

Certificate Signing Request (CSR) Generation for a Third-Party Certificate on a Wireless Control System (WCS)

Document ID: 98599

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Certificate Signing Request (CSR)

CSR Generation Using a WCS

- Import a Pre-Existing Key/Certificate Pair to the WCS

Verify

Troubleshoot

- Keyadmin.bat tool will not generate CSR in install directory

Related Information

Introduction

This document explains how to generate a Certificate Signing Request (CSR) in order to obtain a third-party certificate using a Wireless Control System (WCS) and how to upload the certificate onto the WCS.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Knowledge of how to install and configure WCS for basic operation
- Knowledge of self-signed and digital certificates, and other security mechanisms related to Public Key Infrastructure (PKI)

Components Used

The information in this document is based on these software and hardware versions:

- WCS version 4.1.91.0

Note: CSR generation that uses a WCS is only supported starting with WCS version 4.1.91.0.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Certificate Signing Request (CSR)

A certificate is an electronic document that you use in order to identify a server, a company, or some other entity and to associate that identity with a public key.

A self-signed certificate is an identity certificate that is signed by its own creator. That is, the person who created the certificate also signed off on its legitimacy.

Certificates can be self-signed or can be attested by a digital signature from a certificate authority (CA).

CAs are entities that validate identities and issue certificates. The certificate that the CA issues binds a particular public key to the name of the entity that the certificate identifies, such as the name of a server or device. Only the public key that the certificate certifies works with the corresponding private key possessed by the entity that the certificate identifies. Certificates help prevent the use of fake public keys for impersonation.

A CSR is a message that an applicant sends to a CA in order to apply for a digital identity certificate. Before a CSR is created, the applicant first generates a key pair, which keeps the private key secret. The CSR contains information that identifies the applicant, such as a directory name in the case of an X.509 certificate, and the public key chosen by the applicant. The corresponding private key is not included in the CSR, but is used to digitally sign the entire request.

The CSR can be accompanied by other credentials or proofs of identity required by the certificate authority, and the certificate authority can contact the applicant for further information. For the most part, a third-party CA company, such as Entrust or VeriSign, requires a CSR before the company can create a digital certificate.

CSR generation is independent of the device on which you plan to install an external certificate. Therefore, a CSR and a private key file can be generated on any individual machine which supports CSR generation. CSR generation is not switch-dependent or appliance-dependent in this case.

This document explains how to generate CSR for a third-party certificate using the Cisco WCS.

CSR Generation Using a WCS

CSRs on a WCS can be generated using a tool available in the WCS installation directory. This tool is called **keyadmin.bat**.

Note: If the WCS is installed on Linux, you will have to use the **keyadmin.sh** tool available at **/opt/WCS4.1/bin/**. This example shows how to generate a CSR and import the signed certificate using a WCS installed on a Microsoft Windows 2003 server.

Complete these steps in order to access the tool:

1. Go to the **Command prompt** available with Windows.
2. Go the WCS installation directory, then to the folder **bin**.

Here is an example:

```
C:\CD Program Files
```

```
C:\Program Files>CD WCS4.1

C:\Program Files\WCS4.1> cd bin

C:\Program Files\WCS4.1\bin>
```

This folder will have the **keyadmin.bat** tool which is used to generate the CSR.

3. Complete these steps in order to generate the CSR:

a. Enter this command:

```
keyadmin -newdn -csr genkey [csrFileName]
```

This generates a new key/self-signed certificate pair, and output the CSR to the specified file. The **-newdn** flag causes it to prompt for the distinguished name fields for the certificate. It is important to specify the final hostname that will be used to access the WCS in the CN field of the DN in order to avoid browser warnings.

Here is an example:

```
C:\Program Files\WCS4.1\bin>keyadmin -newdn -csr genkey C:\TEST\CSR-WCS.PEM

The WCS server is running
Changes will take affect on the next server restart
Enter the domain name of the server: TS-WEB
Enter the name of your organizational unit: ABC
Enter the name of your organization: XYZ
Enter the name of your city or locality: Sanjose
Enter the name of your state or province: CA
Enter the two letter code for your country: US
Generating RSA key
Configuring Apache server for key
Writing certificate signing request to C:\TEST\CSR-WCS.PEM
```

Once the command is executed, the CSR information is generated and written to the file.

The CSR information looks like this:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICnCCAYYCAQAwWTELMakGA1UEBhMCVVMx CzAJBgNVBAGTAkNBMRAdGyYDVQQHEwdTYW
MQwwCgYDVQQKEwNYWVoxDDAKBgNVBAsTAF0FCQzEPMA0GA1UEAxMGVFMtV0VCMiIBIjANBgkq
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAKL5lKTAwwe/HjKHSEoDcpNWvqv3iyGjmb5MHA132/++Q2HqZ
nXicy36VEscDKGYF4b+QMvR4jmRY5vwKioripPlhTKIt5xcIhESDR9k8fw62lWHV7nSulvWF0zFn
9NJm7X+1+2pUL8A1M5eMEq9uievVVFd5NJZOvmolli5lRJ3sjcHZhfnfO5cF2pLfHDTia00fPPM1P
U2+fZ5qYTvWsZbB0hsS32xDrnEvSB5zzCpgzhNC0/BjaWq2f+uZxsATN3s1L3G9upNp0dch0HKJW
+gxb0F0757f0NATZkAtg6q6lLMNVmXWsIlQkMmhXsPCNCWRlVlDCHTI02bdgeMst6wIDAQABoAAw
DQYJKoZIhvcNAQEEBQADggEBAHhBMMi0KYf/Mog19pWhnBDV50TU52NNmN3lm9lCpag6OerhHrg
U16fPx9v847ix9gPa53J9It0/4d2t3QAsISIDiXmMhjvwnxpTUGjmquHAJbx4vNQc8UX9V016O4/
UxOiRYA20Cegyuaq2ExoIsJCKWwymIoHS5Hpn2n9Qrulzny57097g1TrJUNdleVklg6R9lVWvdS+
bEUGfG0iSKCTn6foz2XECbvKL5QRSZM47CD3qpKnXE7FbJh9CCzNghzDt01WmtGYHhaiVLxnDKL1
C7qaEvx2DvVMEbcJ0WV5q9kvxKlY+FI5e42irQFDXnYJe45LmRnRj3tKd971+d8=
-----END NEW CERTIFICATE REQUEST-----
```

b. Now that your CSR is ready, copy and paste the CSR information into any CA enrollment tool.

In order to copy and paste the information into the enrollment form, open the file in a text editor that does not add extra characters. Cisco recommends that you use Microsoft Notepad or UNIX VI. Refer to the website of the third-party CA for more information on how to

submit the CSR through the enrollment tool.

After you submit the CSR to the third-party CA, the third-party CA digitally signs the certificate and sends back the signed certificate via email.

- c. Once you get back the signed certificate from the CA, you can install it to replace the original self-signed certificate by entering this command:

```
keyadmin importsignedcert [certFileName]
```

The certificate and the key are stored at
C:\ProgramFiles\WCS4.1\webnms\apache\conf\ssl.crt.

The certificate should be a signed X.509 certification in PEM format, and it must match the private key that was originally generated by the **genkey** command (see step 1). Therefore, if you generate a key again before you import the certificate, it will reject the certificate.

Import a Pre-Existing Key/Certificate Pair to the WCS

The WCS also has provisions to import a pre-existing key/certificate pair. In order to perform this, enter this command:

```
keyadmin importkey [keyFileName] [certFileName]
```

The key should be a PEM-encoded RSA private key with a line that starts with BEGIN RSA PRIVATE KEY, or it can be a PEM-encoded RSA private key in PKCS8 format with a line that starts with BEGIN PRIVATE KEY. In either case, the key must not be password protected.

The certificate should be a PEM-encoded X.509 certificate that matches the key.

Verify

Complete these steps in order to verify if the configuration works as expected:

1. After you import the signed certificate on to the WCS, restart the WCS for the changes to take effect.
2. Access the WCS using the web browser.

If the signed certificate is valid and has a matching domain name, then the user should go right to the login page without the problem with the certificate popup warning dialog.

Troubleshoot

Keyadmin.bat tool will not generate CSR in install directory

When **keyadmin.bat** is performed in the **WCS\bin** directory on Windows, this error is generated:

```
Generating RSA key
Configuring Apache server for key
Writing certificate signing request to
Error generating key java.security.KeyStoreException: Could not create CSR
C:\Program Files\WCS4.x\bin>
```

In order to resolve this issue, define a filename in some other directory besides the installation directory of the WCS. Here is an example:

```
C:\Program Files\WCS4.2.81.0\bin>keyadmin -newdn -csr genkey C:\TEST\CSR-WCS.PEM
```

```
The WCS server is running
Changes will take affect on the next server restart
Enter the domain name of the server: cisco
Enter the name of your organizational unit: cisco
Enter the name of your organization: cisco
Enter the name of your city or locality: SJ
Enter the name of your state or province: CA
Enter the two letter code for your country: US
Generating RSA key
Configuring Apache server for key
\Writing certificate signing request to C:\TEST\CSR-WCS.PEM
```

Related Information

- [Certificate Signing Request \(CSR\) Generation for a Third-Party Certificate on a WLAN Controller \(WLC\)](#)
- [Wireless Control System Troubleshooting](#)
- [Wireless Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Apr 23, 2008

Document ID: 98599
