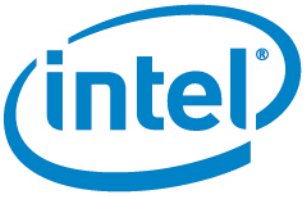


# Intel® vPro™ Technology

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

Document Release Date: December 1, 2012

# Revision History

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

# 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) 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)

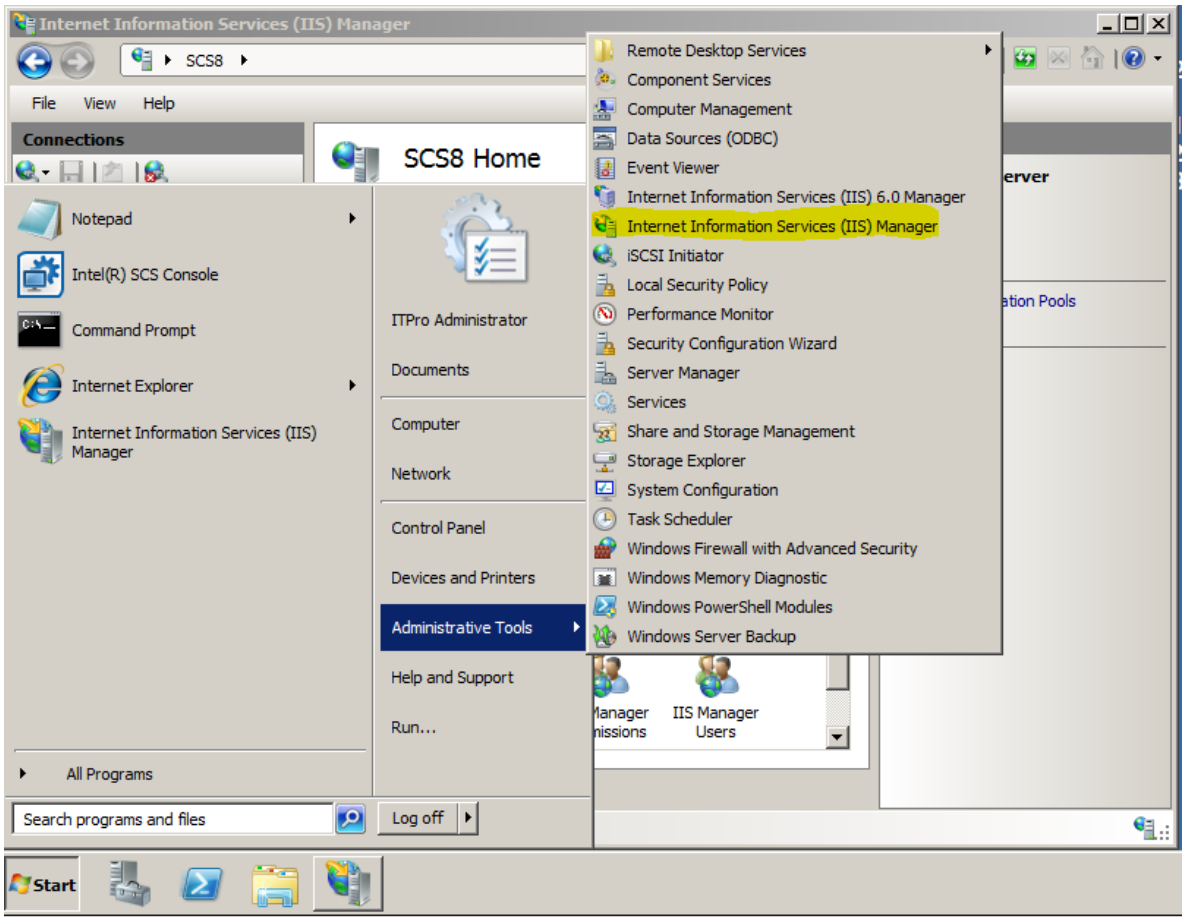
3. Microsoft* Internet Information Service (IIS) running on the server that is hosting the remote configuration service
4. Account permissions to install the certificate

# 2 Create a Certificate Signing Request

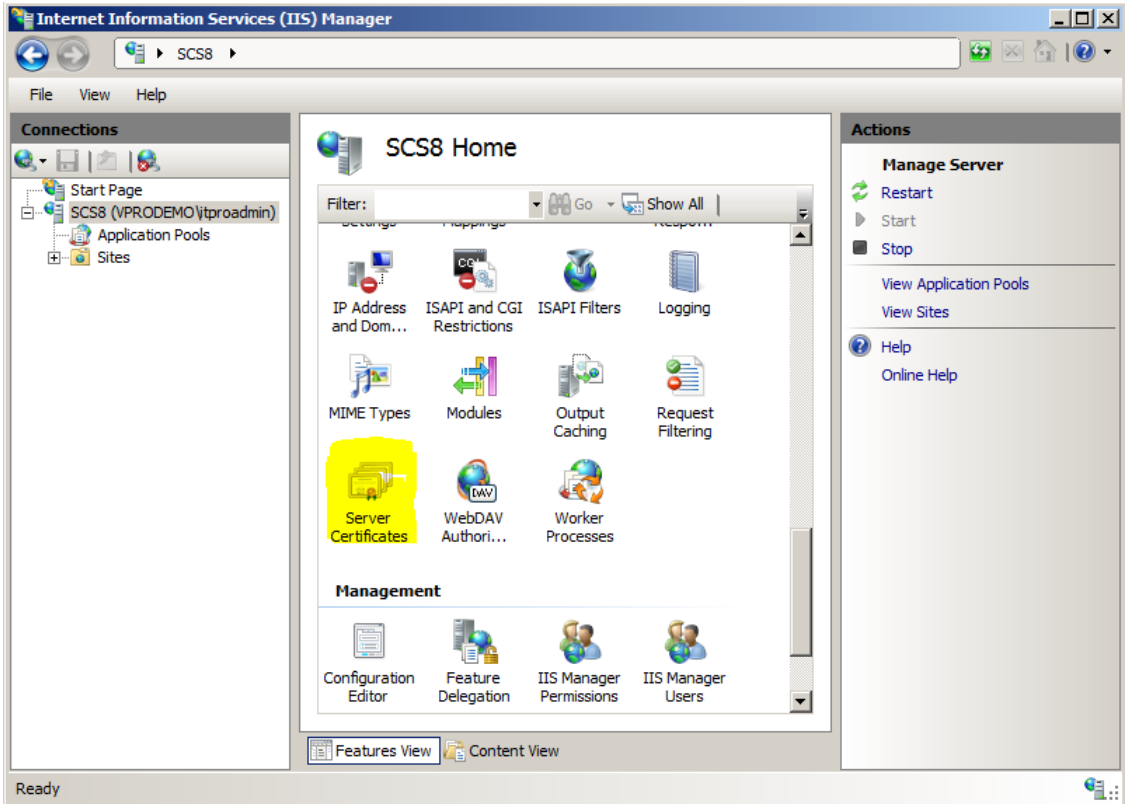
The following instructions were captured using Microsoft* Internet Information Services (IIS) for Windows* Server 2008 R2.

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

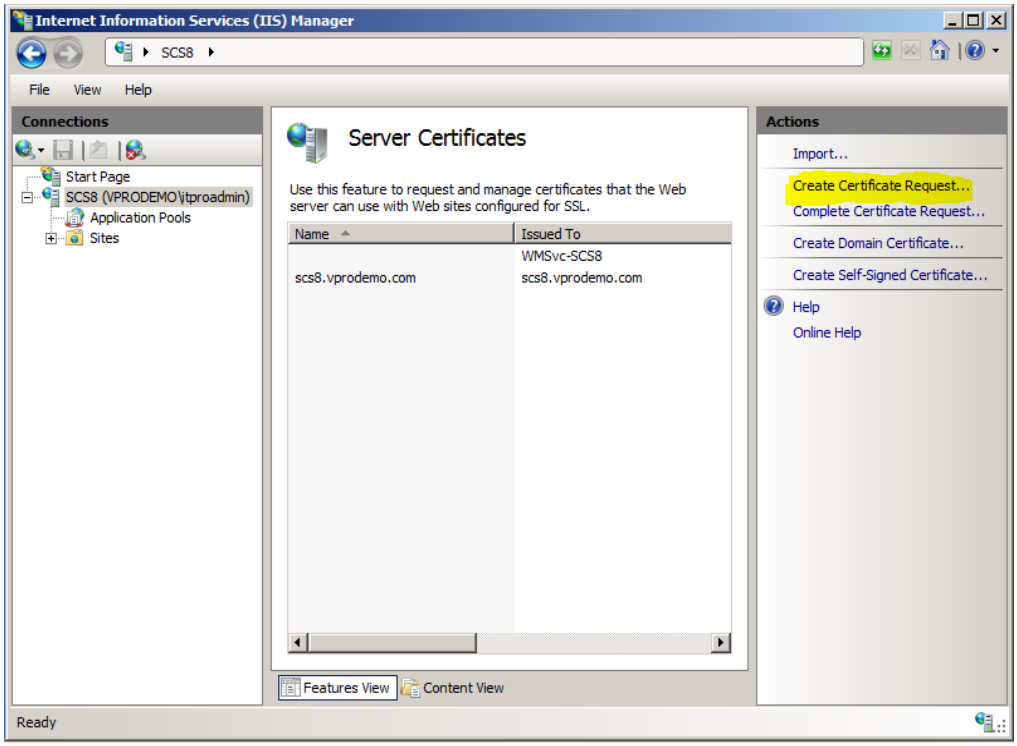
1. On your Intel SCS remote configuration server, open Programs→Administrative Tools→Internet Information Services (IIS) Manager.



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.

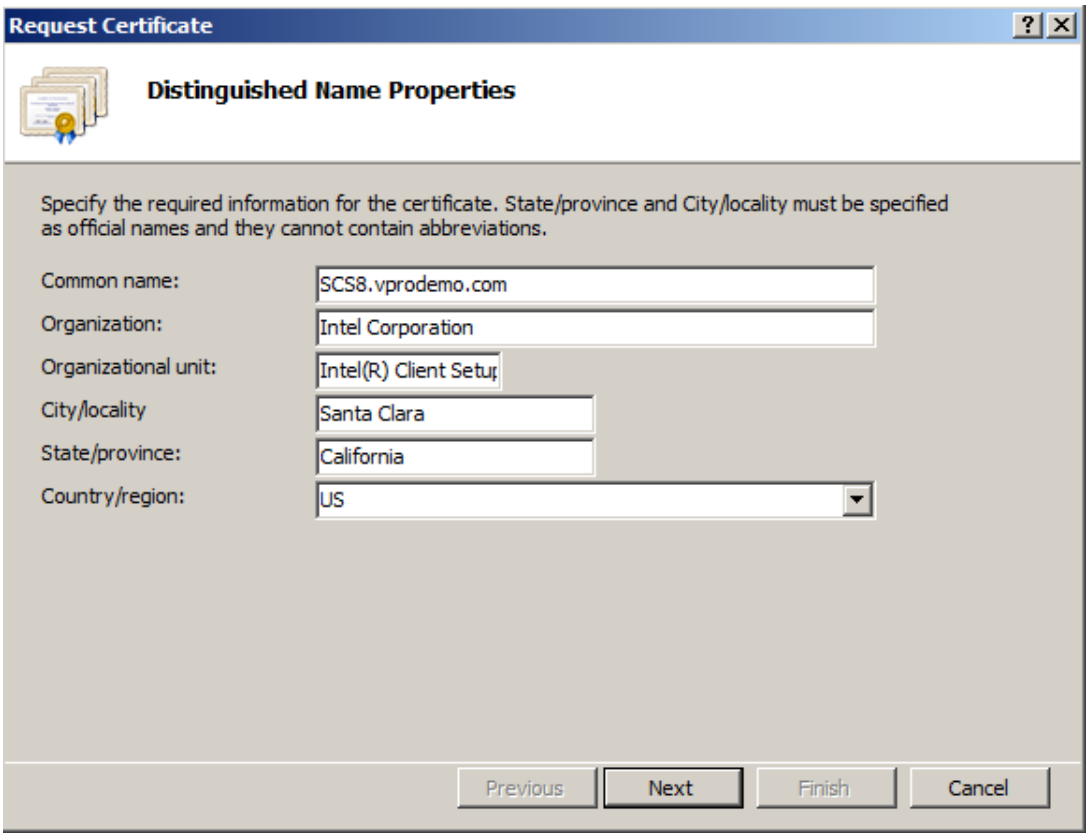
You can verify the DHCP Option 15 setting by running the SCSDiscovery utility (provided with Intel Setup and Configuration Software) on the client. The DHCP Option 15 setting is called the OSSpecificDNSSuffix.

**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.

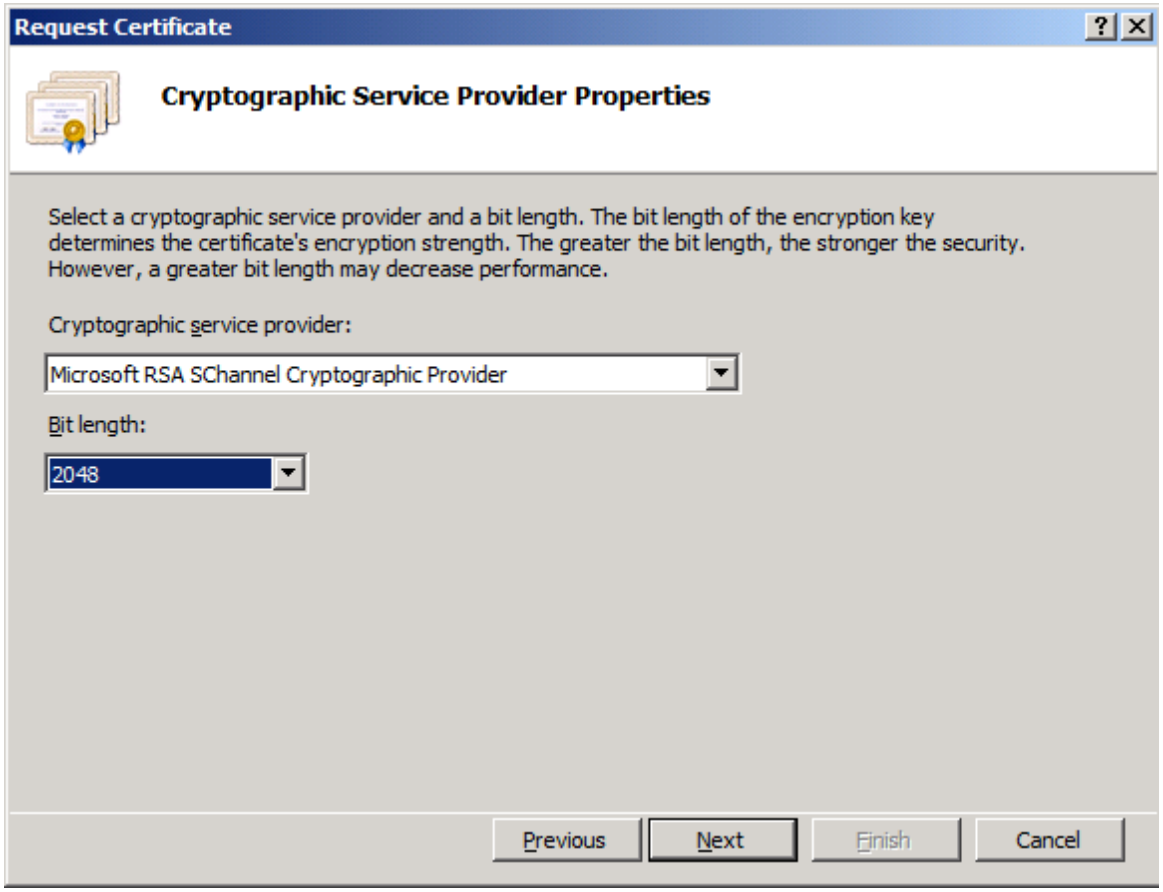
- **Organization**: The name of the organization that is requesting the certificate and owns the domain
- **Organizational Unit**: Intel(R) Client Setup Certificate

  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

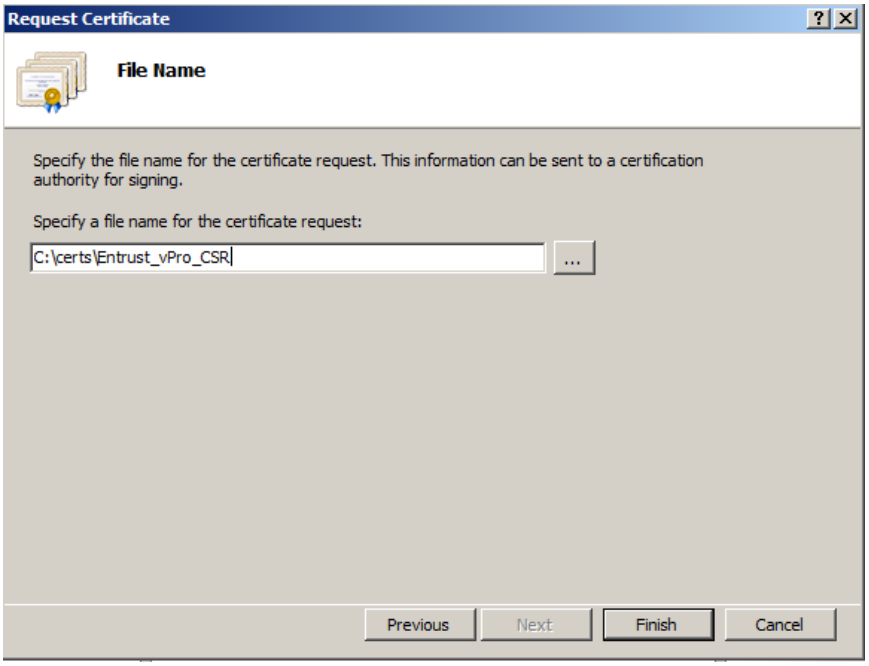



Choose **Next.**

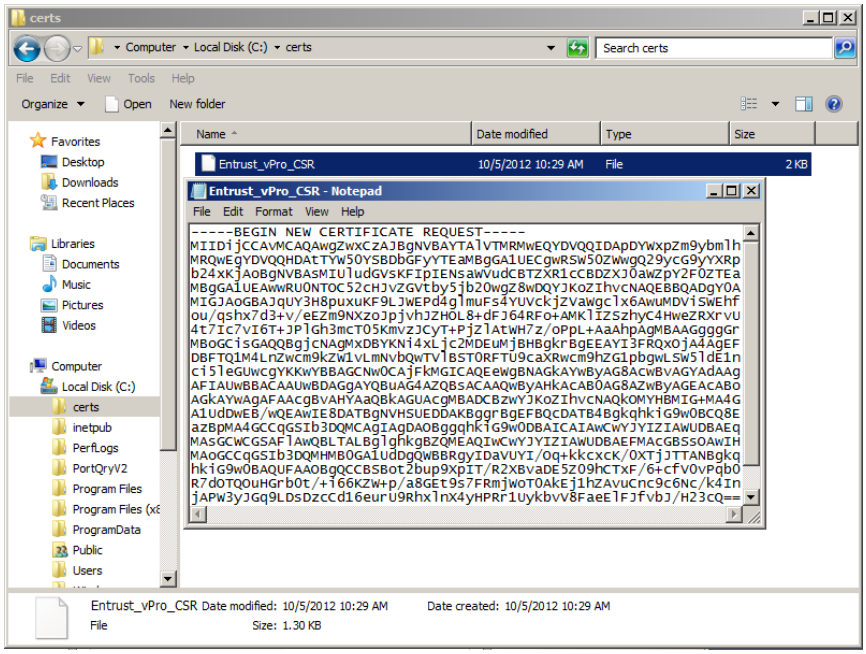
5. Leave the Cryptographic Service Provider set to **Microsoft RSA SChannel Cryptographic Provider** and select **2048** as your key Bit length. Choose **Next.**



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



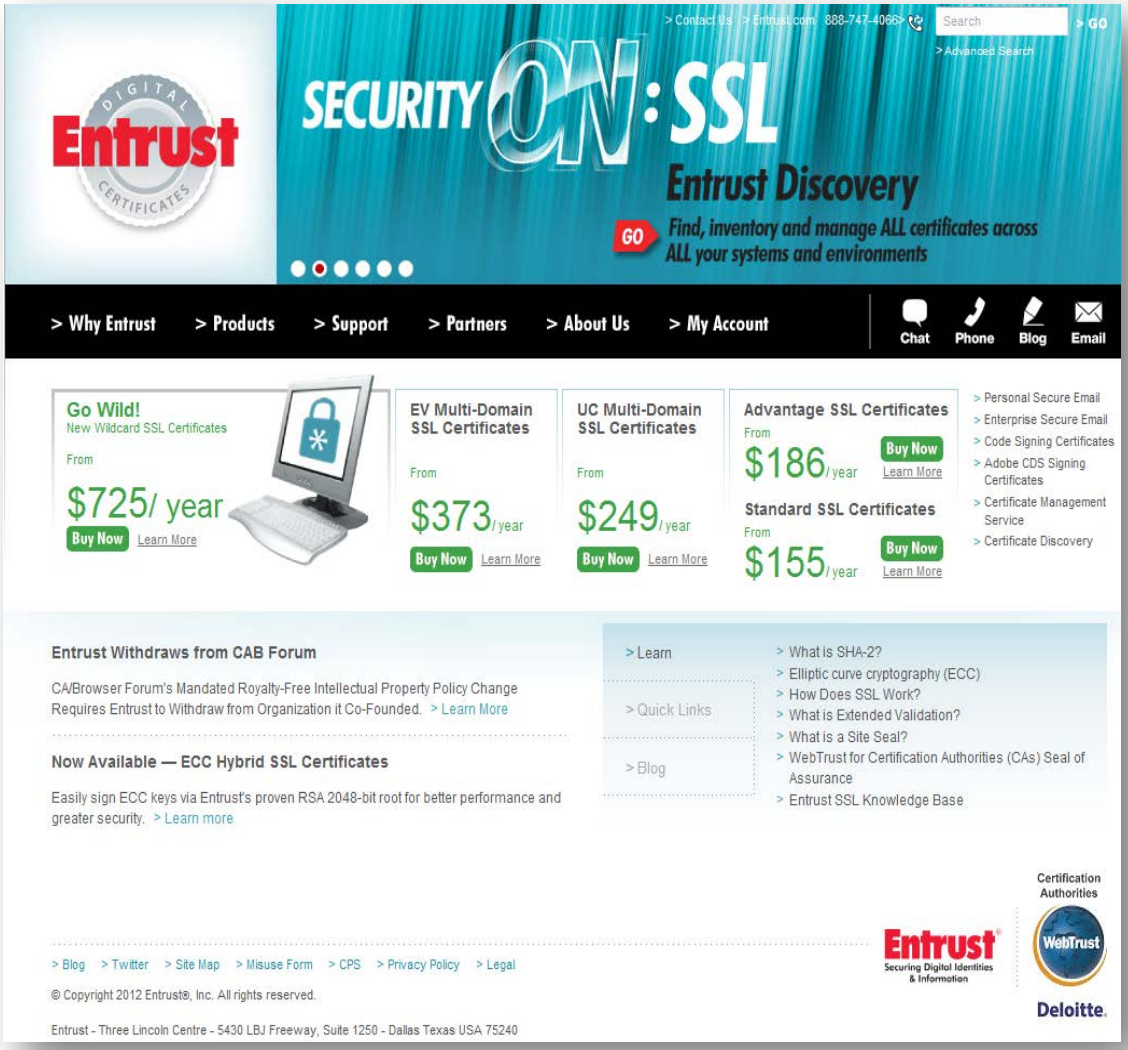

7. This file, Entrust_vPro_CSR in our example, will be used to submit your request to Entrust for an Intel AMT Setup and Configuration certificate. You can open the file in Notepad to view encrypted certificate request.



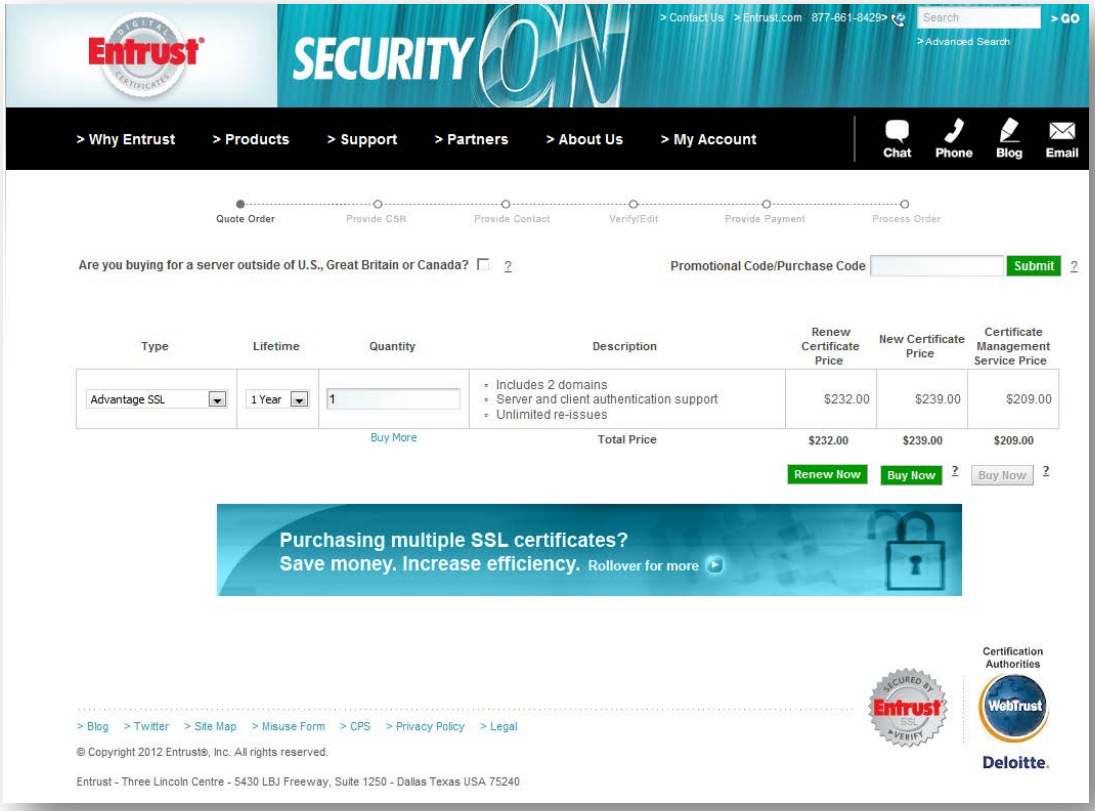
# 3 Send the Certificate Request to Entrust*

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**.

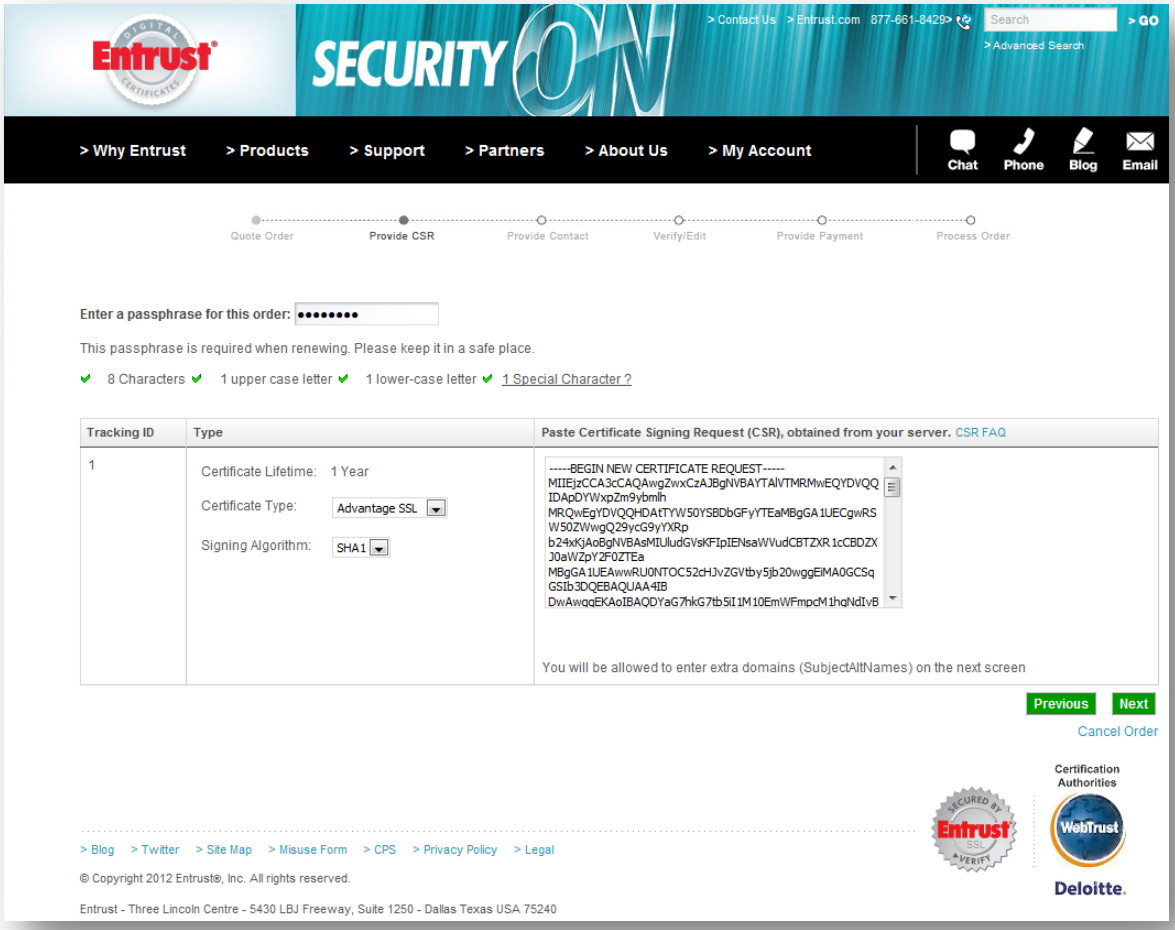


3. From the **Quote Order** menu**,** confirm **Advantage SSL** is chosen and choose **Buy Now**.



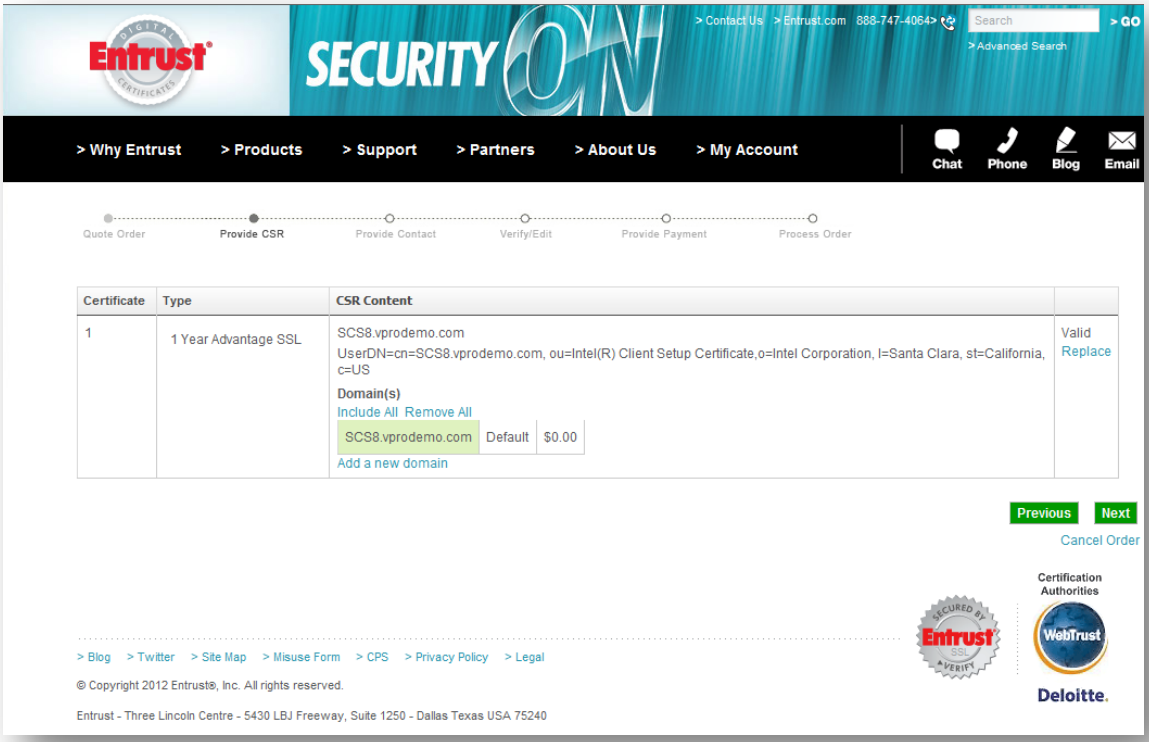
4. At the **Provide CSR** menu, enter a secure passphrase and paste the CSR in the window. The passphrase will be used later in the process.

   Confirm the following:
   - Lifetime of the certificate
   - Certificate Type
   - Desired signing algorithm



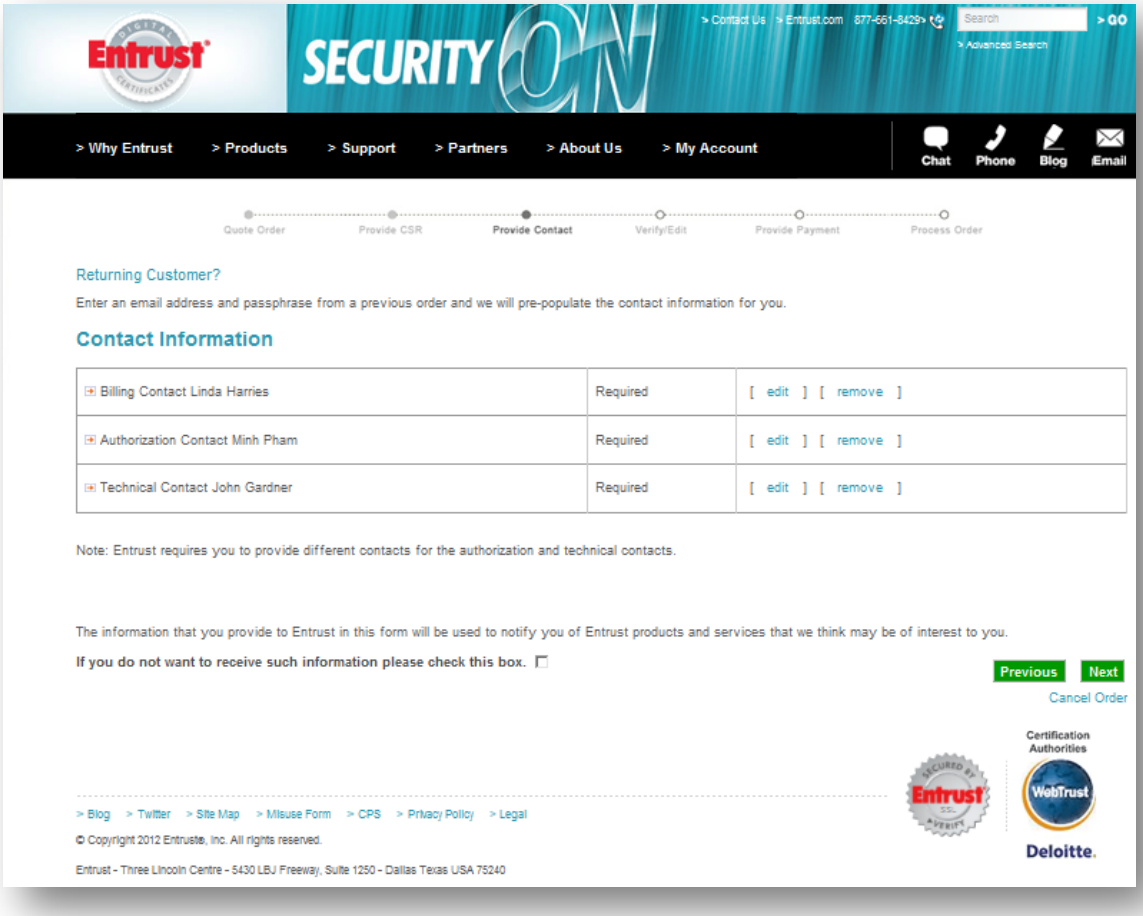

Click **Next.**

5. Verify that the CSR fields are correct.



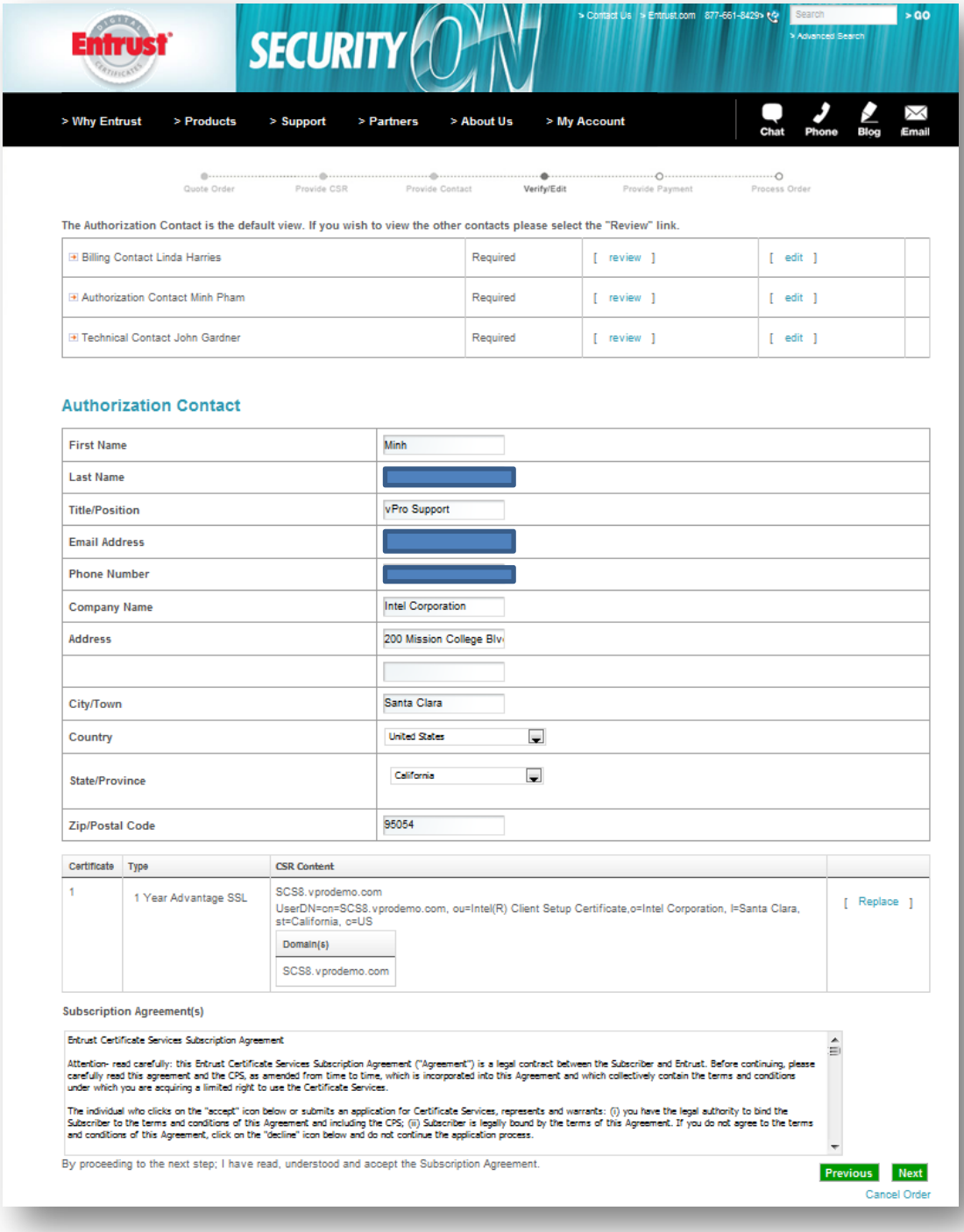

Choose **Next**.

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



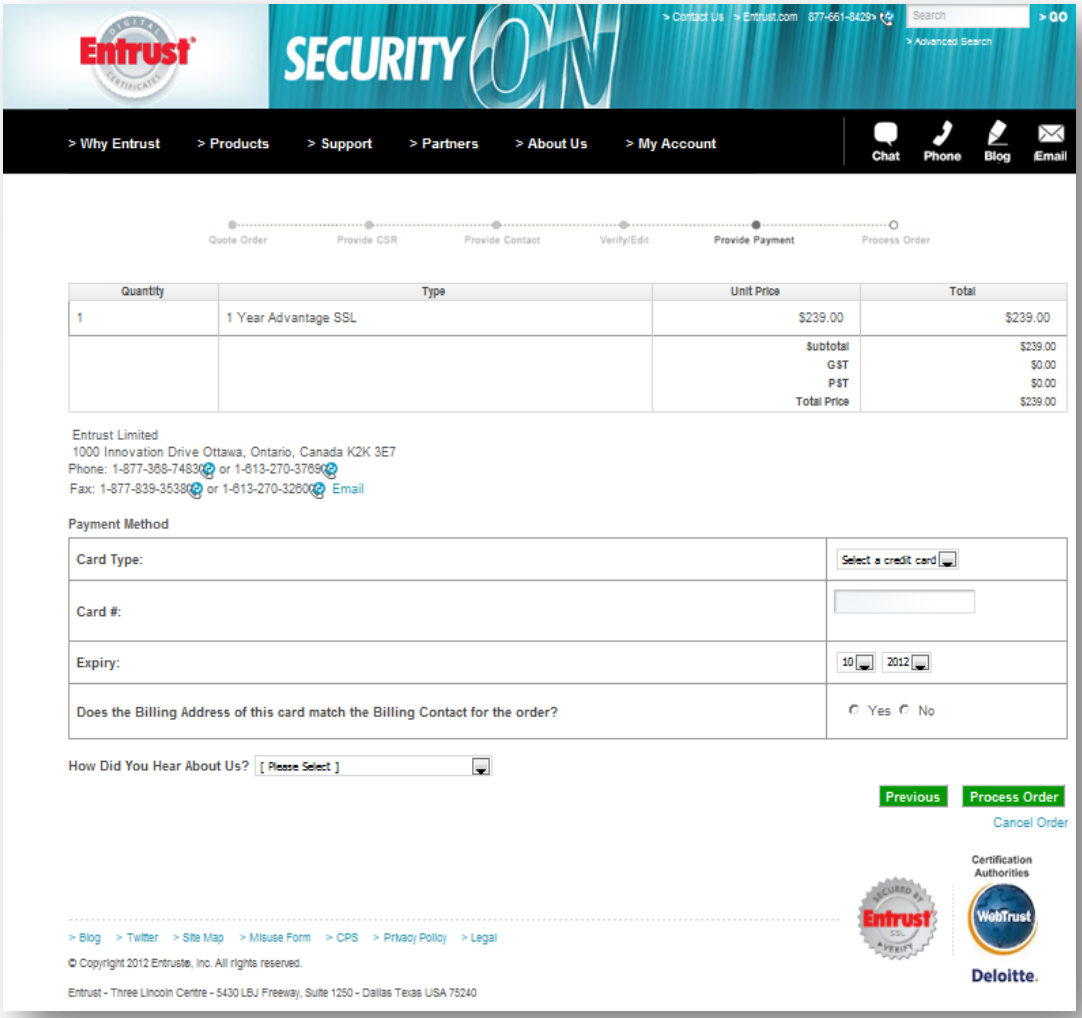

Choose **Next**.

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




Choose **Next**.

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

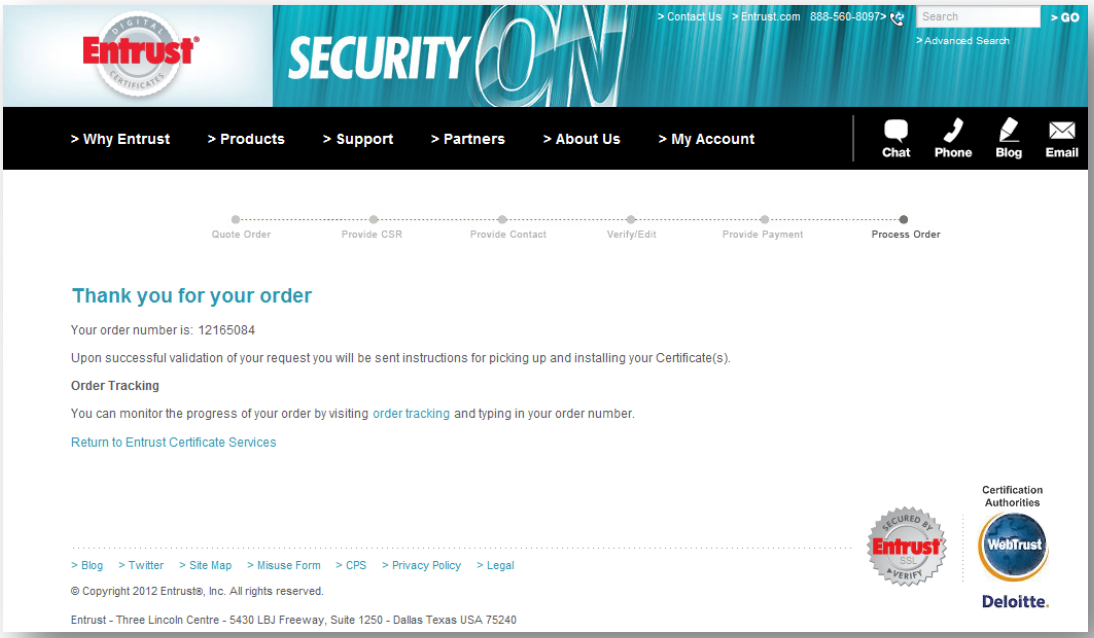


9. From the **Process Order** menu, you will see the order number.

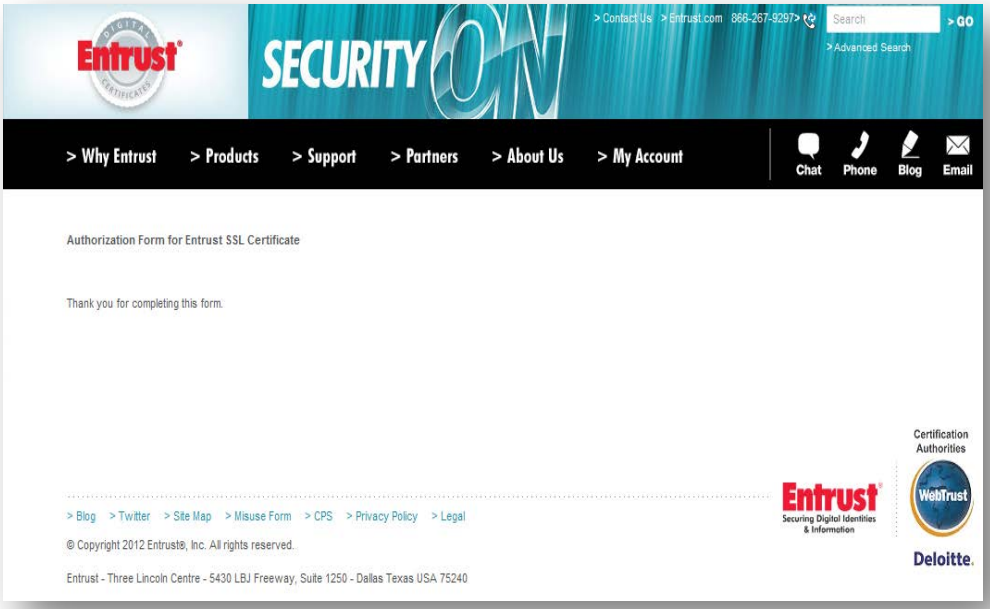
   Securely store the order number along with the passphrase you supplied during the online enrollment process. Verification of the order will take 3 to 5 business days, after which time you will then be sent instructions for picking up and installing your Advantage SSL Certificate(s).

   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

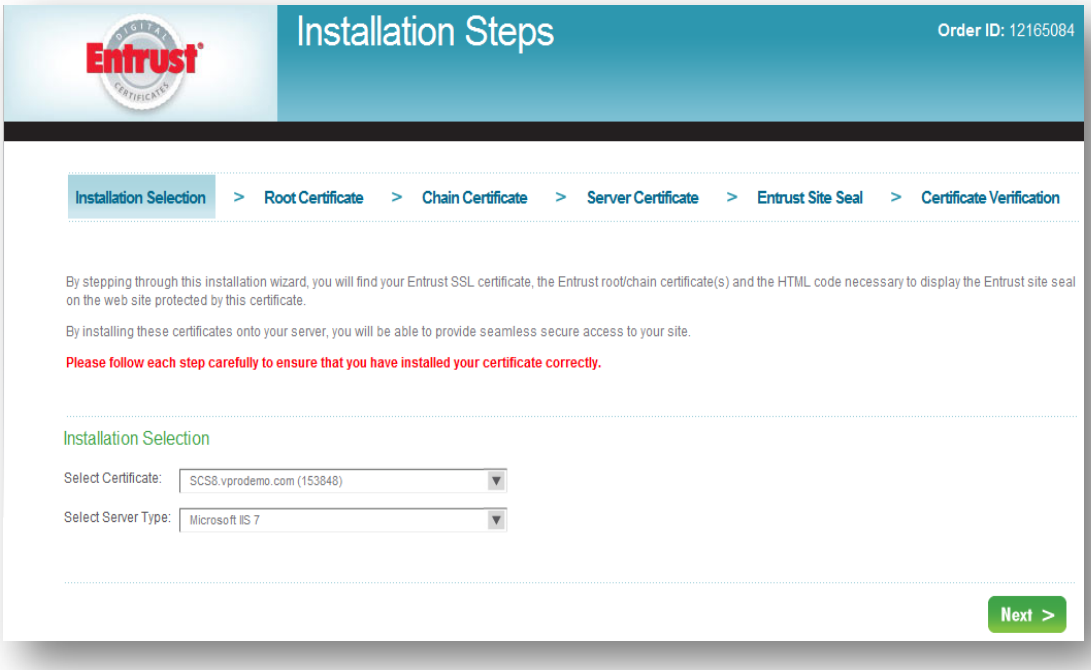


10. A confirmation email is sent to the authorized contact. The authorized person is presented with a link to approve the consent form. Once approved, the process continues to the next phase: checking the Domain name, Corporation, and Final Phone Call.

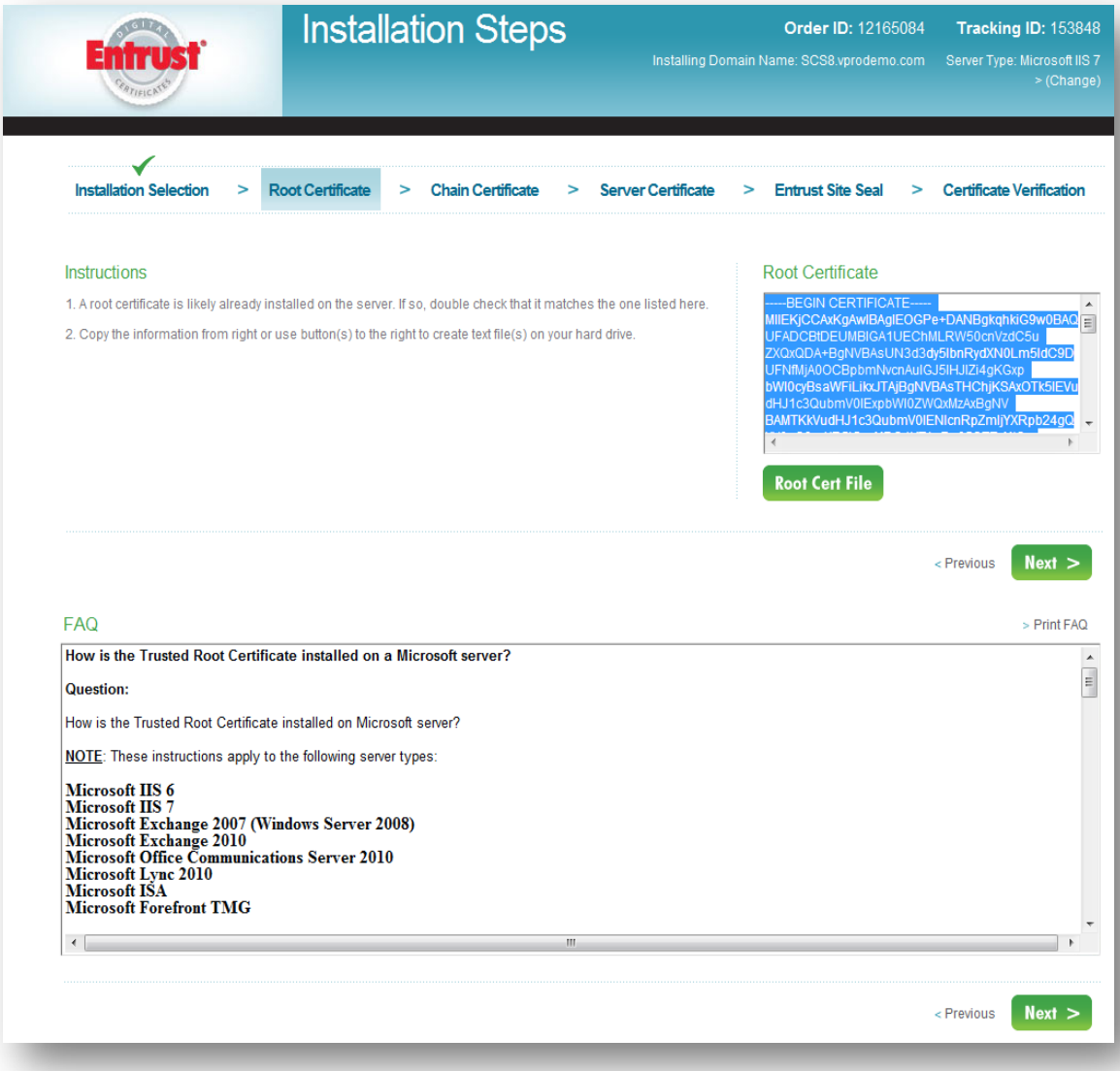


11. Once the security verification process has been completed, a link to the certificate download page is provided with installation steps.

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

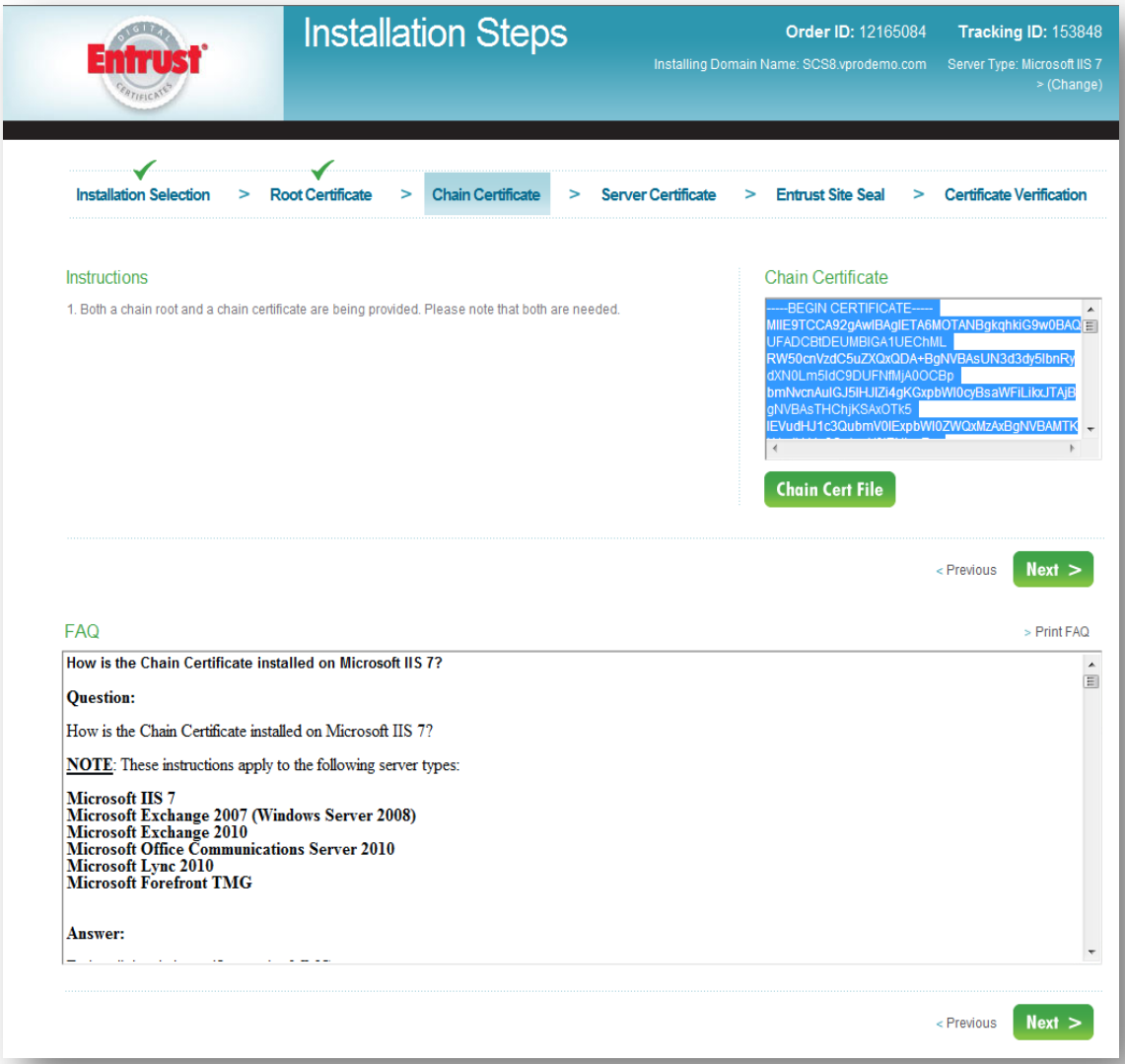


12. From the **Root Certificate** menu, copy and paste the Root Certificate that is displayed into a text file. Save it as a .cer file. In this example, we named the file "Server_Certificate.cer".



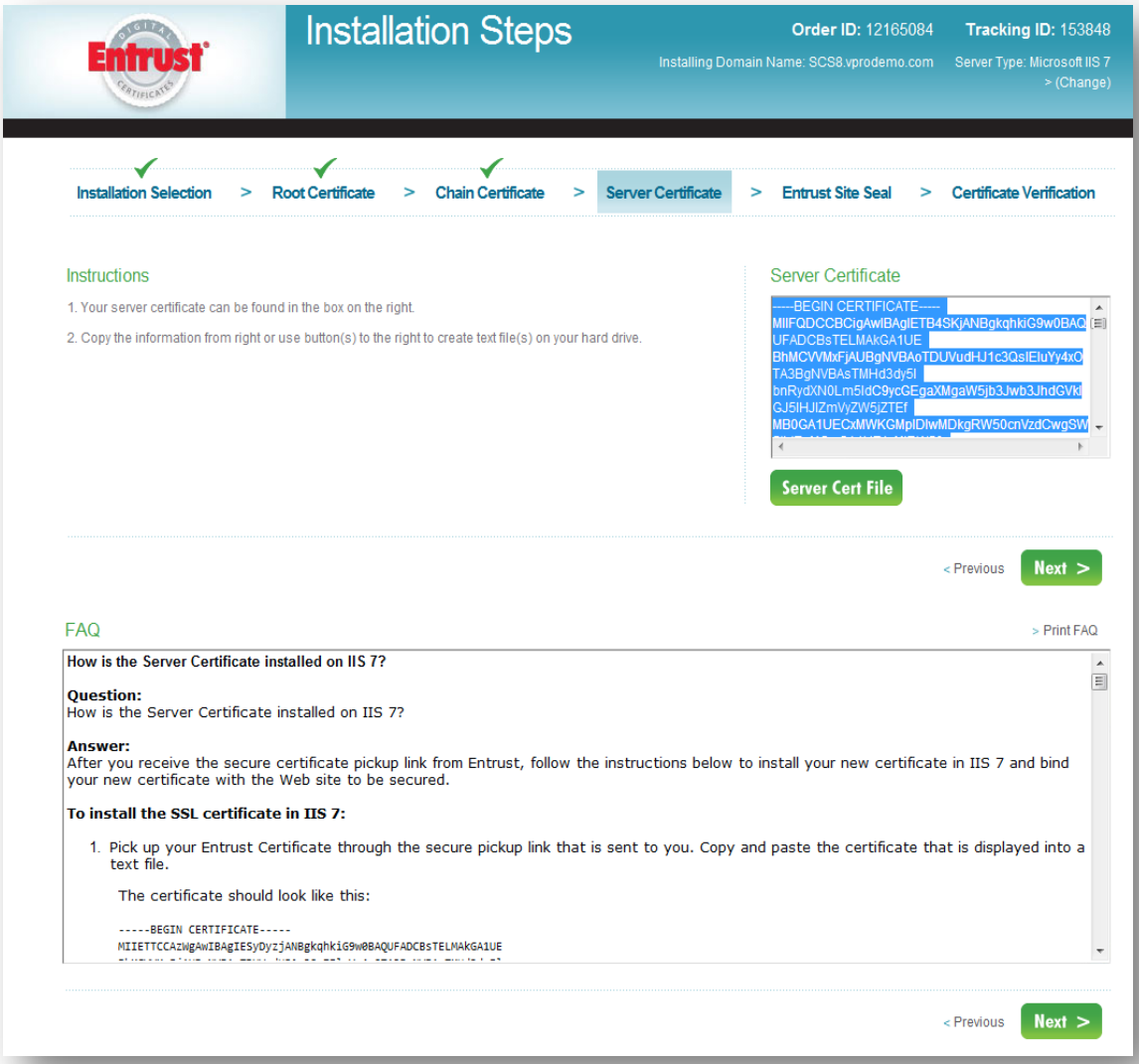

Choose **Next**.

13. 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".




Choose **Next.**

14. 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".

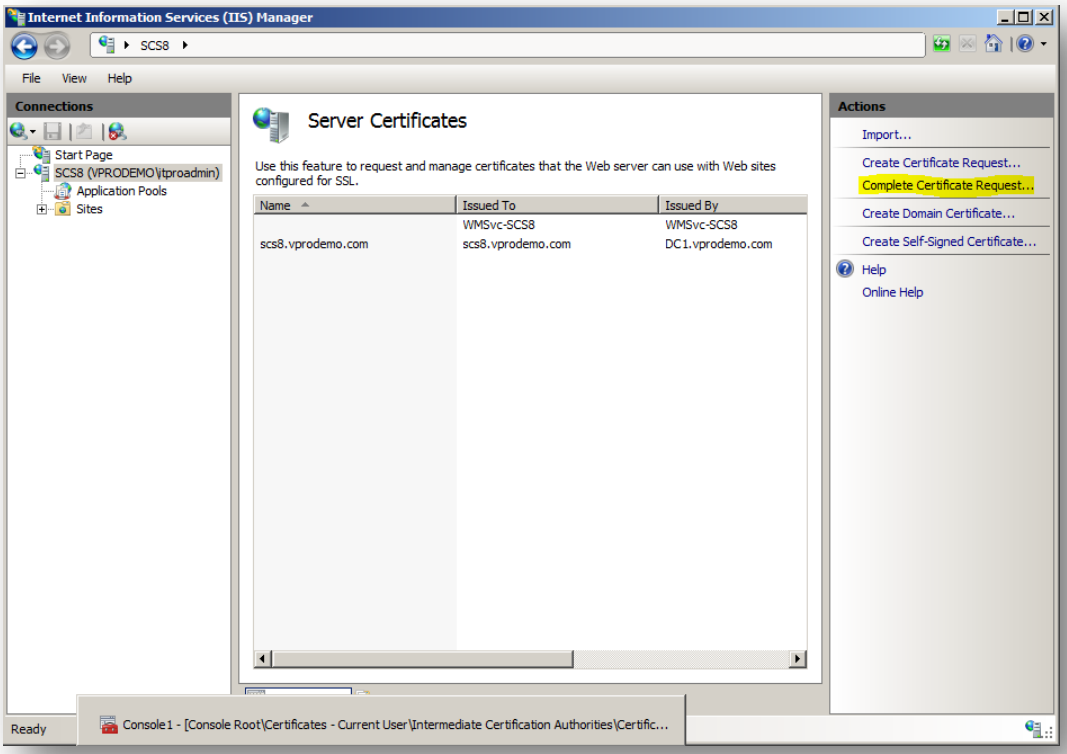



Choose **Next.**

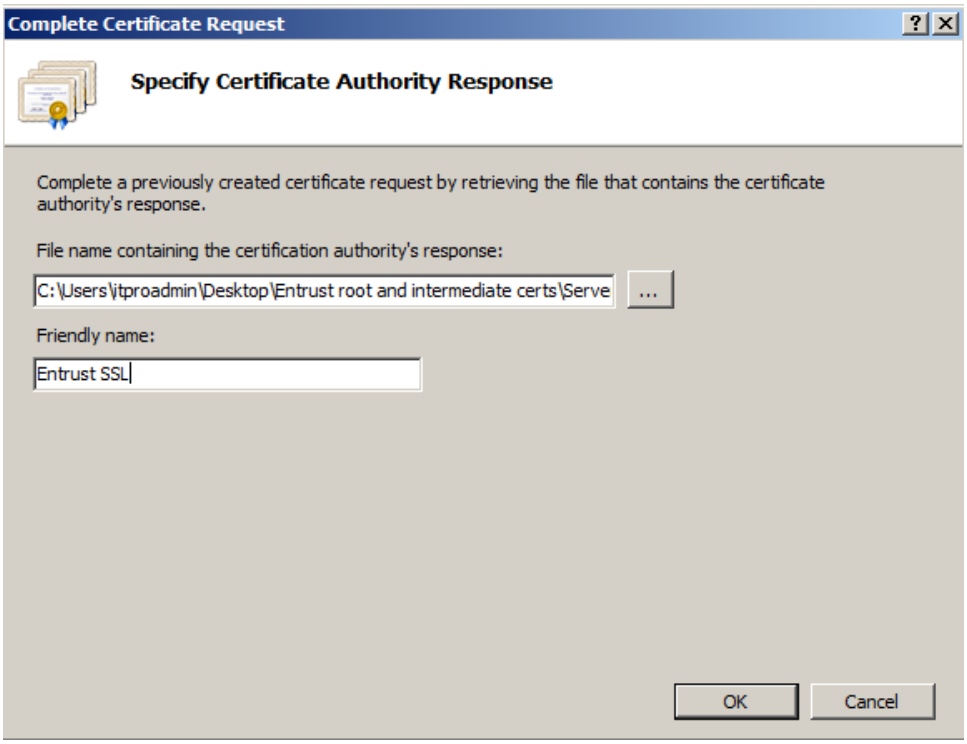
15. (Optional) Complete the next two steps, if desired:
    - Entrust Site Seal
    - Certificate Verification

# 4 Prepare the Certificate

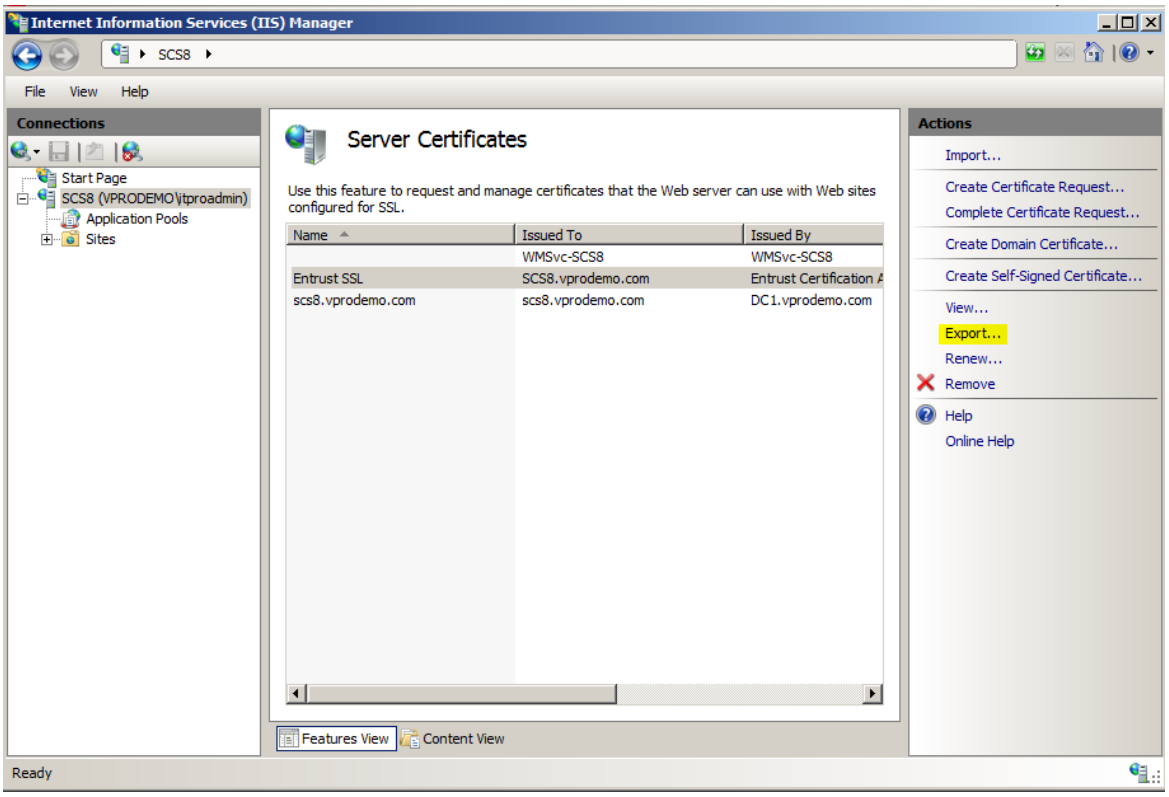
1. In Internet Information Services (IIS) Manager, select the **Complete Certificate Request** on the Actions menu.



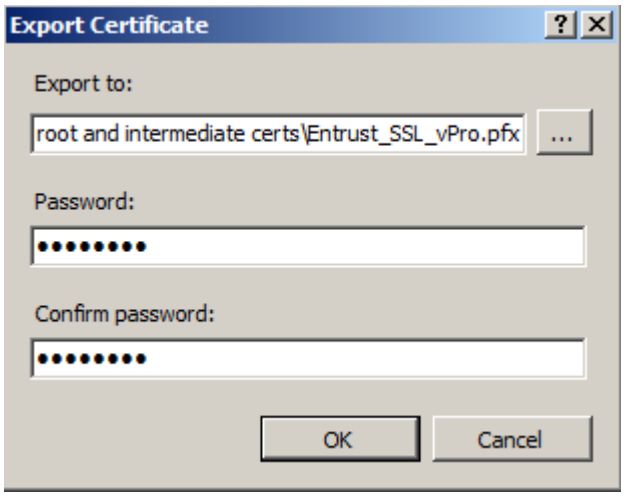
2. Navigate to the **Server Certificate** file that was saved as Server_Certificate.cer. Enter a Friendly name, and then choose **OK**.



3. 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.




4. 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

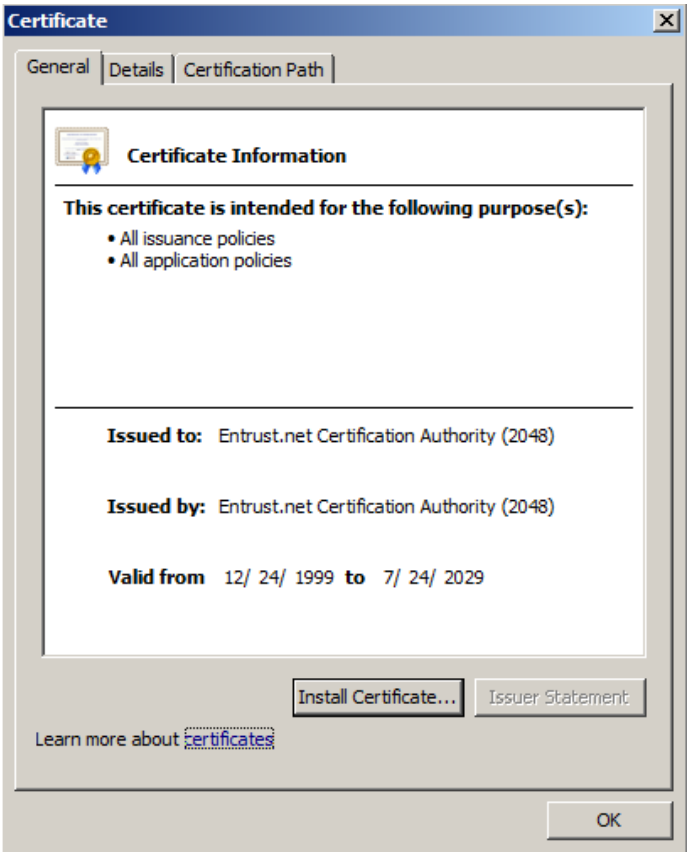
This section will show you how to do the following:

- 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

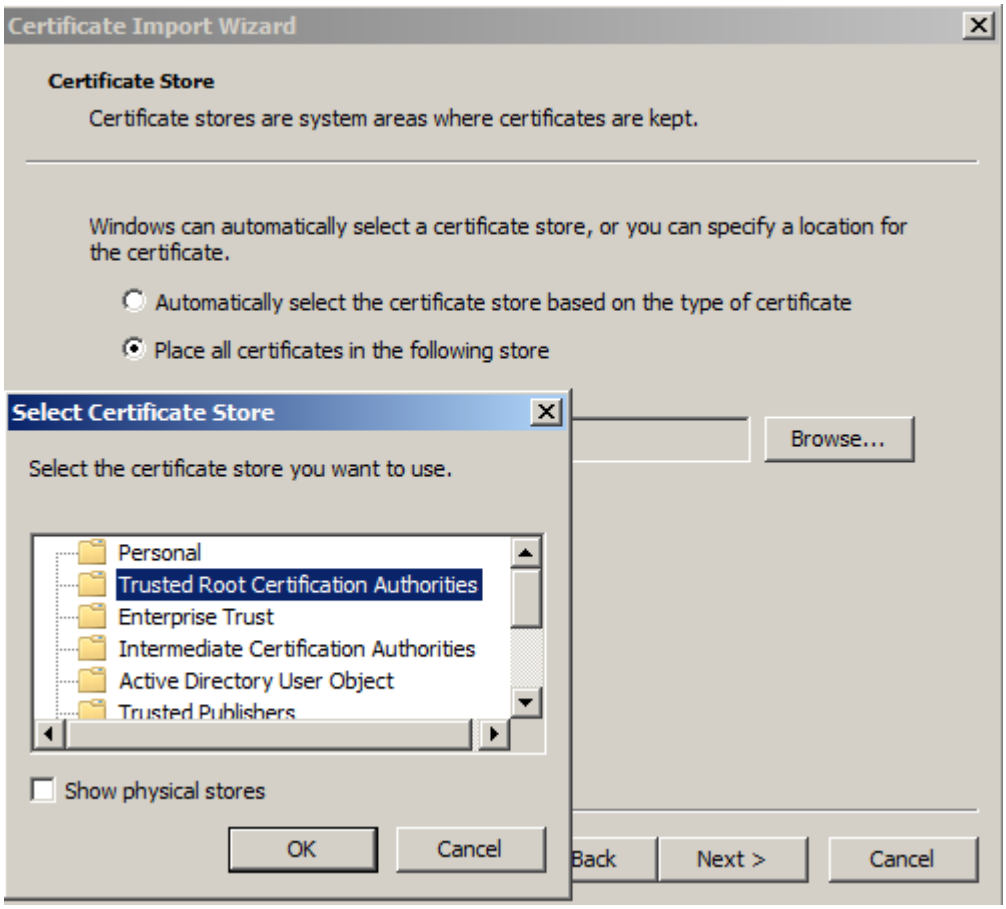
## 5.1 Install the Root Certificate

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.

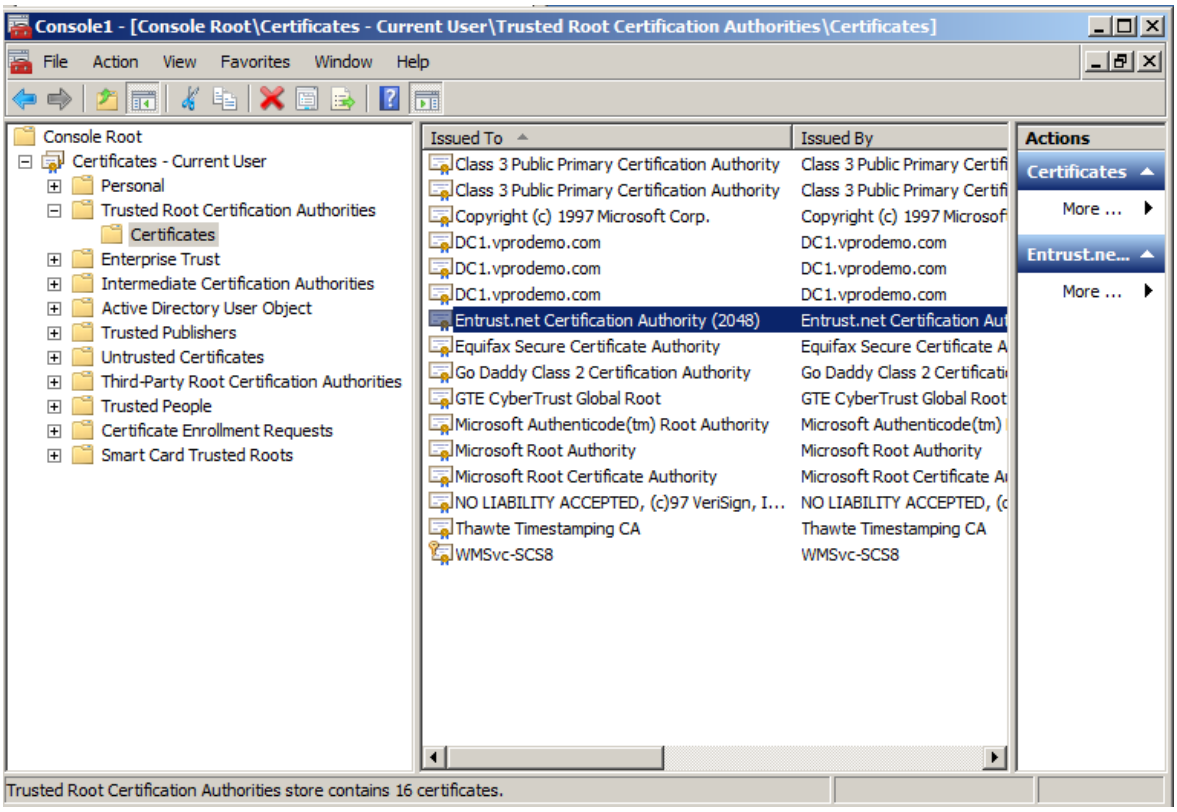
1. Logon as the service account for the RCS server.
2. Double-click the **Root_Certificate.cer** file where you saved it. Choose **Install Certificate.**



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



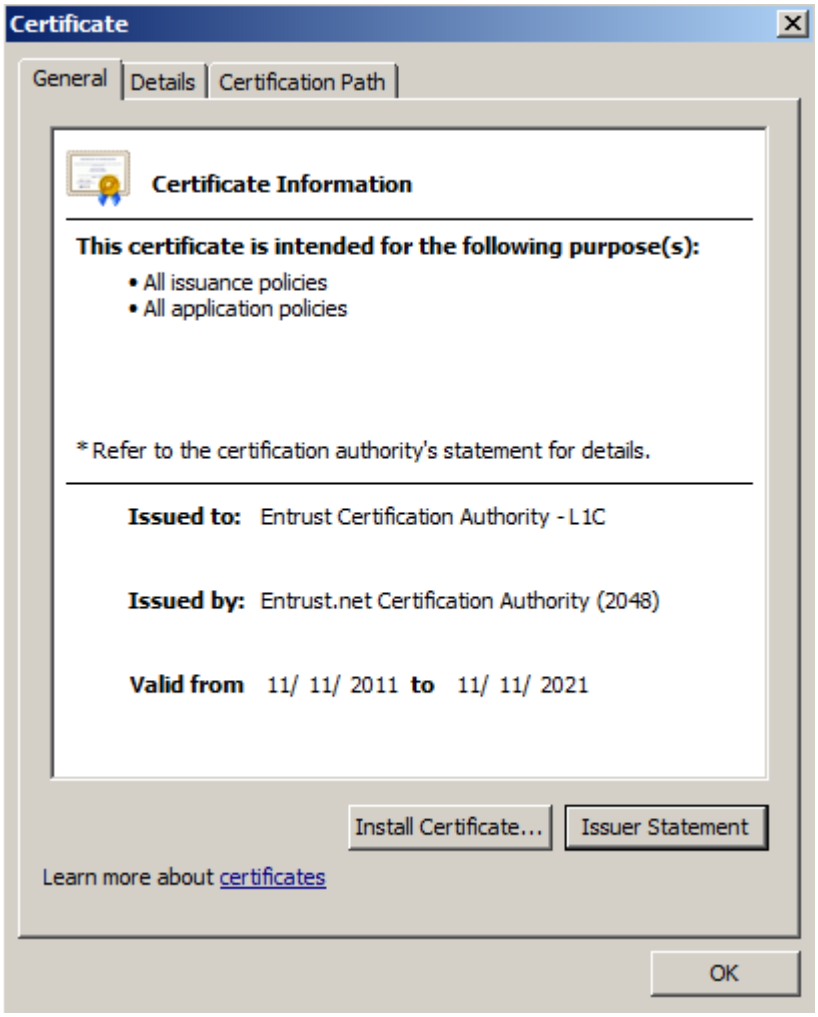
The certificate is now installed in the Trusted Root Certificate Authorities store.



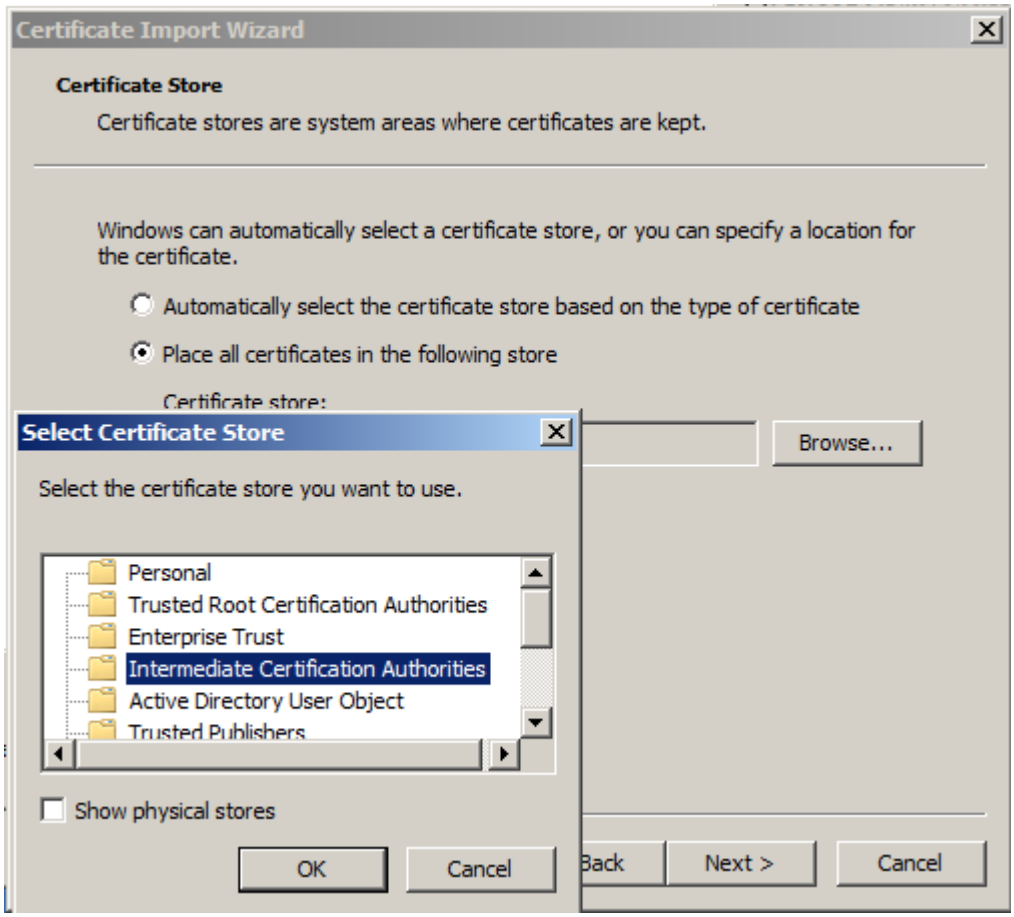

## 5.2 Install the Chain Certificate

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

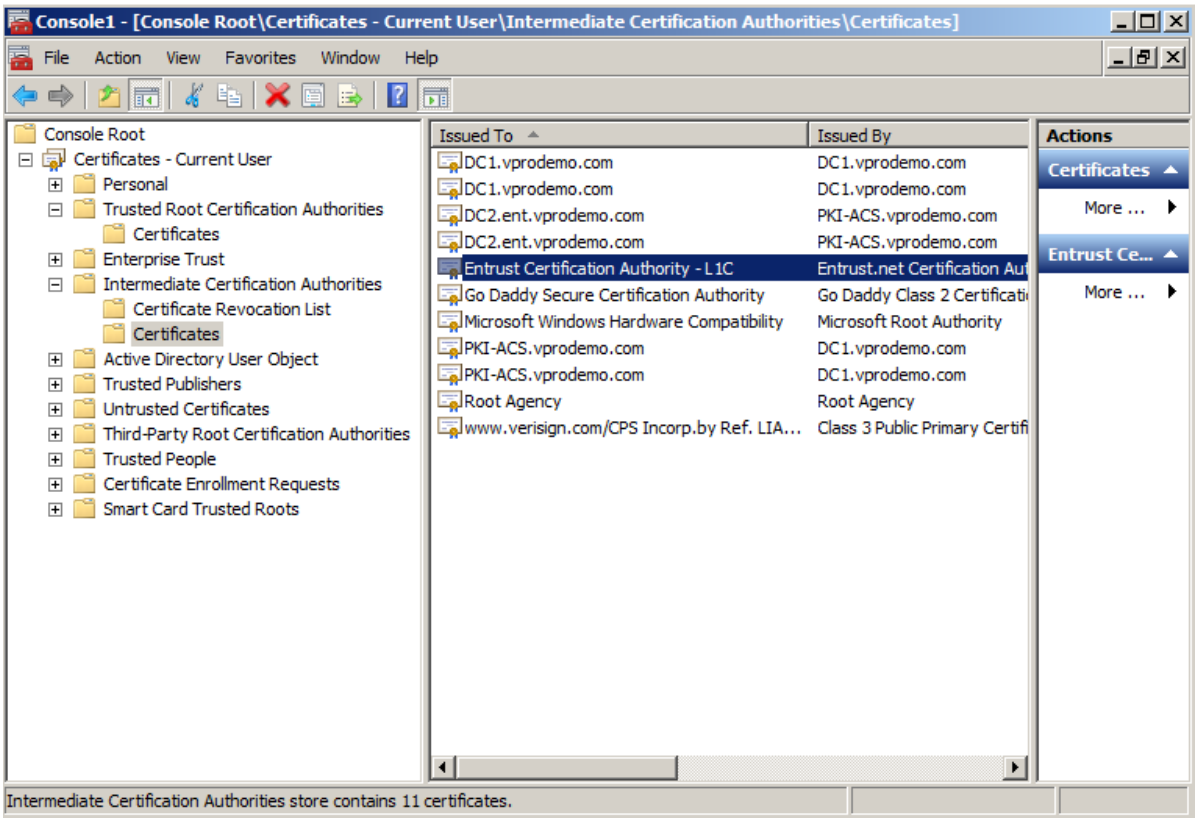
1. Double-click the **Chain_Certificate.cer** file where you saved it. Choose **Install Certificate**.



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



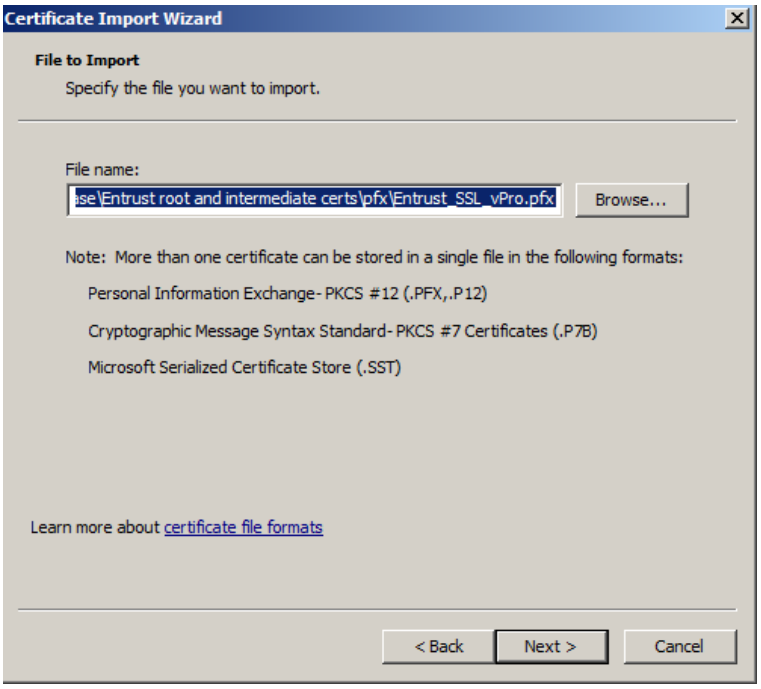
The certificate is now installed in the Intermediate Certificate Authorities store.



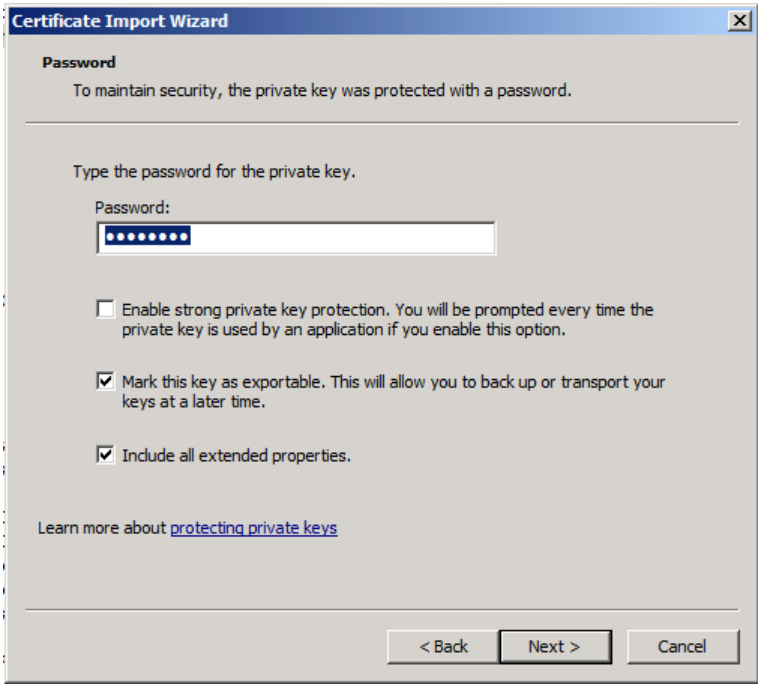

## 5.3 Install the pfx Certificate

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**.

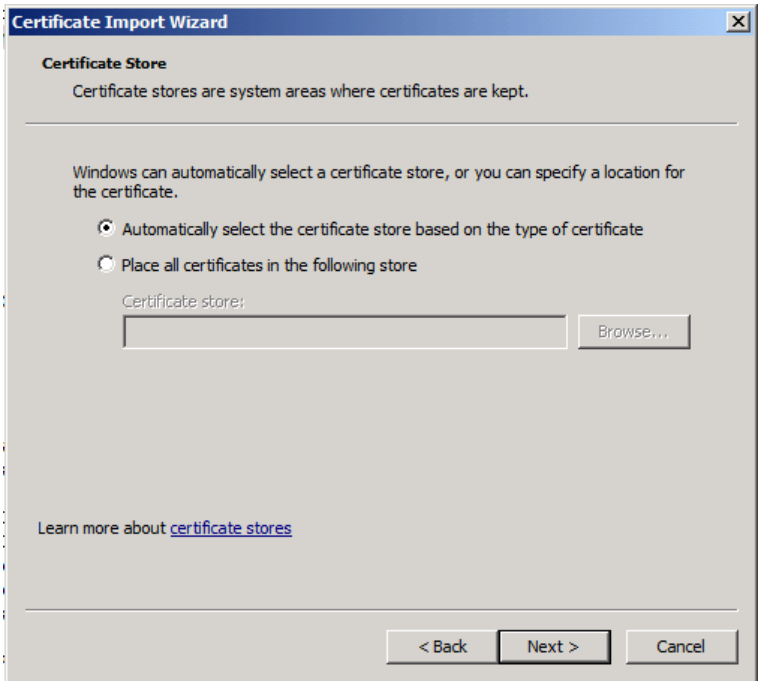
1. Double-click on the Entrust_SSL_vPro.pfx file where you saved it. Choose **Next**.



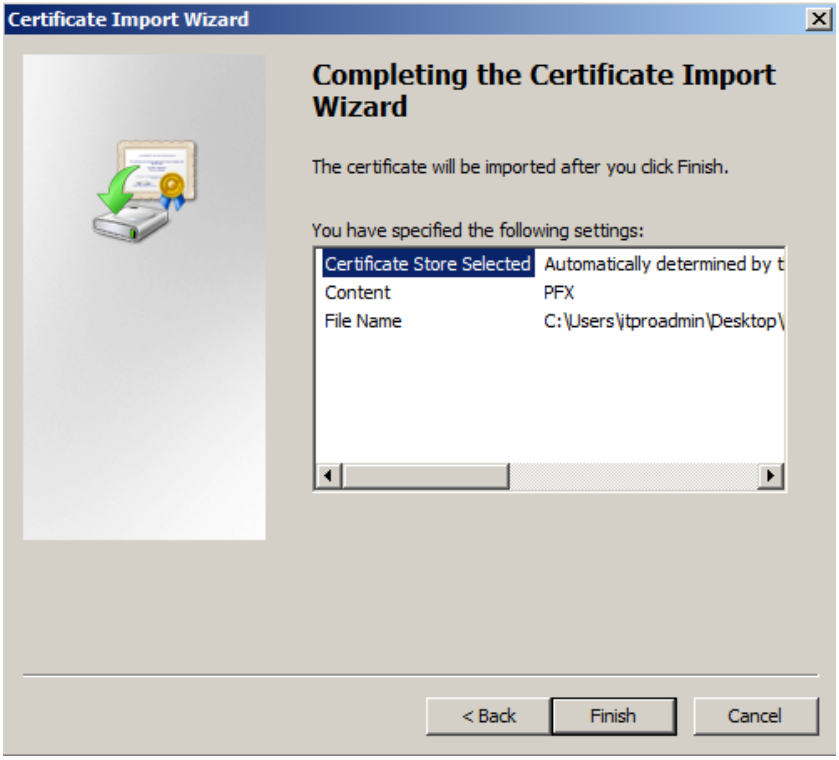

2. Enter in the password and select **Mark Key as exportable** and **Include all extended properties**. Choose **Next**.



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



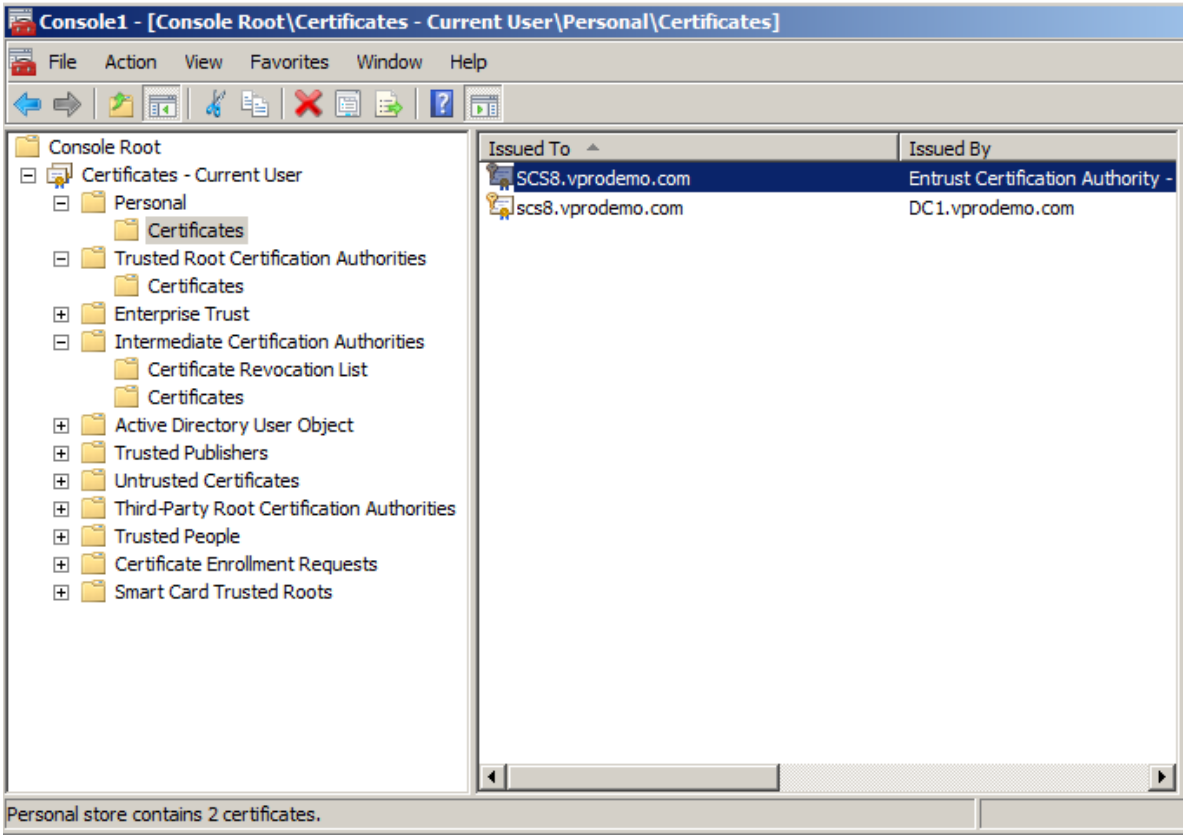

4. Choose **Finish.**



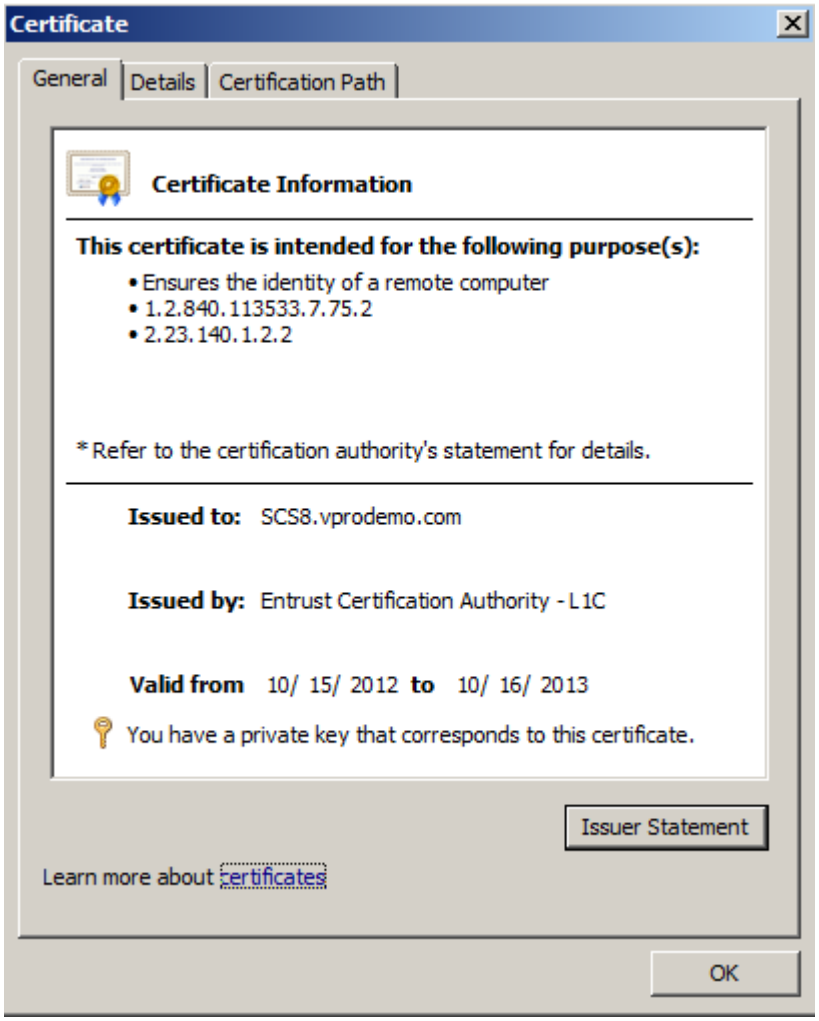

The certificate is now installed in the Current User Personal Certificates store.

## 5.4 Verify the Certificate Chain

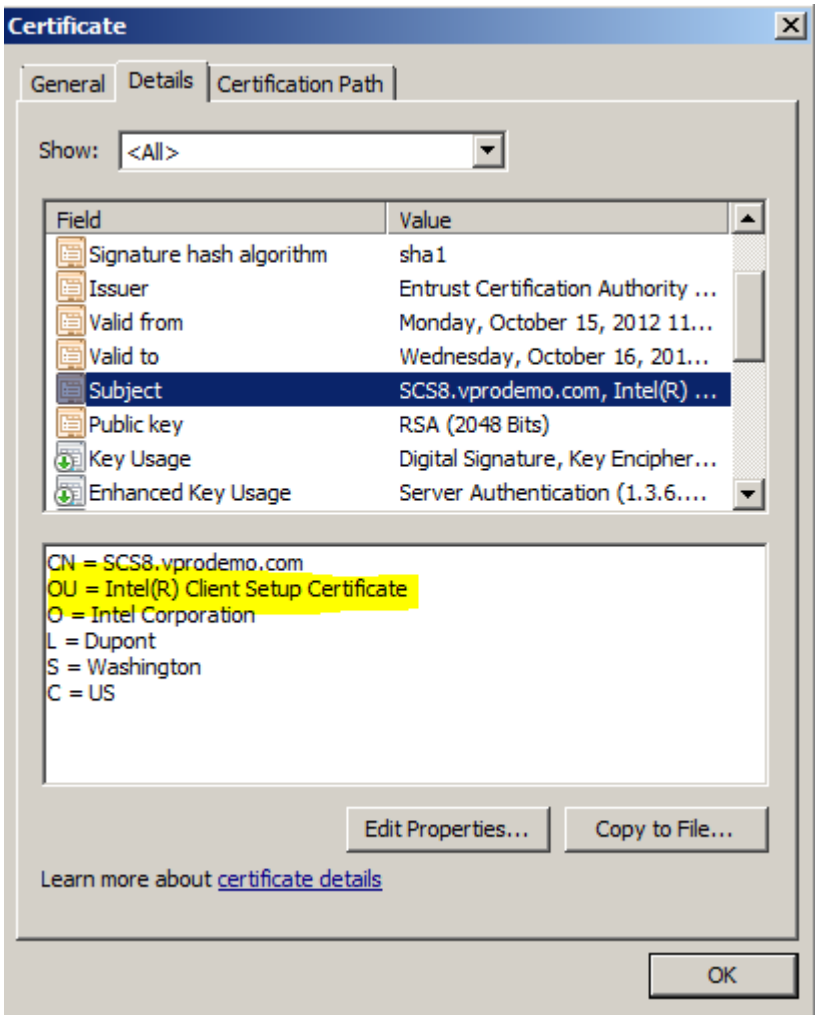
1. To verify the chain, double-click the imported certificate. In this example **SCS8.vprodemo.com** issued by Entrust.



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.



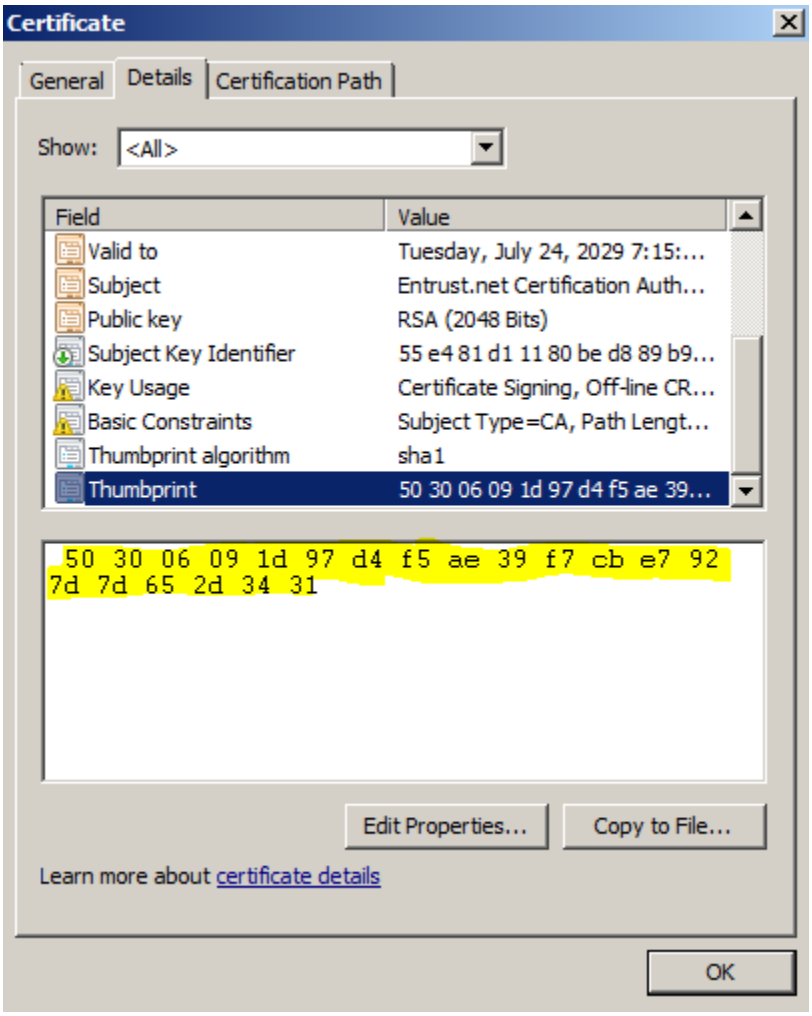
3. From the Details menu, select **Subject** and then verify the OU of **"Intel(R) Client Setup Certificate"** is present. Click the **Certificate Path** tab.



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.