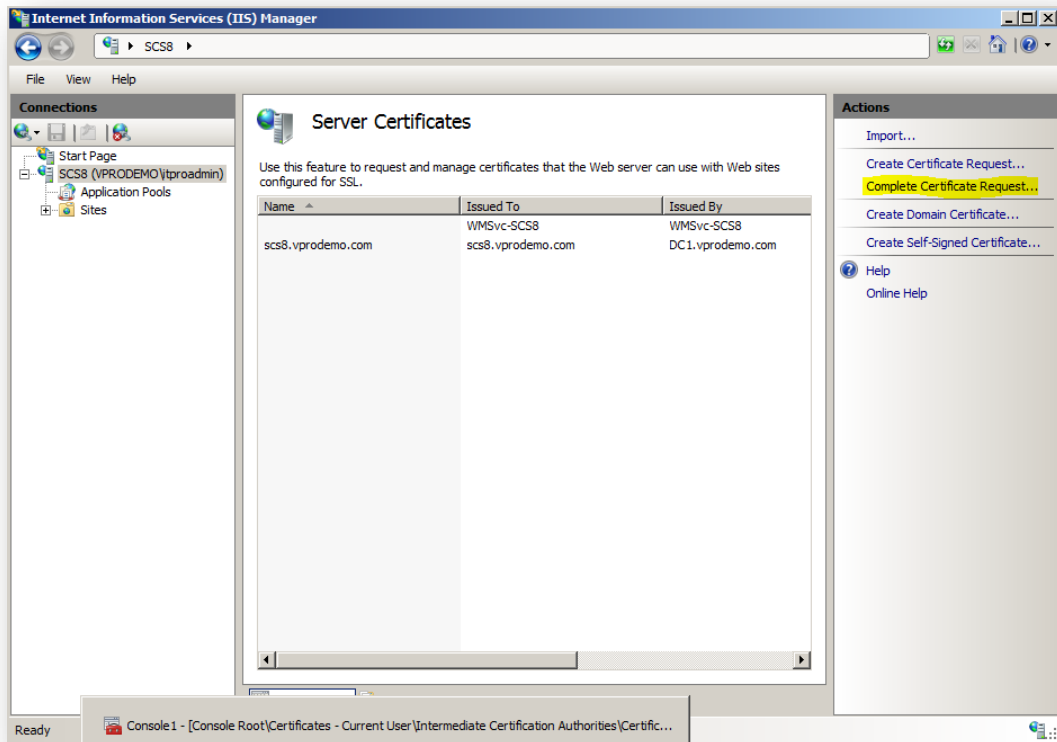
< Previous **Next >**

Choose **Next**.

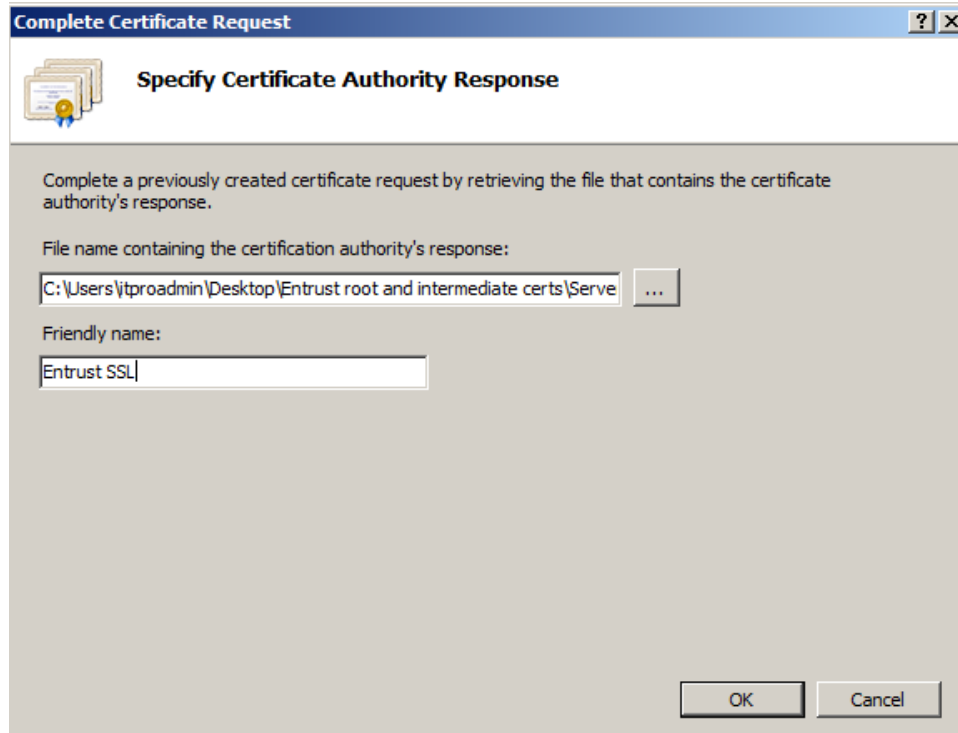
15. (Optional) Complete the next two steps, if desired:
 - Entrust Site Seal
 - Certificate Verification

4 Prepare the Certificate

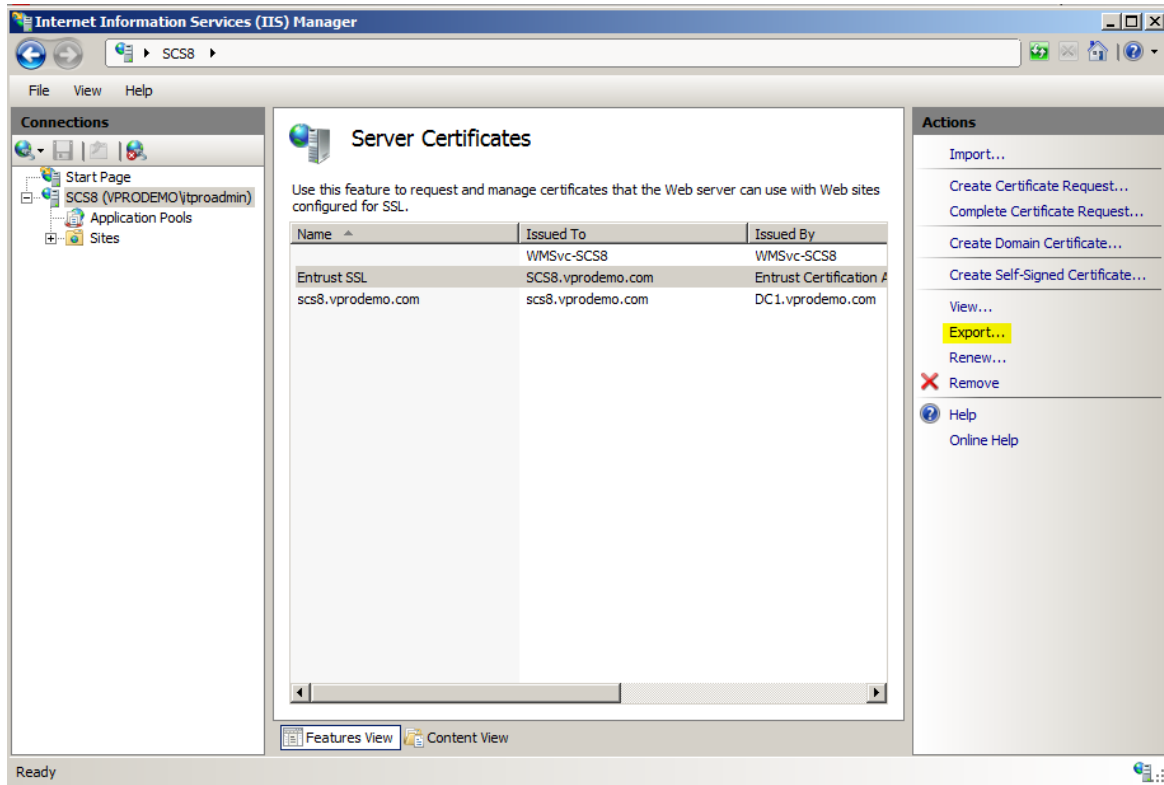
1. In Internet Information Services (IIS) Manager, select the **Complete Certificate Request** on the Actions menu.



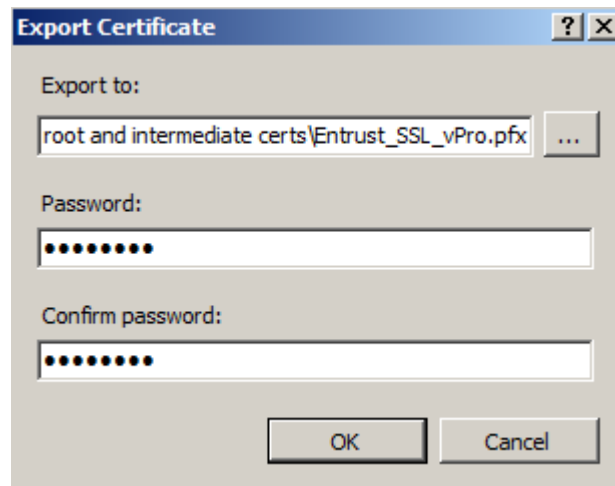
2. Navigate to the **Server Certificate** file that was saved as Server_Certificate.cer. Enter a Friendly name, and then choose **OK**.



- You will now see the Intel AMT Setup and Configuration Certificate in your Server Certificates list. Highlight this certificate and then choose **Export...** in the Actions menu.



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



Choose **OK**.

5 Install the Certificate

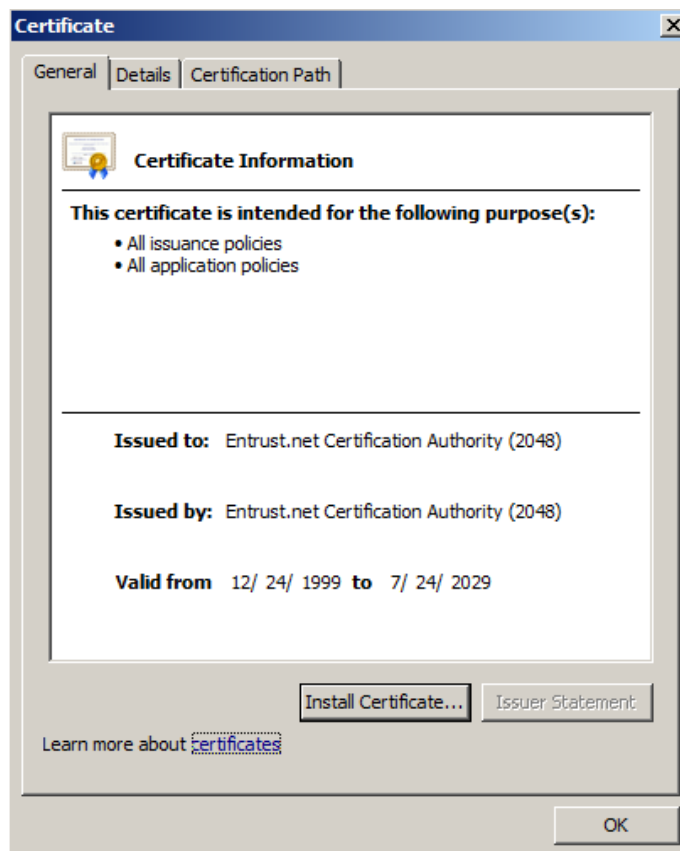
This section will show you how to do the following:

- Install the root and intermediate certificates (these certificates form part of the chain from the certificate that you purchased.
- Install the pfx certificate that you purchased
- Verify that the certificate is installed correctly

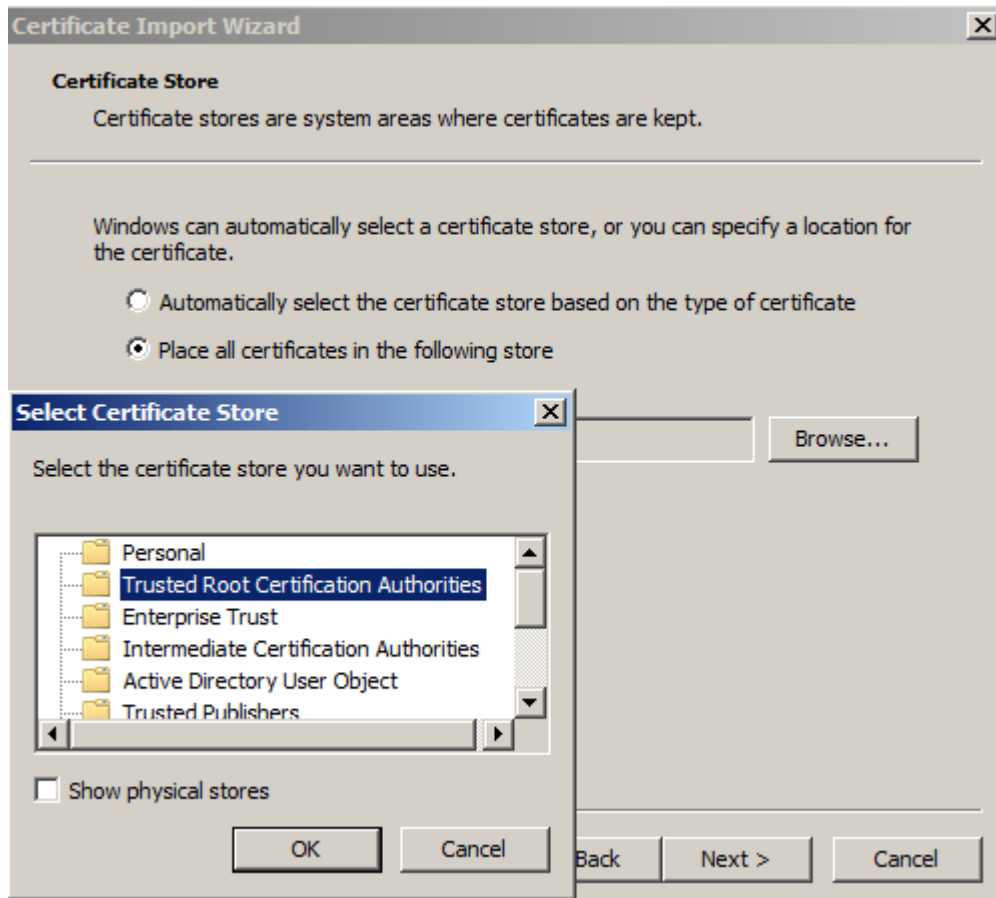
5.1 Install the Root Certificate

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

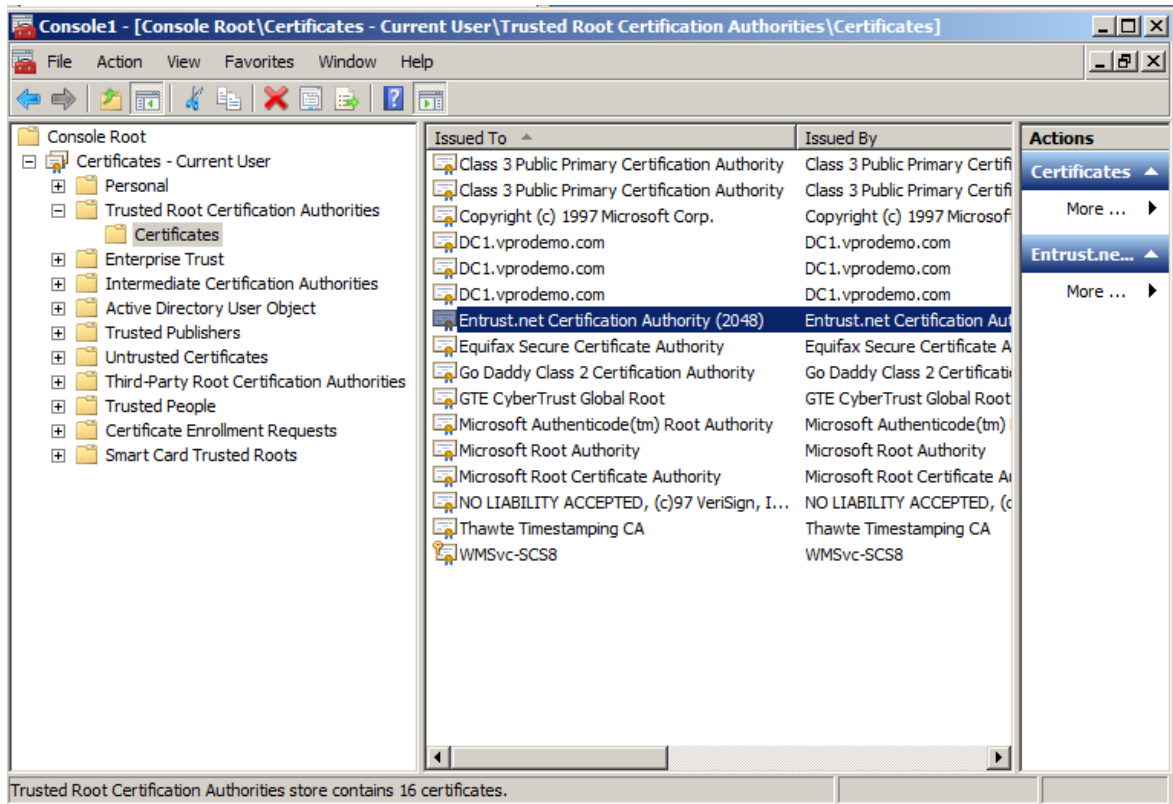
1. Logon as the service account for the RCS server.
2. Double-click the **Root_Certificate.cer** file where you saved it. Choose **Install Certificate**.



3. Choose Place all certificates in the following store radio button and then select Trusted Root Certificate Authorities. Click OK then Next.



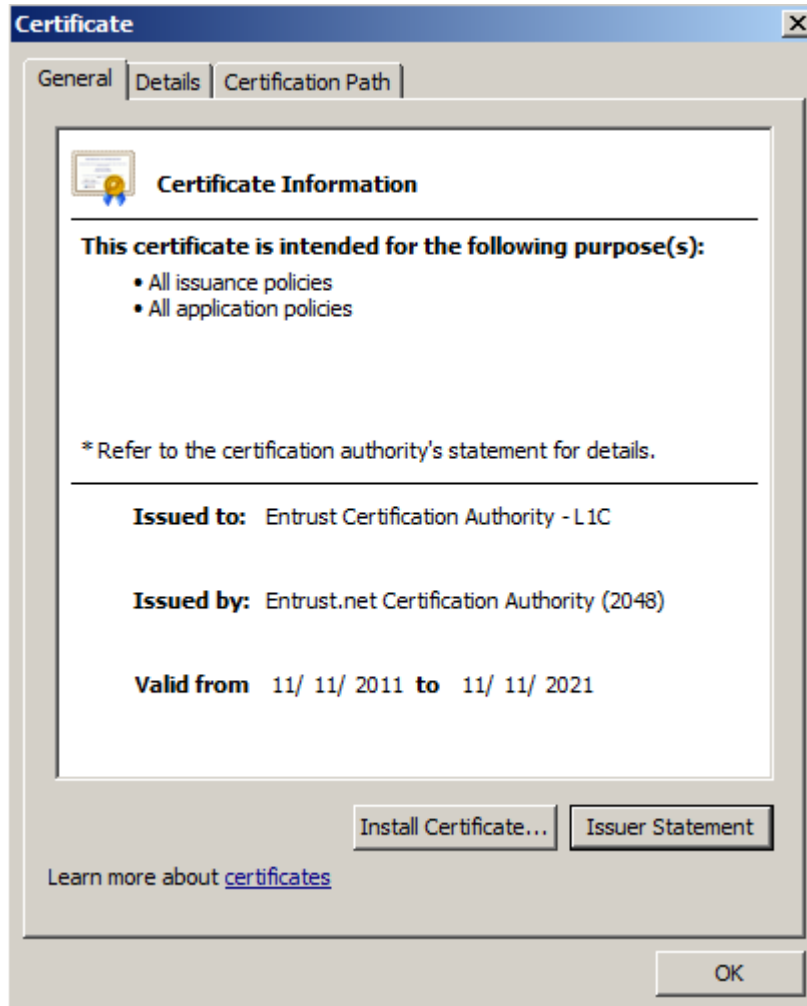
The certificate is now installed in the Trusted Root Certificate Authorities store.



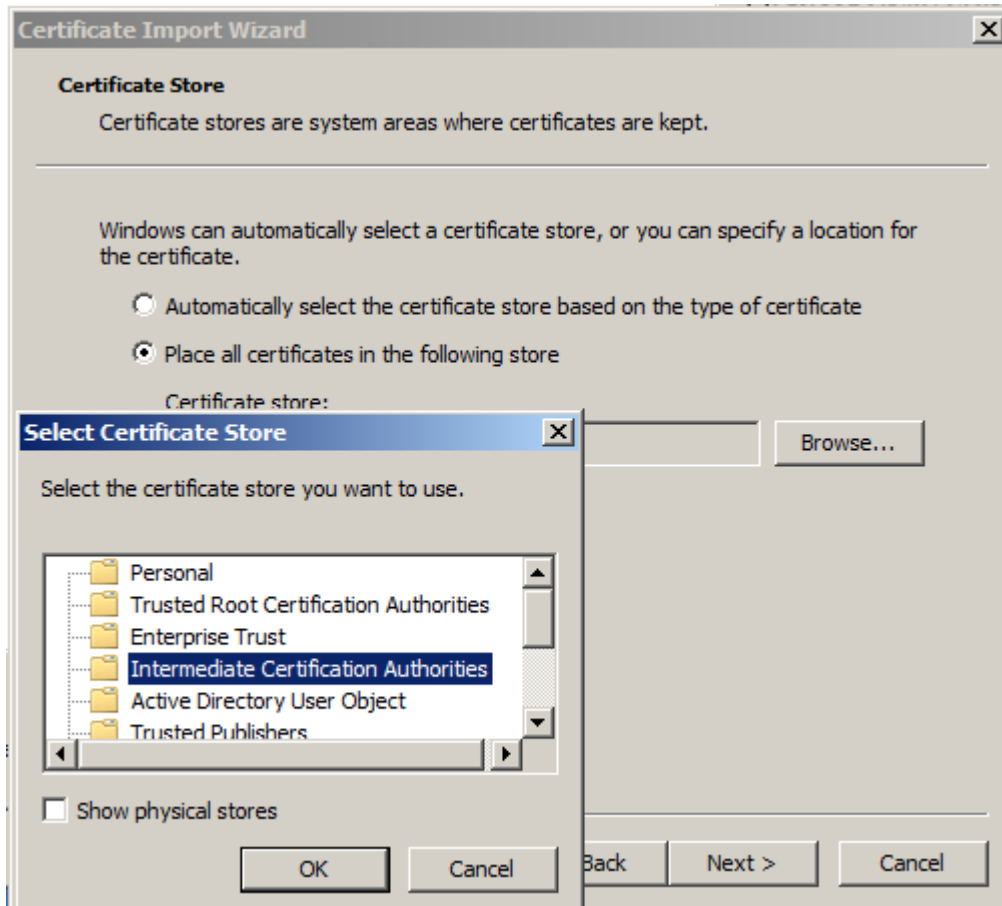
5.2 Install the Chain Certificate

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

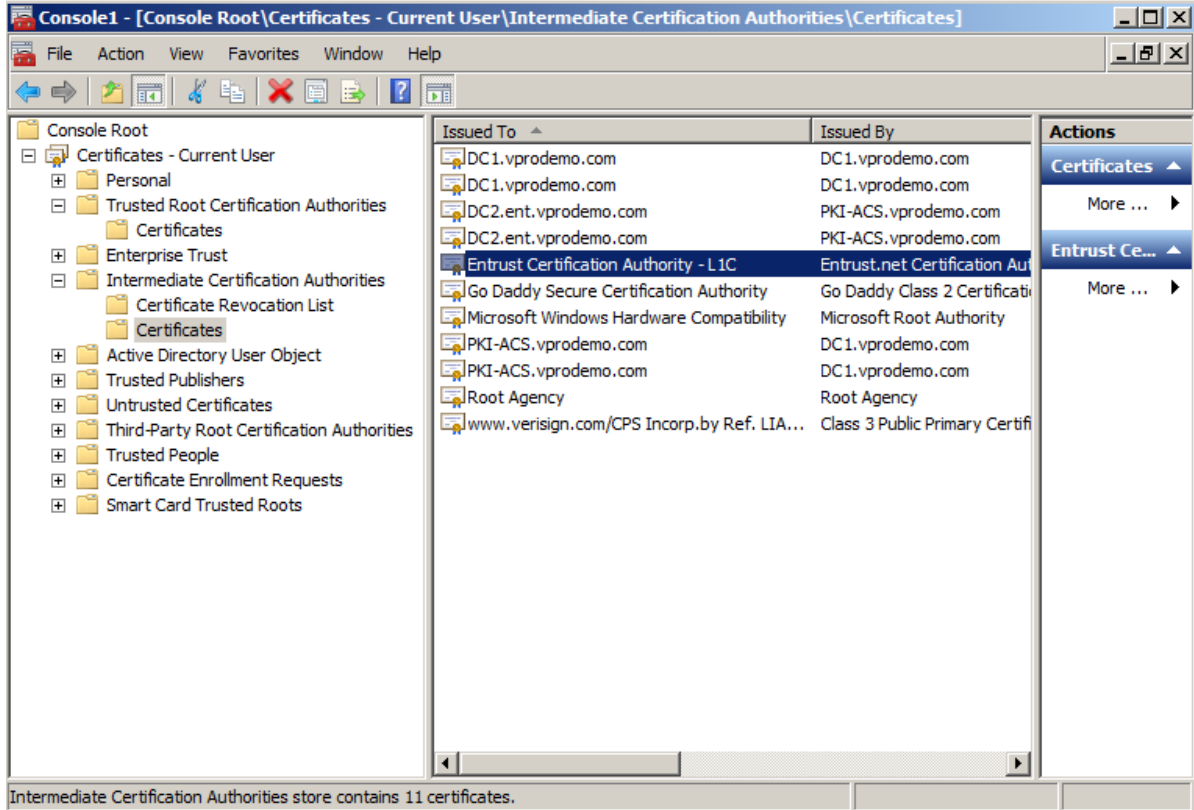
1. Double-click the **Chain_Certificate.cer** file where you saved it. Choose **Install Certificate**.



2. Choose **Place all certificates** in the following store radio button and then select **Intermediate Certificate Authorities**. Click **OK** then **Next**.



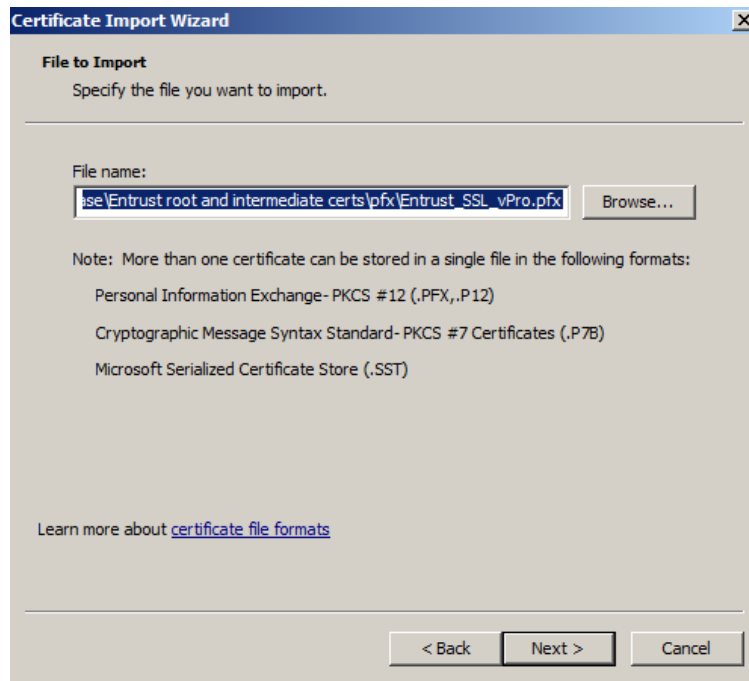
The certificate is now installed in the Intermediate Certificate Authorities store.



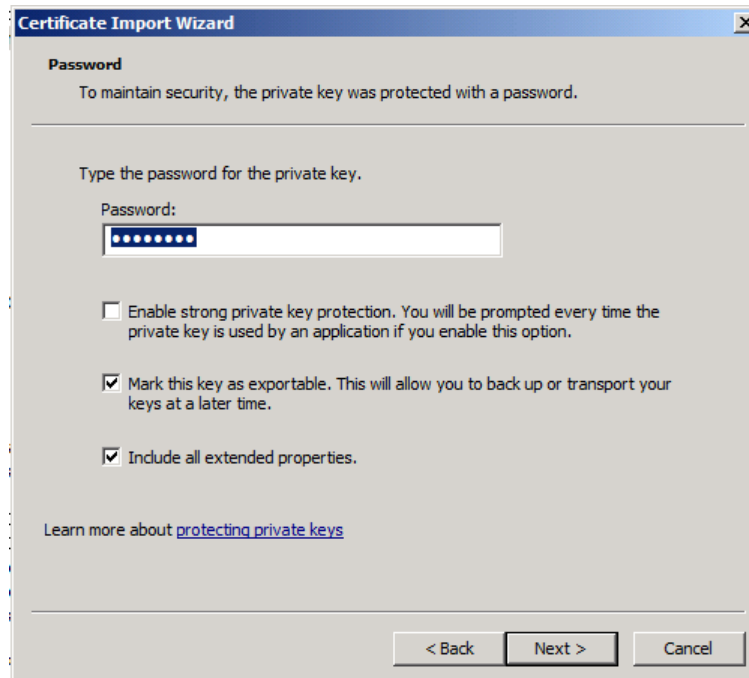
5.3 Install the pfx Certificate

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**.

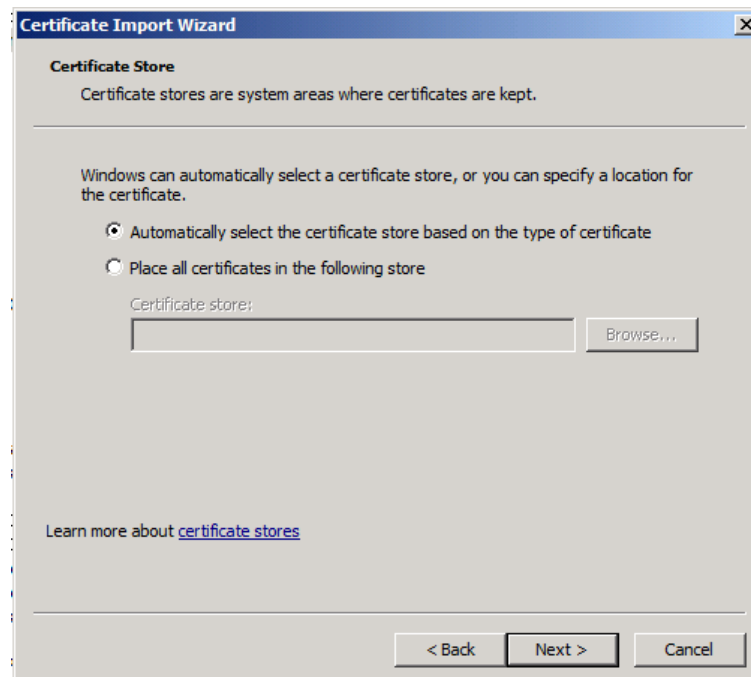
1. Double-click on the Entrust_SSL_vPro.pfx file where you saved it. Choose **Next**.



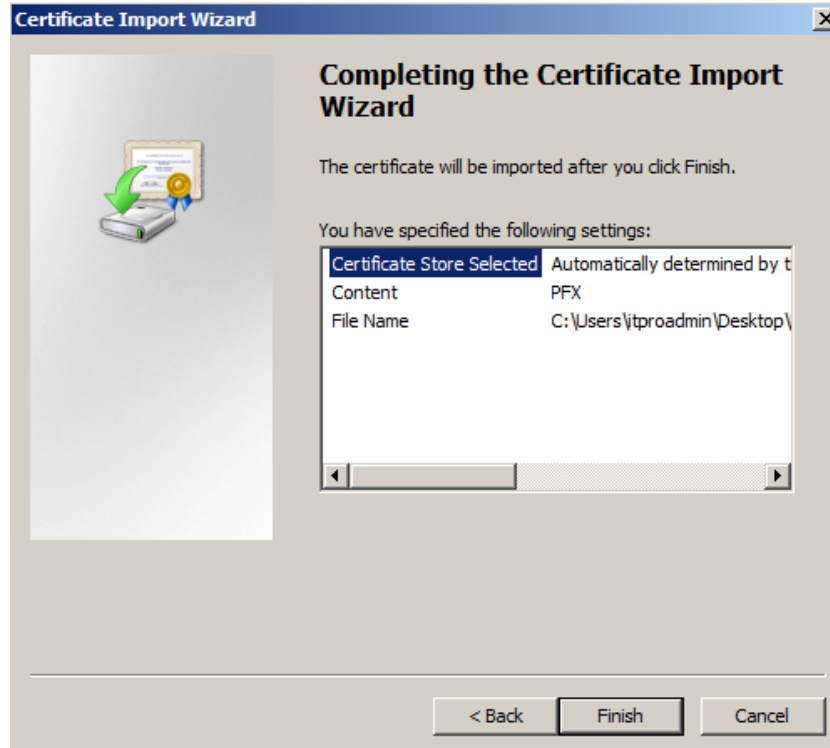
2. Enter in the password and select **Mark Key as exportable** and **Include all extended properties**. Choose **Next**.



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



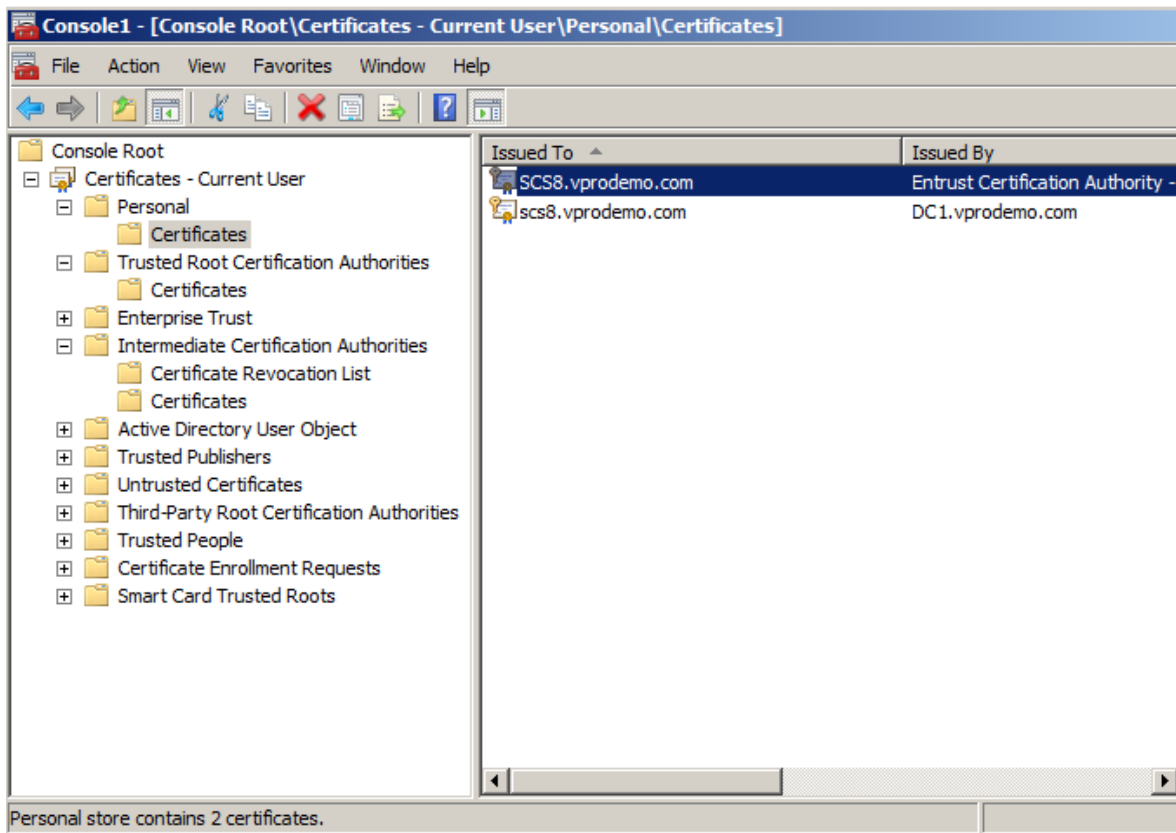
4. Choose **Finish**.



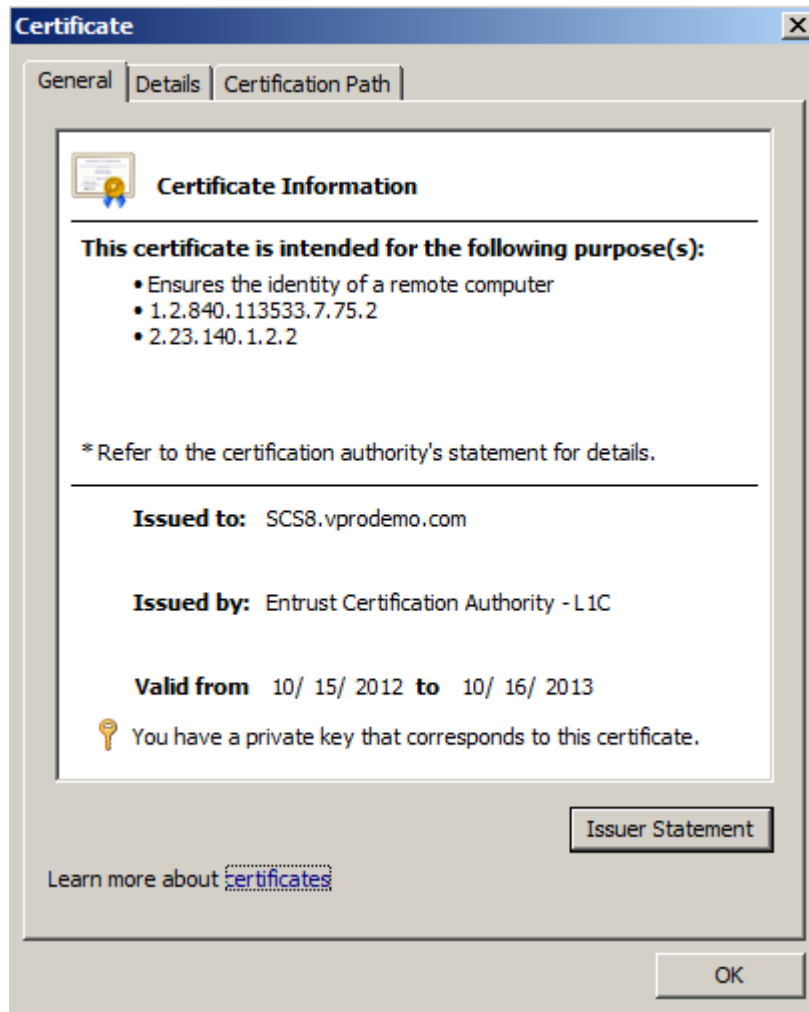
The certificate is now installed in the Current User Personal Certificates store.

5.4 Verify the Certificate Chain

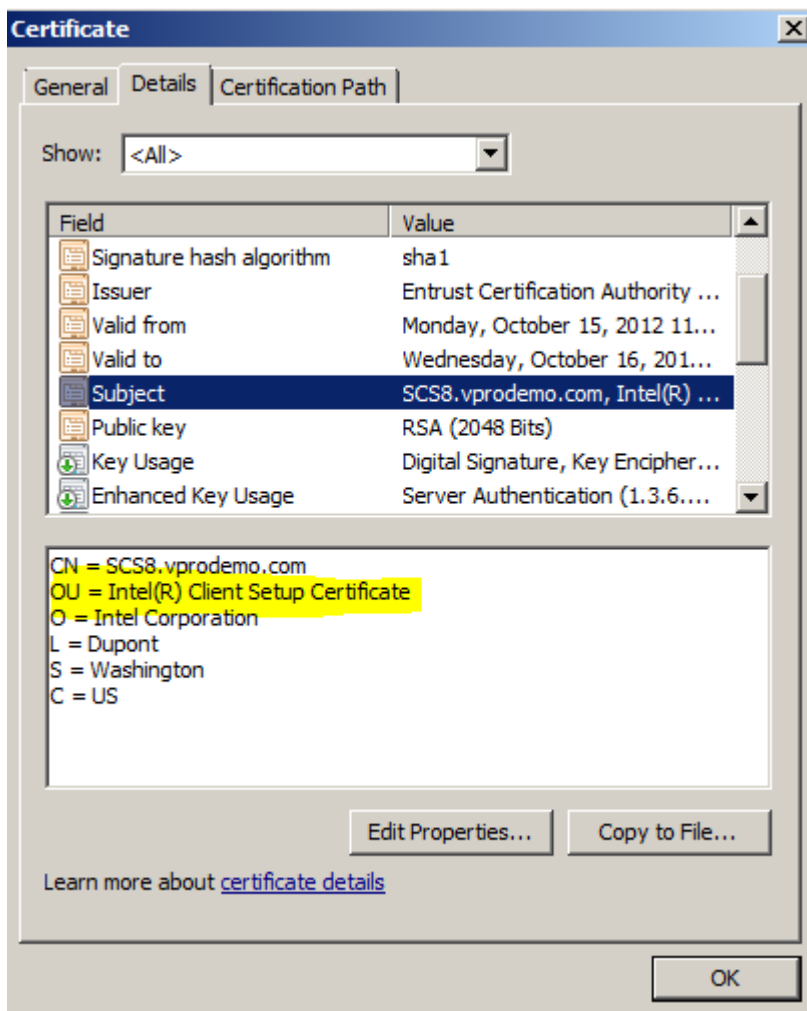
1. To verify the chain, double-click the imported certificate. In this example **SCS8.vprodemo.com** issued by Entrust.



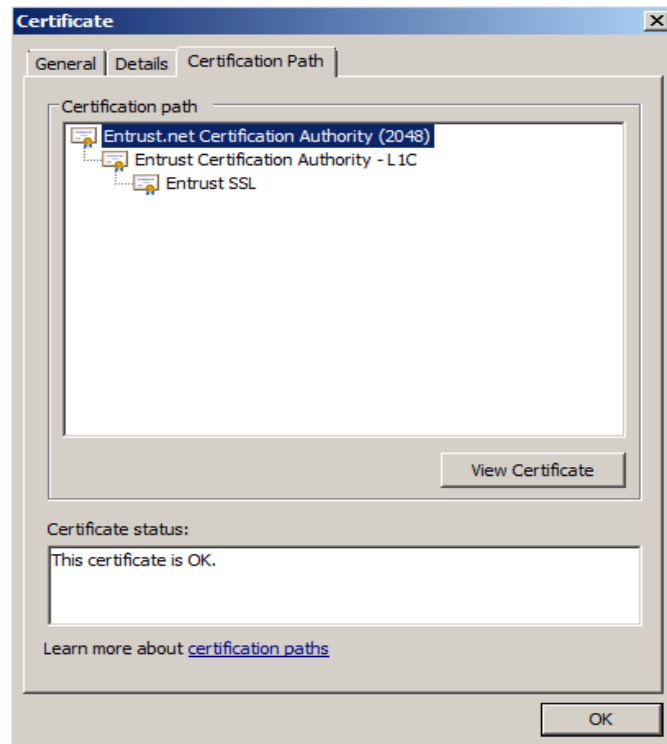
2. In the Certificate Information menu, confirm that there are no errors. Check that the private key corresponds to the certificate. Click the **Details** tab.



3. From the Details menu, select **Subject** and then verify the OU of “**Intel(R) Client Setup Certificate**” is present. Click the **Certificate Path** tab.



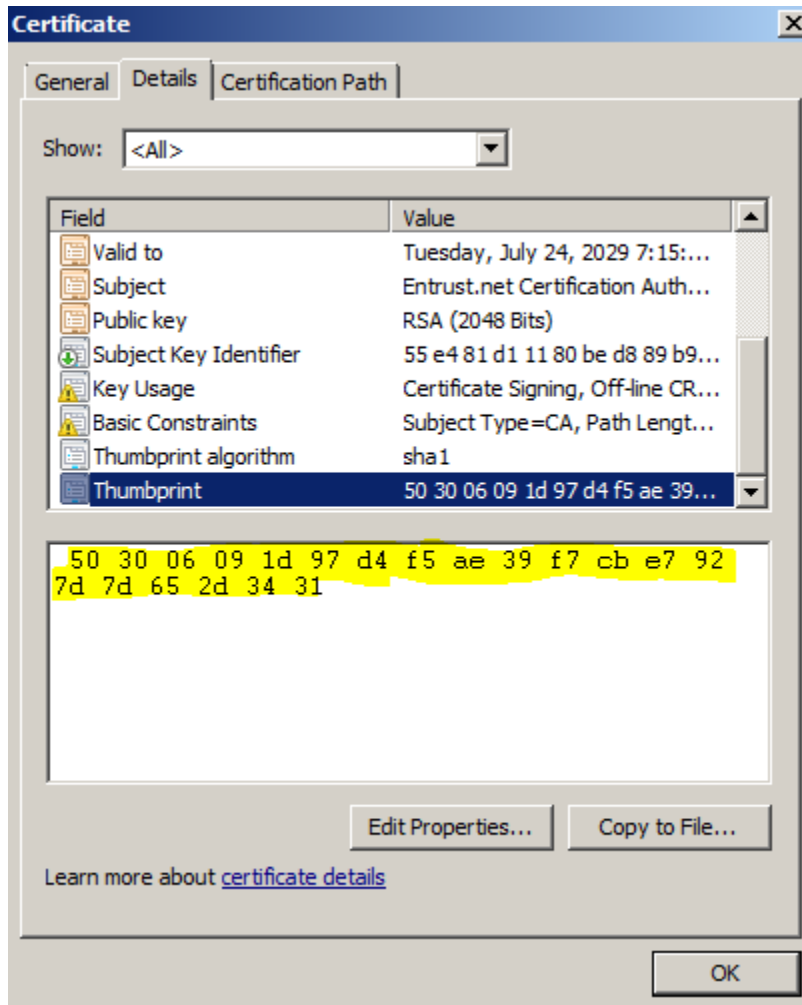
4. Check that the certificate is mapped to the intermediate Certificate Authorities as shown. Double-click on the root cert **Entrust Certificate Authority (2048)**.



5. Verify there are no errors with the root certificate and then click **Details**.



6. 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 setup and configured. Follow the instruction in the Intel SCS documentation to try Host Based Configuration in Admin Control mode. If successful, then your certificate is installed correctly.

If you purchased a wildcard or UCC certificate, then you should repeat the tests in the other domains/subdomains.