



## Intel® Remote Configuration Certificate Utility

### Frequently Asked Questions

#### General Info

1. [What operating system do I have to use to run the wizard?](#)
2. [What configurations are required prior to running the wizard?](#)
3. [What user privileges do I need to have in order to run the application?](#)
4. [Why do I have to use Certificate Authority?](#)
5. [How does certificate signing work?](#)
6. [Can different users and servers be used to generate a certificate?](#)
7. [Is it possible to make a back-up of the private key?](#)
8. [Do I need to own the domain that I am going to use for purchasing a certificate?](#)
9. [Does this tool provision a client system for me?](#)

#### Certificate Install

10. [Do I have to use your wizard to install the certificate?](#)
11. [How can I access the certificate after it is installed?](#)
12. [What are the next steps after I install the certificate?](#)

#### Working with Vendors

13. [How do I determine if a certificate response is valid?](#)
14. [How do I save the certificate response?](#)

#### GoDaddy\*

15. [Can I use GoDaddy's 'Standard SSL'?](#)
16. [What should I enter in the "Company Name" field in the wizard, if I have purchased a certificate from GoDaddy?](#)

#### Comodo\*

17. [What certificates does Comodo support?](#)

#### VeriSign\*

18. [What certificates are supported by VeriSign managed PKI accounts?](#)
19. [How does the May 17, 2009 VeriSign Root migration affect remote configuration certificates?](#)

#### Other Considerations

20. [What needs to be done in the Certificate Authority to support UCC Certificates?](#)
21. [What if I want to install a certificate type the utility does not recommend?](#)

## **General Info**

### **Q1. What operating system do I have to use to run the wizard?**

A. In order to install and run our wizard you must use Microsoft\* Windows\* Server 2003.

### **Q2. What configurations are required prior to running the wizard?**

A. In order to successfully run and complete the wizard:

1. You must install and configure Microsoft Certificate Authority on your server.
2. You must configure DHCP with option 15 on your domain.
3. You must have Microsoft .Net 3.0 or higher installed.

### **Q3. What user privileges do I need to have in order to run the application?**

A. You must have Domain Administrator privileges to be able to run this application.

### **Q4. Why do I have to use Certificate Authority?**

A. Secure Socket Layer (SSL) requires the use of a certificate authority (CA). The CA prevents "man-in-the-middle" attacks on your web server. You need to be certain that no third party is intercepting communications and violating the integrity or privacy of your transmissions. This implementation uses the Microsoft\* Certificate Authority.

### **Q5. How does certificate signing work?**

A. After you create a CSR, a 'public' file is generated. This is the text that you will submit to the vendor. Associated with this 'public' portion of the CSR is a 'private' key. This key is automatically generated and saved to the user's certificate enrollment request. This private key must be present in order to successfully install the vendor's certificate response.

### **Q6. Can different users and servers be used to generate a certificate?**

A. No. The same user who generates the CSR must install the response on the same server as the one used to generate the certificate.

### **Q7. Is it possible to make a back-up of the private key?**

A. Yes. Open Microsoft Management Console (MMC), browse to certificates, look in the user's 'Current Enrollment Requests', then right click on the file and select 'export'.

**Q8. Do I need to own the domain that I am going to use for purchasing a certificate?**

A. Yes. You must own the domain that you will use to purchase a certificate. As part of the process, all vendors will verify that the domain name requested in the CSR matches up with the domain and the purchaser's information.

**Q9. Does this tool provision a client system for me?**

A. No. Its purpose is only to aid in certificate selection and installation. You will need to use the Intel® Setup and Configuration Service (Intel® SCS) or your management console provider's solution for remote Intel® AMT provisioning (MS SCCM\*, SMS\*, Alteris\*, LanDesk\*, etc.). For further information please refer to the Intel® SCS documentation found on this page:

<http://software.intel.com/en-us/articles/download-the-latest-version-of-intel-amt-setup-and-configuration-service-scs/>

**Certificate Install**

**Q10. Do I have to use your wizard to install the certificate?**

A. No. You can also follow vendor instructions for installing the certificate if you choose not to use our tool for installation.

**Q11. How can I access the certificate after it is installed?**

A. After a certificate is installed, it is possible to export the certificate for back-up and to transfer the certificate to other servers.

In order to access the certificate, open Microsoft Management Console (MMC) and go to user store. The certificate should be located in the 'personal' folder. Right click on the certificate and select export. Be sure to export the certificate with its private key.

**Q12. What are the next steps after I install the certificate?**

A. The next step is to provision the client systems. Provisioning (also referred to as activation) is outside the scope of this application. For further information please refer to the Intel® Setup and Configuration Service documentation found on this page:

<http://software.intel.com/en-us/articles/download-the-latest-version-of-intel-amt-setup-and-configuration-service-scs/>

## Working with Vendors

### Q13. How do I determine if a certificate response is valid?

A. Certificate vendors will email the certificate response. This will either be a .cer or a .crt file, or a text blob. Double click on the certificate to open it for viewing. If you can't open it, you will most likely get an error when you try to specify this file as a certificate response when running the Intel® Remote Configuration Certificate Utility (Intel® RCFG Utility).

### Q14. How do I save the certificate response?

A. When the vendor sends you a text reply:

1. Create a new text document.
2. Copy the content of the text blob from "----BEGIN NEW CERTIFICATE REQUEST----" to "----END NEW CERTIFICATE REQUEST----".
3. Rename your document to 'filename.cer' and save.
4. Try to open this file.
5. If this doesn't work, the vendor may have sent you a full certificate chain.
  - a. Rename the file to 'filename.p7b'
  - b. Open the .p7b file
  - c. Navigate to the certificate, right click on the certificate name and select 'export'. This will save the certificate file and the wizard can use it for the install.

## GoDaddy\*

### Q15. Can I use GoDaddy's 'Standard SSL'?

A. No. You must purchase 'Deluxe SSL' or 'Premium SSL' from GoDaddy. 'Standard SSL' will not work.

### Q16. What should I enter in the "Company Name" field in the wizard, if I have purchased a certificate from GoDaddy?

A. If you have purchased a certificate from GoDaddy, enter the name of your business in the "Company Name" field in our wizard **unless** you purchased a certificate for a small business/sole proprietor, in which case the "Company Name" field must match the name of the person who is requesting the certificate.

## Comodo\*

### Q17. What certificates does Comodo support?

A. At this time, Comodo only supports 'Standard SSL' certificates, which include the following certificate options:

1. Standard SSL
2. Multiple Standard SSL
3. Top Level Domain support

## VeriSign\*

### Q18. What certificates are supported by VeriSign managed PKI accounts?

A. Only Wildcard & UCC certificates are supported for VeriSign managed PKI accounts.

### Q19. How does the May 17, 2009 VeriSign Root migration affect remote configuration certificates?

A. On May 17, 2009 VeriSign upgraded all SSL Certificates to a new root. Please see this VeriSign document for information from VeriSign specific to how this change affects remote configuration certificates.

## Other Considerations

### Q20. What needs to be done in the Certificate Authority to support UCC Certificates?

A. Before creating the CSR you will need to change a flag in your Certificate Authority (CA). This must be performed on the server that the certificate service is running on. Follow these steps:

- 1) Close the Intel® RCFG Certificate Utility
- 2) Open a command window on the CA server (from Start → Run → CMD)
- 3) Execute the following command from the command prompt:  
C:> Certutil -config <server\cname> -setreg policy\EditFlags +EDITF\_ATTRIBUTESUBJECTALTNAME2  
- Where <server\cname> is the server FQDN & CA name used for remote configuration
- 4) Then restart certificate server from the command prompt:  
C:> Net stop certsvc  
C:> Net start certsvc
- 5) Run the Intel® RCFG Certificate Utility (UCC certificates are now supported)

### Q21. What if I want to use a certificate type the utility does not recommend?

A. The Intel® RCFG Certificate Utility will make a recommendation based on information you provide regarding basic environmental considerations. Inputting specific information will result in the tool generating the following certificates:

- Standard SSL – list only a single DHCP option 15 value (example: server.company.com)
- Wildcard SSL – list at least 2 DHCP option 15 values, all values must have same domain prefix (example: server1.company.com and server2.company.com)
- UCC SSL – list at least 2 DHCP option 15 values with different domain prefixes (example: server.company.com and server.company.net)

## Still have questions?

Contact us at: [support\\_dopd\\_swe@intel.com](mailto:support_dopd_swe@intel.com)

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. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

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 by visiting Intel's Web site at [www.intel.com](http://www.intel.com).

Intel® Active Management Technology requires the computer system to have an Intel(R) AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off.

Copyright © 2008 Intel Corporation. All rights reserved. Centrino, Intel, Intel logo, Intel vPro are trademarks of Intel Corporation in the U.S. and other countries.

\*Other names and brands may be claimed as the property of others. Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries.