webMethods Certificate Toolkit

User's Guide

Version 7.1.1

January 2008

webMethods

Document ID: CERT-UG-711-20080128

Table of Contents

About This Guide

This guide describes how to install and use the webMethods Certificate Toolkit. It contains information for administrators and developers of webMethods products about creating and managing digital certificates for use with webMethods products.

To use this guide effectively, you should understand the basic concepts described in the *webMethods Integration Server Administrator's Guide* and the *webMethods Developer User's Guide*.

Document Conventions

Convention	Description
Bold	Identifies elements on a screen.
Italic	Identifies variable information that you must supply or change based on your specific situation or environment. Identifies terms the first time they are defined in text. Also identifies service input and output variables.
Narrow font	Identifies storage locations for services on the webMethods Integration Server using the convention *folder.subfolder:service*.
`Typewriter font`	Identifies characters and values that you must type exactly or messages that the system displays on the console.
UPPERCASE	Identifies keyboard keys. Keys that you must press simultaneously are joined with the "+" symbol.
\	Directory paths use the "\" directory delimiter unless the subject is UNIX-specific.
[ ]	Optional keywords or values are enclosed in [ ]. Do not type the [ ] symbols in your own code.

Additional Information

The webMethods Advantage Web site at http://advantage.webmethods.com provides you with important sources of information about webMethods products:

- **Troubleshooting Information.** The webMethods Knowledge Base provides troubleshooting information for many webMethods products.
- **Documentation Feedback.** To provide feedback on webMethods documentation, go to the Documentation Feedback Form on the webMethods Bookshelf.
- **Additional Documentation.** Starting with 7.0, you have the option of downloading the documentation during product installation to a single directory called "_documentation," located by default under the webMethods installation directory. In addition, you can find documentation for all webMethods products on the webMethods Bookshelf.

1 Overview of the webMethods Certificate Toolkit

What Is the Certificate Toolkit?

The webMethods Certificate Toolkit is a utility you can use to easily create a digital certificate for your webMethods Integration Server.

The digital certificate, used during Secure Sockets Layer (SSL) communications, helps ensure that communications between your Integration Server and clients are secure. When the server and a client communicate, the server presents its certificate to the client. The certificate attests to the identity of your server. In other words, the client can be sure it is communicating with your organization.

Obtaining the digital certificate is just one step in making communications with your Integration Server secure. Once you have obtained a digital certificate, you must configure your Integration Server to use SSL. Instructions for doing so are provided in "Managing Server Security" in the *webMethods Integration Server Administrator's Guide*.

In addition, you can control access to the Integration Server through access control lists, listening ports, client authentication, and Integrated Windows authentication. For a more in-depth explanation of securing your Integration Server, refer to "Managing Server Security" in the *webMethods Integration Server Administrator's Guide*.

Installing the webMethods Certificate Toolkit

Important! This section provides only instructions that are specific to installing the webMethods Certificate Toolkit. For complete instructions on using the webMethods Installer, see the *webMethods Installation Guide*.

Install webMethods Certificate Toolkit 7.1.1 on the same machine as Integration Server 7.1.1. The Certificate Toolkit supports the same platforms as webMethods Integration Server and uses the JRE you install for Integration Server.

To install the webMethods Certificate Toolkit:

1. Shut down the Integration Server.
2. From the webMethods Advantage Web site at http://advantage.webmethods.com, download the IS_7-1_CertToolkit.zip file.

3 On Windows platforms, unzip IS_7-1_CertToolkit.zip into the *webMethods_directory*\IntegrationServer directory.

On Unix platforms, extract the contents of IS_7-1_CertToolkit.zip into the *webMethods_directory*/IntegrationServer directory.

To do this, use the following jar utility:

(from the IntegrationServer directory)
../jvm/<platform_jvm>/bin/jar -xvf <download_directory>/IS_7-1_CertToolkit.zip

In the above syntax, <download_directory> is the directory where you downloaded the .zip file from the webMethods Advantage Web site.

4 Start Integration Server.

Starting the webMethods Certificate Toolkit

The Certificate Toolkit must be running in order for you to create a digital certificate for your Integration Server.

To start the Certificate Toolkit on Windows

1 At a command line, type the following command to switch to the CertificateToolkit directory:

```
cd IntegrationServer_directory\CertificateToolkit
```

2 Type the following command to start the toolkit:

```
bin\ssltoolkit.bat
```

To start the Certificate Toolkit on UNIX

1 At a command line, type the following command to switch to the CertificateToolkit directory:

```
cd IntegrationServer_directory\CertificateToolkit
```

2 Type the following command to start the toolkit:

```
bin/ssltoolkit.sh
```

3 Execute this script running in X-Windows.

Note: Run this script when logged on as a non-root user. Running the script as root might reduce the security of your system.

Uninstalling the webMethods Certificate Toolkit

Important! This section provides only instructions that are specific to uninstalling the Certificate Toolkit. See the *webMethods Installation Guide* for instructions for uninstalling other webMethods components.

To uninstall the webMethods Certificate Toolkit

1. Shut down the Integration Server.
2. Delete the *webMethods_directory*\IntegrationServer\CertificateToolkit\lib\certkit.jar.
3. Optionally, if you do not want to save the files you created after you installed the Certificate Toolkit (for example, user-created certificates), delete the *webMethods_directory*\IntegrationServer\CertificateToolkit directory.

2 Obtaining a Digital Certificate Integration Server

Overview

This chapter describes the steps you must follow to set up a digital certificate for your webMethods Integration Server. The chapter has two parts:

- "Generating a Certificate Signing Request and Sending It to the Certificate Authority"—In this section you use the Certificate Toolkit to generate a Certificate Signing Request and send the request to a Certificate Authority.
- "Saving Your Certificate"—In this section you obtain your certificate and use the Certificate Toolkit to make it available to your Integration Server. If necessary, the Certificate Toolkit converts the certificate to Distinguished Encoding Rules (DER) format, which the Integration Server requires.

Generating a Certificate Signing Request and Sending It to the Certificate Authority

The following procedure describes how to use the webMethods Certificate Toolkit to create your private key and a Certificate Signing Request (CSR) and send your request to your Certificate Authority (CA).

Step	Description
Step 1	Generate the private key.
Step 2	Generate the Certificate Signing Request.
Step 3	Send your request to the Certificate Authority.
Step 4	Wait for the response; check with your Certificate Authority on the status of your request.

Step 1 Generating a Private Key

1 Start the Certificate Toolkit.

2 From the **Certificate Toolkit** menu, select **Generate a private key** and click **Next**.

3 From the **Generate a Private Key** screen, specify the following:

For this parameter…	Specify…
Key size	A key size or accept the default of 1024. 2048 is more secure than 1024, but might slow processing. Use 1024 for ordinary transactions and 2048 for high-value transactions.
Algorithm	The webMethods Certificate Toolkit uses the RSA Public-Key algorithm.
Enter file name	Name of the file that you want to hold the private key you are about to create. The default is CertToolkit.
Select a location for private key	The directory path of the file to which you want the toolkit to write your server's private key.

4 Click **Next**.

Note: Depending on your machine and the key size you selected, key generation can take several minutes.

When the Certificate Toolkit has successfully generated the key, a dialog displays stating the key has been generated. Click **OK**.

The **Create a Certificate Signing Request (CSR) including the Public Key** screen displays. If you want to continue and create the CSR, follow the instructions under "Generate the Certificate Signing Request" below. If you do not want to create the request now, click **Back** to return to the **Certificate Toolkit** menu.

Note: In the next step, the toolkit creates a *public* key from the private key just created.

Step 2 Generating the Certificate Signing Request

1 If it is not already started, start the Certificate Toolkit and select **Generate a Certificate Signing Request (CSR) including Public Key**. See "Starting the webMethods Certificate Toolkit" on page 9 for instructions.

2 Specify the following information.

For this parameter…	Specify…
Select the file that contains the private key	The directory path and file name of the file that contains the private key you created earlier.
Enter CSR file name	The name of the file to which the Certificate Toolkit is to write the request. Later, you will send the information in this file to your CA. The toolkit uses the PEM encoding format (creates header information that includes the version number and the encryption algorithm used to encrypt the private key) and adds `pem` as the file extension. For example, if you specify `csrfile`, the toolkit names the file `csrfile.pem`.

Note: The toolkit creates a *public* key from the private key you created earlier. The toolkit attaches the public key to the certificate Id information (name, organization, etc.) and sends it as part of the Certificate Signing Request.

3 In the **Server Information** portion of the screen, specify the following information:

For this parameter…	Specify…
Host name	Name of the host server on which the certificate will reside, for example, IntegrationServer.yourcompany.com.
Department	Your department within your company or organization.
Organization	Your company or organization.
City	City in which your company is physically located.
State	State in which your company is physically located. For example, if your company is incorporated in Delaware but located in California, specify California. This field is optional.
Country	Country in which your company is physically located.

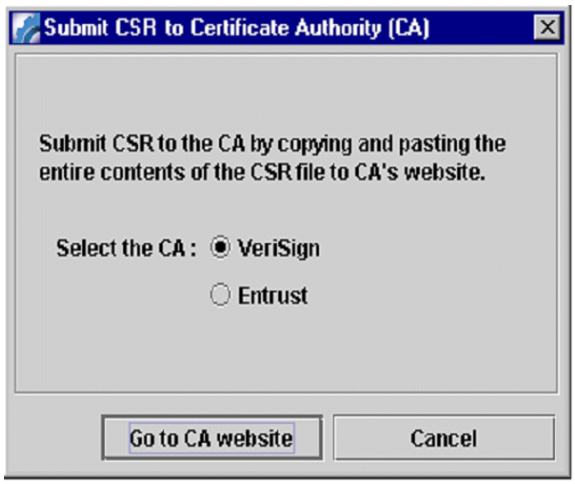
For this parameter…	Specify…
Contact E-Mail	E-mail address of the person to receive the response from the CA.
Revocation Password	A password you can give to your CA later if you decide to revoke your certificate. For example, if you think someone has stolen your private key, you must supply this password to your CA before they can revoke your certificate.

4 Click **Next**.

After the toolkit has successfully created your CSR, it displays a dialog to that effect.

5 Click **OK**.

The toolkit displays the following dialog:



6 Select VeriSign or Entrust and click **Go to CA website**.

If you want to use a different CA, click **Cancel** to go back to the toolkit menu, then **Exit** to exit the toolkit. Use the method required by your CA to submit your CSR to them.

Step 3 Sending the Certificate Signing Request to the CA

The method you use to send your CSR to the CA depends on your CA. If you just used the Certificate Toolkit to create a CSR and chose VeriSign or Entrust as your CA, you will be at VeriSign's or Entrust's website and will be asked to copy your CSR from the file it is stored in and paste it into a field on the website. Other CAs might have you send the request in an e-mail.

When you have finished submitting your request, you are returned to the Certificate Toolkit.

After your CA approves your request (this can take an hour for a test certificate or a number of days for a permanent certificate) they will send you a response. The form of

the response depends on the CA, but typically they will send it in an e-mail or they will require you to go to their website and obtain the response from there.

Step 4 **Waiting for a Response and Checking the Status**

Typically the CA will give you a PIN and a link to Web site so that you can check the status of your request. Monitor the status periodically. If the request seems to be taking too long, contact your CA.

Saving Your Certificate

Eventually, your CA will send you a response, either through e-mail or their website. The response might contain just your digital certificate with your public key, or it could contain a chain of certificates consisting of your certificate (with your public key) and the CA's own certificate. Typically, you will copy the response to a file of your choice, for example `Certificate.txt`.

The following procedure describes how to install the certificate or certificates on your webMethods Integration Server.

Note: The toolkit automatically converts certificates that are in a non-DER format to DER format.

Making the Certificates Available to Your Integration Server

1. Start the Certificate Toolkit. See "Starting the webMethods Certificate Toolkit" on page 9 for instructions.
2. Select **Convert and Save Certificates for use with webMethods Software certificates**.
3. Supply the following information:

For this parameter…	Specify…
Select the file that contains the CA's response	The directory path and name of the file that contains the response from the CA.

4. Click **Next**.

5 Enter information in the following fields:

For this parameter…	Specify…
Enter certificate file name	Name of the file to which you want the toolkit to write the converted version of your server's certificate, for example: `MyServerCert`. The toolkit automatically appends the `der` extension.
Select a location for the certificate	The directory path of the file to which you want the toolkit to write your server's certificate. Make sure the directory is in a location the Integration Server can access, such as *IntegrationServer_directory*\config

If the CA's response contains their certificate as well, you will see these fields:

For this parameter…	Specify…
Enter CA certificate file name	The name of the file to which you want the toolkit to write the converted version of the CA's digital certificate. Typically you will have a directory set aside just for CA certificates.
Select a location for the CA's certificate	The directory path of the file to which you want the webMethods Certificate Toolkit to write the converted version of the CA's certificate. Make sure the directory is in a location the Integration Server can access, such as *IntegrationServer_directory*\config.

6 Click **OK**.

If you did not receive the CA's certificate, see "What to Do if the Certificate Authority Does Not Send You Their Own Certificate" below.

Now you are ready to configure your Integration Server to use SSL. Refer to the section "Configuring the Server to Use SSL" in the chapter "Managing Server Security" in the *webMethods Integration Server Administrator's Guide*.

What to Do if the Certificate Authority Does Not Send You Their Own Certificate

Sometimes a CA will send a signed version of the certificate for your Integration Server without including a copy of the CA's certificate. You need a copy of the CA's certificate to ensure secure communication; therefore if you did not receive one, try one of the following methods to obtain one:

- **Contact the Certificate Authority**—some Certificate Authorities allow you to copy their certificate from their website. If that option is not available, get in touch with your CA through their website, e-mail, or by phone and ask them to send you the certificate.
- **Import it from your browser**—most Web browsers that support SSL are shipped with the certificates of well-known Certificate Authorities. Some browsers provide a method for you to import the certificate from the browser to a file. The method you use to obtain the certificate depends on your browser.
- **Import it from the Integration Server's certificate**—You might be able to obtain the CA's certificate by following the certificate path from your Integration Server's certificate. On an NT machine, double click your converted certificate file, for example `certificate.der`. Select the **Certification Path** tab. If the CA certificate is available, it will appear above your certificate in the path. Double click this file and copy the CA certificate to a file with the der extension, for example `cacert.der`. Place the file in the directory where you store CA certificates.

Index