Certificate Validation Module (CVM) 2.04 Release Notes

These release notes accompany the delivery of VeriSign Certificate Validation Module (CVM) 2.04's release.

What's New in VeriSign's Certificate Validation Module 2.04?

Note CVM 2.04 now supports V2 CRLs (Certificate Revocation List).

This release of Certificate Validation Module (CVM) 2.04 contains the following new features.

Microsoft Internet Information Server (IIS) and Microsoft ISA Server Configuration Option

A new configuration option is added to CVM for the Microsoft Internet Information Server (IIS) and Microsoft ISA Server. This option appears when you use `valConfig.exe` to configure the parameters in CVM.

ISA-Install Option

This option tells the target platform on which CVM plug-in is used. It can either be Microsoft ISA Server or Microsoft IIS Server. A value of **Yes** means that CVM plug-in is used on Microsoft ISA Server and is **No** for Microsoft IIS Server. The default value is **No**.

CVM on Microsoft ISA Server

CVM is now supported on Microsoft ISA Server. There are no additional features for ISA server.

- **Requirements**: Microsoft ISA Server 2000 SP1 with Hotfix 178 on Windows 2000 server.

Steps to install CVM on ISA Server

To configure CVM on the ISA server, follow these steps:

1. Stop the Web server

   Open the Microsoft ISA Management Console and stop the Web proxy service.

2. Unzip the CVM software and copy the subdirectories to the ISA server

   - Copy the three subdirectories from the `Nt\server\cvm\iis` directory to `C:\VeriSign\cvm`
   - Copy the plug-in `dlls` from `Nt\server\cvm\iis\bin\` into the ISA installation directory (for example, `c:\Program Files\Microsoft ISA Server`)

3. Configure the ISA Web Proxy Server to use the Secure Socket Layer (SSL) protocol

   If you do not already have a Server Certificate for your Web server, you must obtain one before configuring the Web server. Go to **http://www.verisign.com/** for details on obtaining a Server Certificate.

   Ensure that your Web server is configured to use the Secure Sockets Layer (SSL) protocol (required for using VeriSign Digital ID) by completing the following procedures:

   a. In the Microsoft ISA Management Console, select the properties for your server.

   b. Open the **Incoming Web Request** tab.

   c. Select the **listener** and edit its properties.

      – Select the server certificate by clicking **Select**.

– Ensure that both checkboxes **Use a server certificate to authenticate to web clients** and **Client certificate (secure channel only)** are selected.

d Check the boxes **Enable SSL listeners** and **Ask unauthenticated users for authentication**. This will ensure that the server uses SSL protocol and request the client browser for a certificate before continuing.

4 Run the CVM configuration program (`valConfig.exe`)

The `valConfig.exe` enables you to write values into the Windows NT/Windows 2000 Registry. Run the `valConfig.exe` program located in `C:\VeriSign\cvm\config\valConfig.exe`. The *valConfig* dialog box appears (Figure 1-1). Refer to Appendix A "CVM Configuration Values" of *Managed PKI Certificate Validation and Parsing Guide* for descriptions and values to use when running `valConfig.exe`.

You must run this program before using the CVM filter. Check **Yes** for **isa-install** option**.**

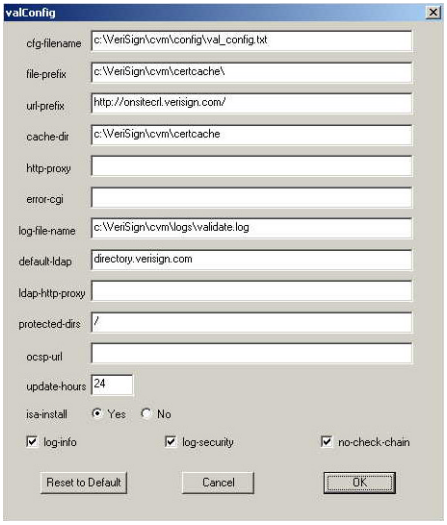

Figure 1-1 *valConfig* dialog box

5 Edit the Trust Configuration File (val_config.txt)

Follow the instructions in Step 5, “Edit the Trust Configuration File (val_config.txt)” in “Installing and Configuring the CVM for Your Web Server” of *Managed PKI Certificate Validation and Parsing Guide*.

6 Create the log directory

Create the log directory where you specified your log file in the `valConfig.exe`. For example, for the *log-file-name* in Figure 1-1 on page 3 you would create: **`C:\VeriSign\cvm\logs`**.

During the CVM installation, important information is written to the log file you specify in the `valConfig.exe` configuration utility. This information is useful for ensuring the CVM is installed correctly. Consult these log files if problems arise.

7 Install the CVM Web filter in the ISA server.

Use the sample Visual Basic script `cvmRegister.vbs` (provided along with package) to register the CVM plug-in in the ISA Server. You can change the priority and direction in this script as per your requirement. The default priority is **Medium** and direction is **Incoming Web Requests**.

8 Restart the Web Proxy service in the ISA Server.

CVM on iPlanet 6.0 Web Server

CVM is now supported on iPlanet 6.0 Web server. There are no additional features for iPlanet 6.0.

- **Requirements**: iPlanet 6.0 Web server on Windows NT/2000, Solaris, HPUX.

Steps to install CVM on iPlanet 6.0 Server

To configure CVM on iPlanet 6.0 server, follow steps 1 - 3 as described in Chapter 5, “Installing and Configuring the CVM Plug-In for Netscape/iPlanet Enterprise Server,” of *Managed PKI Certificate Validation and Parsing Guide*. For step 4, ‘Edit the configuration files’, proceed as shown below:

1 Edit the file `<iPlanet-install-dir>/<server-name>/config/magnus.conf` file by adding the following lines in the end:

Note The line breaks in the sample lines below occur only due to the limits of the width of the page. There are only two lines. Even if many options are used, they must all be placed in the same line. Do not put a space after commas or use the **Enter** key in either of the two lines.

```
Init fn="load-modules" funcs="vsCheckCertInit,vsCheckClientCert"
shlib="<value>"

Init fn="vsCheckCertInit" cfg-filename="<value>" file-prefix="
<value>" url-prefix="<value>" ocsp-url="<value>" cache-dir="<
value>" log-security="<value>" log-info="<value>" default-ldap
="<value>" update-hours="<value>" no-check-chain="<value>" err
or-cgi="<value> http-proxy="<value>" ldap-http-proxy="<value>"
LateInit="yes"
```

Note The `Init fn` lines are added in `obj.conf` file in iPlanet 4.x Web server, whereas in iPlanet 6.0 they are added in `magnus.conf` file. An additional parameter **`LateInit`** is added for 6.0 Web server.

Use only the options that are appropriate for your implementation. For example, use either `url-prefix="<value>"` or `ocsp-url="<value>"`. Do not use both, as shown in the example. Some options are used by Microsoft IIS/ISA only.

2 Turn on the authorization function in `<iPlanet-install-dir>/<server-name>/config/obj.conf` file by adding following line:

```
AuthTrans fn="vsCheckClientCert"
```

To turn the authorization function on for all objects (the simplest method) add the line immediately after the `<Object name=default>` line.

Note For more details on the configuration options, see *Managed PKI Certificate Validation and Parsing Guide*.

Continue with steps 5 - 6 as described in the Chapter 5, "Installing and Configuring the CVM Plug-In for Netscape/iPlanet Enterprise Server," of *Managed PKI Certificate Validation and Parsing Guide*.

Upgrading to CVM 2.04

This section describes how to upgrade your current version of CVM to CVM 2.04. If you are installing CVM for the first time, see *Managed PKI Certificate Validation and Parsing Guide* for installation instructions

Upgrading For Netscape/iPlanet Enterprise Server

If you use Netscape iPlanet Enterprise server as your Web server follow these instructions to upgrade your existing version of CVM to CVM 2.04 while retaining your existing CVM settings:

1. Stop your Web server(s).
2. Unzip or untar the CVM 2.04 file into a temporary directory.
3. Locate the directory where you installed the binary files (`.so`, `.sl` or `.dll`) for your previous version of CVM. For example, Solaris users may have installed the CVM binary files in `/usr/local/lib or /usr/lib` and NT users may have installed the CVM binary files into `\NETSCAPE\SuiteSpot\bin\https`.
4. Copy the CVM 2.04 binary files (`.so,.sl or.dll`) from the temporary directory into the directory where you installed the binary files for your previous version of CVM. Overwrite the existing binary files if prompted.

Note Ensure that you do not overwrite any configuration files you may have edited in previous installations of CVM or you may lose your CVM settings.

5. Restart your Web server(s).
6. Verify that CVM is running properly with the correct version.

a Look for the version number in the start up message in your web server log file.

b Present a revoked certificate to your Web server. CVM denies access to the Web server if running properly.

Upgrading for Microsoft Internet Information Servers

The `valConfig.exe` shipped with this version use the configuration settings from `RegKey\Software\VeriSign\Validate\2.0`. If you are using the CVM version 1.x then you should reconfigure the configuration parameters in CVM 2.04.

Do not run `valConfig.exe` when upgrading from CVM 2.03. You can do so if you want to make additional configuration changes.

If you use Microsoft Internet Information server as your Web server follow these instructions to upgrade your existing version of CVM to CVM 2.04 while retaining your existing CVM settings:

1 Stop your Web Publishing and IIS Admin services.

2 Unzip the CVM 2.04 file into a temporary directory. (Unzipping this file creates several sub-directories under the temporary directory, including `<temporary directory>\Nt\server\cvm\iis\bin`).

3 Locate the directory where you installed your previous version of CVM. For example, you may have installed CVM into `C:\VeriSign\Validate`.

4 Copy all of the files from the `<temporary directory>\Nt\server\cvm\iis\bin` sub-directory created in Step 2. Paste these files into the directory where you installed your previous version of CVM. Also paste these binary files into the directory `C:\InetPub\Scripts`. If prompted overwrite the existing binary files.

Note Ensure that you do not overwrite any configuration files you may have edited in previous installations of CVM or you may lose your CVM settings.

5 Restart your Web publishing and IIS administrator services.

6 Verify that CVM is running with the correct version.

a. Look for the version number in the start up message in your CVM log file.

b. Present a revoked certificate to your Web server. CVM denies access to the Web server if running properly.

Support and Service

Call **1-800-579-2848**, to speak with a customer support representative. (Overseas and other customers who are unable to dial a U.S. 800 number, call **1-650-426-3535**.)

You can submit low-severity issues or questions in an e-mail message. Customer Support e-mail address is: **enterprise-pkisupport@verisign.com**.

Use e-mail only for low severity issues or questions. The turnaround time for e-mail requests is longer than for telephone requests.

For details on support, refer to *Enterprise Support and Service Overview*.