INSTALLATION AND CONFIGURATION GUIDE

Axway Desktop Validator

Version 4.12.1

Tuesday, October 11, 2016

This documentation describes the following Axway software:

Axway Desktop Validator

Contents

Introducing Axway Desktop Validator 1

The Axway Desktop Validator *Installation and Configuration Guide*, 4.12.1 describes the installation, configuration, and administration of the Axway Desktop Validator (DV). It is intended for administrators familiar with installing and configuring software on the Windows operating system and for users familiar with the fundamentals of PKI and digital certificate validation from key applications within their enterprise.

About Desktop Validator

Desktop Validator is a Microsoft Cypto API (CAPI) compliant revocation trust provider, enabling transparent validation of digital certificates from any CAPI compliant application. Desktop Validator runs as a service on 32-bit and 64-bit Microsoft Windows platforms and can be invoked to validate standard X.509v3 digital certificate issued by any Certificate Authority (CA).

By communicating with the Axway Validation Authority product, a sophisticated digital certificate status responder, Desktop Validator can check the status of digital certificates in real time. Desktop Validator can also validate certificates using a Certificate Revocation List (CRL) and can greatly enhance the performance and reliability offline through caching and advanced high-availability functionality. Desktop Validator can also follow certificate extensions such as AIA or CRLDP.

Using Desktop Validator on enterprise desktop systems, enterprises ensure that mission-critical operations such as system and network authentication, sending and receiving secure email, communicating with secure web servers, or authoring and reading digitally signing documents, are not compromised by expired or revoked digital certificates. Desktop Validator leverages native Microsoft Windows Cryptographic API (CAPI) for seamless integration with all CAPI enabled client or server applications on the desktop system.

A key application of Desktop Validator is smart card login. To enable Axway's revocation checking for users' smart card certificates, Desktop Validator Enterprise is installed on the Domain Controller and Desktop Validator Standard is installed on the client systems. Desktop Validator can check for revocation status using different protocols, CRLs, or cache to ensure performance and a high degree of reliability.

You can install and configure Desktop Validator on a single system or across multiple systems using a pre-configured instance of Desktop Validator (silent installation package) and a software distribution mechanism such as Microsoft Windows Group Policy Object (GPO), Microsoft's Systems Management Server (SMS), System Center Configuration Manager (SCCM), or Computer Associates' Unicenter.

Accessibility at Axway

At Axway, we strive to create accessible documentation for all our users.

This section describes the accessibility features of Desktop Validator documentation.

Accessibility features of the documentation

The product documentation provides the following accessibility features:

- *Keyboard-only navigation* on page 2
- *Screen reader support* on page 2
- *Support for high contrast and accessible use of colors* on page 2

The accessibility of the documentation has been tested with JAWS.

Keyboard-only navigation

- The documentation source code contains ARIA (Accessible Rich Internet Applications) to improve the natural tab order and add focus where needed.
- ARIA landmarks are used to identify the main elements of the online help windows.

Screen reader support

- The documentation structure is clear and the source code of the online help can easily be interpreted by JAWS.
- The PDF documents are tagged to provide a logical reading order.

Support for high contrast and accessible use of colors

- The documentation can be used in high-contrast mode.
- There is sufficient contrast between the text and the background color.

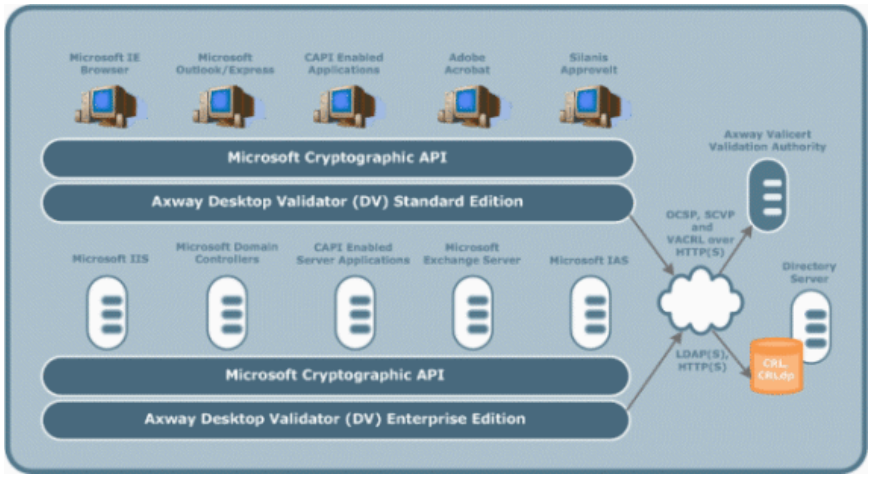
Desktop Validator architecture

Desktop Validator determines the status of a digital certificate by communicating with the Axway Validation Authority Server or any other standards compliant server using real-time protocols such as the Online Certificate Status Protocol (OCSP, IETF RFC 2560) or Server-based Certificate Validation Protocol (SCVP, IETF RFC 5055).

Desktop Validator can also determine the status of a digital certificate by checking it against a Certificate Revocation List (CRL, IETF RFC 5280), which can be obtained using Lightweight Directory Access Protocol (LDAP, IETF RFC 2251), Hypertext Transfer Protocol (HTTP, IETF RFC 2616), File Transfer Protocol (FTP), or from file locations

The CoCRL and VACRL protocols are proprietary mechanisms developed by Tumbleweed/Axway to obtain information contained in a CRL through bandwidth friendly means.

Additionally, Desktop Validator supports securing all supported communication protocols using open standard Secure Sockets Layer (SSL) or Transport Layer Security (TLS).



The basic validation process is as follows:

An application such as an email client or an application server is presented with a digital certificate used to perform a secure transaction such as digitally signing an email message or authenticating a user.

The application notifies the CAPI layer of the need to validate the certificate.

The CAPI layer passes the request to the Desktop Validator revocation trust provider which sends a request to the Desktop Validator service running on the system.

The Desktop Validator service first checks its Revocation Response Cache (unless caching has been explicitly disabled) to see if it can validate the certificate using a cached response. If it cannot, Desktop Validator will attempt to check the status of the certificate based on the validation protocols and policies configured which will be explained in greater detail.

Desktop Validator will return a response back to the Desktop Validator revocation status provider indicating the status of the certificate (Good, Revoked, Unknown, or Expired) or indicating that it was unable to verify the certificate.

The Desktop Validator service might also generate an alert in the notification area (formerly called the system tray), log the operation, and update the cache depending on configuration settings.

The Desktop Validator revocation trust provider in turn passes the certificate status back to the invoking application via CAPI.

Since a valid digital certificate must "chain" up to a trusted root, the application must determine the certificate path and validate every intermediate certificate. See *Certificate validation concepts* on page 75 for more information on certificate chains.

Desktop Validator determines which validation protocol to use based on CA-specific or default configuration policies which defines the validation protocols. Desktop Validator validation is also controlled by a number of other policies and settings as discussed in the chapter on configuring Desktop Validator. For improved performance and reliability, Desktop Validator can maintain several separate, configurable caches.

- An in-memory repository of all certificate validation responses, regardless of the validation protocol used.
- A disk-resident CRL repository of all CRLs obtained either as needed to validate a specific certificate, pre-fetched on demand or on a scheduled basis.
- An in-memory CRL repository of CRL data for specific CAs.

Desktop Validator capabilities

Desktop Validator is available in Standard and Enterprise editions:

- Desktop Validator Standard provides certificate validation support for client applications on Microsoft Windows platforms.
- Desktop Validator Enterprise provides certificate validation support for both client and server applications on Microsoft Windows platforms. Desktop Validator Enterprise is required for use of server applications such as Domain Controllers, IIS, and so on.

Note This document uses the term Axway Desktop Validator to refer to the common capabilities of the two product models. A distinction between Enterprise and Standard is made where capabilities differ.

The following table indicates differences in capabilities between Desktop Validator Standard and Enterprise products.

Capability	Desktop Validator Standard	Desktop Validator Enterprise
Client Applications (Internet Explorer, Outlook, Outlook Express, Adobe Acrobat)	X	X
Server Applications (Internet Information Server, Domain Controller, Exchange OWA, Microsoft VPN, IAS)	NO	X
Revocation Status Response Caching	X	X
CRL Caching - disk	X	X

Capability	Desktop Validator Standard	Desktop Validator Enterprise
CRL Caching - memory	NO	X
CRL Scheduled Download	X	X
Export Configuration File for Import	X	X
Export Configuration File for Group Policy Administrative Template Distribution	NO	X
Export Silent Install Package	NO	X

Desktop Validator Standard and Enterprise have the same screens. However, options that are only available in Desktop Validator Enterprise will be grayed out in Desktop Validator Standard, letting you know that you must upgrade to the Enterprise edition in order to use these capabilities.

Desktop Validator documentation set

Desktop Validator provides the following documentation including this guide:

- *Axway Desktop Validator™ Installation and Configuration Guide*
- *Axway Desktop Validator Release Notes*

Axway Global Support

Axway Global Support offers technical support for Axway products.

Axway also offers product customization and special services through the Axway Professional Services Organization. Contact Axway Global Support for more information.

When contacting Axway Global Support, have the following information:

- Product version and operating system version.
- The text of the error or warning message.
- A description of the problem and attempts made to fix the problem.
- You can contact Axway Global Support using one of the following methods:

Online

https://support.axway.com

Email

support@axway.com

Phone

Go to https://support.axway.com. Click the **Contact Axway Support** link to display our list of regional support contact phone numbers, and then locate the phone number appropriate for your location.

Installing Desktop Validator on a single system 2

This chapter provides instructions for installing Desktop Validator on a single system, starting and stopping the Desktop Validator service, viewing the event log, and uninstalling the Desktop Validator application.

Installation overview

Before you begin the installation process, make sure that the appropriate system requirements are met.

A typical Desktop Validator deployment consists of the following:

- Administrator installs Desktop Validator on a single system, as described in the procedures in this chapter.
- Administrator configures Desktop Validator as described in *Configuring Desktop Validator* on page 27 and the supporting chapters and verifies that all aspects of digital certificate validation through Desktop Validator are operational.
- Administrator automates installation and configuration of Desktop Validator on client systems as described in *Installing Desktop Validator* on page 8.

System requirements

This section covers the general system requirements for installing Desktop Validator. Desktop Validator 4.12.1 supports 32-bit and 64-bit Windows platforms.

Requirement	Standard	Enterprise
Memory (minimum)	1 GB	2 GB
Disk Space (minimum	1 GB	10 GB

Requirement	Standard	Enterprise
Operating Systems	Windows XP SP3 Windows 7 Windows 8.1 Windows 10	Windows XP SP3 Windows 2003 R2 Windows 2008 R2 Windows 7 Windows 8.1 Windows 10 Windows Server 2012 R2

If you are using DV Enterprise and want to cache CRL data in memory, your system should have sufficient memory to accommodate at least *six times* the disk size of the CRL data to be cached.

Installing Desktop Validator

This section describes how to install Desktop Validator on your system.

Before installing Desktop Validator

Ensure you have administrative privileges on the machine where you are installing Desktop Validator. If you are upgrading, you do not need to uninstall any previous supported Desktop Validator version before performing the upgrade.

Close all CAPI-compliant applications that can be Desktop Validator-enabled (you will be prompted to close them during the install process).

To install the Desktop Validator on Windows

1. Start the installation wizard by locating and double clicking the applicable `.exe` file.
    - MS Windows 32-bit:
        - `DesktopValidator-Win32-release-Standard.exe`
        - `DesktopValidator-Win32-release-Enterprise.exe`
    - MS Windows 64-bit:
        - `DesktopValidator-x64-release-Standard.exe`
        - `DesktopValidator-x64-release-Enterprise.exe`
2. Read the software license agreement and if you agree, click **I accept** to continue installation. If you do not agree, click **I do not accept** to exit the installer.
3. Enter your user information and company name on the customer information page; and choose if desktop shortcuts should be installed for the current user only, or installed for all users of the computer.

The Desktop Validator software is automatically installed for all users on the system. However, users without Administrator privileges will have a read-only view of configuration options, and will not be able to make any modifications to the configuration options set by the Administrator.

4. Click **Next** to install Desktop Validator to the default destination folder, or click **Change** to enter a different destination folder. The wizard is now ready to install.
5. Click **Install** to begin installation.
6. After installation is complete, click **Finish** to exit the installer.
7. To ensure Desktop Validator is fully operational, restart the machine.

Note When performing a remote installation, you *must* reboot the system after executing a software push.

Starting and stopping Desktop Validator

Desktop Validator runs as a Microsoft Windows service.

Note You must be logged on as an Administrator or a member of the Administrators group to perform this procedure.

1. Start the Services control panel. For example in Windows XP, click Start, click Control Panel, click Administrative Tools, and then double-click *Services*.
2. Select the Axway Desktop Validator service in the details panel.
3. Click **Start**, **Stop**, or **Restart** Action menu.

   Alternatively, right-click the *Axway Desktop Validator* service, and then click **Start**, **Stop**, or **Restart**.

Note Restarting the Desktop Validator service will flush all in-memory caches.

Viewing Desktop Validator Events in the Windows

By default, Desktop Validator uses the Windows Event Log to record all of its operations. You can configure Desktop Validator to use a log file in addition to or instead of the Windows Event Log. For more information, see *Configuring logging options* on page 64. The Desktop Validator Event Log can be viewed and managed using the **Windows Event Viewer**.

1. Start the Windows Event Viewer. For example, press Windows+R and type `eventvwr` or access it through the Windows Control Panel.

   For the Microsoft Windows XP, *Audit Failure* and *Audit Success* are event types, shown in the Type column of the Event Log, not as keywords. For Microsoft Windows 8.1, shown here, the Event Type for both *Audit Failure* and *Audit Success* is *Information*. The icon is the same for all

Information events. However, the event contains *Audit Success* or *Audit Failure* as keywords, and the event IDs are different as shown in the Event IDs table in *Desktop Validator Event IDs for the Windows Event Log* on page 10

2. Select the *Axway* log in the tree on the left.
3. The Desktop Validator events are listed in the results pane on the right.
4. Double-click an event, or right click an event and select *Event Properties* to view the event details.
5. The event log details contain useful information about the operation Desktop Validator performed. Using a typical event as an example, we can determine that Desktop Validator performed a Certificate Revocation Status check on behalf of the Microsoft Excel application, that the status of the certificate was good, and, if you scroll down, that Desktop Validator used its cache as the source of revocation status.

Desktop Validator Event IDs for the Windows Event Log

Previously, only one event ID was used to log all Desktop Validator messages into the Windows event log. The event ID was equal to 1 for all messages that included configuration change notifications, certificate validation results and errors. Desktop Validator 4.10 introduced different event IDs for certificate validation results. This feature allows system administrators to filter out the event log entries based on the validation status to be monitored.

Event ID 1 reports generic informational, warning, or error messages. Event IDs 10 – 17 report certificate status. The following table lists event IDs that are assigned to different types of messages.

Event ID	Event Type	Comment
1	Information, Warning, Error	System configuration changes and other notifications from Desktop Validator. All messages that do not involve certificate validation fall into this category.
10	Audit Success	Successful validation of the certificate with status **Valid**.
11	Audit Success	Validation is inhibited for the specified certificate.
12	Audit Success	Desktop Validator was unable to successfully validate the certificate in question. Returning **Good** status (per configuration option)

Event ID	Event Type	Comment
13	Audit Failure	Successful validation of the certificate with status **Revoked**.
14	Audit Failure	Desktop Validator was unable to successfully validate the certificate in question. Returning **Revoked** status (per configuration option)
15	Error	Successful validation attempt of the certificate with status **Unknown**.
16	Error	Desktop Validator encountered connectivity problems trying to validate the certificate.
17	Error	Certificate path validation failed for the specified certificates.

To manage the Desktop Validator Event Log

1. Right-click **Tumbleweed** in the console/tree display, and select **Properties**. The *General* tab appears.
2. Specify log parameters for the maximum size of the log and how often to overwrite events in the log.
3. To clear the log, click **Clear Log**.
4. To show only events of a particular type or events from a specific time period, select the **Action > Filter Current Log** menu and define filter parameters to display only events of particular types or from a specific period of time.

For example, to see only events where the certificate status was Revoked select **Audit Failur**e in the Keywords list and click **OK**. To remove the filter and display all events, open **Filter Current Log** again and click **Clear** and **OK**.

Uninstalling Desktop Validator

Close any CAPI compliant applications that are DV-enabled, such as Microsoft Outlook, Internet Explorer, Outlook Express and IIS, while uninstalling Desktop Validator or you might be prompted to so during the uninstall.

1. Click **Start**, click **Control Panel**, double-click **Add/Remove Programs** or **Uninstall a program**, depending on your version of Windows.
2. In the **Change or Remove Programs** section, select Desktop Validator from the list of Currently Installed Programs.

3. Click **Change/Remove**.

   A dialog box prompts you to confirm that you want to remove the program and all its components.

4. Click **Yes**.

   The InstallShield Wizard launches, showing the **Modify**, **repair**, or **remove** window.

5. Select **Remove**.
6. Click **Next**.

   A small dialog box opens to confirm removal of this program and all of its components.

7. Click **OK**.
8. When the uninstall completes, click **Yes**.

Installing Desktop Validator on multiple systems 3

This chapter provides instructions about how to do an automated installation (silent installation) and configuration of Desktop Validator to deploy the Desktop Validator across multiple systems simultaneously.

Silent installation overview

Silent installation is used to distribute, install and configure Desktop Validator across multiple systems simultaneously to make sure digital certificate validation through Desktop Validator is enabled, and to make sure enterprise-wide certificate validation policies are simultaneously enforced.

A silent installation can be done several ways: using Command-Line, GPO, SMS, SCCM or an Auto-Run enabled CD-ROM.

Creating a silent installation package

A standard process for using a pre-configured instance of Desktop Validator to create a silent installation package follows:

1. Install and properly configure Desktop Validator on a single system.
2. Export "silent" installation package based on that configuration.
3. Distribute and install the silent installation package.

Using installation package to update configuration

To update the configuration of previously installed instances of Desktop Validator on multiple target systems, an administrator must:

1. Properly configure Desktop Validator on a single system as described in *Configuring Desktop Validator* on page 27.
2. Export the configuration options in a format suitable for the distribution mechanism to be used for the update.

Two commonly used mechanisms for centrally managing software distribution and update on the Microsoft platform are Group Policy (GPO), Systems Management Server (SMS), and System Center Configuration Manager (SCCM). Other mechanisms such as Computer Associates' UniCenter are also compatible with Desktop Validator.

Refer to the appropriate vendor documentation for more information on how to use these products.

3. Distribute and install the configuration updates.
4. If you are distributing updated configuration with the Silent Installer package, be sure to run the `upgrade.bat` file *not* the `install.bat` file if Desktop Validator has already been installed on the machines.

Installing Desktop Validator using Group Policy

Microsoft best practices call for Windows administrators to manage application installation, updates, and removal centrally with Group Policy.

Administrators use Group Policy to define specific configurations for groups of users and computers by creating Group Policy settings. Group Policy settings are linked to an Active Directory container (such as a site, domain, or organizational unit). The Group Policy settings are applied to the users and computers in that Active Directory container, allowing administrators to configure the users' environment once and rely on the system to enforce the policies as defined.

Group Policy software installation requires a Windows Installer package (.msi) for the application that is to be installed. The package is often supplied with the software. If a program does not have a Windows Installer package, the Administrator must generate one. This package along with the program files and components must be placed in a shared network directory, called a software distribution point. The Windows Installer will read from this distribution point in order to install the application on the target system.

Group Policy allows the software to be either assigned to users or computers (mandatory software distribution) or published to users (allowing users to optionally install software through Add/Remove Programs in the Control Panel). When an application is assigned to the computer, the application is advertised and the installation is performed when it is safe to do so. Typically, this happens when the computer starts up, so that there are no competing processes on the computer. This requires a "silent" install process that does not require user input. In fact, a silent install is recommended even if the software is assigned to users to install to make sure the software will be installed and configured exactly the way the Administrator intended it.

A silent installation process can be accomplished through software application specific mechanisms or through the use of Group Policy Administrative Templates. Administrative Templates are the primary means of configuring a client computer's registry settings through Group Policy. Administrative Template `.adm` files are not the actual settings that are deployed to client operating systems. The `.adm` file is simply a template file (implemented as text file with an `.adm` extension) that provides the friendly name for the setting and an explanation. This template file is used to populate the user interface. In addition to providing configuration information for silent installation, Administrative Templates can also be used to push out configuration changes to all systems once software has been installed.

For more information, see the Microsoft Windows Server 2003 Techcenter, *"Best Practices for Group Policy Software Installation."*

Microsoft Systems Management Server 2003

The Desktop Validator installation package you created can be distributed to client systems using SMS. Since SMS distribution is considerably more complex and the installation procedures will be very site specific, the exact steps will not be provided in this manual. However, the user is referred to "Chapter 5 Distributing Software" of the Microsoft Systems Management Server 2003 manual available as part of the SMS distribution package or on the Microsoft Web site. For more information, see the *Microsoft Systems Management Server 2003 Operations Guide*, Chapter 7, "Creating Software Installation Packages with SMS Installer."

SMS software distribution options

SMS provides the following options to distribute software.

- **Rich distribution** - Software distribution can be directed to computers based on collected information including network and hardware configuration, group membership, and software installation status.
- **Dynamic distribution** - If an SMS client computer is added to a group, software is automatically sent to the client according to predefined administrative settings for that group. Likewise, new computers matching predefined destination attributes (such as Internet Protocol (IP) subnet or installed video card) automatically receive specified packages or driver updates.
- **Courier Sender** - Courier Sender allows software to be sent between SMS sites by CD or other media rather than across the network. This is particularly useful in situations where the available network bandwidth is low or too expensive to use for the delivery of large packages.
- **Download and run** - Administrators can have clients download packages directly from an SMS 2003 distribution point. An option can be set to download the entire program to the client computer and then run the program.
- **Add or Remove Programs integration** - An SMS software package can be advertised and configured in the Add or Remove Programs in Control Panel.

Additionally SMS supports Elevated Rights installations, allowing applications requiring administrative access during installation to be partially installed with administrative privileges and still have user-specific options installed with a user account. SMS also enables distribution of one package with multiple installation parameters, so that the package can be conditionally installed to different collections according to defined criteria. For example, the same package can be distributed to different collections using a different scheduled installation setting for each collection.

For more information, see the *Microsoft Systems Management Server 2003 Operations Guide*, Chapter 5, "Distributing Software."

SMS software update options

- SMS provides the following options for updating software.
- **Distribute Software Updates Wizard** - Uses inventory information to analyze the applicable software update status for client computers, provides a method of reviewing and authorizing suggested software updates, downloads authorized software updates and installation information, builds packages and advertisements tailored to specifications for each software update or set of updates, and distributes software update advertisements to client computers by using SMS software distribution.
- **Software Updates Installation Agent** - Evaluates advertised software updates against missing or previously installed updates on an SMS client computer and installs the applicable updates.
- **Persistent Notification for Software Updates** - An icon appears in the notification area (formerly called the system tray) whenever a user is logged on and there are pending, but uninstalled, software updates. When the computer is in compliance the notification area icon does not appear.

  The notification area icon can be used to check for upcoming installations, schedule installations and reboots to occur at convenient times of the day, and install software updates immediately.
- **Unattended software update installation** - Provides a method to deploy mandatory updates to client computers silently. No notification icon appears in the notification area.

  Scheduled installations - Provides a way to restrict installation of software updates to certain hours on certain days.

For more information about software update management with SMS 2003, see the *Microsoft Systems Management Server 2003 Operations Guide*, Chapter 6, "Managing Software Updates."

Microsoft System Center Configuration Manager 2007

The Microsoft System Center Configuration Manager (SCCM) 2007 provides a comprehensive solution for change and configuration management for the Microsoft platform. With SCCM, an administrator can upgrade and configure each computer from a central location or from multiple locations. The administrator can schedule individual software files or software programs for distribution to specific computers, and can initiate unattended software installations to selected computers.

Software installation packages can come ready-to-install from Windows Installer or can be created with the SCCM Installer (which is available by download from Microsoft and is not included with the standard SCCM 2007 product distribution). SCCM can generate software packages for distribution from any Windows Installer file. Windows Installer configuration files contain all the information

needed to generate an SCCM software package which can support SCCM features self-repair and appropriately timed installation. For more information, see http://www.microsoft.com/systemcenter/configurationmanager/en/us/default.aspx.

Check the product online help or the Microsoft web site for information about software distribution and update options.

Using Desktop Validator silent installation package

Group policy can control a target object's registry, NTFS security, audit and security policy, software installation, logon/logoff scripts, folder redirection, and Internet Explorer settings. The policy settings are stored in Group Policy Objects (GPOs). A GPO is internally referenced by a Globally Unique Identifier (GUID). Each one can be linked to multiple sites, domains or organizational units. In this way, potentially thousands of machines or users can be updated using a simple change to a single GPO. This reduces the administrative burden and costs associated with managing these resources.

An installation package refers to the program files and configuration files needed to install a software application on a system. The installation process is managed by the Windows Installer. Windows Installer is an operating system service that performs all installation-related tasks: copying files onto the hard disk, making registry modifications, creating shortcuts on the desktop, and displaying dialog boxes to query user installation preferences when necessary. A silent installation package refers to an installation package that is pre-configured, requiring no user input during the installation process, and hence is suitable for automated distribution and installation throughout an enterprise.

You can create a silent Desktop Validator Installation package by using the Import/Export tab of the Desktop Validator Configuration application as previously discussed in *Configuring Desktop Validator* on page 27.

The installation package will be created in the Desktop Validator program directory. If you installed Desktop Validator in the default location, your installation package will be created in:

```
C:\Program Files\Tumbleweed\Desktop Validator\dvpackage
```

The installation package consists of the Desktop Validator program files, current Desktop Validator instance configuration information, the necessary Installer configuration `.msi` file, the Group Policy/Administrative Template files required for Group Policy distribution, and an Autorun.inf file required for distribution using an Auto-Run enabled CD-ROM

Note If the package is to be distributed via a network-based mechanism such as Group Policy, SMS, or SCCM, you must create the Desktop Validator installation package in a shared network folder (distribution point) with appropriate permissions to allow access from all target system to the Desktop Validator distribution package.

Auto-run enabled CD-ROM

The most basic way to distribute Desktop Validator is using an Auto-Run enabled CD-ROM. This is accomplished by burning a CD-ROM with the silent installation package created on the source system. The CD-ROM can be used to automatically install and configure Desktop Validator on a target system.

Before using the CD-ROM on the target system:

- Ensure that you have administrative privileges on the machine on which you are installing Desktop Validator.
- If you are upgrading, it is not necessary that you uninstall any previous Desktop Validator version before performing the upgrade.
- Close all CAPI compliant applications that can be Desktop Validator-enabled (or you will be prompted to close them during the install process).

Installation

To automatically install the pre-configured version of the Desktop Validator, insert the CD-ROM containing the Desktop Validator installation package you created into the CD-ROM drive.

Since the CD-ROM is Auto-Run enabled, the Desktop Validator installer will be automatically started. The package on the CD-ROM contains all necessary configuration information so the installation will complete without requiring any user input. Once the installation completes, the target system will have an instance of the Desktop Validator software that is installed and configured exactly the same as the instance on the source system.

Group Policy

To automatically install and configure Desktop Validator using Group Policy, you must perform the following steps:

1. Start the Active Directory Users and Computers snap-in.

   To do this, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, right-click your domain, and then click **Properties**.
3. Click the **Group Policy** tab, and then click New.
4. Type the name for this policy (for example, *Tumbleweed Desktop Validator* distribution), and then press **ENTER**.
5. Click **Properties**, and then click the **Security** tab.

6. Clear the **Apply Group Policy** option for the security groups that you want to prevent from having this policy applied. Select the **Apply Group Policy** option for the groups to which you want to apply this policy. When you are finished, click **OK**.
7. Select the group policy object that you just created (for example, *Tumbleweed Desktop Validator* distribution), and click **Edit**.
8. Under *Computer Configuration*, expand *Software Settings*.
9. Right-click **Software installation**, point to **New**, and then click **Package**.
10. In the Open dialog box, type the full Universal Naming Convention (UNC) path to Desktop Validator Microsoft Installer `.msi` configuration file in the shared network folder distribution point that contains the Desktop Validator installation package that you created.

    For example, type `\\file server\share\dvpackage\Tumbleweed Desktop Validator.msi`.

    IMPORTANT: Do not browse to the location. Ensure that you type in the UNC path to the shared folder.
11. Click **Open**.
12. Click **Assigned**, and then click **OK**.

    The Desktop Validator installation package is listed in the right pane of the *Group Policy* window.
13. Close the *Group Policy* snap-in, click **OK**, and then quit the *Active Directory Users and Computers* snap-in.

    When the client computer starts, Desktop Validator will be automatically installed and configured.

Note To make Desktop Validator available for installation from the *Add/Remove Programs* tool in Control Panel rather than automatically installed when computer is started, you must publish the Desktop Validator package to computer users rather than assign it to the computer. This and other options such as Redeploying and Removing software are discussed in greater detail on the Microsoft Web site.

Distributing Desktop Validator configuration updates

Once Desktop Validator has been installed and configured on multiple systems, Desktop Validator configuration updates can be distributed in several ways.

Using the silent installation package

The most automated way to distribute Desktop Validator configuration updates is to generate a silent installation package using the reconfigured instance of Desktop Validator and distribute the new installation package as described in the previous section.

When the new installation package is installed, the instance of Desktop Validator on the target system will be silently reconfigured with the new settings. Additionally, the installer checks the Desktop Validator program files on the target system against the ones in the installation package. If the target system Desktop Validator program files are different, then they will be replaced with the ones in the install package, otherwise they will not be replaced. This ensures that Desktop Validator cannot be accidentally reconfigured with options that are not consistent with the program files installed on the target system.

Using a configuration file

You can create a configuration file by using the **Import/Export** tab of the Desktop Validator Configuration application as previously discussed in *Configuring Desktop Validator* on page 27. Create the configuration file in a shared network folder with appropriate permissions to allow access from all target systems.

Importing the configuration file

The configuration file can be manually imported through the **Import/Export** tab of the Desktop Validator Configuration Application or through the `dvconfig.exe` command-line utility discussed later in this chapter. The command-line utility can be invoked in a script, allowing the Desktop Validator configuration file import to be automated using various mechanisms. This approach can be used to update configuration Desktop Validator using SMS or other software distribution and configuration management systems.

Update Registry

Importing the Desktop Validator configuration from older versions through registry files is not supported. Importing the Desktop Validator configuration from older versions is only supported through text files. Since the configuration text file is not validated in any way, it is possible for a potentially corrupt configuration file to render Desktop Validator, other applications, or even Windows unoperational on the target system. Always back up the registry prior to making any changes.

Distributing the Group Policy Administrative Template

The Desktop Validator configuration file can also be distributed using a Group Policy Administrative Template. If this is the first time you are distributing Desktop Validator configuration updates this way, you must create the Group Policy and add the Administrative Template by performing the following steps:

1. Start the Active Directory Users and Computers snap-in.

   To do this, click Start, point to Programs, point to Administrative Tools, and then click Active Directory Users and Computers.
2. In the console tree, right-click your domain, and then click Properties.
3. Click the Group Policy tab, and then click New.

4. Type the name for this policy (for example, Axway Desktop Validator configuration), and then press ENTER.
5. Click Properties, and then click the Security tab.
6. Clear the Apply Group Policy option for the security groups that you want to prevent from having this policy applied. Select the Apply Group Policy option for the groups to which you want to apply this policy. When you are finished, click OK.
7. Selecting the group policy object that you just created (for example, Axway Desktop Validator configuration), click Edit.
8. Under Computer Configuration, right-click Administrative Templates, and then click Add/Remove Templates.
9. In the Add/Remove Templates dialog box, click Add.
10. Navigate to the folder containing the Desktop Validator `.adm` file that you would like to add. The Desktop Validator Administrative Template file `dv.adm` is located in the directory where you installed Desktop Validator. The default location is `C:\Program Files\Tumbleweed\Desktop Validator`. Select the `dv.adm` file, and click **Open**.
11. In the Add/Remove Templates dialog box, click **Close** to dismiss the dialog indicating the `.adm` was successfully loaded. The Desktop Validator policy template has been added successfully and you will see DESKTOP VALIDATOR displayed in the console tree.

You only need to add the Desktop Validator Administrative Template once. However, you must edit it every time you want to distribute a new configuration file.

Editing the Desktop Validator Administrative Template

1. Start the Active Directory Users and Computers snap-in.

   To do this, click Start, point to Programs, point to Administrative Tools, and then click Active Directory Users and Computers.
2. In the console tree, right-click your domain, and then click Properties.
3. Click the Group Policy tab, click the Desktop Validator group policy object created earlier (that is, Tumbleweed Desktop Validator configuration), and click Edit.
4. Expand Computer Configuration, Add/Remove Templates, DESKTOP VALIDATOR, and double click Configuration to display the properties of the Administrative Template. The settings properties dialog contains five fields: Location, ModificationId, Type, RefreshPeriod, and MaxRefreshSalt. Use the values in the following table to specify these options.

Option	Type	Value	Description
ModificationId	Text	Alphanumeric string	Unique ID identifying current configuration modification. Must be changed to trigger configuration update.

Option	Type	Value	Description
Location	Text	Path and file name of desired Desktop Validator configuration file	Specifies Desktop Validator configuration file to be imported. Configuration file was previously exported via Desktop Validator UI.
Type	Numeric	0	Specifies the format of Desktop Validator configuration file. 0 = text
RefreshPeriod	Numeric	0 - 30000000	Specifies time interval (in seconds) after which Desktop Validator configuration will be reloaded (enforced). 0 = no refresh after first upload. Refresh period must be at least 300 seconds.
MaxRefreshSalt	Numeric	0 - 86400	Maximum value for random time (in seconds) added to refresh period. 0 = no random time is added to refresh period.

Do not specify a path containing the local directory and file name. Ensure that you use the UNC path to the shared folder.

5. Enter the ModificationId in the ModificationId field when the Desktop Validator configuration was created.

   ModificationId will contain the ModificationId of the last known modification (you must modify this value manually every time the configuration changes).

6. Edit the location box and enter the UNC path containing the Desktop Validator configuration file you exported.

   The following is an example of Windows built-in distributed system with high availability:

   ```
   \\<domain>\netlogon\axway\<filename>
   ```

   IMPORTANT: Do not specify a path containing the local directory and file name. Ensure that you use the UNC path to the shared folder.

7. Specify the type of the format of the configuration file.
8. Specify the RefreshPeriod.
9. Specify the MaxRefreshSalt time.
10. Click **OK** to close the dialog box.

When the client computers start, Desktop Validator will automatically be updated with the new configuration settings.

Command-line installation and configuration

Axway Desktop Validator can be silently installed and configured using the command-line. This allows Desktop Validator installation and configuration to be automated using one of the many scripting mechanisms available in Windows. It also enables Desktop Validator software distribution and configuration to be managed using third-party or custom software management solutions, such as Microsoft Systems Management Server.

Silent command-line installation

To install Desktop Validator silently on to a user's desktop without being prompted for any values and using the default values, use the following command:

```
DesktopValidator-x64-release-Enterprise.exe /s /v"/qn"
```

The default installation directory will be *C:\Program Files\Tumbleweed\Desktop Validator*. To install Desktop Validator into a different directory use the following command:

```
DesktopValidator-x64-release-Enterprise.exe /s /v"/qn
INSTALLDIR=[InstallDirPath]"
```

Controlling short-cut configuration

The command-line parameter SHORTCUTS controls the creation of shortcuts in the Desktop Validator installer. It can accept the following values:

Value	Meaning
0	No shortcuts
1	Only Start menu shortcuts are installed
2 or any other number	Both Desktop and Start menu shortcuts are installed

Note If run as upgrade on an existing Desktop Validator installation with any of the shortcut options, the installer will update the shortcuts according to the option used.

Note The default behavior of the Desktop Validator installer remains the same as in previous Desktop Validator versions and both shortcuts are created if the option is not specified.

To install Desktop Validator with no shortcuts created:

```
DesktopValidator-x64-release-Enterprise.exe /v"shortcuts=0"
```

Command-line configuration (dvconfig.exe)

The `dvconfig.exe` utility is a command-line utility that can be used to export and import Desktop Validator configuration settings. Export Desktop Validator configuration settings to a file after Desktop Validator has been installed, configured and verified. Importing Desktop Validator configuration settings from a file will automatically reconfigure the instance of Desktop Validator in which the file is imported.

Note Files exported through the GUI can be imported through the command-line utility or vice versa.

The `dvconfig.exe` utility can be used to create a silent Desktop Validator installation package or to silently reconfigure existing instances of Desktop Validator. It can also be used to create a backup of a working Desktop Validator configuration prior to experimenting with configuration changes.

The `dvconfig.exe` utility that is part of the standard DV distribution can be found in the Desktop Validator installation directory. The utility has the following command-line format:

```
dvconfig.exe -command [READ|WRITE] -file [filename.txt] ]
```

To do an export

Use the **command READ** flag to have `dvconfig.exe` read the Desktop Validator registry contents and output them as a text format configuration file.

To do an import

Use the **command WRITE** flag to have `dvconfig.exe` write the contents of the specified file to the Windows registry. The utility will perform basic validation of the values being set prior to writing them to the Registry.

Examples of validation include removing leading or trailing white space, ensuring any URL specified is syntactically correct, and required fields are specified. If an error is detected in the file, `dvconfig.exe` will display an error message and abort the operation. This ensures the Registry is not accidentally corrupted by using a malformed file.

The command assumes that `filename.txt` includes the full path to the file. If no path is specified, the file is assumed to be in the current directory.

The following is an example of using the utility to read the Desktop Validator registry contents to the file `dvregistry.txt`:

```
dvconfig.exe -command read -file dvregistry.txt
```

The following is an example of using the utility to write the contents of the file `dvregistry.txt` to the registry:

```
dvconfig.exe -command write -file dvregistry.txt
```

Successful command execution results in the following:

```
dvconfig: Operation completed successfully
```

Silent command-line uninstall

To silently uninstall the Axway Desktop Validator, use the following command:

```
DesktopValidator-x64-release-Enterprise.exe /s /x /v"/qn"
```

Note The commands provided are for Desktop Validator Enterprise. If you are using Desktop Validator Standard, the same commands can be executed using the *`DesktopValidator-x64-release-Standard.exe`*.

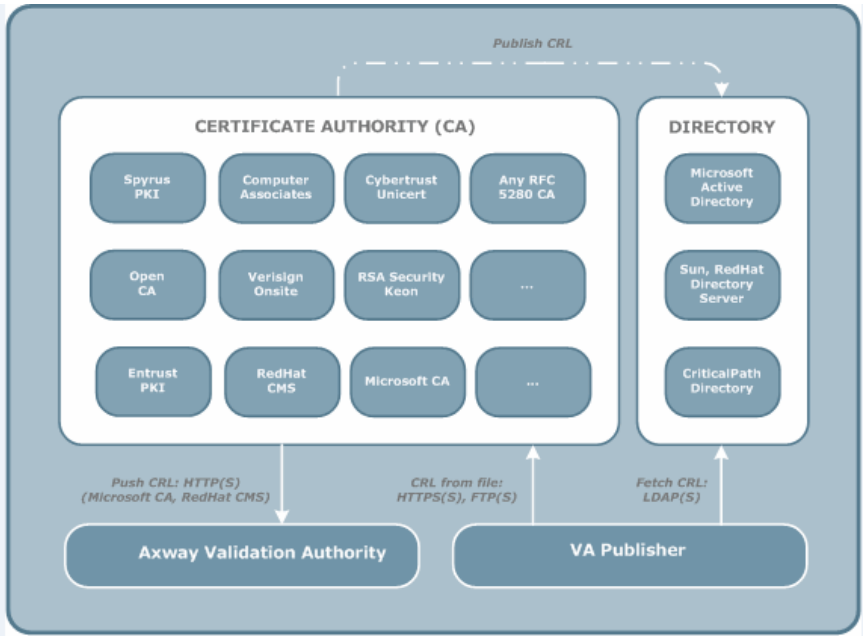
Configuring Desktop Validator 4

This chapter provides an overview of certificate validation, a list of configuration options available, and instructions on how to configure options in Desktop Validator.

Validation overview

To modify Desktop Validator settings you must be logged on as an Administrator or a member of the Administrators group. Desktop Validator users without Administrator privileges will have a read-only view of configuration options.

When configuring Desktop Validator, it is helpful to understand how Desktop Validator performs certificate validation. The following illustration describes how Desktop Validator determines which certificate validation information to use to validate the certificate.



Desktop Validator enables administrators to specify CA-specific validation options and a default validation policy that applies to all certification authorities in the user's CAPI stores.

If Desktop Validator is unable to obtain the certificate status information using the first validation option in the list of validation options, and additional validation options (failover validation options) are configured, Desktop Validator attempts to obtain the certificate status information from those failover validation options. Each validation option is attempted in order until the status information is obtained. If Desktop Validator is unable to obtain certificate status information from any of the validation options, validation fails for the certificate and an error is logged.

CA-specific options set

Desktop Validator checks to see if CA-specific configuration options are set for the issuer of the certificate being validated. If set, Desktop Validator uses this issuer-specific policy to validate the certificate using one or more of the following protocols: OCSP, SCVP, CRL, VACRL, OCSP Using AIA, CRL using DP and Compact CRLs.

Default validation options set

If CA-specific options are not configured, Desktop Validator uses the default validation policy, if configured, to check the revocation status of the certificate.

Default validation options not set

If neither CA-specific nor default validation policies are configured, Desktop Validator will return **Unknown** status. This behavior can be modified by using the Desktop Validator option **"Response status if validation info is not configured"**.

Accessing Desktop Validator configuration application

You can access the Desktop Validator *Configuration* application in any of the following ways:

- Double-click the desktop shortcut.
- Use the Start menu.
- Double-click the Axway Desktop Validator icon in the notification area (formerly called the system tray).

Viewing Desktop Validator settings

The Desktop Validator *Configuration* panel allows administrators and end-users to view current configuration settings for the application:

1. Click **About**... to view system information, including the Desktop Validator version and build number. For example, DV 4.12.33 signifies Desktop Validator version 4.12 and build number 33.

   The **About Desktop Validator** dialog box appears.
2. Click **System Info...** for detailed information on your system.

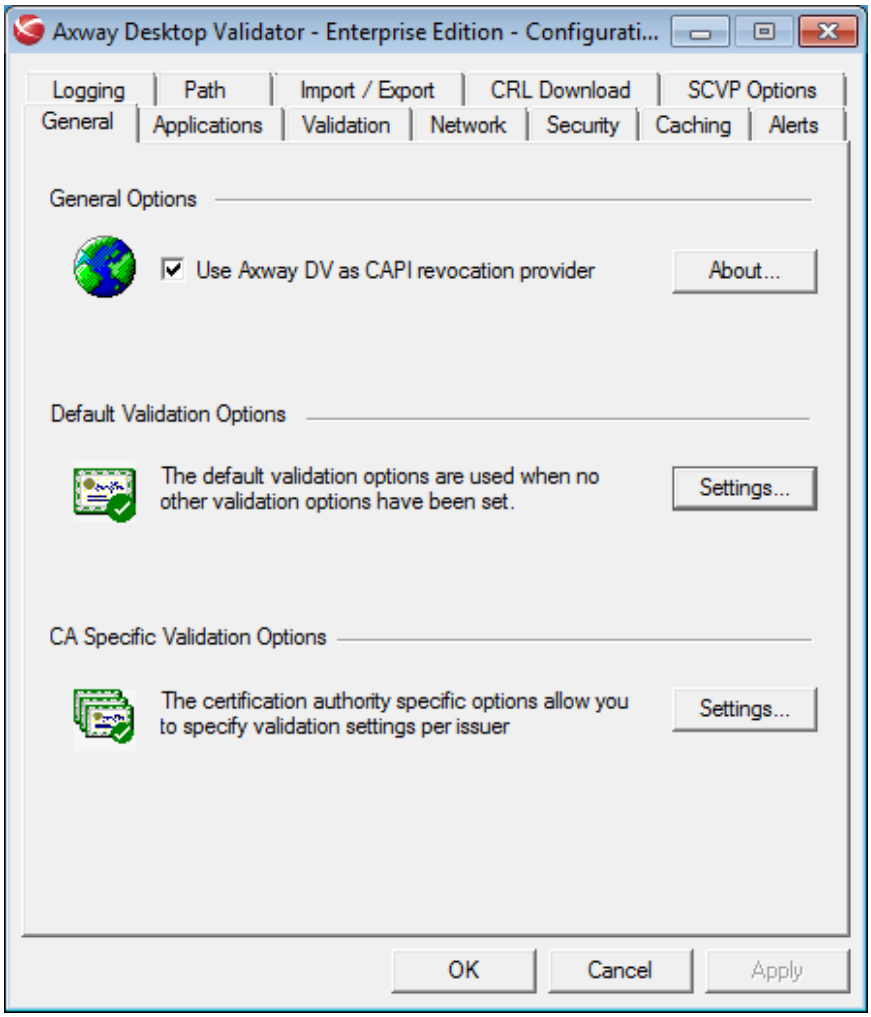
Configuration options list

These configurations options are displayed as property tabs in the property dialog box. How to use each tab is discussed in this chapter.

Tab	Description and Reference
General	Configures default and CA-specific validation options. See *Configuring General options* on page 30.
Applications	Configures applications to validate certificates using Desktop Validator. See *Configuring Application options* on page 44.
Validation	Configures protocol-specific and general validation options. See *Configuring Validation options* on page 46.
Network	Configures proxy server settings and connection time-out values. See *Configuring Network options* on page 50.
Security	Configures validation request signing. See *Configuring Security options* on page 54.
Caching	Configures revocation status caching and CRL caching policies. See *Configuring Caching options* on page 56.
Alerts	Configures notification alerts to specific Desktop Validator events. See *Configuring Alert options* on page 60.
Logging	Configures Desktop Validator logging options. See *Configuring logging options* on page 64.
Path	Configures certificate path processing options. See *Configuring certificate path processing* on page 66.
Import/Export	Allows Desktop Validator configuration options to be imported and exported for automated installation and configuration. See *Configuring Import/Export* on page 67.
CRL Download	Allows administrators to configure a download schedule for CRLs that Desktop Validator can use to validate certificates. See *CRL Download* on page 70.
SCVP Options	Configures SCVP options for validation policy. See *Configuring SCVP Options* on page 72.

Configuring General options

When you launch the Desktop Validator *Configuration* application, the **General** tab of the dialog box is displayed.



Note If you start the Desktop Validator *Configuration* application as a user, not an administrator, the controls are unavailable, so you cannot change the configuration. To run Desktop Validator as Administrator, first right click on the Desktop Validator application in the system notification area and choose **Close**. Then locate the Desktop Validator System Tray Utility in the Start menu, right click and **Run As Administrator**, then follow the OS prompts. If the Desktop Validator tray utility is run as Administrator it will not provide alert pop-ups for the user who is logged into the system, unless that user is the Administrator.

When making changes to any of the Desktop Validator Configuration options, save or cancel your changes by using one of the buttons at the bottom of the dialog box.

- Click **OK** to apply and save any changes made and close the application.
- Click **Cancel** to close the application without saving changes.
- Click **Apply** to save the changes made without closing the application so you can continue to make further changes.

General options selections

Use the **General** tab to set Axway as the CAPI revocation provider and to configure default or CA-specific validation options.

Use Axway Desktop Validator as CAPI revocation provider

You must select the **Use Axway DV as CAPI revocation provider** option to enable digital certificate validation using Desktop Validator. If you clear this option, Desktop Validator will no longer be used to validate certificate status (making all subsequent Desktop Validator configuration information irrelevant).

Default validation options and CA-specific validation options

Default validation options are used to validate all certificates, irrespective of the issuing CA. If CA-specific options are configured, Desktop Validator uses those options rather than the default when validating certificates issues by that CA. See *Configuring Validation options* on page 46.

Note If the default validation option is cleared, Desktop Validator will be unable to verify certificates in cases when CA-specific options are absent for a particular CA. By default, Desktop Validator will return Unknown status when unable to verify status. You can modify this behavior by using the Desktop Validator Option: **Response status if validation info is not configured.**

Certificate validation protocols

You can specify the same seven certificate validation protocols for both the default validation options and for CA-specific validation options. (Some of these are not protocols in the strict sense of the term.)

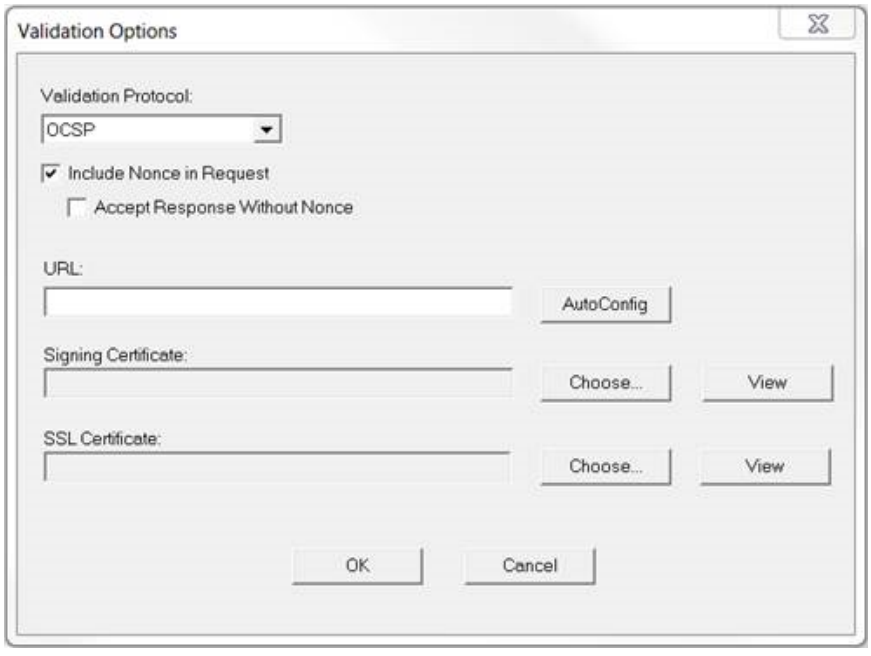
Validation Protocol	Description
OCSP Online Certificate Status Protocol	Desktop Validator must communicate with a Validation Authority Server to validate the certificate, therefore you must add at least one source.
OCSP Using AIA	When the AIA extension is present in the certificate and is enabled on Desktop Validator, Desktop Validator uses the data contained in the AIA extension to validate the certificate. No URL is required.
CRL Certificate Revocation List	Desktop Validator must obtain the CRL needed to validate the certificate, therefore you must add at least one CRL source. Use CRL as the CA-specific validation protocol to obtain a CRL from a location other than the one specified in the certificate CRL distribution point (CRLDP). This supports obtaining the CRL from an Issuing Distribution Point (IDP).You can specify that Validation Authority pre-fetch the CRL into the disk cache on a scheduled basis and that Validation Authority cache the CRL in memory. See *Configuring Caching options* on page 56 and *CRL Download* on page 70. You can use group configuration to enable validation options across more than one system simultaneously.
CRLDP Certificate Revocation List Distribution Point	Desktop Validator uses the CRL distribution point specified in the certificate to obtain the CRL needed to validate the certificate, therefore no further configuration is required.
SCVP Server-based Certificate Validation Protocol	Desktop Validator must communicate with a Validation Authority Server in order to validate the certificate, therefore you must add at least one Validation Authority Server source.
VACRL Validation Authority Certificate Revocation List	Desktop Validator must communicate with a Validation Authority Server in order to validate the certificate, therefore you must add at least one Validation Authority Server source.VACRL reduces network bandwidth usage because the Validation Authority Server generates delta CRL information customized for the requesting Desktop Validator.

Validation Protocol	Description
Compact CRL Compact Certificate Revocation List	Desktop Validator must communicate with a Validation Authority Server in order to validate the certificate, therefore you must add at least one Validation Authority Server source.Compact CRL is attractive for low bandwidth environments because it further reduces the size of the CA-issued CRLs by removing data like revocation date and reason.

Note If the validation protocol selected is CRL based, Desktop Validator will cache any CRL obtained in the local file system cache and use the cached CRL according to the specified caching policies. For more information on caching, see *Configuring Caching options* on page 56.

Validation options

Specify the options for each validation protocol using the *Validation Options* dialog box.



The following list describes the function of each **Validation Options** field. The table in *Validation Options Fields* on page 35 indicates which fields are required, optional, or unavailable for each validation protocol.

- **Validation Protocol**—Select the certificate validation protocol from this list.

- **Include Nonce in Request**—Select this to have Desktop Validator insert the nonce extension when communicating with this specific Validation Authority Server. The nonce extension is used to cryptographically bind a request to a response to ensure fresh responses and, therefore, protect against "replay attacks."
- **Accept Response Without Nonce**—Select this to have Desktop Validator accept responses without nonce. This allows Desktop Validator to take advantage of servers that do support nonce, while also being able to communicate with servers that do not.
- **URL**—Type the URL for the Validation Authority Server or CRL repository. For a Validation Authority Server, the URL protocol must be HTTP or HTTPS. For the CRL repository, the URL protocol must be HTTP, HTTPS, LDAP, LDAPS, or FILE. For both a Validation Authority Server or CRL repository, specify the port if required. If no ports then default ports are assumed based on the protocol used (80 for HTTP and 443 for HTTPS). The address in the URL can be IPv4, IPv6, hostname, or FQDN formats.

  Note An IPv6 address in a URL must be enclosed with square brackets (for example, http://[abcd::1]:80).

- **AutoConfig**—Recommended. Click this when it is available to obtain the Validation Authority OCSP response signing certificate and the SSL certificate from the Validation Authority Server. (The SSL certificate is fetched when the Validation Authority Server is configured for SSL). This action also verifies that the Validation Authority Server is running and that Desktop Validator can communicate with it. After you obtain the certificates, click **View** to verify their authenticity, for example, by checking their thumbprints. For third-party OCSP responders, click the **Choose** buttons to obtain these credentials manually.
- **Test CRL**—Click this command button to check the configuration, the availability of the server, the communications between Desktop Validator and the server, and the availability of the CRL. This does not apply to default validation options so the button does not appear in the dialog box.
- **Signing Certificate**—Click **Choose** to open the **Select Certificate File** dialog box. Locate the certificate file on a local or network file system. Validation Authority uses the signing certificate to verify the signature on validation responses from a Validation Authority Server or on CRLs that are signed using a different key from that used to generate the certificates. **AutoConfig** can populate this field. Click **View** to view the selected certificate.
- **SSL Certificate**—Click **Choose** to open the **Select Certificate File** dialog box. Locate the certificate file on a local or network file system. VA uses the SSL certificate for communication with a Validation Authority Server or CRL repository when an SSL communication protocol is specified. **AutoConfig** can populate this field. Click **View** to view the selected certificate.

Validation Options Fields

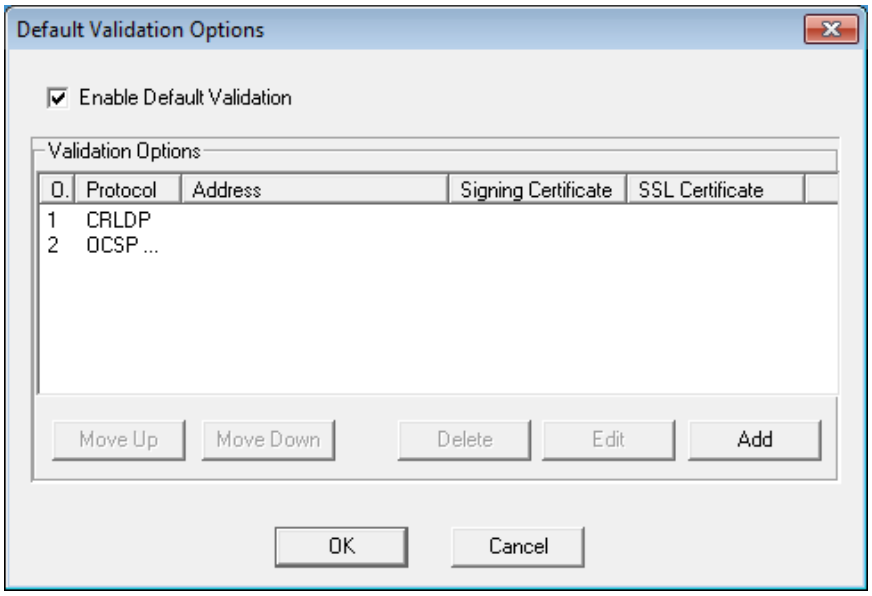
Validation Protocol	Nonce	Address	AutoConfig	Test CRL	Signing Certificate	SSL Certificate
OCSP	Available	Required: Validation Authority Server URL	Available	Not available	Required	Required for SSL
OCSP Using AIA	Available	Not available	Not available	Not available	Not applicable	Not applicable
CRL	Not available	Required: CRL repository URL	Not available	Available	Required only if the CA certificate is not used to sign the CRLs	Required only if communication between Desktop Validator and the server is over SSL
CRLDP	Not available	Not available	Not available	Not available	Not applicable	Not applicable
SCVP	Available	Required: Validation Authority Server URL	Available	Not available	Required	Required for SSL
VACRL	Not available	Required: Validation Authority Server URL	Available	Available	Required	Required for SSL
Compact CRL	Not available	Required: Validation Authority Server URL	Available	Available	Required	Required for SSL

Setting default validation options

You can set default validation options for Desktop Validator to use if CA-specific options do not apply.

You can set default validation options individually, or you can configure validation options to be applied to a group of systems using a Basic URL to set the validation protocol.

1. On the **General** tab, under *Default Validation Options*, click **Settings** to open the *Default Validation Options* dialog box.



2. Select **Enable Default Validation** to configure global validation policy.

   You can configure a list of validation sources. If revocation information cannot be obtained from one source or if the source is unavailable, then, and only then, the next source in the list is used. For example, since Desktop Validator always stores downloaded CRL data locally on disk, configuring OCSP as the first validation option and VACRL or CRLDP as an additional option ensures that Desktop Validator can validate certificates even when the network is unavailable and an OCSP cannot reach the Validation Authority Server.

   When configured to use SCVP protocol, Desktop Validator will not failover to the next validation source if the certificate chain status received is "Path-Not-Built" or "Path-Not-Valid".

   You can configure Desktop Validator to dynamically reorder the source list upon failover. For more information, see *Configuring Validation options* on page 46.

3. Use the command buttons perform the following actions:

   - **Move Up**—Move the selected validation source higher in the list.
   - **Move Down**—Move the selected validation source lower in the list.
   - **Delete**—Remove the selected validation source from the list.
   - **Edit**—Open the *Validation Options* dialog box to view or modify the selected validation source.
   - **Add**—Open the *Validation Options* dialog box to specify a new validation source.

See *Configuring Validation options* on page 46 for description of the protocols available for validation sources. See *Validation options* on page 33 for descriptions of the fields in the *Validation Options* dialog box. Complete the *Validation Options* dialog box for each certificate validation protocol required for default validation.

Group configuration for CRL validation

To quickly and efficiently configure validation options to be applied to a group of systems, Desktop Validator supports a template-type variable used in a single Basic URL to define the dynamic part of the complete CRL URL location. This option is only available for CRL protocol configuration.

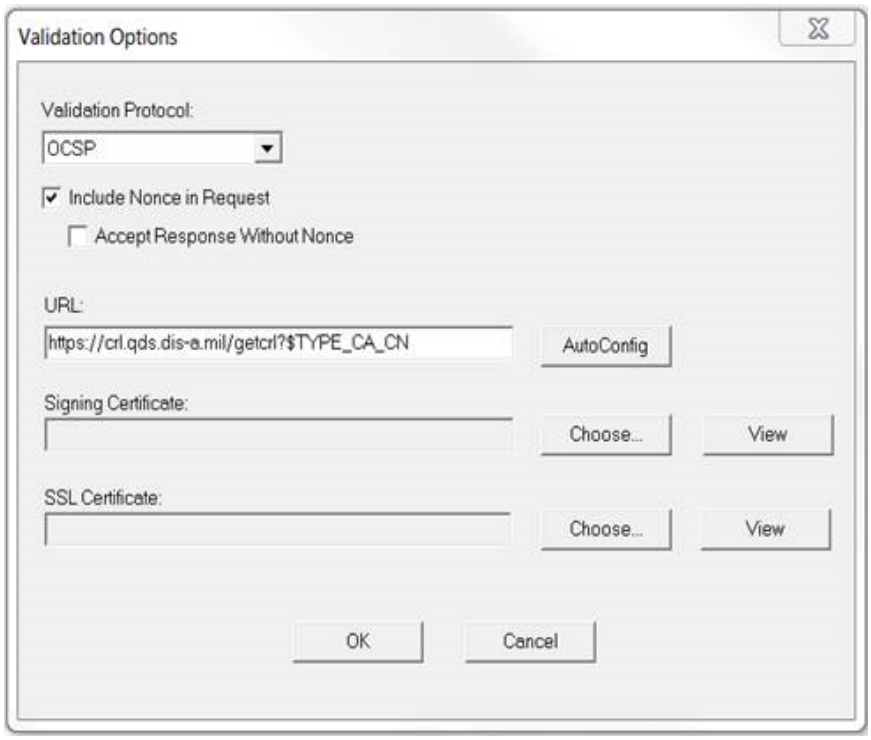
A Basic URL is an incomplete URL location that uses template-type variables to define format of the complete URL. The Basic URL includes LDAP, HTTP, or FILE protocol, hostname, port, and one provided template-type variable. As an option, the URL can include base DN or a URL identifying a common part of the CRL storage location.

Revocation status reports in event and file logs include the complete URL location of downloaded CRLs.

Desktop Validator supports three types of variables to define the dynamic part of the complete CRL URL location:

Variable	Description
`$TYPE_CA_DN$`	Represents CA subject name (DN name) in URL
`$TYPE_CA_CN$`	Represents CA common name (CN name) in URL
`$TYPE_CA_PUBKEY_HASH$`	Represents CA public key has (SHA1) in URL

If any of the previously specified variables is used in the URL, Desktop Validator will dynamically compute a complete URL at the time of validation. Only one variable can be used within a single URL. Variables cannot be combined into one URL.



LDAP, HTTP, and File URL Examples

The following examples show how to do group CRL configuration using the following variables: Subject Name (`$TYPE_CA_DN$`), Common Name (`$TYPE_CA_CN$`), and Directory (`$TYPE_CA_PUBKEY_HASH$`); and URLs: LDAP, HTTP, FILE URL.

Two examples are provided for HTTP and FILE URL. Each example has 3 components and is based on using a CA certificate with the following Subject (DN) name:

```
cn=DoD CLASS 3 Root CA,ou=PKI,ou=DoD,o=U.S. Government,c=US
```

LDAP URL: Subject Name variable

CA represents the subject name (DN name) in the URL (`$TYPE_CA_DN$`).

Complete URL Schema

```
<ldap_host_port>+<encoded_ca_subject_
name>+?certificaterevationlist;binary
```

Basic URL

```
ldap://ds-3.cpki.chamb.disa.mil/$TYPE_CA_
DN$?certificaterevocationlist;binary
```

Computed URL

```
ldap://ds-3.c3pki.chamb.disa.mil/cn%3dDoD%20CLASS%203%
20Root%20CA%2cou%3dPKI%2cou%3dDoD%2co%3dU.S.%20Government%
2cc%3dUS?certificaterevocationlist;binary
```

HTTP URL: Subject Name variable

CA represents the subject name (DN name) in the URL (`$TYPE_CA_DN$`).

Complete URL Schema

```
<http_host_port>+<cgi_command>+<encoded_ca_subject_name>
```

Basic URL

```
https://crl.chamb.disa.mil/downloadmanager?REQ_ACTION=DOWNLOAD_
CRL&FORM_PARAM_DN=$TYPE_CA_DN$
```

Computed URL

```
https://crl.chamb.disa.mil/downloadmanager?REQ_ACTION=DOWNLOAD_
CRL&FORM_PARAM_DN=cn%DDoD+CLASS+3+Root+CA%2Cou%3DPKI%2c+ou%DDoD%
2C+o%3DU.S.+Government%2C+c%3DUS
```

HTTP URL: Common Name variable

CA represents the subject name (DN name) in the URL (`$TYPE_CA_DN$`).

Complete URL Schema

```
<http_host_port>+<cgi_command>+<encoded_ca_common_name>
```

Basic URL

```
https://crl.gds.disa.mil/getcrl?$TYPE_CA_CN$
```

Computed URL

```
https://crl.gds.disa.mil/getcrl?DoD+CLASS+3+Root+CA
```

Directory variable

CA represents CA public key hash (SHA1) in the URL (`$TYPE_CA_PUBKEY_HASH$`).

Complete URL Schema

```
<file_basic_url>+<ca_public_key_hash_dirname>+latest.crl
```

Basic URL

```
file://c:\archive\crls\$TYPE_CA_PUBKEY_HASH$\latest.crl
```

Computed URL

```
file://c:\archive\crls\1OF193F340AC91D6DE5F1EDC006247C4F25D9671\
latest.crl
```

Filename variable

CA represents CA public key hash (SHA1) in the URL (`$TYPE_CA_PUBKEY_HASH$`).

Complete URL Schema

```
<file_basic_url>+<ca_public_key_hash_filename>+.crl
```

Basic URL

```
file://c:\archive\crls\$TYPE_CA_PUBKEY_HASH$.crl
```

Computed URL

```
file://c:\archive\crls\1OF193F340AC91D6DE5F1EDC006247C4F25D9671.crl
```

If you are using Desktop Validator in a direct trust model, continue to the next paragraph. If you are using Desktop Validator in a Validation Authority-delegated trust model, skip to Validation Authority-Delegated Trust Model.

Using Desktop Validator in different trust models

You can use Desktop Validator in any one of the three trust models described in this section.

Direct Trust Model

In the Direct Trust Model, Desktop Validator directly trusts the signing certificate of one or more Validation Authority(s) it is configured to communicate with. The downside of the direct trust model is that if the Validation Authority key were to be changed on account of compromise or renewal, all configured Desktop Validator clients must be updated.

Select the **AutoConfig** button to automatically obtain the Validation Authority OCSP response certificate and the SSL certificate (if the VA Server is configured for SSL).

In addition to fetching (obtaining) the necessary certificates, this option tests the communication between Desktop Validator and Validation Authority. When possible, obtain the certificates using auto configuration.

Note **AutoConfig** works only with the Axway Validation Authority Server. If not using the Axway Validation Authority Server, use the **Choose** buttons to manually select the OCSP signing and SSL certificates.

CA-Delegated Trust Model

In the CA-delegated Trust Model, the Validation Authority(s) get their response signing credentials issued by the CA that issued the certificate that has to be validated. The benefit of this model is that since clients already trust the issuer of the certificate to be validated, they do not have to directly trust the Validation Authority's signing credentials. As such, if the Validation Authority signing credentials were to be replaced, there is no impact on client configuration (which only includes the CA certificate).

When operating in the CA-delegated trust model, Validation Authority Servers typically get their response signing credentials issued for a short period of time to avoid the necessity of checking for the Validation Authority's revocation status.

VA-Delegated Trust Model

The Validation Authority-delegated Trust Model combines the best of the Direct and CA-delegated Trust Models while avoiding the pitfalls of both. In this model, the Validation Authority gets its response-signing credentials from a *Root VA* that typically remains offline. This *Root VA* only issues response-signing credentials to one or more *Tier-1 VAs* that communicate with the Desktop Validator clients for revocation status. Desktop Validator clients only need to trust the Root Validation Authority. Changes in the signing credentials of the *Tier-1 VAs* has no impact on the client configuration.

Desktop Validator clients also have the capability to query the *Root VA* to directly obtain the revocation status of the *Tier-1 VAs*, which mitigates the necessity for these servers to have short-lived certificates.

1. Use the **Choose** buttons to select the Signing Certificate (certificate of the issuer of the Signing Certificate used to validate the digitally signed OCSP responses from the Validation Authority Server) and the SSL Certificate (if Desktop Validator will communicate with the Validation Authority Server using SSL (https)).

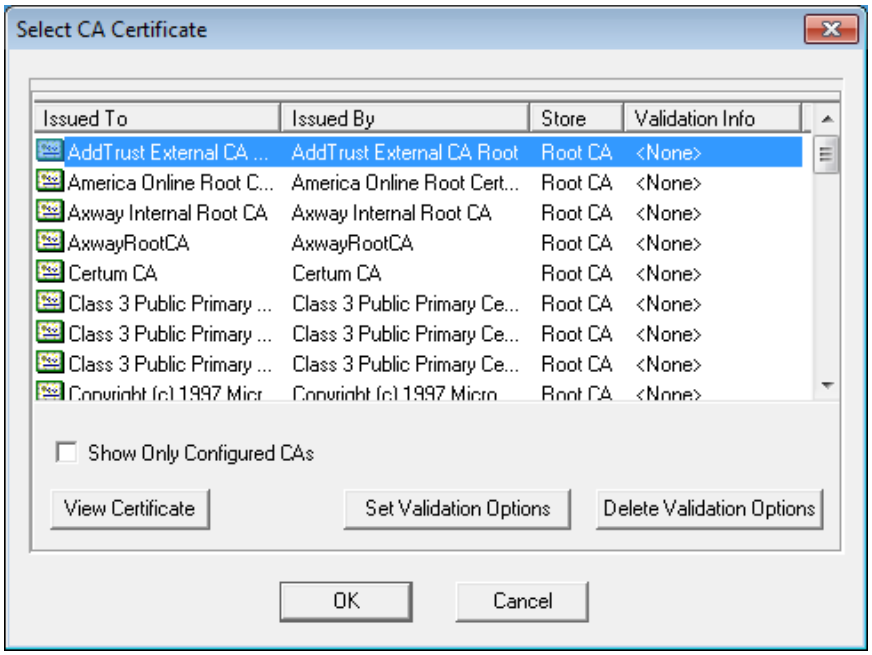
   The **Choose** button allows you to select the Signing or SSL Certificate file from the local file system or any network file Desktop Validator is able to access.
2. Click **View** to view the Signing or SSL certificates.
3. When you have specified all the necessary information in the *Validation Options* dialog box, click **OK** to add the URL to the validation source list.
4. Click **OK** to save the changes made in the *Default Validation Options* window and to exit the screen.

Setting CA-specific validation options

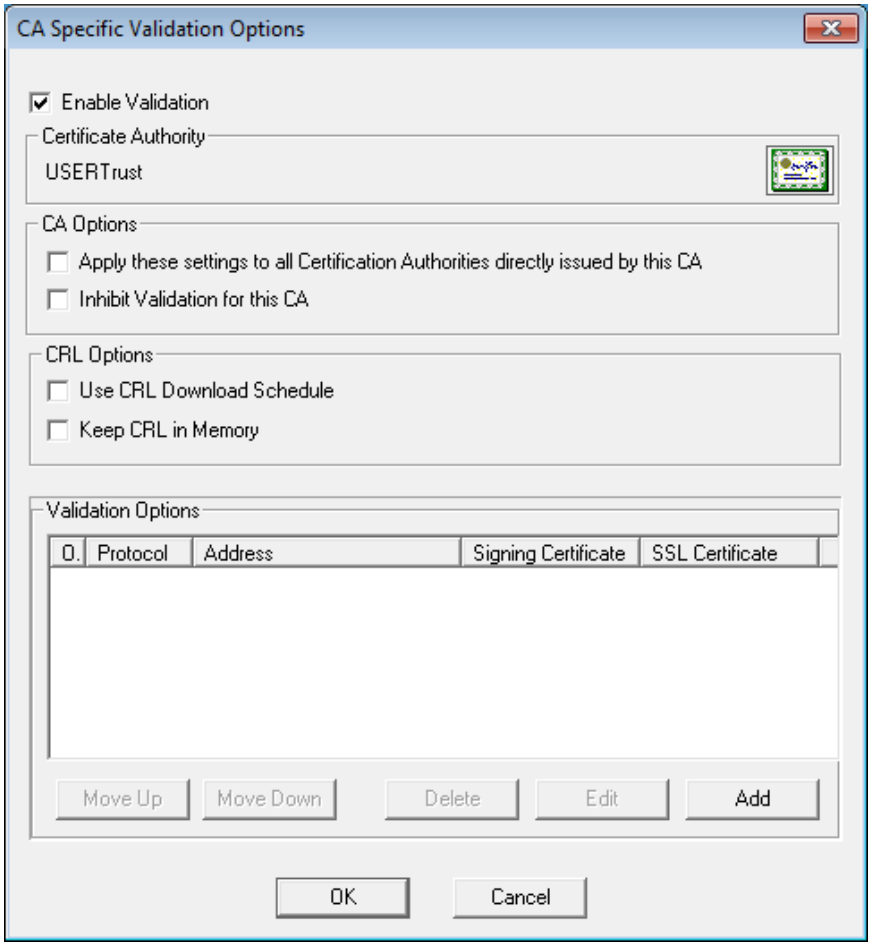
Use CA-specific validation to assign validation options for obtaining revocation data for specific CAs. If no validation options are configured for a particular CA, Desktop Validator uses the default validation options.

1. On the **General** tab, under *CA Specific Validation Options*, click **Settings** to open the *Select CA Certificate* dialog box.

   The *Select CA Certificate* dialog box is displayed, showing the CAs for which there are certificates in your system certificate store.



2. (Optional) To sort the certificates in the dialog box by CA (Issued To), Issuing CA (Issued by), Certificate Store, or Validation Info, click the appropriate title in the heading bar.
3. (Optional) To display only those CAs that are currently configured with custom options, select **Show Only Configured CAs**.
4. (Optional) To display more information about a selected certificate, click **View Certificate**.
5. To configure CA-specific validation options, select one or more certificates and click **Set Validation Options** to open the *CA Specific Validation Options* dialog box.



For a single CA, the *Select CA Certificate* dialog box displays in the Certificate Authority box the identification of the CA and a certificate icon you can click to view the certificate information. For multiple CAs, this box indicates "<Multiple Section>."

CRL validation is also available for all directly issued CAs using Root (Issuer) based CA specific validation options.

New Issuer Based CA-specific options are also supported by the Basic URL.

To set CA-specific validation options in the CA Specific Validation Options dialog box

1. To configure custom validation for the selected CAs, select **Enable Validation**. (Otherwise, Desktop Validator uses the default validation options for the CAs).
2. (Optional) To also set validation options for all certification authorities directly issued by the selected CAs, select **Apply these settings to all Certification Authorities directly issued by this CA**.

3. (Optional) To completely disable validation checking for the selected CAs, select the **Inhibit Validation** for this CA. In which case, Desktop Validator does not perform any certificate validation for the selected CAs. Desktop Validator will just return (and log) "valid" status for all certificates issued under this CA.

   Select the **Inhibit Validation for this CA** option *only* if there are CAs that are not security critical in your environment.

4. To configure Desktop Validator to download the CRL on a routine scheduled basis, select **Use CRL Download Schedule**.

   If more than one source is provided for the CRL, the schedule download will only obtain the CRL from the first available source on the list. For more information, on setting up scheduled CRL downloads, see *CRL Download* on page 70.

5. To configure Desktop Validator to cache the CRL in memory, select **Keep CRL in Memory**. This option is only available in Desktop Validator Enterprise.

   When dealing with large CRLs (greater than 10 MB), make sure that your system has sufficient memory to accommodate loading the CRL in memory, or use Compact CRL.

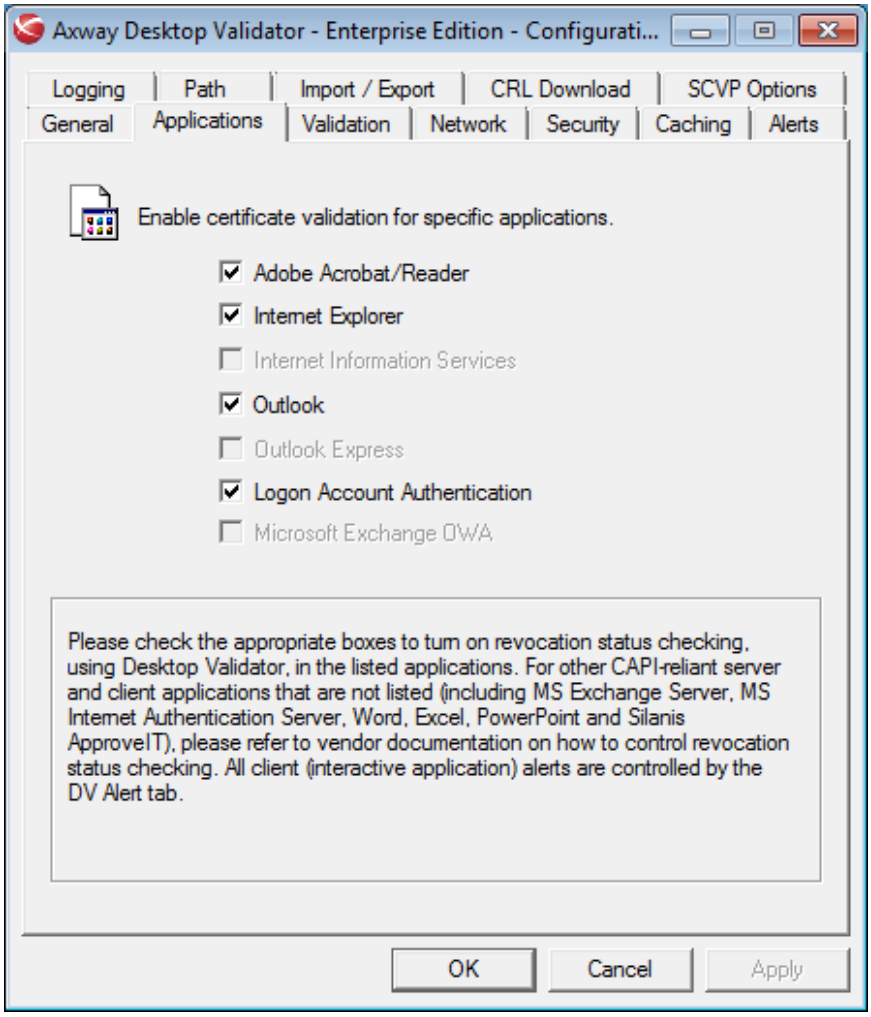
6. To configure validation options for the selected CAs, use the *Validation Options* group box.

   Setting CA-specific validation options is similar to setting default validation options. See *Configuring Validation options* on page 46. Complete the *Validation Options* dialog box for each certificate validation protocol required for the CA-specific validation.

Configuring Application options

Desktop Validator enables transparent digital certificate validation for all Microsoft CAPI-enabled applications. However, some applications require additional configuration. Desktop Validator provides support for automating the additional configuration required for seamless integration. To configure applications that will use Desktop Validator to validate certificates, use the **Applications** tab.

Click the **Applications** tab on the Desktop Validator *Configuration* application.



The applications available in the dialog box are based on your specific Desktop Validator product model, as shown in the following table.

Application	Desktop Validator Standard	Desktop Validator Enterprise	Comments
Adobe Acrobat	Yes	Yes	Versions 8, 9, 10, and 11 are CAPI compliant and will use Desktop Validator for certificate validation.
Internet Explorer	Yes	Yes	

Application	Desktop Validator Standard	Desktop Validator Enterprise	Comments
Internet Information Systems (IIS)	No	Yes	Option disabled if IIS is not installed on the system.
Logon Account Authentication	No	Yes	Enables validation for domain controller authentication
Outlook	Yes	Yes	
Outlook Express	Yes	Yes	
Microsoft Exchange OWA	NO	Yes	N/A

If one of these applications is not listed on your system, refer to your software license for authorized product use.

Select the appropriate options to enable the applications.

For other CAPI-compliant server and client applications that are not listed such as MS Internet Authentication Server, Word, Excel, PowerPoint and Silanis ApproveIT, refer to vendor documentation on how to control revocation status checking.

Configuring Validation options

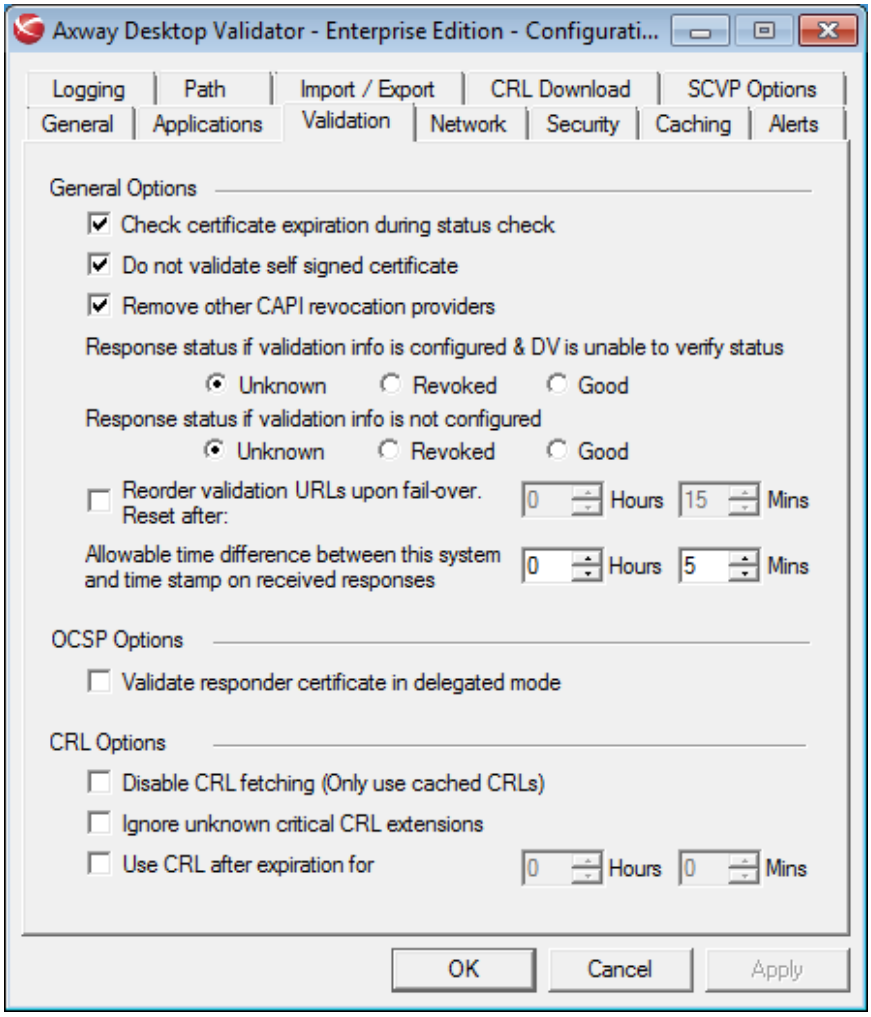
The **Validation** tab further refines the rules Desktop Validator uses for validating certificates. Three selections are available from this tab: General Options, OCSP Options, and CRL Options.

Desktop Validator will always try the first validation option first and failover to the additional options only if none of the validation sources previously tried are available.

Click the **Validation** tab on the Desktop Validator *Configuration* application.

Configuring General Options

From the **Validation** tab, select the appropriate options from one of the following general CA-specific certificate validation options.



Option	Description
Check certificate expiration during status check	Instructs Desktop Validator to verify that certificates are not expired. If Desktop Validator is asked to validate an expired certificate, it will return a status of Unknown (Default) or as Configured (Revoked or Good). This ensures that calling applications do not accept expired certificates.
Do not validate Self Signed Certificate	Instructs Desktop Validator to bypass revocation checking on a self-signed (root) certificate.

Option	Description
Remove other CAPI revocation providers	Instructs Desktop Validator to remove all registered CryptoAPI revocation providers other than Axway, so that Desktop Validator is the only source of revocation information. It is highly recommended that this option be enabled, otherwise should return that a specific certificate could not be validated as Good or Revoked based on the configured policies, CAPI can call another revocation provider. This can introduce a security issue or potential application lock-up while attempting to obtain revocation status from multiple providers. Desktop Validator saves a list of all CryptoAPI revocation providers on the system and restores all providers when this option is cleared.
Response status if validation info is configured & DV is unable to verify status	Instructs Desktop Validator to return a status of Unknown (Default) or as configured (Revoked or Good) for those certificates it fails to validate.
Response status if validation info is not configured	Instructs Desktop Validator to return Unknown (Default) or as configured (Revoked or Good) for those certificates it is unable to validate. If Good is selected, users are able to logon to the local system when a network outage prevents validating the user's certificate by querying a VA Server or obtaining the CRL from the distribution point in their certificate.
Reorder validation URLs upon fail-over. Reset after:	Instructs Desktop Validator to dynamically reorder the list of revocation data sources in used with each validation URL whenever failover occurs. Resets back to the original order after a specified number of hours and/or minutes. Applies to validation sources only. Use the Event Log to check for changes to the validation source ordering.
Allowable time difference between this system and time stamp on received responses	Extends the validity period (in hours or minutes) of a CA or VA response by a small fixed amount of time to accommodate for potential system clock mismatch between local system time and the time on the VA or CA system. Default is 0 hours, 5 minutes and it is recommended to keep this value small to avoid introducing invalid responses. Use of Network Time Protocol (NTP) is recommended to ensure the time on all systems in your PKI is synchronized. Times are automatically adjusted to GMT which might otherwise result in Desktop Validator receiving a response that is not within its stated validity period.

Configuring OCSP Options

From the **Validation** tab, select the appropriate option to configure CA-Specific certificate validation OCSP options.

Option	Description
Validate responder certificate in delegated mode	Instructs Desktop Validator to validate the VA Responder OCSP signing certificate. This option only applies when operating in the IdenTrust model for certificate validation.

Configuring the cert ID hash algorithm

The default cert ID hash algorithm instructs Desktop Validator which hash algorithm to use when generating the issuing information for the certificate for which the status is being requested. The algorithm does not affect the signature algorithm of the response, that is determined by the issuing CA. This setting affects backward compatibility with versions of Validation Authority Responder prior to 4.12.1. Previous versions only supported SHA1.

The default cert ID hash algorithm is SHA1. To configure Desktop Validator to use a different cert ID hash algorithm, edit the registry:

`HKEY_LOCAL_MACHINE/SOFTWARE/Tumbleweed/Desktop Validator/Validation`

- `CertIdHash`

CertIdHash can be set to:

SHA224 (0x00000001)

SHA256 (0x00000002)

SHA384 (0x00000003)

SHA512 (0x00000004)

CertIdHash defaults to 0 (0x00000000) in the key to indicate that SHA1 will be used as the cert ID hash algorithm. If this entry is not present in the registry, a value of SHA1 will be assumed by default.

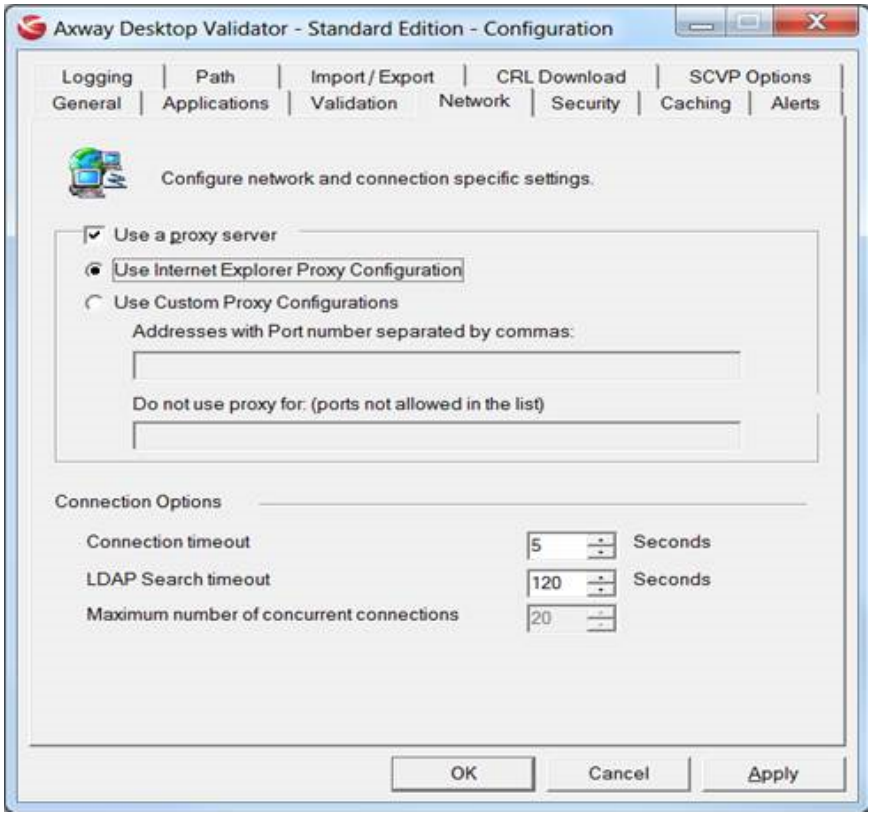
CRL Options Selections

From the **Validation** tab, select the appropriate options to configure CRL options for CA-specific certificate validation.

Option	Description
Disable CRL fetching (Only use cached CRLs)	Instructs Desktop Validator to use locally cached CRLs and not connect via the network to obtain any CRLs. Desktop Validator will only use a cached CRL while it is valid. If a specific certificate validation requires consulting a cached CRL which has expired or a CRL not present in cache, the operation will fail because Desktop Validator will be unable to check certificate status. It is recommended that this option only be used on a limited, temporary basis to disconnect the system from the network for a specific period of time. Enabling this option will also disable any scheduled CRL downloads (pre-fetching).
Ignore unknown CRL critical extensions	Instructs Desktop Validator to ignore unknown extensions, such as private extensions, when processing a CRL even if the extension is marked critical.
Use CRL after expiration for	Instructs Desktop Validator on the number of hours and/or minutes it is acceptable to use an expired CRL. Enabling this option does not impact CRL download or caching. Unless CRL fetching has been disabled, Desktop Validator will still attempt to obtain a CRL if it is not in cache or is no longer valid based on caching policy, or if a scheduled download has been configured. However, if this option is enabled, should Desktop Validator be unable to obtain an unexpired CRL, it will use the expired CRL as long as the expiration date is within the period of time specified.

Configuring Network options

The **Network** tab allows you to configure network and connection specific settings. Click the **Network** tab on the Desktop Validator *Configuration* application.



Network Settings

Select **Use a proxy server** to configure Desktop Validator to use a proxy server when communicating with a revocation data source using of any of the Desktop Validator supported protocol. If selecting this option, select from one of the following proxy configurations.

Option	Description
Use a proxy server	Configures Desktop Validator to use a proxy server when communicating with a revocation data source using any of the Desktop Validator supported protocol.
Use Internet Explorer Proxy Configuration	Instructs Desktop Validator to use the IE proxy configuration. This includes support for reading proxy configuration from a proxy.pac file. See *Configuring Internet Explorer Proxy Settings* on page 52 for more information on configuring IE proxy settings.
Use Custom Proxy Configurations	Provides the proxy configuration information that Desktop Validator will use.

If you select **Use Custom Proxy Configuration**, configure the option.

Field	Description
Addresses with port number separated by commas	Enter a proxy address followed by the port number (for example, 192.168.5.50:3128). The address can be IPv4, IPv6, or a hostname. You can also include the keyword DIRECT to indicate a direct connection. **Note** IPv6 addresses on the proxy list must be enclosed in square brackets (for example, [adcd::1]:3128).
Do no use proxy for (ports not allowed in the list)	Specify the server(s) for which a proxy should not be used in this field. Fields can accept computer names (localmachine), canonical hostnames (localmachine.Axway.com), IPv4 addresses (192.168.5.50) or IPv6 addresses (2620:ac:82:8208:75:7181::13a3). Use wildcards to match domain and hostnames or IPv4 addresses and CIDR notation to match IPv6 addresses. For example: localmachine.*.com;192.*.*.*,*.*.*.50;2620:ac::/32. Multiple entries can be separated with a semicolons, ";" commas, "," or a blank space.

Configuring Internet Explorer Proxy Settings

This section describes how to configure proxy settings for IE. Start Internet Explorer then go to **Tools > Internet Options** and select the **Connections** tab. Click the **LAN Settings** button. Proxy information can either be automatically configured or manually entered.

Using Automatic Configuration

If your environment uses automatic proxy configuration, check the **Use Automatic Configuration Script** box.

1. Enter the location of the proxy automatic configuration file in the **Address** field.
2. Check the **Automatically Detect Settings** box to have the settings be applied and have any future changes to the configuration be automatically detected.

Using Manual Configuration

If your environment does not use automatic proxy configuration, then you must enter it manually, so check the **Use a proxy server** box.

1. Enter the URL for the proxy server in the **Address** field and the port number in the **Port** field. The address of the proxy server can be entered as IPv4, IPv6, or a hostname. You can also include the keyword DIRECT to indicate a direct connection.

   The default port for the proxy is 8080.

2. Click **Advanced** to further configure the proxy settings.
3. You can specify proxy servers on a per protocol basis. You can also use the **Exceptions** field to indicate IP addresses for which going through a proxy server is not required. To enter multiple IP addresses, separate then with semicolons. The exceptions IP addresses can be entered as IPv4, IPv6, or a hostname.

   Desktop Validator does not use the **Bypass proxy server for local addresses** fields.
4. Click **OK** to apply the changes or **Cancel** to close the window without applying your changes.

Automatic proxy configuration files are written in Java script and have a `.pac` or `.js` extension. Below is a typical example of a configuration file which allows a client such as internet Explorer or Desktop Validator to connect to local hosts directly but connect via proxy to all others.

```
function FindProxyForURL(url, host)
{
if (isPlainHostName(host))
return "DIRECT";
else
return "PROXY proxy:80";
}
```

Automatic proxy configuration files can be quite complex depending on the environment. More information on automatic proxy configuration is available in the *Microsoft Internet Explorer 6 Administration Kit Service Pack 1: Deployment Guide*.

Connection Settings

Use the following options listed under Connection Options to set connection options for network protocols.

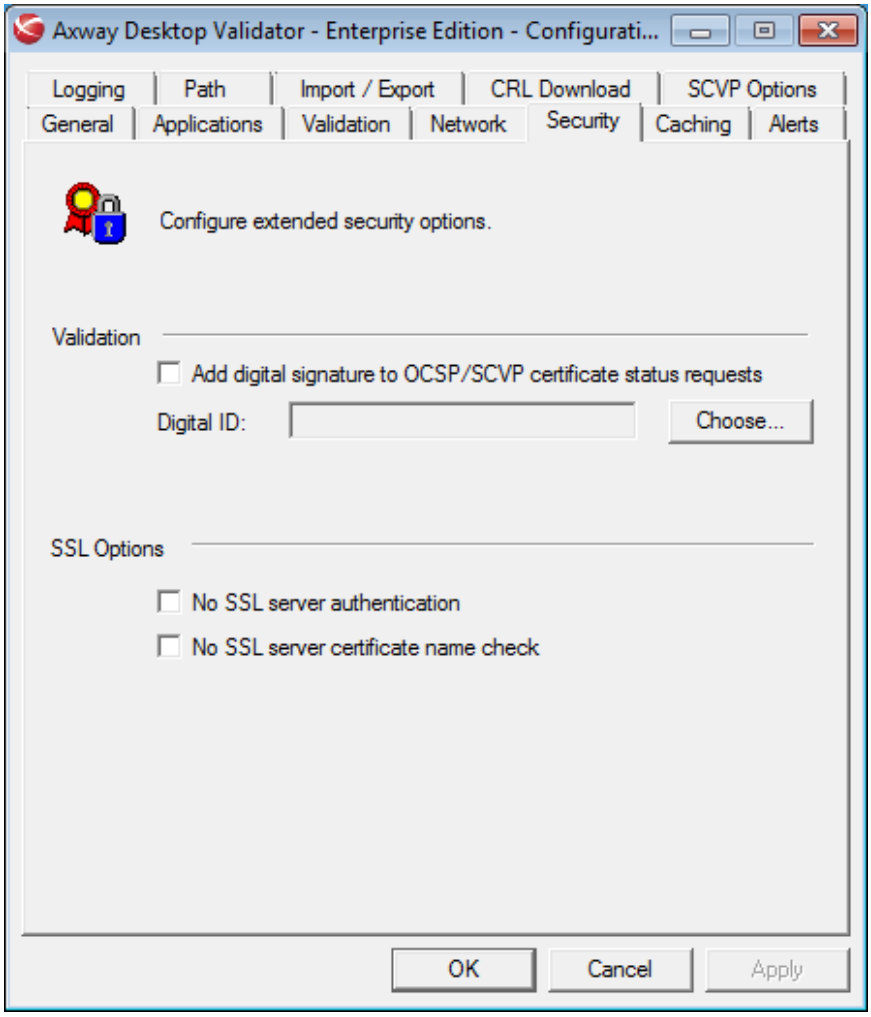
Option	Description
Connection time-out	Overrides the default operating system network connection time-out. Use the arrow keys to increase or decrease the **Seconds** values. Desktop Validator allows this amount of time to establish a connection before timing out. Default is 22 seconds for Windows, 4 minutes for Solaris. If the **Connection time out** value is set to zero, the default operating system network connection time-out is used. This value only applies to an unreachable remote host and not to a downed host. Desktop Validator immediately detects a downed remote host and returns to the client.

Option	Description
LDAP Search time-out	Specifies the amount of time Desktop Validator should wait to get results back from an LDAP Directory Search operation.
Maximum number of concurrent connections	Indicates the number of concurrent network connections (sockets) that Desktop Validator can keep open when communicating with a revocation information source. The default value is 20, which should be sufficient for most applications. This value can only be set if using Desktop Validator Enterprise and is greyed out on Desktop Validator Standard. If using Desktop Validator Enterprise with MS applications, you might need to increase the number of maximum concurrent connections based on the performance requirements of your environment.

Configuring Security options

The Validation Authority you are using to validate CA-Specific certificates might require Desktop Validator to sign all validation requests. If so, you must configure request signing using the validations selections from the **Security** tab found on the Axway Desktop Validator dialog box.

Click the **Security** tab to display the following dialog box. Two options are provided; Validation and SSL Options.



Validation Option

Select **Add digital signature to online certificate status requests** to instruct Desktop Validator to sign outgoing validation requests.

Ensure that the selected digital ID is accessible for all Log On users of Desktop Validator. For some applications, for example, IIS or Domain Controller, a Log On user can be the local system account or any other account.

Click **Choose** to locate the signing certificate that Desktop Validator attaches to signed requests. Desktop Validator must also have access to the private key corresponding to this certificate.

Choosing a certificate requires the user to provide a password to unlock the private key during use. If Desktop Validator is configured for a server (Axway Desktop Validator Enterprise), use "Low security (Crypto API)" mode to prevent prompting for the password. For example, you would use low security if using Desktop Validator in an Identrus configuration.

SSL Options

Select the appropriate SSL options.

Option	Description
No SSL server authentication	Instructs Desktop Validator to not authenticate revocation data source SSL certificates when sending validation requests or downloading CRLs.
No SSL server certificate name check	Instructs Desktop Validator to not match the certificate name with the site name Desktop Validator is attempting to connect to for validation responses. These SSL options are only relevant for Desktop Validator communicating with revocation sources over SSL and does not prevent Desktop Validator from validating SSL certificates encountered by Desktop Validator enabled applications.

Changing a Certificate

To change the certificate used for signing requests, go to the Security tab of Axway Desktop Validator Options dialog box and choose another certificate.

Configuring Caching options

Desktop Validator can cache the certificate revocation status responses returned to applications irrespective of the validation URL used to generate the response. This is very important because in order to validate a certificate, a client application must validate all the certificates encountered in the certificate chain back to the root in order to perform numerous certificate validation operations invoking Desktop Validator.

For example, to read an email message signed with a user certificate issued in a simple two-level PKI hierarchy (root and intermediate CAs), MS Outlook invokes Desktop Validator three times for each certificate as it constructs the chain, for a total of nine validation operations. Using caching in such instances improves the utilization of system and network resources and provides a better end-user experience.

If revocation status response checking is enabled, Desktop Validator will cache responses based on the amount of time you specify (relative to when the response was produced) and based on the amount of memory you specify is available for caching.

Desktop Validator will not cache responses where the Validation Authority Server returned the status of the certificate as Unknown. Desktop Validator will continue to make attempts to determine the status of the certificate. When configured to use SCVP protocol, Desktop Validator will cache "Path-Not-Built" and "Path-Not-Valid" certificate chain status.

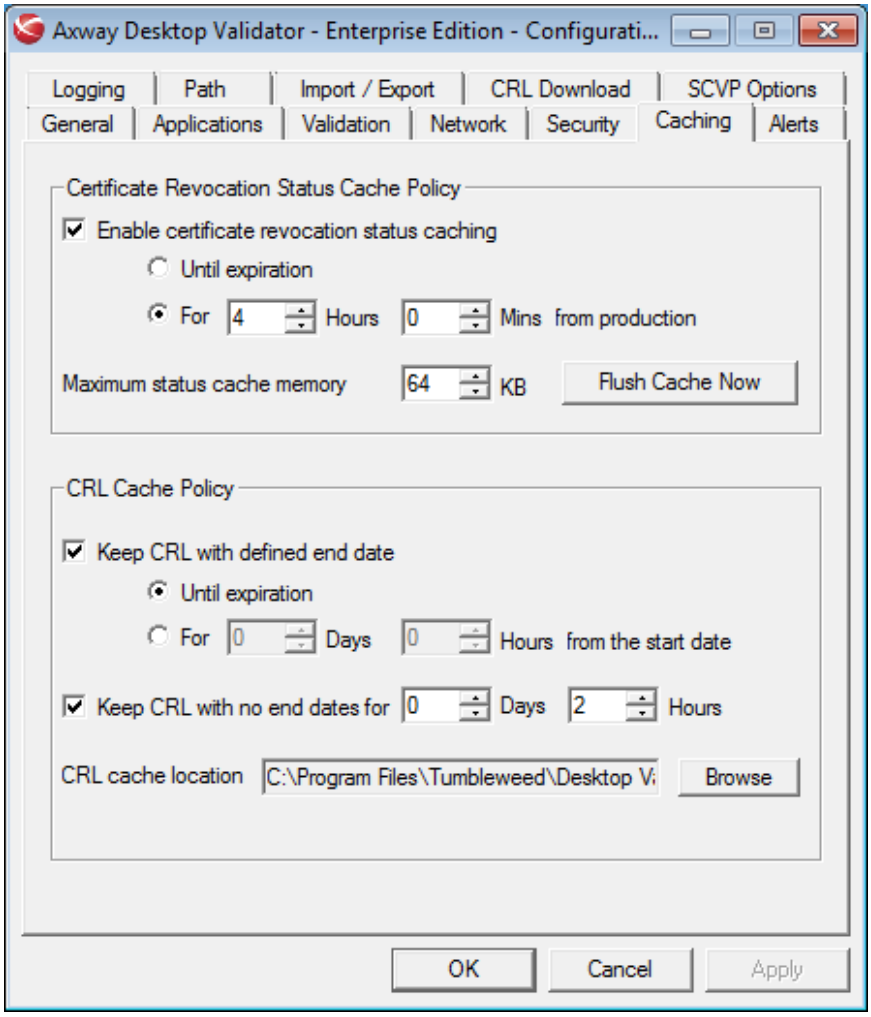
When utilizing a CRL based validation URL, Desktop Validator will automatically cache any CRL fetched to disk. By default, all CRLs are cached until they expire. However, you can configure Desktop Validator to apply different caching policies.

Additionally, if you are using Desktop Validator Enterprise, when configuring CA-specific validation URLs, you can specify whether the CRL obtained for a specific CA should be cached in memory as well as on disk. Desktop Validator will use the same CRL caching policies for memory and disk caching.

The in-memory caches maintained by Desktop Validator will be cleared and re-loaded whenever the Desktop Validator service is restarted or reconfigured. Desktop Validator maintains caches that are shared across all applications on the system and will not be cleared or reloaded when applications are stopped or restarted.

Setting caching options

The **Caching** tab on the Desktop Validator *Configuration* application displays two main policy selections: Certificate Revocation Status Cache Policy, and CRL Cache Policy.



Setting certificate revocation status cache policy

Select **Enable certificate revocation status caching** to enable caching. It is on by default. Specify how long the responses should be kept in cache and/or select to flush cache.

Option	Description
Until Expiration	Instructs Desktop Validator to keep the responses in cache until they expire based on the value of the NextUpdate value in the OCSP/SCVP response or the CRL used to generate the response. If NextUpdate item is not present in the validation response, Desktop Validator will not cache the status.

Option	Description
For __ Hours __ Minutes from Production	Instructs Desktop Validator to keep responses in cache for no longer than the specified amount of time based on when the response was produced (by Responder if using OCSP/SCVP-based validation URL or by Desktop Validator if using the CRL-based validation URL). The default is 4 hours, but you can use the arrow keys to increase or decrease the Hours and Minutes values. This time represents the maximum time Desktop Validator will cache a response. It is possible for responses to be cached for less time depending on memory availability.
Maximum Status Cache Memory	Default value is 64 KB, which is sufficient for storing approximately 2,000 validation responses. Applies only to the response cache. For Desktop Validator Enterprise, the actual amount of memory used by Desktop Validator for caching might be greater if CA-specific validation options have been configured to cache CRLs in memory. Use the arrow keys to increase or decrease the number which represents the amount of memory (KB) Desktop Validator allocates to the cache.

Setting CRL cache policy

Select one or both of the caching policies desired. The NextUpdate value of the CRL indicates the date which the next CRL will be issued and the current CRL will expire. However, it is possible for the next CRL to be issued before the indicated date (but not after).

Option	Description
Keep CRL with defined end date	Enable the options to be available to specify the date or length of time the caching policy is enforced. Setting this option allows for a CRL to be cached for a period of time less than the expiration but does not allow a CRL to be cached past its expiration.
Until expiration	Instructs Desktop Validator to cache the CRL until it expires (default). Desktop Validator will not attempt to obtain a newer CRL until the cached CRL expires or unless the CRL is scheduled for download.
For ___ Days ___ Hours from start date	Instructs Desktop Validator to cache the CRL for a specific period of time based on when the CRL was obtained. Use the arrow keys to increase or decrease the Hours and Minutes values.

If you set a validation policy that allows a CRL to be used for a specified period of time after its expiration, Desktop Validator will still try to get a newer CRL before using the expired CRL. An expired CRL will be used only if a newer CRL cannot be obtained.

Option	Description
Keep CRL with no end dates for _ days _hours	Use to cache CRLs that do not have a specified expiration date. If this option is cleared, the CRL will not be cached. Use the arrow keys to increase or decrease the Days and Hours values.
CRL Cache Location	Desktop Validator will use to store CRLs being cached. A CRL can be "manually" cached by placing it in this directory; a CRL can also be forced out of cache by removing it from this directory.

Delete this text and replace it with your own content.

Configuring Alert options

Desktop Validator can display information about certificate validation events in pop-up alerts near the notification area (formerly called the system tray). When Desktop Validator displays an alert, you can see the result of a validation event immediately without viewing the Windows Event Log or the Desktop Validator log file.

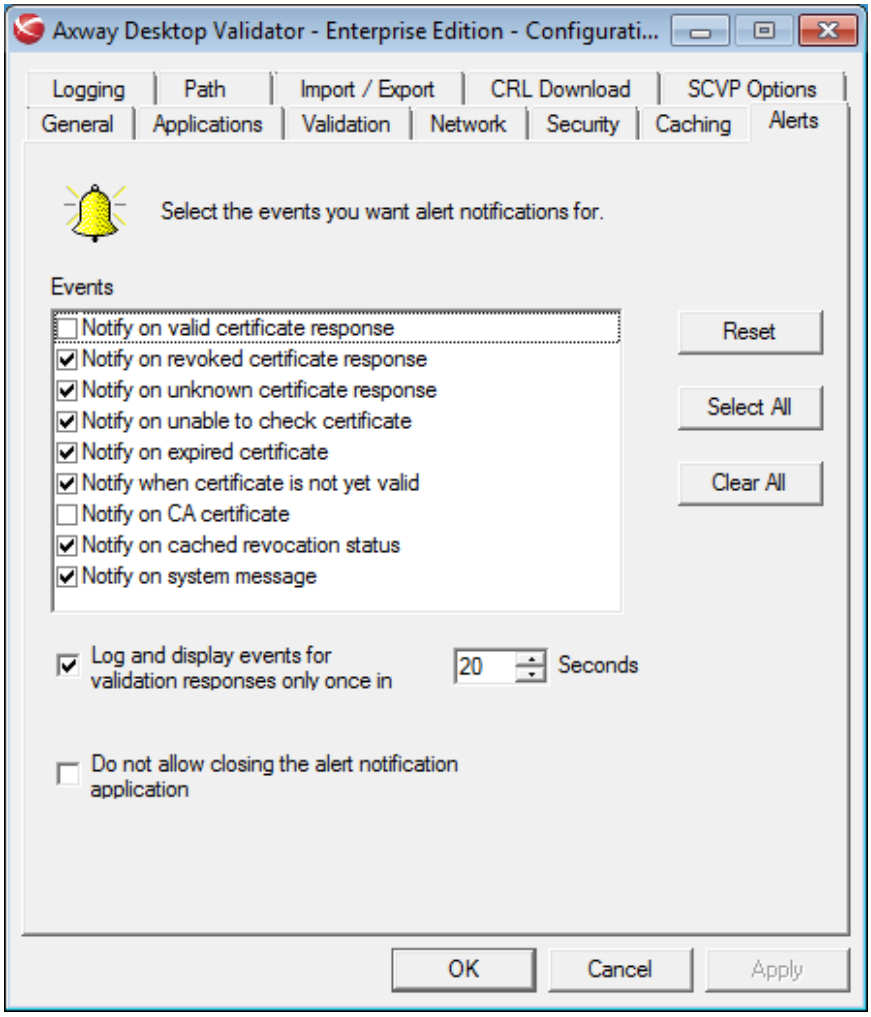
Use the **Alerts** tab to configure notification of certificate validation events.

While it is displayed, you can click an alert to see more detail about the alert in the *Desktop Validator Event Description* dialog box. To configure URLs to display instead of the dialog box, see *Configuring logging options* on page 64.

Setting events for alert notification

On the **Alerts** tab, you can choose one or more of eight notifications to receive. You can also suppress duplicate notifications by setting the minimum time between notifications of the same revocation status response.

Click on the **Alerts** tab on the Desktop Validator *Configuration* application, and the **Alerts** options dialog box is displayed.



Select from the following event notification options.

Option	Description
Notify on valid certificate response	Desktop Validator provides notification if the status of the certificate being validated is Good. This event is not enabled by default.
Notify on revoked certificate response	Desktop Validator provides notification if the status of the certificate being validated is Revoked. This event is enabled by default.

Option	Description
Notify on unknown certificate response	Desktop Validator provides notification if the status of the certificate being validated is Unknown. This event is enabled by default. A certificate status of Unknown means Desktop Validator was able to perform the validation operation and successfully communicated with a Validation Authority Server which returned the Unknown status. You might never see Unknown alerts if Desktop Validator has been configured to map Unknown to either Valid or Revoked using *Validation Options*. This alert is displayed if Desktop Validator is configured to check for expired certificates.
Notify on unable to check certificate	Desktop Validator provides notification if it is unable to validate the certificate. This event is enabled by default. This alert usually implies an error state. For example, Desktop Validator configuration might need to be modified or there is a system error such as the network being down.
Notify on expired certificate	Desktop Validator provides notification if the certificate being validated has expired. This event is enabled by default.
Notify when certificate is not yet valid	Desktop Validator provides notification if the certificate being validated is not yet valid. This event is enabled by default. This alert can result from the time on the local system not being properly set. Make sure the system time is correctly set.
Notify on CA certificate	Desktop Validator provides notification if the certificate being validated is a CA certificate. This event is not enabled by default.
Notify on cached revocation status	Desktop Validator provides notification even if the revocation response returned was from cache. This event is enabled by default.
Notify on system message	Desktop Validator provides notification if there is a system message. This event is not enabled by default.

Setting time limit to log and display alerts

Select the **Log and display alerts for validation responses only once in __ Seconds** to instruct Desktop Validator to only log and alert once in the specified number of seconds when returning the same revocation status response.

Since many applications implement a recursive approach to chain verification, Desktop Validator might be invoked to validate the same certificate numerous times in a very short time period which can flood the event log and generate many pop-ups.

Type a value or use the arrow keys to increase or decrease the number of seconds. The default period is 20 seconds.

Disable closing the tray utility

To prevent users from accidentally closing the Desktop Validator tray utility, enable the **Do not allow closing of the alert notification application option**. The close option in the context menu will be grayed out.

Reset, select all and clear all

To re-enable default settings, click the **Reset** button. To be notified of all events, click the Select All button. Click the Clear All button if you prefer not to be notified of any events.

Customizing the certificate status detail message

While an alert is displayed, you can click it to see detail about the certificate being validated and the validation transaction. By default, this information is shown in a dialog box.

The system administrator can customize this display by replacing the dialog box with a web page. There can be a different web page for each validation result, **Valid**, **Revoked,** and **Unknown**.

To configure the web pages, edit the registry and create the following values in the key shown:

`HKEY_LOCAL_MACHINE\Software\Axway\Desktop Validator\Alerts`

- `urlRevokedCert`
- `urlValidCert`
- `urlUnknownCert`

Each values is the full URL that is sent to the default web browser. For example, the value of `urlValidCert` might be `http://wsrvr.myco.com/DV/validCert.html`.

Delete this text and replace it with your own content.

Configuring logging options

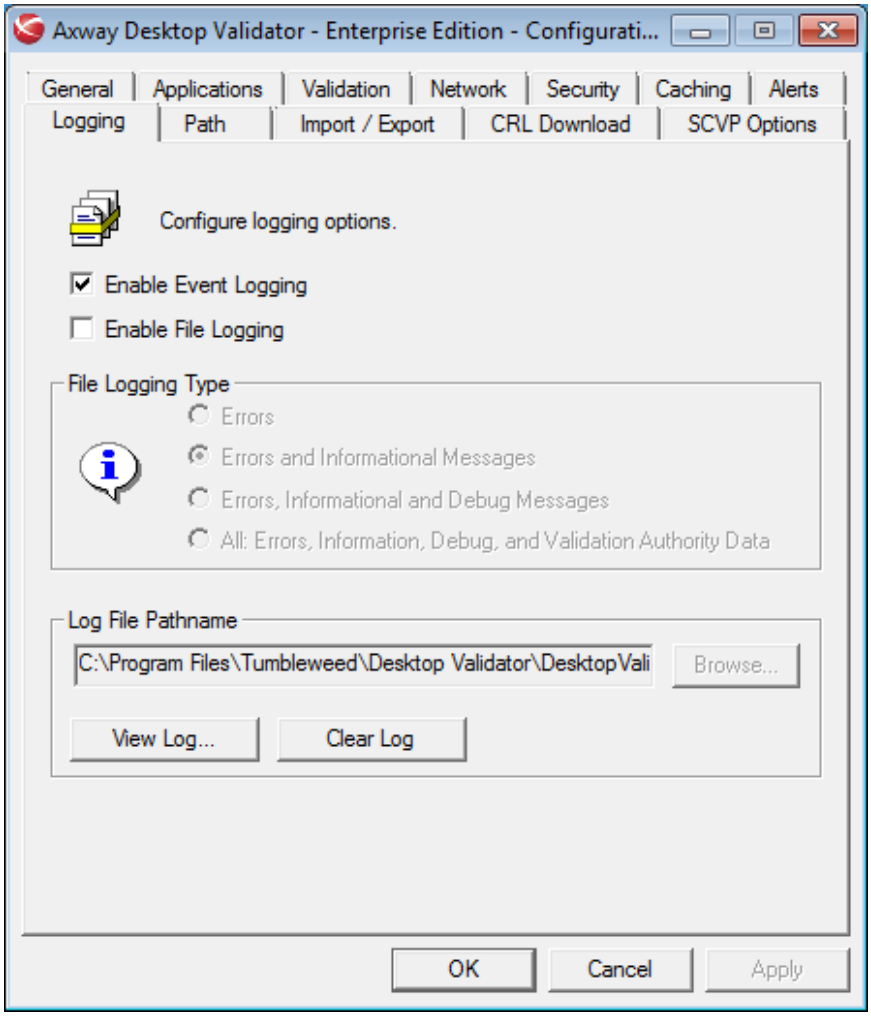
Desktop Validator provides two options to configure logging: Microsoft Windows Event logging or system file logging. The native Microsoft Windows Event Log option is the default installation configuration.

Configuring Desktop Validator to log to a file in addition to or instead of the Microsoft Windows Event Log, enables Desktop Validator to provide more detailed information useful for troubleshooting.

Note To avoid disk space issues, use File Logging for troubleshooting purposes only.

Note Desktop Validator does not support Windows Server 2008 R2 event log forwarding. Configuring Windows Server 2008 R2 event log forwarding may cause server to hang on reboot.

Click on the **Logging** tab on the Desktop Validator *Configuration* application and the Logging Options dialog box appears. Use this tab to also view and clear logs.



Setting MS Windows Event logging

Select **Enable Event Logging** to log events to the Windows Event log. This option is on by default.

Note It may be necessary to setup a local service with full control to access and log internet settings events.

Setting system file logging

The file logging option enables Desktop Validator to provide detailed system information written to a file. Select **Enable File Logging** to write system and error logs to a file.

Select from one of the following file logging types to specify the type of information for Desktop Validator to log.

Logging Option	Description
Errors	Writes errors to the file.
Errors and Informational Messages	Writes errors and informational messages to the file.
Errors, Informational and Debug Messages	Writes error, informational, and debug messages to the file.
All: Errors, Information, Debug and Validation Authority Data	Writes all possible logging and system information to the file.

Use the **Log File Pathname** field to specify the location that Desktop Validator writes the log information to. Specify the full path name or click Browse to select the log file location.

Viewing log file

To display the log file, click the **View** button.

Clearing log file

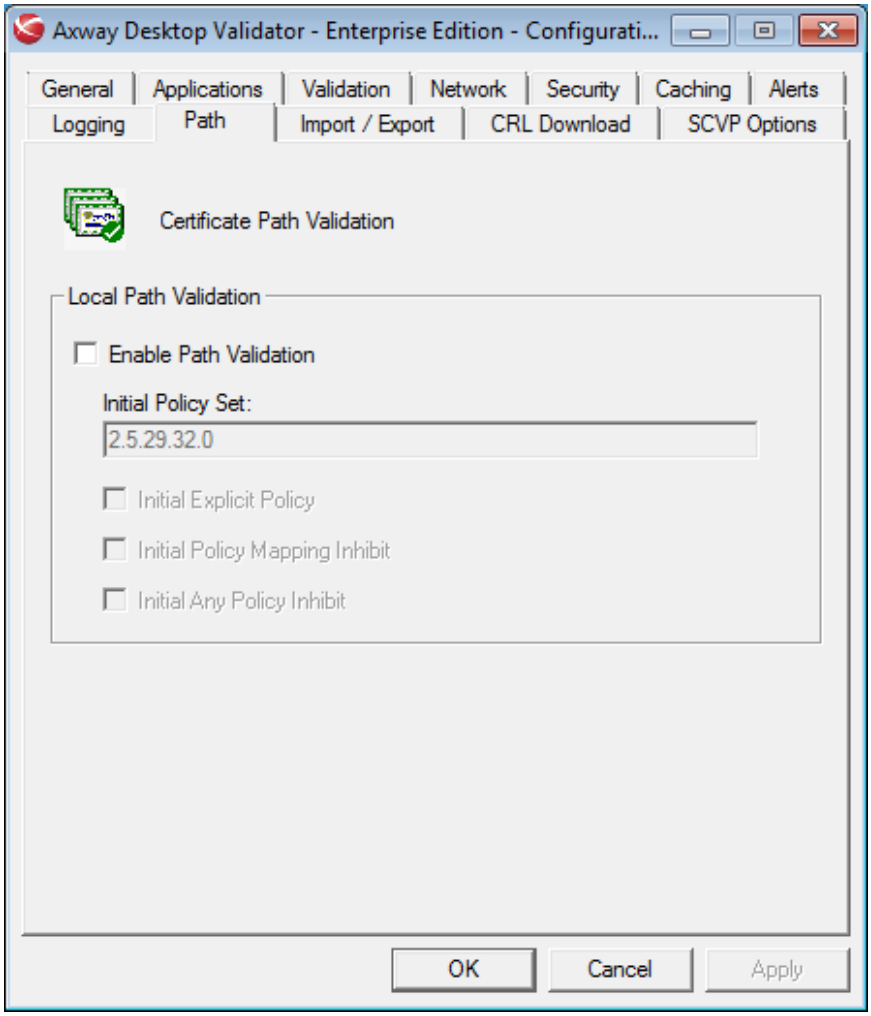
To delete all content from the log file, click the **Clear Log** button.

Configuring certificate path processing

Certificate path processing is an advanced option not normally used in most installations. See RFC 3280 for more details.

Axway Desktop Validator supports certificate path validation by constructing a chain to a trusted root in the local CAPI store and ensure that certificate path is in accordance to the specified path policies. Desktop Validator will return a status of Revoked for certificates that do not chain to a trusted root in accordance to the specified path policies. This allows organizations to override the default path validation performed by applications prior to calling Desktop Validator and ensure that only certificates that comply with the specified path policies are considered valid.

Click the **Path** tab on the Desktop Validator *Configuration* application to display the following dialog box.



Use the following options to configure certificate path validation using the local CAPI store.

Select **Enable Path Validation** to require path validation as part of the certificate validation operation performed by Desktop Validator. The local system certificate store will be used to construct the certificate path irrespective of the validation option used (e.g. OCSP, SCVP, or CRL).

Field	Description
Initial Policy Set	Enter one or more certificate policy object identifiers. Separate multiple entries using semicolons (;). The default value for the Initial Policy Set is 2.5.29.32.0, which indicates that the certificate policies in the chain must be validated, but not according to any particular certificate policy. If wildcard policies are in effect, these policy identifiers are ignored.
Initial Explicit Policy	Indicates an acceptable policy identifier needs to explicitly appear in the certificate policies extension field of all certificates in the path. If this option is cleared, an explicit match with a particular policy is not required.
Initial Policy Mapping Inhibit	Indicates whether policy mapping is allowed in the certification path. If this option is selected, policy mapping is forbidden in the certification path.
Initial Any Policy Inhibit	Indicates whether the anyPolicy extension should be processed as an initial condition for path validation if it is included in the certificate. If this option is selected, policy specified in the *anyPolicy* certificate extension will be ignored.

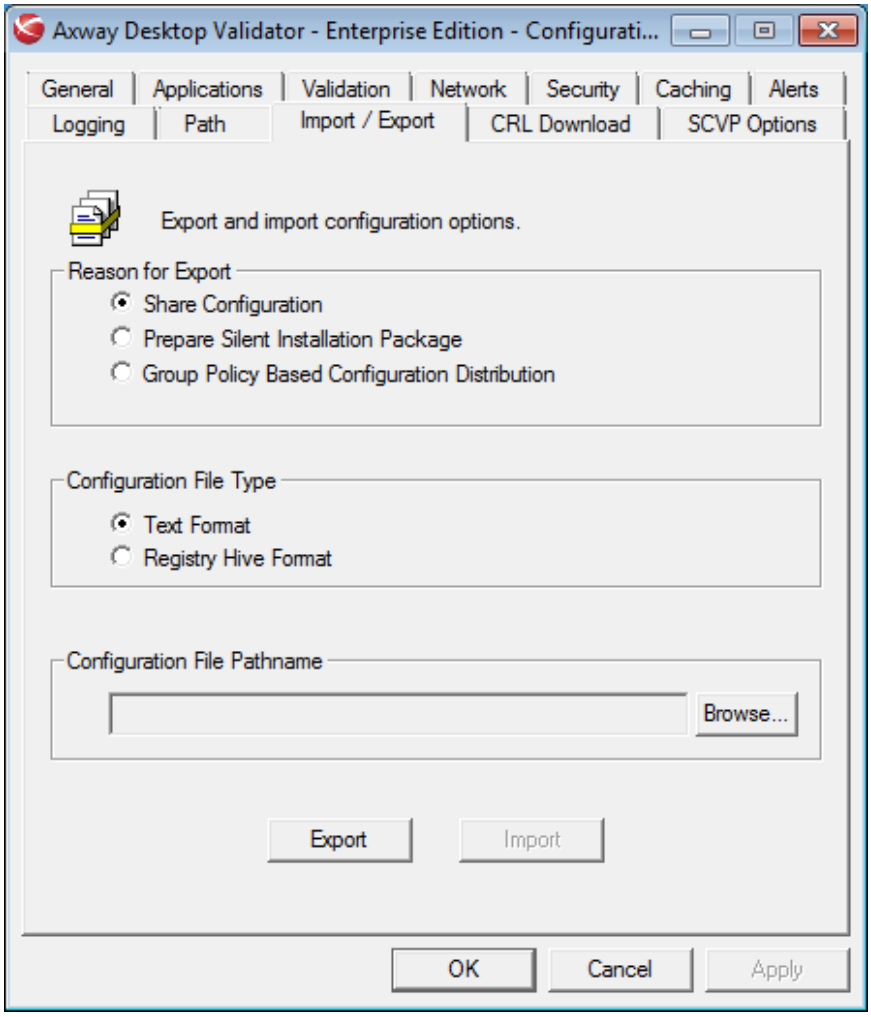
For more information see RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

Configuring Import/Export

You can use the Import/Export feature to import or export Axway Desktop Validator configuration data to allow automated configuration of Desktop Validator. If you are using Desktop Validator Enterprise you can also use this dialog box to prepare distribution packages that can be used for silent installation and configuration for large-scale Desktop Validator deployments.

Silent installation and configuration of Desktop Validator for large-scale deployment is discussed further in *Installing Desktop Validator on multiple systems* on page 13.

Click the **Import/Export** tab on the Desktop Validator *Configuration* application to display the following dialog box. **Reason for Export**, and **Configuration File Type** configurable options is displayed.



Setting reason for exporting data

Choose from one of three items to indicate the reason for exporting configuration data by clicking on the radio button.

Creating installation packages is limited to Desktop Validator Enterprise. If you are using Desktop Validator Standard these options will be greyed out and not available for selection.

Reason for Export	Description
Share Configuration	Instructs Desktop Validator that the configuration data will be exported to or imported from another system running Desktop Validator.

Reason for Export	Description
Prepare Silent Installation Package	Instructs Desktop Validator to create a package consisting of software and configuration data that can be used to silently install and configure Desktop Validator on other systems.
Group Policy Based Configuration Distribution	Instructs Desktop Validator to create the necessary Group Policy Administrative Template and configuration data that can be used to deploy Desktop Validator on other systems using the Group Policy mechanism available on Microsoft Windows server platforms.

Specifying configuration file type

Specify the configuration file format you would like Desktop Validator to import or export by selecting the **Text Format** or **Registry Hive Format** radio button.

File Type	Description
Text Format	Instructs Desktop Validator to generate an internal representation format text file. This is the default format.
Registry Hive Format	Instructs Desktop Validator to generate a Windows Registry Hive format file.

Note Registry Hive format files can be used to directly update the Windows system registry and do not need to be imported into Desktop Validator. This is not recommended since there is no validation of the configuration options in the file prior to updating the registry. This is discussed further in *Installing Desktop Validator on multiple systems* on page 13.

For Share Configuration

If the reason for export is to Share Configuration, input the path name of the file to be imported from or exported to. You can use the **Browse** button to select a file.

For Silent Installation Configuration

If the reason for export is to Prepare a Silent Installation Package, the File Pathname will be greyed out to indicate the package will be created in the default location `C:\Program Files\Axway\Desktop Validator\dvpackage`.

Finish Import/Export

Click the **Import** or **Export** button to have Desktop Validator perform the desired export or import.

For additional information on how to use this functionality to automate the installation and configuration of Desktop Validator, Refer to *Installing Desktop Validator on multiple systems* on page 13.

CRL Download

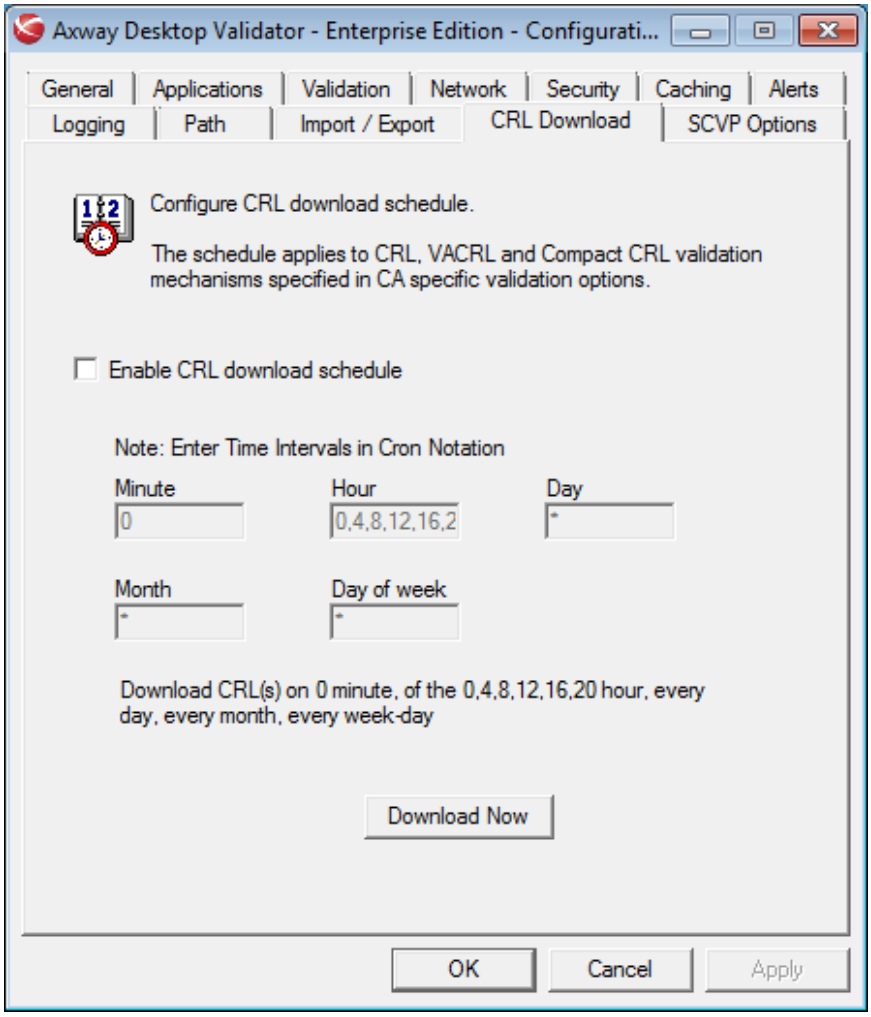
When you configure Desktop Validator with CA-specific validation protocols that rely on CRLs, you can specify whether a given CRL should be downloaded (pre-fetched) into the cache on a scheduled basis. The **CRL Download** tab allows you to set the schedule that Desktop Validator will use to download these CRLs as well as perform other operations related to downloading CRLs.

Before downloading a CRL that is currently cached, Desktop Validator checks if the CRL available at the source URL is newer than the CRL in the cache, and will not download unless it is. The scheduler can be configured to attempt downloads frequently since a CRL will not actually be downloaded unless it needs to be.

Note The CRL Download schedule does not affect the CRL caching policies. For information on configuring caching, see *Configuring Caching options* on page 56.

Configuring CRL Download options

Click the **CRL Download** tab from the Desktop Validator *Options* dialog box.



Select **Enable CRL download schedule** to configure download of CRLs required for CA-specific validation, verify scheduled downloads occurred and determine if a new CRL was loaded into the cache by checking the Desktop Validator log.

Enter the appropriate value in each of the following fields as to when the scheduler should run. The schedule is specified in UNIX style Cron notation.

Field	Description
Minute	Refers to the number of minutes after the hour, values can range from 0 to 59 or * to indicate all. The default value is 0.
Hour	Refers to the hours of the day in military time, values can range from 0 to 23 or * to indicate all. The default value is "0,4,8,12,16".
Day	Refers to the days of the moth, values can range from 1 to 31 or * to indicate all. The default value is *.

Field	Description
Month	Refers to the months of the year, values can range from 1 to 12 or * to indicate all. The default value is *.
Day of week	Refers to the week days, values can range from 0 to 6 or * to indicate all. The default value is *.

The default values specify the scheduler will be run starting at midnight, every four hours, every day, every month, every day of the week.

Downloading

To perform an immediate download of all scheduled CRLs, select the **Download Now** button to start the download.

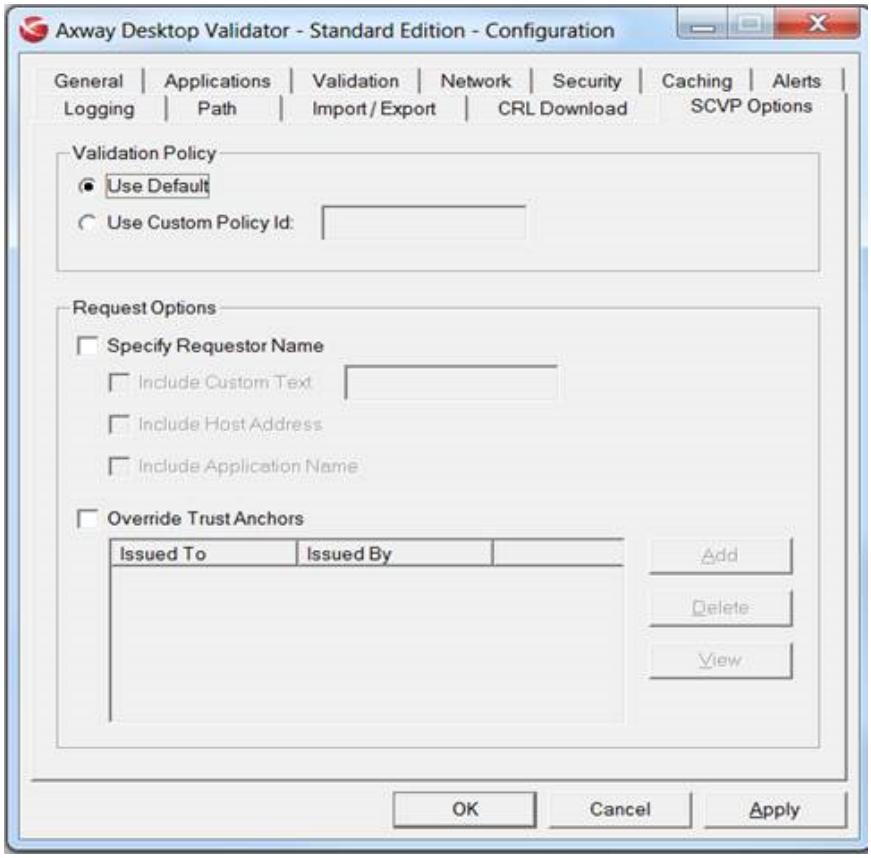
To download a single CRL, use the CRL Information screen accessible from the setting CA-Specific Validation options dialog box.

Downloading all CRLs is useful to do before disabling CRL-fetching when a system will be disconnected from the network, and network based validation cannot be performed.

Configuring SCVP Options

Server-Based Certificate Validation Protocol (SCVP) is an Internet Engineering Task Force (IETF) standards track protocol for validating certificates defined by RFC 5055. It can reduce the work Desktop Validator performs in building and validating certification paths (also called certificate chains) because Desktop Validator can use it to delegate some or all certificate handling to the Validation Authority Server. When responding to a request, the Validation Authority Server returns information on certification paths and their validity.

The **SCVP Options** tab on the Desktop Validator *Configuration* application displays three options: **Validation Policy**, **Request Options**, and **Override Trust Anchors**. Desktop Validator SCVP Options are optional. Desktop Validator will use the Default Validation Policy in all SCVP requests unless a specific Custom Policy Id is configured.



Validation Policy

The Validation Policy option defines the certification path processing that the Desktop Validator wants the SCVP server to use during certificate validation.

Desktop Validator can request the SCVP server's default validation policy or another validation policy.

Option	Description
Use default policy	The default validation policy corresponds to the standard certification path processing as defined in RFC 5280 with server-chosen default values.
Use custom policy ID	The object identifier (OID) representing particular validation policy supported by SCVP server.

Request options

Requestor Name is an optional identifier used by Desktop Validator to include in the request.

The Requestor Name option allows you to specify an identifier as a combination of the following three optional elements: custom text, computer's IP address (in either IPv4 or IPv6 format), and the name of the calling application.

When you select the check box for **Specify Requestor Name**, the check boxes for the other options are enabled. You can select any of these or none. If you decide later that you don't want to use this option, simply deselect the check box for **Specify Requestor Name**, and the other options are disabled. However, this information remains configured and can be reactivated by reselecting the check box for **Specify Requestor Name**.

Option	Description
Specify Requestor Name	Desktop Validator uses the optional Requestor Name item to include an identifier in the request.
Include Custom Text	Includes the specified custom text in the Requestor Name field.
Include Host Address	Includes the hostname of the computer running Desktop Validator service. Desktop Validator includes hostname in short form and not FQDN form.
Include application name	Includes the name of the application that requested certificate validation.

Override Trust Anchors

The Trust Anchors specify the trusted anchor certificates at which the certification path must terminate if the path is considered to be valid.

This option allows Desktop Validator to overwrite trust anchors supported by the SCVP server.

You can select the **Add** button to add CA certificates to serve as trust anchors for this policy. You can delete listed trust anchors by highlighting the one you want to delete and clicking the **Delete** button. You can select a trust anchor and click the **View** button to view the certificate, or you can double click the trust anchor in the list to view the certificate.

Option	Description
Override trust anchors	List of trust anchors Desktop Validator will use instead of the trust anchors configured for the SCVP server.

Certificate validation concepts A

This appendix provides an overview of certificate validation concepts.

Overview of certificate validation

Axway Desktop Validator certificate validation occurs within the context of the public key infrastructure (PKI), specifically, a PKI framework that uses X.509 digital certificates. Validation consists of determining that a certificate is still "Good" for the validity period for which it was issued.

X.509 v3 certificates

The X.509 certificate standard, in particular Version 3, was developed primarily by the Internet Engineering Task Force (IETF) PKIX working group. X.509 v3 certificates contain:

- Version number of the X.509 standard to which the certificate conforms
- Serial number
- Algorithm identifier
- Validity period
- Subject to whom the certificate is issued
- Subject public key
- Issuing authority signature

The issuing authority is known as a Certificate Authority (CA). An end-entity (EE) holds the certificate issued by a CA and uses the certificate to identify itself.

Certificate authorities

A PKI uses private-public key cryptography to provide entity authentication, non-repudiation, data integrity, data confidentiality, and access control. PKI relies on digital certificates, defined in the ISO X509v3 standard, containing information identifying a user and their public key. A CA receives the public key from a user private-public key pair along with some information regarding the user identity. After verifying the information, the CA issues a digital certificate signed with its private key. This means that anyone who receives a certificate and trusts the CA can trust that the user supplying the certificate is who they say they are, and that the public key contained in the certificate belongs to the certificate owner.

Validation Authority

A Validation Authority (VA) provides a universal clearing house for establishing the validity of a digital certificate. The VA represents a centralized store of aggregated CRLs (a VA can aggregate CRLs from one or more different CAs). This store of certificate status data is continuously available and accessible to PKI-enabled applications through several standard real-time protocols. These protocols (discussed in *Certificate validation protocols* on page 78) allow PKI applications to obtain the status of a specific certificate rather than the raw cumulative CRL periodically published by the CA. Thus, introducing a VA that addresses the scalability and access issues associated with CA certificate validation in PKI, as well as the audit requirements for secure transactions.

Certificate chains

A certificate chain consists of a certificate of the public key owner signed by one CA, and additional certificates, as needed, of CAs signed by other CAs leading to the root certificate at the start of the chain. The "trusted root" certificate is the basis of the certificate chains used to validate and authenticate certificates belonging to users of the framework.

The process of searching for a certificate based on a certificate issuer field is known as chain building. This process occurs iteratively until a trusted root is encountered.

Trust models

Certificate validation implies trust between the client and the validating authority. Validation is conducted using three basic trust models: Direct, VA-delegated, and CA-delegated. These trust models provide benefits in different environments, so not all are applicable to a given application.

Direct

Direct trust occurs when the client requesting validation has established a direct trust relationship with the Validation Authority. Since the client directly trusts the Validation Authority certificate as a trusted authority, the Validation Authority can sign revocation responses with a self-issued digital certificate on behalf of any CA. The advantage of this model is that it requires no trust chain to be established under a CA, thus reducing the risk/exposure to the CA for creating this chain. The disadvantage of this approach is that the directly trusted Validation Authority certificate needs to be distributed to the applications that will be making validation queries. When the Validation Authority certificate expires, the clients must be updated to trust a new directly trusted Validation Authority certificate.

VA-Delegated

VA-delegated trust is a derivative of the direct trust model. It enables a directly trusted Validation Authority to delegate responsibility to a "subordinate" Validation Authority, further addressing scalability and operational domain issues that often arise in PKI. The directly trusted Validation Authority has a self-issued digital certificate referred to as a "root" Validation Authority certificate. The directly trusted Validation Authority uses this root certificate to issue a digital certificate to a subordinate Validation Authority, which in turn uses this digital certificate to sign client responses. In order for a client to trust the subordinate Validation Authority, it must establish the certificate chain back to the directly trusted Validation Authority. The certificate depth is limited to one level, meaning the subordinate Validation Authority certificates can only be used to sign client responses, and cannot be used to issue other signing certificates.

This model is operationally more secure since a particular subordinate Validation Authority could be compromised without compromising the directly trusted Validation Authority (root VA) or any other subordinate Validation Authority. Additionally, since the Validation Authority root certificate is self-issued, the Validation Authority can also provide a check and balance for the trustworthiness of the CA itself, ensuring trust in the CA by providing the mechanism for revoking it. If the CA itself is breached, perhaps by someone posing as an employee of the CA and issuing its own false certificates, the Validation Authority is able to revoke the entire CA if needed. The VA-delegated model has its advantages: only one trust point for the root Validation Authority needs to be distributed to clients. However, an extra OCSP query needs to be sent to check the subordinate Validation Authority certificate to make sure it has not been revoked. With OCSP caching support at the clients, OCSP responses for common certificates (for example, subordinate Validation Authority certificates) can be held for a configurable amount of time, reducing the number of required queries.

CA-Delegated

CA-delegated trust occurs when a CA has explicitly given permission to a Validation Authority to respond to revocation requests on its behalf. This is similar to the VA-delegated trust model except that the certificate used by the Validation Authority to sign responses chains back to the issuing CA rather than to the directly trusted Validation Authority; the trusted root is the CA and not the Validation Authority. In order to trust the Validation Authority, the client must still establish the certificate chain back to the CA, but in many cases this might not require any additional operations since the client already trusts the CA. This model relies on certain extensions to the digital certificates that all participants in the PKI must recognize. Additionally, since the CA and Validation Authority are under different administration boundaries in most operational environments, a CA is potentially opening itself up for liability by delegating validation to a different entity. This model has one clear advantage over the others: only CA trust points must be distributed. The main disadvantage is that the CA must delegate CA responsibility to a Validation Authority. If the Validation Authority is compromised, the CA is compromised, with respect to the integrity of the status information known about the CA. This is why for CA-delegated mode, the CA and Validation Authority Servers must have practically equivalent physical security requirements.

Certificate validation protocols

Validation Authority handles PKI client application requests for digital certificate status using a server referred to as a *Responder*. The client interacts with the Responder using various protocols, each of which is supported by Desktop Validator:

- Online Certificate Status Protocol (OCSP)
- Online Certificate Status Protocol using Authority Information Access (OCSP Using AIA)
- Server-based Certificate Validation Protocol
- Certificate Revocation Lists (CRLs)
- Compact Certificate Revocation Lists (Compact CRLs)
- CRL Distribution Points (CRLDPs)
- VACRL Protocol (CRL/CRL Deltas)

OCSP

The Online Certificate Status Protocol (OCSP), defined by the IETF in RFC2560, enables applications to determine whether an identified certificate(s) appears in a CA published CRL by querying a Responder. The Responder consults its store (built by obtaining CRLs published by CAs) and returns the status of the certificate(s) identified, including potential revocation information (such as when and why the certificate was revoked). Additionally, to provide a secure and auditable transaction, the Responder includes the time the response was produced and the length of time that it can be trusted. The Responder digitally signs the entire response using its Validation Authority certificate.

Since the Responder does not have access to the actual certificate being checked, prior to submitting its request to the Responder, the client must:

- Cryptographically verify that the subject certificate was in fact issued by the corresponding CA.
- Verify that the issuing CA is indeed trusted for signing certificates.
- Verify that the subject and issuer certificates are not expired.

Once it receives a response from the Responder, the client must establish whether it trusts the Validation Authority as per the trust models previously discussed.

OCSP is conducted over HTTP or HTTPS and TCP/IP and benefits from the ubiquity of these underlying protocols.

OCSP Using AIA

When the AIA extension is present in the certificate and is enabled on the Desktop Validator, Desktop Validator uses the data contained in the AIA extension to validate the certificate.

SCVP

Server-based Certificate Validation Protocol (SCVP) is an IETF standard (RFC 5055) that would allow a client to completely off-load certificate handling to the Responder. Rather than sending just certificate identification information as in the OCSP protocol, a client using SCVP sends the entire certificate to the Responder. When using SCVP, the Responder is responsible for performing the verification done by the client prior to submitting a request to the Responder when using OCSP. This provides benefits such as simplifying client implementations and allowing companies to centralize their trust and policy management. For the most part, client implementations and policy management are already simplified by using validation toolkits, which are easy to integrate and configure, that encapsulate all the necessary client side functionality. Furthermore, client toolkits provide greater flexibility in terms of the various operational environments in which PKIs are being deployed.

CRLs

CRLs are lists of revoked certificates. As each certificate is revoked, an entry is added to the CRL and the CRL is re-signed by the issuing CA. When using CRLs, an application must download a CRL to determine if a certificate it is using is revoked. Unfortunately, due to their cumulative nature, CRLs can be quite large, out of date, and their use is not auditable.

Compact CRLs

Uses optimized and efficient data structure that represents Certificate Revocation List (CRL). The validation based on Compact CRL mirroring is very practical for low-bandwidth environments, where downloading full scale CRLs is not possible due to limited network bandwidth. Compact CRLs cannot be used for CAs that issue certificates with non-sequential serial numbers.

CRLDPs

CRLDPs is an extension to the X.509 certificate that identifies how CRL information is obtained. If the certificate contains a CRLDPs extension, Desktop Validator uses the extension to determine where to obtain the CRL to validate the certificate.

VACRL Protocol

It is possible for the client to maintain a store of certificate status information by obtaining either a cumulative CRL (used to initially establish the client's CRL store) or *CRL Deltas*, which are updates to the CRL based on the age of the last CRL obtained by the client. CRL Deltas list serial numbers of certificates revoked or suspended since the date the last CRL was obtained, and also include the number of those certificates which were earlier suspended but are now valid again. The transaction is conducted over HTTP or HTTPS and the client uses a standard POST operation to make its

request. The Responder will either return the cumulative CRL signed by the CA or it will manufacture the appropriate CRL Deltas for that client and sign the response using its Validation Authority certificate (which the client will verify as per the discussion on trust models). The client uses the response it obtained from the Responder to build its own local CRL store. This allows a client application to validate certificates even when it does not have real-time access to the Validation Authority (as is necessary for OCSP) while addressing the scalability issue inherent in the client always having to obtain a cumulative CRL. This protocol, known as the VA CRL, or VACRL, protocol, is not mutually exclusive with OCSP and is often used by enterprises with PKI in conjunction with OCSP as a backup alternative.

PKI concepts

B

This appendix provides an overview of public key infrastructure (PKI) concepts. It includes the following sections:

Installing PKI Trust Points

PKI Trust Points are the trusted Certification Authorities (CAs) in your hierarchy, issuing certificates to subordinate CAs and end-entities. This section describes how to import this trust into your system for Microsoft applications.

1. Start Internet Explorer.
2. Select **Tools > Internet Options**.
3. Click **Certificates** on the **Content** tab.

   The *Certificates* dialog box is displayed.
4. Double-click the certificate to add CA certificates into MS CryptoAPI stores.

   This invokes the Certificate Install wizard. Follow the wizard to place the certificates in the appropriate certificate stores

Removing PKI Trust Points

You can remove CA certificates that are not trusted from your trust database to control the entities you wish to trust in your PKI.

1. Start Internet Explorer.
2. Select **Tools > Internet Options**.
3. Click **Certificates** on the **Content** tab.

   The *Certificates* dialog box is displayed.
4. Click the **Trusted Root Certificate Authorities** tab and select the Certificate Authority you want to delete from the list.
5. Click **Remove**.

Generating, requesting, and importing keys and certificates

Applications have different methods for generating, requesting, and importing keys and certificates.

Microsoft Internet Information Server console provides a GUI for generating, requesting, and importing keys and certificates.

1. Click the **Properties** tab of the Web Server (IIS).
2. Select the **Directory Security** option.
3. Click **Server Certificate**.

   The Certificate Wizard is displayed. Follow the wizard to generate new Web Server certificates, assign existing certificates and import new certificates or previously saved versions from back-up files.

Configuring SSL for Microsoft client applications

1. Click the **Properties** tab of the Web Server (IIS).
2. Select the **Directory Security** option.
3. In the Secure Communications section, click **Edit**.

Note You must generate and import your web site certificates before configuring applications to use SSL

Adding a certificates to a server store

1. Log on to the server as an administrator.
2. Click **Start > Run**.
3. Type *mmc* and click **OK**.
4. On the *File* menu, click **Add/Remove Snap-in > Add**.
5. Under *Snap-in*, double-click **Certificates**, select *Service* account, and then click **Next**.
6. Select *Local Computer* and click **Next**.
7. Optional: Save the created console for future use by selecting **File > Save As** from the menu.
8. Right click **All Tasks > Import** to add the certificate to the store.

Specifying URLs to obtain CRLs and revocation information

Client applications such as Desktop Validator can be configured to automatically download CRLs from Web Servers or LDAP repositories on a CA-specific basis by specifying the Uniform Resource Locator (URL) of the CRL repositories.

Similarly, it is possible to configure Desktop Validator to point to OCSP Responder locations such that requests can be made to obtain the revocation status of specified end-entity or CA certificates.

See *Installing Desktop Validator* on page 8 for more information on each of these items.

Enabling and disabling Desktop Validator in common applications C

This appendix provides information and procedures on how to enable and disable Desktop Validator in Microsoft Internet Explorer browser, Microsoft Outlook and Outlook Express email client applications, Microsoft Internet Information Server (IIS) for Desktop Validator Enterprise, Microsoft Exchange 2007 Outlook Web Access (OWA) using S/MIME for Desktop Validator Enterprise, Windows 2008 R2 Domain Controller and Smart Card Logon.

Using Desktop Validator with Internet Explorer

Desktop Validator enables your Internet Explorer (IE) browser to use Desktop Validator to validate certificates encountered when:

- Establishing Secure Socket Layer (SSL) connections to secure Web servers
- Downloading signed content from the Internet (files signed with Authenticode)

When IE encounters a digital certificate it will first check that the certificate is not expired. It will then check that the certificate chains to a trusted root certificate in the CAPI store. If IE can successfully construct the certificate chain, Desktop Validator will be invoked via CAPI to validate every certificate in the chain.

Since IE must first determine that the certificate chains up to a trusted root CA, it is important to make sure that you have a certificate for every root CA required in your environment. If IE cannot construct the certificate chain, Desktop Validator will not be invoked to validate the certificate.

If Desktop Validator has been configured to display alerts, then you will see a Desktop Validator pop-up in your notification area (formerly called the system tray) whenever IE uses Desktop Validator to validate a certificate. It is possible that Desktop Validator has been configured not to alert if the certificate is valid or if the certificate status is returned from cache as well as in certain other cases, so you might not see a pop-up.

Note See *Configuring Alert options* on page 60 for more information on controlling Desktop Validator pop-ups.

Desktop Validator will generate a log message every time it is called on to validate a digital certificate encountered by IE. In the Desktop Validator log, the event will identify the Calling Application as Microsoft Internet Explorer and there will be additional information about the certificate, the status, and the type of validation performed. For more information on Desktop Validator logging, see *Configuring logging options* on page 64.

Configuring Desktop Validator for Internet Explorer

To configure the Desktop Validator to enable validation for Internet Explorer double-click the **Axway Desktop Validator** icon in the Windows notification area (formerly called the system tray) in the bottom right corner of the Windows desktop. Click the **Applications** tab.

Note If the Applications tab is not available, make sure the **Use Axway DV as CAPI revocation provider** option on the General tab is selected.

1. Check the check box for **Internet Explorer** to enable validation for IE.
2. Click **OK** to update the changes or **Cancel** to exit without enabling validation for the application.

Configuring Internet Explorer

You must next configure IE to perform certificate revocation status checking.

1. Double-click the **Internet Explorer** icon on your Windows desktop. The *Internet Explorer* browser appears.
2. Click **Tools > Internet Options > Advanced**. The *Advanced* options screen appears.
3. Scroll down to the Security section and make your selection.

Option	Description
Check for publisher's certificate revocation	Enable validation for certificates used to sign Internet content such as signed ActiveX controls.
Check for server certificate revocation	Enable validation for certificates presented by servers when establishing SSL connections.

4. Click **OK** to save your changes or **CANCEL** to exit the screen without making changes. If you made changes, you must restart IE for the changes to take effect.

Validating Signed Content Certificates

Once you have configured Axway Desktop Validator and the IE browser as previously described, all certificates used to sign files that you download through HTTP or FTP will be validated.

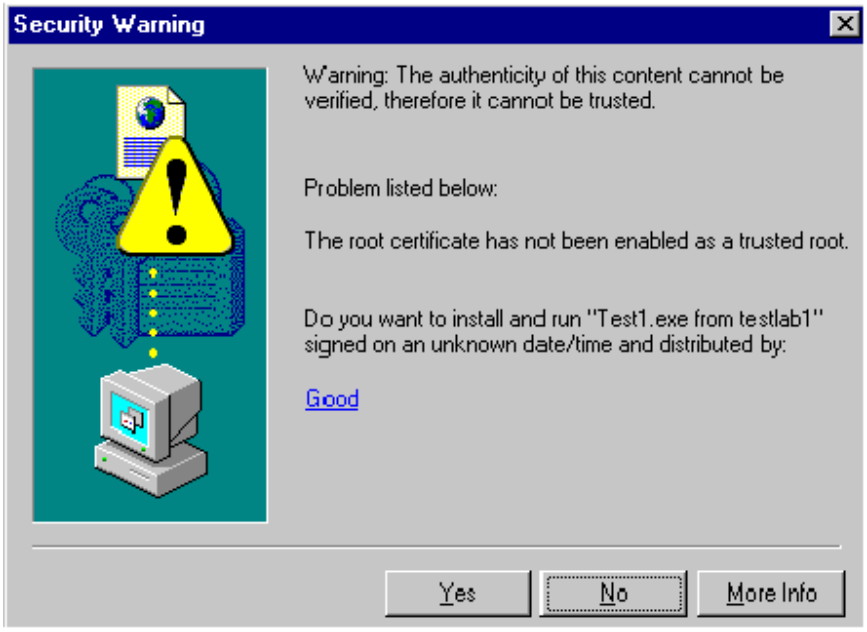
For example, if the downloaded file is signed with a revoked certificate, IE will indicate the problem with the certificate.

Unless Desktop Validator has been configured not to alert, then you will see a Desktop Validator pop-up indicating Desktop Validator has checked the status of the certificate and found it to be revoked.

If the downloaded file is signed with a valid certificate, IE will indicate that the authenticity of the publisher was successfully verified by the trusted root CA that the certificate chained under.

If Desktop Validator has been configured to alert for valid certificates (not the default), then you will see a Desktop Validator pop-up indicating Desktop Validator has checked the status of the certificate and found it to be valid.

As mentioned, IE will first attempt to construct the certificate chain. If the certificate encountered does not chain up to a trusted root CA in the CAPI store, IE will indicate that the certificate cannot be verified.



Since IE cannot construct the certificate chain in this case, Desktop Validator will not be called to validate any certificate so there will be no Desktop Validator pop-up or log event generated.

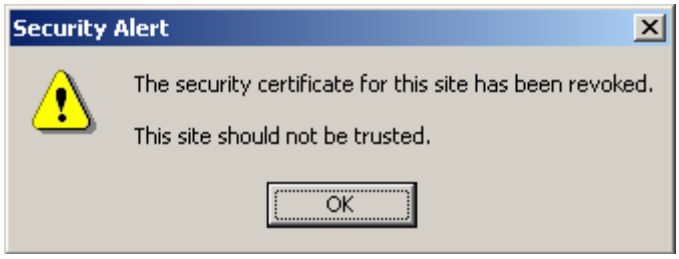
Validating SSL Server Certificates

Once you have configured the Axway Desktop Validator and the IE browser as previously described, IE will use Desktop Validator to authenticate SSL server certificates. If the SSL certificate is not valid, IE displays a status dialog indicating the reason:

- The certificate is revoked
- The certificate is expired
- The certificate issuer is unknown

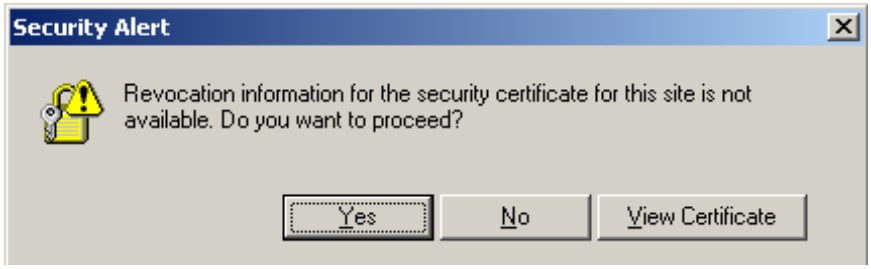
Note If the certificate is valid, IE will not display a message but you will see a yellow lock icon in the bottom right of the screen frame indicating a successful SSL connection has been established.

For example, if the server presents a revoked SSL certificate, IE will indicate the problem with the certificate.



Unless Desktop Validator has been configured not to alert, you will see a Desktop Validator pop-up indicating Desktop Validator has checked the status of the certificate and found it to be revoked.

If the certificate status cannot be determined either because the certificate chain cannot be constructed or because Desktop Validator was unable to verify the certificate status or the status was Unknown, IE will indicate the server's certificate could not be validated.



If IE was not able to construct the certificate chain, Desktop Validator was not called to validate any certificate so there will be no Desktop Validator pop-up or log event generated. Otherwise, unless Desktop Validator has been configured not to alert, you will see a Desktop Validator pop-up indicating Desktop Validator attempted to check the status of the certificate and was either unable to or determined it was Unknown.

If the Desktop Validator default validation protocol is configured to use a source that cannot determine the status of certificates issued by that source, the certificate status will be Unknown. For best results, set the default validation protocol to CRLDP (instructing Desktop Validator to use the CRL Distribution Point specified in the certificate to determine the status of the certificate) and that CA-specific OCSP and SCVP validation protocols be configured for CAs the source knows about.

Using Desktop Validator with Outlook and Outlook Express

This section provides information on using Desktop Validator to validate digital certificates when using Microsoft Outlook and Outlook Express.

Desktop Validator enables your Microsoft Outlook and Outlook Express email client applications to use Desktop Validator to validate certificates encountered when sending, receiving or reading digitally signed and/or encrypted email messages.

When the Outlook or Outlook Express email client application encounters a digital certificate it will first check that the certificate is not expired. It will then check that the certificate chains to a trusted root certificate in the CAPI store. If the certificate chain is successfully constructed, Desktop Validator will be invoked via CAPI to validate every certificate in the chain.

Since the Outlook and Outlook Express email client applications must first determine that the certificate chains up to a trusted root CA, it is important to make sure that you have a certificate for every root CA required in your environment. If the certificate chain cannot be successfully constructed, Desktop Validator will not be invoked to validate the certificate.

If Desktop Validator has been configured to display alerts, then you will see a Desktop Validator pop-up in your notification area (formerly called the system tray) whenever Microsoft Outlook or Outlook Express use Desktop Validator to validate a certificate. It is possible that Desktop Validator has been configured not to alert if the certificate is valid or if the certificate status is returned from cache as well as in certain other cases, so you might not see a pop-up.

Note See *Configuring Alert options* on page 60 for more information on controlling Desktop Validator pop-ups.

Desktop Validator will generate a log message every time it is called on to validate a digital certificate encountered by Outlook or Outlook Express. In the Desktop Validator log, the event will identify the Calling Application as either Microsoft Outlook or Microsoft Outlook Express and there will be additional information about the certificate, the status, and the type of validation performed.

Note See *Configuring logging options* on page 64 for more information on Desktop Validator logging.

Enabling and disabling Desktop Validator for Outlook/Outlook Express

Verify Microsoft Outlook and Outlook Express are enabled by default in Desktop Validator. Double-click the **Axway Desktop Validator** icon in the Windows notification area (formerly called the system tray) in the bottom right corner of the Windows desktop. The *Axway Desktop Validator Configuration* application appears.

1. Click the **Applications** tab. The *Applications* dialog box is displayed.

   If the Applications tab is not available, make sure the Use **Axway DV as CAPI revocation provide** option on the General tab is selected.
2. Check the check boxes for **Outlook** and **Outlook Express** to enable validation for Microsoft Outlook and Microsoft Outlook Express.
3. Click **OK** to update the changes or **Cancel** to exit without enabling validation for the application.

Since Microsoft Outlook and Outlook Express are CAPI compliant applications no additional configuration is required

Reading Email

This section describes how the Desktop Validator operates when you use Microsoft Outlook to read signed email messages.

Valid Certificates

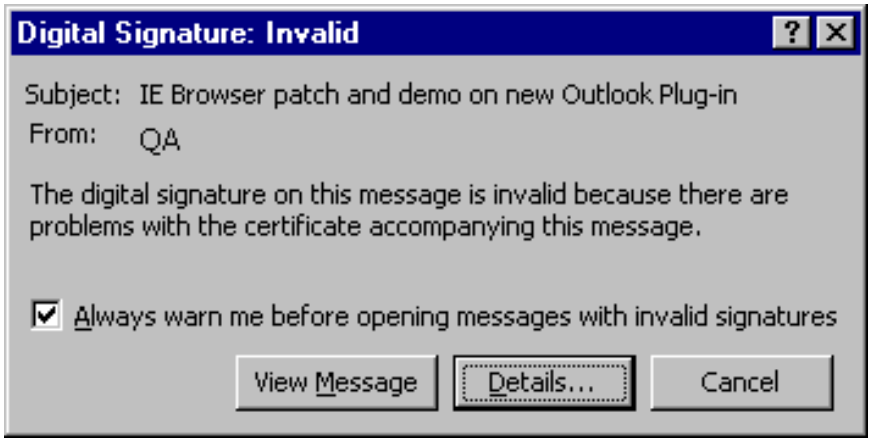
If you click to open a message with a valid signature, the *Digital Signature details* dialog appears.

This alert displays the subject of the message, the sender and information that the message is valid.

If Desktop Validator has been configured to alert for valid certificates (not the default), then you will see a Desktop Validator pop-up indicating Desktop Validator has checked the status of the certificate and found it to be valid.

Invalid Certificates

If you click to open a message that has been signed by an invalid certificate, an Invalid Signature alert appears.



This alert displays the subject of the message, the sender and information that the message is invalid.

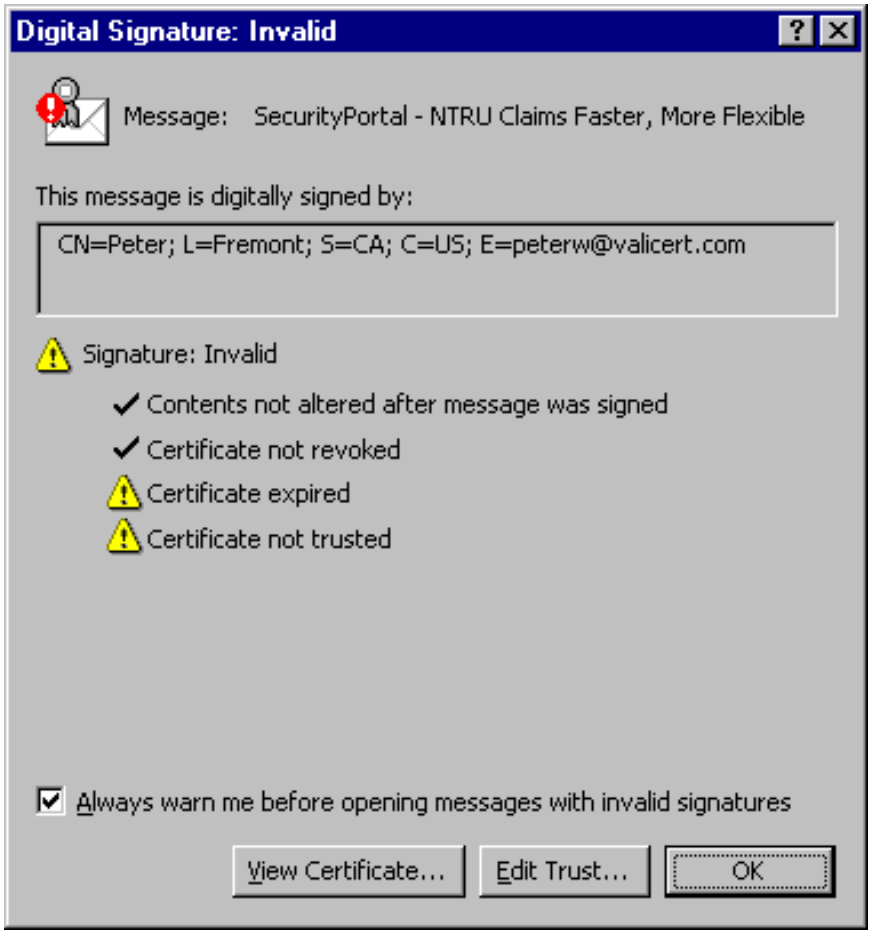
The alert contains an option to specify that you want to be warned before opening messages with invalid signatures. By default, it is selected. Clear the option if you do not want to be warned before opening messages with invalid signatures.

The alert also displays the following three buttons.

- **View Message** - click to ignore the warning and open the message.
- **Details** - click to view the details of the signature and its status.
- **Cancel** - click to cancel the action of opening the message.

To determine whether to continue and view the message or to abort and cancel opening the message, view the details of the invalid signature to get more information.

Clicking **Details** on the Invalid Signature alert displays the distinguished name on the certificate used to sign the message and the signature status.



The signature status shows a yellow warning icon if:

- The contents of the message were altered after signing
- The certificate is revoked
- The certificate has expired
- The certificate is not trusted

The dialog box displays the following two buttons.

Button	Action
View Certificate	Opens the *View Certificate* window to the *General* tab, allowing you to inspect certificate details.
Edit trust	Opens the *View Certificate* window to the *Trust* tab. **OK**—closes the *Signature Details* window.

Unless Desktop Validator has been configured not to alert, then you will see a Desktop Validator pop-up indicating Desktop Validator has checked the status of the certificate and found it to be revoked.

Using Desktop Validator Enterprise with IIS

This section provides information on using Desktop Validator Enterprise with Microsoft Internet Information Server.

Desktop Validator Enterprise enables your Internet Information Server (IIS) version 7.0 or later, to use Desktop Validator to validate certificates presented by clients who want to establish secure connections using SSL.

Note Enabling digital certificate validation in IIS is only supported in Desktop Validator Enterprise edition. If you are using Desktop Validator Standard you must upgrade to Desktop Validator Enterprise to obtain this capability.

When IIS encounters a digital certificate it will first check that the certificate is not expired. It will then check that the certificate chains to a trusted root certificate in the CAPI store. If IIS can successfully construct the certificate chain, Desktop Validator will be invoked via CAPI to validate every certificate in the chain.

Since IIS must first determine that the certificate chains up to a trusted root CA, it is important to make sure that you have a certificate for every root CA required in your environment. If IIS cannot construct the certificate chain, Desktop Validator will not be invoked to validate the certificate.

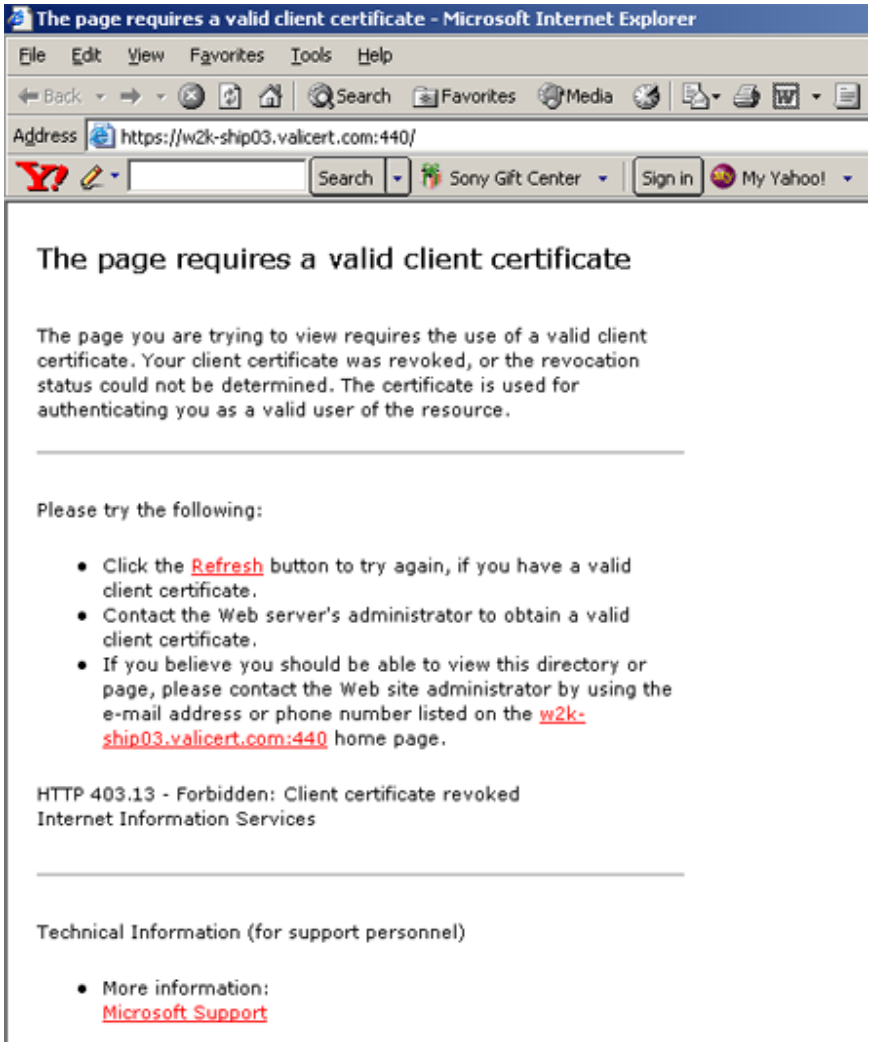
If Desktop Validator has been configured to display alerts, then you will see a Desktop Validator pop-up in your notification area (formerly called the system tray) whenever IIS uses Desktop Validator to validate a certificate. It is possible that Desktop Validator has been configured not to alert if the certificate is valid or if the certificate status is returned from cache as well as in certain other cases, so you might not see a pop-up.

Note See *Configuring Alert options* on page 60 for more information on controlling Desktop Validator pop-ups.

Desktop Validator will generate a log message every time it is called on to validate a digital certificate encountered by IIS. In the Desktop Validator log, the event will identify the Calling Application as Microsoft Internet Information Server and there will be additional information about the certificate, the status, and the type of validation performed.

Note See *Configuring logging options* on page 64 for more information on Desktop Validator logging.

Users who attempted to access the IIS server using a certificate that was not valid will get a screen indicating that they cannot access the server without a valid certificate.



Enabling Validation for IIS

You configure Desktop Validator to enable validation for IIS from the **Applications** tab.

1. Click the **Applications** tab in the *Desktop Validator Options* dialog box.

   This option is applicable only if you selected the **Use Axway DV as CAPI revocation provider** option on the General tab.

2. Select **Internet Information Services** to enable validation for IIS.
3. Click **OK** to update the changes or **Cancel** to exit without enabling validation for the application.

Configuring IIS

To enable IIS to use Desktop Validator to validate client Secure Sockets Layer (SSL) certificates, IIS must be configured for SSL with Client Authentication. To do so, you must:

- Set up SSL on IIS following the instructions at http://www.iis.net/learn/manage/configuring-security/how-to-set-up-ssl-on-iis.
- Require SSL following the instructions at http://technet.microsoft.com/en-us/library/cc732367(WS.10).aspx.
- Require 128-Bit SSL following the instructions at http://technet.microsoft.com/en-us/library/cc755203(v=ws.10).aspx.
- Require client certificates following the instructions at http://technet.microsoft.com/en-us/library/cc753983(WS.10).aspx.

Using Desktop Validator Enterprise with Exchange Outlook Web Access

This section provides information on using Desktop Validator Enterprise with Outlook Web Access (OWA) for Microsoft Exchange 2003 and Microsoft Exchange 2007.

Desktop Validator Enterprise enables your Microsoft Exchange Outlook Web Access (OWA) application to validate certificates encountered by users reading or sending digitally signed email messages using the Secure/Multipurpose Internet Mail Extensions (S/MIME) standard.

Outlook Web Access provides access to Exchange through a Web browser. In previous versions of Exchange, there was no support for S/MIME in OWA. Exchange 2003 and Exchange 2007 include full support for nearly all message security services in OWA through the S/MIME control for IE 6 or later. The S/MIME control provides similar S/MIME functionality that other full S/MIME clients such as Outlook and Outlook Express provide.

It is helpful to understand the architecture of OWA with the S/MIME control at a high-level before discussing the specifics of implementing and using it. Understanding the architecture will help you understand how the specific pieces fit together.

OWA relies on the interaction of the Web browser (IE 6 and higher) and the Exchange server to provide the functionality for an e-mail client. The S/MIME control is a Component Object Model (COM) object that also uses dynamic HTML (DHTML) to support the basic message security services: digital signatures and message encryption.

The user's client system and the Exchange server handle different aspects of digital certificates, depending on the digital certificate operation that is required. OWA on the user's client system handles digital certificates that contain the user's private keys, but never sends the private keys to the Exchange server. The Exchange server handles digital certificates that contain other users'

public keys. The Exchange server validates all digital certificates that contain both public and private keys by validating their expiration dates, validating the trust relationships, and checking their revocation status.

Support for OWA is provided automatically by the Exchange server. There are no additional components that the Exchange a server administrator needs to install. However, some configuration changes are required on both the user's client system and the Exchange server before Outlook Web Access with the S/MIME control can be used.

This chapter how to configure OWA and enable digital certificate validation using Desktop Validator Enterprise. Be sure to install the Exchange server before installing and configuring Desktop Validator. Refer to the appropriate Exchange manuals for instructions on installing the Exchange server.

Information contained in this chapter was obtained from the *Exchange Server Message Security Guide* available in the Microsoft Exchange Server TechCenter on the Microsoft web site at http://technet.microsoft.com/en-us/library/aa996417.aspx.

Enabling Validation for OWA

You must first configure Desktop Validator to enable validation on both the client system and Exchange server.

1. Double-click the **Axway Desktop Validator** icon in the Windows notification area (formerly called the system tray) in the bottom right corner of the Windows desktop.

   The *Axway Desktop Validator Configuration* application is displayed.

2. Click the **Applications** tab.

   If the Applications tab is not available, make sure the **Use Axway DV as CAPI revocation provider** option on the General tab is selected.

   The *Applications* dialog box is displayed.

3. Enable Desktop Validator for the appropriate application.

   a. On the client system, select **Internet Explorer** to enable validation for Internet Explorer.

   b. On the Exchange server system, select **Microsoft Exchange OWA** to enable validation for Microsoft Exchange Outlook Web Access usage

   If the **Microsoft Exchange OWA** option is not available (greyed out), you are using Desktop Validator Standard and must upgrade to Desktop Validator Enterprise before continuing.

4. Click **OK** to update the changes or **Cancel** to exit without enabling validation for the application.

5. If you are enabling certificate validation on the Exchange server system, you must restart the Microsoft Exchange Information Store.

   a. Click **Start > Settings > Control Panel**.

   b. Double-click **Administrative Tools**.

   c. Restart the **Microsoft Exchange Information Server** from the list of applications.

Configuring a User's Client System for OWA

Configuring a user's client system to support Outlook Web Access (OWA) with the S/MIME control requires you to perform two steps:

1. Install and configure the S/MIME control to the client system.
2. Make the appropriate digital certificates available on the client system.

Installing and Configuring the S/MIME Control

To use OWA with the S/MIME control, the client system on which the user is running Internet Explorer must have the OWA with the S/MIME control installed. S/MIME functionality in OWA cannot be used on a system that does not have the OWA with the S/MIME control installed.

Note Outlook Web Access with the S/MIME control requires that the client system use Microsoft Windows® 2008 R2, XP SP3, 7, 8.1, or 2012 R2 and Internet Explorer 8 or later. You cannot use the S/MIME control with other browsers installed on the client system.

To install OWA with the S/MIME control, the user downloading and installing the control must have administrator privileges on the workstation.

1. Logon to OWA.

   To support OWA S/MIME control, the computer must have Windows 2008 (or later) and IE 8.0 (or later).

2. Click **Options** in the **Navigation Pane**.

   If the **Navigation Pane** is collapsed, click **Go to options**.

   The *Options* page is displayed.

3. Click **Download** under E-Mail Security.

   Click **Yes** for any security options that appear.

   The S/MIME control will be downloaded from the Exchange Server to the local computer for installation. Following the S/MIME control installation, the following two options are provided on the *Options* page under E-Mail Security:

   - **Encrypt contents and attachments for outgoing messages**
   - **Add digital signature to outgoing messages**

   These options represent the default settings for a message composed using OWA. Even if neither default is selected, users can encrypt or sign individual messages from within the message. Similarly, the default options can be disabled for individual messages.

Configuring the default email security settings

1. Select **Encrypt contents and attachments for outgoing messages** to automatically enable encryption when composing a message.

2. Select **Add digital signature to outgoing messages** to automatically add a digital signature when composing a message.
3. Click **Save** to save any changes.
4. Click **Close**.

For the S/MIME control to operate properly, the IE zone to which the user is connecting for Outlook Web Access must have the following settings:

- Download signed ActiveX controls set to Prompt or Enable.
- Run ActiveX controls and plug-ins set to Enable (or Administrator approved with the S/MIME control as an approved control).
- Script ActiveX controls marked as safe for scripting set to Enabled.

Verify that IE is appropriately configured. By default, these settings are enabled in the Internet and intranet zones.

Make the appropriate digital certificates available on the client system

The Exchange server provides digital certificate validation for all certificates. When using OWA with the S/MIME control, the Exchange server also performs most certificate handling related to public keys. However, when handling digital certificates related to the user's private keys, the S/MIME control on the user's client system obtains the digital certificate that is stored on the user's client system. OWA with the S/MIME control retrieves digital certificates for private keys on the user's client system by accessing the Personal certificate store of the current logged on user. Be sure that all necessary certificates for signing email are loaded into the Personal certificate store on a smart card.

Configuring the Exchange Server

The Exchange Server must support S/MIME for clients.

To verify that your Exchange Server supports S/MIME for clients

1. Click **Start > Programs > Microsoft Exchange > System Manager**.
2. Click **Servers**.
3. Select the appropriate server and click **First Storage Group**.
4. Right-click **Mailbox Store** and select **Properties**.
5. Make sure **Clients Support S/MIME signatures** is enabled.

Enabling support Microsoft Exchange OWA in Desktop Validator will only ensure that the Exchange server will check the revocation status of digital certificates. However, by default, if a user attempts

to send an email message digitally signed or encrypted with a certificate which cannot be validated, OWA displays a warning dialog box that the certificate cannot be verified but allows the e-mail message to be sent. To prevent such email messages from being sent, you must modify the Registry.

To modify the Exchange Server Registry settings

1. Access the Registry:x
   a. Click **Start > Run**.
   b. Type `regedit`.
2. Open the Registry key `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeWeb\OWA`
3. Add the `CheckCRL` key, if not already present, and set it to a value of zero `(0x0)`
4. Restart the Microsoft Exchange Information Store.
   a. Click **Start > Settings > Control Panel**.
   b. Double-click **Administrative Tools**.
   c. Restart the **Microsoft Exchange Information Server** from the list of applications.

Note For more information about Outlook Web Access, go to http://technet.microsoft.com/en-us/library/aa998629.aspx.

To confirm proper Desktop Validator operation with Outlook Web Access, perform the following tasks:

- Send a signed email using OWA
- Send an encrypted email using OWA
- Validate the signed message

To send a signed message

1. Logon to OWA as a user that has a certificate and the S/MIME control installed.
2. Click **New** to compose a new message.
3. Add a recipient to the test message, enter text in the Subject field and enter the message text.
4. Select **Add digital signature to this message** on the toolbar if it is not already selected.

   This option button has an icon showing a certificate over top of an envelope.
5. Clear **Encrypt message contents and attachment**.

   This option button has an icon showing a lock over top of an envelope. This option is cleared because only digital signing is being tested.
6. Click **Send**.
7. Logon as the recipient of the test message and open the message.

   The message should contain the digital signature of the sender.

To send an encrypted message

1. Logon to OWA as a user that has a certificate and the S/MIME control installed.
2. Click **New** to compose a new message.
3. Add a recipient to the test message, enter text in the Subject field and enter the message text.

   Since the recipient's public key is required to encrypt the message contents, the recipient must have previously enrolled in a certificate that supports encryption.
4. Select **Encrypt message contents and attachment** on the toolbar button if it is not already selected.
5. Clear **Add digital signature to this message**.

   This option is cleared because only encryption is being tested.
6. Click **Send**.
7. Logon as the recipient of the test message.

   The message should be encrypted and only viewable by the recipient from a computer that has the user's encryption certificate installed.

To validate a signed message

If the signature of the certificate signing the email (or encrypting the email) is valid and the certificate has not been revoked, the Exchange Server Event Viewer will contain a log entry for successful validation. The following is an example of a successful validation log entry.

```
Certificate Revocation Status
Calling Application: store.exe
Certificate Name: [Certificate DN]
Certificate Issuer: [Issuer DN]
Certificate Serial Number: [Certificate Serial Number]
Revocation Status: [Good/Revoked/Unknown]
Validation Protocol: [OCSP/CRL/SCVP]
Validation Url: [URL of CRL/Responder]
```

Using Desktop Validator with Windows Domain Controller for smart card logon

This section provides an overview on using smart cards to log on in Windows.

Smart cards are a tamper-resistant and portable way to provide security solutions for tasks such as client authentication, logging on to a Windows domain, code signing and securing email.

This appendix describes how to set up Windows domain controller for smart card logon and how Desktop Validator (Desktop Validator) assists in checking the revocation status of the smart card user certificate during logon.

The following assumptions have been made regarding the Desktop Validator and smart card operating environment.

- Active Directory service is installed and running on a Windows Server Domain Controller.
- Domain Name Service (DNS) is available.
- All clients for whom smart card login is required belong to the domain.
- The Certificate Authority (CA) used to issue certificates is a Microsoft CA (MS CA).

  For guidelines on how to enable Smart Card Logon for Windows using third-party CAs, see http://support.microsoft.com/default.aspx?scid=kb;EN-US;q281245.

Most of the information presented in this appendix was obtained from the Microsoft web site. Links that provided particularly useful information include:

- To deploy certification authorities and PKI for an intranet: http://technet.microsoft.com/en-us/windowsserver/bb512919.
- To deploy smart cards to logon to Windows: http://technet.microsoft.com/en-us/enus/library/dd277386.aspx.

Setting up smart card logon for Windows Domain Controller

You must install and configure the Axway Desktop Validator Enterprise edition to enable smart card logon for Windows Domain Controller.

1. Set up a machine with Windows server.

   This server is required to run the Enterprise CA.

2. Install an Enterprise root CA on the Windows server.

   This step will automatically issue a certificate to the Domain Controller. You might have more than one CA in a Windows domain.

   Certificates used for Windows logon have specific requirements that are specified in Certificate Templates readily available in MS CA (see *Using Desktop Validator with Windows Domain Controller for smart card logon* on page 99 for more information on certificate requirements).

   For smart card logon, the following certificate templates are required:

   - Smart Card Logon—used for certificates that are burnt into the smart cards for logon purposes.
   - Smart Card User—used for certificates that are burnt into the smart cards for email signing and logon purposes.
   - Enrollment Agent—used for certificates that are used by users who request smart card certificates on behalf of other users.

Before allowing users to request certificates based on the templates mentioned above, make sure that you limit access to the templates to only those users/groups that will issue smart cards to other users. Instructions on specifying permissions on Certificate Templates are available at: http://support.microsoft.com/kb/239706.

3. Prepare the CA to issue certificates for the templates.

   You can add any number of templates as required for your PKI deployment. Instructions on preparing a CA to issue certificates based on specific templates are available at: http://technet.microsoft.com/en-us/enus/library/cc736358(WS.10).aspx.

4. Generate Enrollment Agent certificates for the person(s) who will be setting up smart cards for users.

   Generate the certificates from the machine from which smart cards will be issued by logging in as the user who will issue smart cards. This is necessary because the Enrollment Agent certificate will be stored in the users' private certificate store on that machine and will be required for signing each smart certificate the user issues. Instructions on how to generate enrollment agent certificates are available at: http://technet.microsoft.com/en-us/enus/library/dd277383.aspx.

5. Set up a smart card reader on the machine where certificates will be issued.

   This is required to burn user certificates on the smart cards. Instructions on how to setup smart cards readers are available at: http://technet.microsoft.com/en-us/library/bb742531.aspx.

6. Set up smart cards for each user who requires smart card based logon.

   Instruction for setting up smart cards for user logon is available at: http://technet.microsoft.com/en-us/library/cc775842%28WS.10%29.aspx.

7. Install a smart card reader on the smart card user's computer.

   This is the same as Step 6, except that the reader is installed on the smart card users' machine. Logon to the machine using the smart card issued in Step 6. Instructions on how to logon using smart cards are available at: http://technet.microsoft.com/en-us/library/bb742531.aspx

Certificate Format Requirements

Smart card certificates have the following specific format requirements:

- The certificate must have a certificate revocation list (CRL) distribution point extension pointing to a valid CRL. This is optional if Desktop Validator is used to check revocation status of smart cards and the domain controller.
- The certificate Key Usage section must contain a digital signature, and a key encipherment.
- The certificate Enhanced Key Usage section must contain:
  - Client Authentication (1.3.6.1.5.5.7.3.2)
  - Smart Card Logon (1.3.6.1.4.1.311.20.2.2)
- The certificate Subject Alternative Name section must contain the Globally Unique Identifier (GUID) of the domain controller object in the directory and the Domain Name System (DNS) name, for example:

- Other Name: 1.3.6.1.4.1.311.25.1 = ac 4b 29 06 aa d6 5d 4f a9 9c 4c bc b0 6a 65 d9 DNS Name=server1.northwindtraders.com

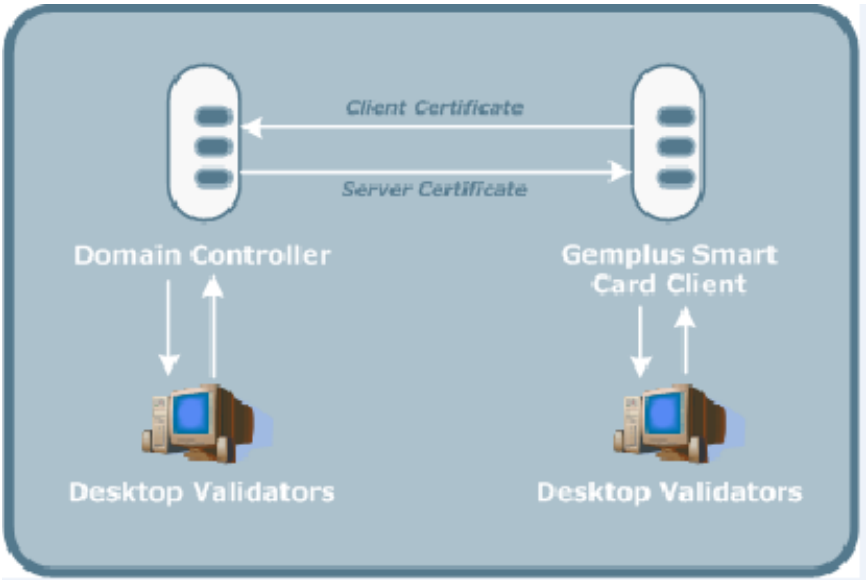
- The certificate template must have an extension with the BMP data value `"DomainController"`.
- You must use the Schannel Cryptographic Service Provider (CSP) to generate the key.

Certificate authentication through Desktop Validator

Desktop Validator can be used to authenticate: Smart card-based client certificates and the Domain Controller certificate.

To enable Axway's revocation checking for users' smart card certificates, Desktop Validator should be installed at the Domain Controller. Installing Desktop Validator on the client machines enables the clients to validate the Domain Controller certificate during logon.

The following figure shows how Desktop Validator is invoked at the Domain Controller and client machines when a user logs in using a smart card.



The following sections provide an overview of the steps needed to configure smart card based logon to a Windows domain.

- Adding CA certificates to Windows
- Importing CA certificates into the Windows certificate store
- Modifying domain and user accounts
- Setting smart card policies
- Troubleshooting

Adding CA certificates to Windows

Using Desktop Validator with Windows Domain Controller for smart card logon on page 99 describes the process for setting up a Windows server to support smart cards. Once this is done, CA certificates must be added to the server. Certificates are added to the server certificate store using the Directory Services Store tool (`dsstore.exe`), which is included in the Windows Resource Kit.

1. Install `dsstore.exe`
2. Obtain a copy of the CA certificates from the CA server and save them to a file as directed by the CA server product documentation.
3. Add the certificate to the Windows server certificate store using the `dsstore.exe` program.

Refer to the Windows Resource Kit for `dsstore.exe` command details.

Importing CA certificates to Windows Certificate Store

Windows requires that any CA issuing smart card logon certificates publish its CA certificates into the NTAuth store in the Active Directory.

Based on your security policy, create a file for each certificate that must be loaded to the NTAuth store.

You might be required to load the CA certificate as well as an email certificate to signing emails. If your policy also includes a certificate for encrypting the email content, you must include that certificate as well.

1. Open Microsoft Windows Notepad and create an LDAP Data Interchange Format (LDIF) file.
2. Include the "`dn`" information.
3. Include the "`changetype`" information.
4. Include the "`add`" information.
5. Include the "`CACertificate`" information.

   Do not include the Begin Certificate and End Certificate lines. Indent every line of the certificate with a space. Add a hyphen following the last line and two carriage returns at the end.
6. Save each file with a `.ldf` extension.
7. Use the `ldifde.exe` tool to import the certificates into the Active Directory.

   The `ldifde.exe` tool is included with the Windows software. The command format is the following:

   ```
   ldifde -i -f filename.ldf
   ```

Modifying domain and user accounts

Microsoft Windows requires that the End User certificate used for Smart Card Logon contain a User Principal Name (UPN) in the Subject Alternative Name extension. The UPN must have the format "user@name.com". In some deployments it might be necessary to add a prefix or suffix to every user account.

To add a suffix to a domain

1. If you have not previously done so, create the console by opening the MMC console and adding the **Active Directory Domain and Trusts** Snap-in.
2. Open the **Active Directory Domain and Trusts** MMC.
3. Right-click **Active Directory Domain and Trusts**.
4. Select **Properties**.

   The *UPN Suffixes* window is displayed.
5. Enter the suffix to add in the Alternative UPN Suffixes: field.
6. Click **Add**.
7. Click **Apply**.
8. Click **OK**.

To modify the user accounts

Users using Smart Card Logon must have their accounts modified to add their certificate to the account and to change the login account name to the EDP-PI number.

1. Add the user's certificate to the account.

   Each user must send you a copy of their certificate.
2. Open the **Active Directory Users and Computers** MMC.
3. Click the + to expand the container for the domain.
4. Click the **Users** folder.
5. Click **View > Advanced Features** to enable Advanced Features, which is required for you to view the user's certificate information.

6. Add the user's certificate to the user's directory entry:
    a. Double-click the user entry you are adding, which causes the user's *Properties* window to appear.
    b. Click the **Published Certificates** tab, which causes the *Published Certificates Window* to appear.
    c. Click **Add from File**.
    d. Select the user's certificate and click **Open**.
7. Add the prefix to the user account:
    a. Double-click the user certificate.
    b. Click the **Details** tab.
    c. Scroll down and click **Subject Alternative Name** and note the Principal Name.
    d. Click the user's **Account** tab.
    e. Change the user's logon name to the prefix and select the suffix from the drop-down list.
    f. Click **OK**.

Setting smart card policies

This section describes smart card policies for interactive logon and logoff behavior.

Configuring smart cards for interactive logon

1. Go to the user's **Account** tab.
2. Check **Smart card is required for interactive logon** in the Account Options portion of the **Account** tab.

Configuring smart card removal behavior

1. Open the **Active Directory Users and Computers** MMC.
2. Right-click the domain and select **Properties**.
3. At the *Domain Properties* window, click the **Group Policy** tab.
4. Click **Edit**.
5. Expand **Default Domain Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options**.
6. Double-click the "Smart card removal behavior" policy.
7. Select **Define this policy setting** and select **Force Logoff** from the drop-down list.
8. Click **OK**.

Troubleshooting smart card logon deployment

When encountering any of the following errors, refer to http://technet.microsoft.com/en-us/library/bb742532.aspxfor more details.

- Status insufficient resources.
- Revocation server offline.
- Certificate has been revoked, but still can be used for smart card logon.
- Client credentials could not be verified.
- The security database on the server does not have a computer account for this workstation trust relationship.
- Invalid Handle.
- The network request is not supported.
- A certificate chain processed correctly, but terminated in a root certificate which is not trusted by the trust provider.
- Windows could not find a certification authority to process the request.
- Certsrv web pages inaccessible, and Virtual Roots do not show up in Internet Services Manager.
- Enrolling for smart card through enrollment station web pages fails with the message:

  "A certification chain processed correctly, but one of the CA certificates is not trusted by the policy provider."
- Configuration information could not be read from the domain controller, either because the machine is unavailable, or access has been denied.
- This operation returned because the time-out period expired.
- The RPC server is unavailable.
- Invalid Parameter.

Using Desktop Validator with Adobe Acrobat

If Adobe Acrobat is already installed on your system before you install Desktop Validator, Acrobat will be automatically enabled. However, if Desktop Validator is installed prior to Adobe Acrobat, you must configure Desktop Validator to recognize Acrobat.

Enabling Adobe Acrobat as an administrator

For the administrator, there are several options to enable Acrobat in Desktop Validator:

- Close Desktop Validator in the tray and then reopen it. The Desktop Validator Applications tab should show that Adobe Acrobat is now enabled.

- Open Desktop Validator and select the Applications tab. Select the check box for **Adobe Acrobat/Reader**, and click **OK**.
- Restart the Desktop Validator System Tray Utility.

Enabling Adobe Acrobat as a user

If Adobe Acrobat is installed after Desktop Validator is installed, restart the Desktop Validator System Tray Utility or log out and log back in.

Glossary

This is a glossary of terms for Axway Desktop Validator.

AES
Advanced Encryption Standard also known as Rijndael, is a block cipher adopted as an encryption standard by the US National Institute of Standards and Technology (NIST) as US FIPS PUB 197 in November 2001.

API
Application Programming Interface is the interface through which an application program interacts with the operating system or other services. The interface also enables interaction between extensions and the main application program. An API usually consists of "calling" conventions that call into the operating system or main application at certain stages of the operation.

CA
Certification Authority, an entity that issues digital certificates.

Certificate Import
The process of taking an issued X509v3 certificate (for OCSP, SCVP, CSC, etc.) and loading it into the VA Admin Server and VA host server. An Identrus defined form of OCSP expressed in format.

CMP
Certificate Management Protocol is a means for Axway Valicert Validation Authority to incorporate instant updates of certificate status information from a CA, without waiting for thepublication of a full CRL.product used by the U.S. DOD community.

CRL
Certificate Revocation List. This contains a list of revoked certificates.

CRLDP
CRL distribution points.

CSC
Certificate Status Check is an IdenTrust defined form of OCSP expressed in XML format.

DER
Distinguished Encoding Rules.

Digital certificate
Defined as per the X509v3 standard, a digital ID or certificate is a method for encoding a public key and associated name information (usually defined as a distinguished name).

DN
Distinguished Name is a unique naming scheme that identifies the subject of a digital certificate.

HMAC
Hashed Message Authentication Code.

Hostname
This the name of the host machine.

Identrus
A company founded by leading world-wide financial institutions in 1999 to provide standards and infrastructure by which technology and services can support 100% trusted transactions in global e-commerce.

Key Generation
The process of generating an RSA public/private key pair either in software or hardware. It is used to sign OCSP, SCVP, or other types of messages.

LDAP
Lightweight Directory Access Protocol, a directory service protocol designed to operate over TCP/IP.

MD5
MD5 message-digest algorithm. The algorithm can reproduce any message of arbitrary length a 128-bit "fingerprint" or "message digest."

Microsoft CA
A popular CA product distributed as part of Windows 2000 and Windows 2003. Microsoft has PKI features in their operating system, and IIS and IE products that work along with the Microsoft CA for issuance of certificates to these products.

Microsoft Cryptographic API (CAPI)
CAPI (Crypto Application Programming Interface) provides a standard way to access encryption, hashing, signing, and authenticating algorithms from a variety of different security vendors. It contains functions that allow applications to encrypt or digitally sign data in a flexible manner, while providing protection for the user's sensitive private key data. All cryptographic operations are performed by independent modules known as cryptographic service providers (CSPs). One CSP, the Microsoft RSA Base Provider, is included with the operating system.

MIME
Multipurpose Internet Mail Extensions is a standard for multi-part, multimedia electronic mail messages and World-Wide Web hypertext documents on the Internet.

My Term
My definition

OCSP
Online Certificate Status Protocol. An IETF protocol (RFC 2560) used to determine the current status of a digital certificate issued by a particular Certifying Authority (CA) without requiringa client to obtain and examine the entire Certificate Revocation List (CRL) issued by that CA.

PKCS
Public Key Cryptography Standards, specifications produced by RSA Laboratories and secure systems developers for the purpose of accelerating the deployment of public-key cryptography.

PKCS#7
Cryptographic Message Syntax Standard. A PKCS standard that describes general syntax for data, such as digital signatures, that can have cryptography applied to it.

PKI
Public Key Infrastructure enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a privatecryptographic key pair that is obtained and shared through a trusted authority.

Private Key
This is the ID of the key used to sign responses. (Only applicable if hardware signing is used.)

Repeater
A keyless OCSP server that can forward OCSP queries to the OCSP Responder or issueresponses from the OCSP response database/cache.

Responder
Accepts OCSP requests that are signed/unsigned over the http(s) protocol from a Repeater.

RSA
According to the RSA security FAQ it is defined in PKCS#1 standard, a public/private key algorithm that is widely used as part of PKI.

S/MIME
Secure MIME.

SCVP
Simple Certificate Validation Protocol is an IETF defined protocol still in draft format that allows a client to completely offload certificate handling to the Responder. Rather than sending only

certificate identification information as in the OCSP protocol, a client using the SCVP protocol will be able to send the entire certificate to the Responder.

SHA-1
Secure Hash Algorithm.

SSL
Secure Socket Layer is a protocol for establishing a secure connection between a client and server, through mutual authentication and an encrypted connection.

TLS
Transport Layer Security is a protocol for establishing a secure connection between a clientand server through mutual authentication and an encrypted connection. Often considered "next generation" of SSL.

Trust Anchors
A trust anchor is an authoritative entity represented through a public key and its associated data. It is used in the context of public key infrastructures. When there is a chain of trust, usually the top entity to be trusted becomes the trust anchor. For example, it can be a certification authority (CA).

VA
Validation Authority is an authorized entity to validate digital certificates.

X.509
A CCITT / ITU standard using certificates for security services within X.500. It uses a public and a private key to encrypt data.