



CHAPTER 6

Updating VPN Client Software on a VPN 3000 Concentrator

There are two ways to update VPN Client software. You can place a new release or update on a web server, called the *update server*, and notify remote users of all client types (Linux, Windows, Mac OS X and so on) where to retrieve and install the updated software. Or, starting with Release 4.6, you can automatically update VPN Client software for Windows 2000 and Windows XP remote users.

This section has the following sections:

[Enabling Client Update \(All Client Types\)](#)

[Updating the VPN Client Software Automatically on Windows 2000 and Windows XP Systems](#)

[Managing Autoupdates](#)

[How Automatic Update Works](#)

For additional information, see the autoupdate white paper in the same download location as the VPN Client Update files on www.cisco.com.

Enabling Client Update (All Client Types)

To update VPN Client software, you must enable Client Update on the VPN Concentrator. When you enable Client Update, you notify VPN Client users that it is time to update the VPN Client software on their remote systems. The notification includes a location containing the update package (the update does not happen automatically).



Note

Each update folder on the web server must contain only one version package from Cisco. If you need more than one version, configure more groups on the VPN Concentrator to update from different web server folders.

Use the Client Update procedure at the VPN 3000 Concentrator to configure a client notification:

-
- Step 1** To enable Client Update, go to Configuration | System | Client Update and click **Enable**.
 - Step 2** At the Configuration | System | Client Update | Enable screen, check **Enabled** (the default) and then click **Apply**.
 - Step 3** On the Configuration | System | Client Update | screen, click **Entries**.

Step 4 On the Entries screen, click **Add**. The VPN Concentrator Manager, displays the Configuration | System | Client Update | Entries | Add or Modify screen.

Step 5 For Client Type, enter the operating systems to notify:

- Windows includes all Windows based platforms.
- Win9X includes Windows 95, Windows 98, and Windows ME platforms.
- WinNT includes Windows NT 4.0, Windows 2000, Windows XP, and Windows Vista platforms.
- Linux.
- Solaris.
- Mac OS X.



Note The VPN 3000 Concentrator sends a separate notification message for each entry in a Client Update list. Therefore your client update entries must not overlap. For example, the value Windows includes all Windows platforms, and the value WinNT includes Windows NT 4.0, Windows 2000 and Windows XP platforms. So you would not include both Windows *and* WinNT. To find out the client types and version information, click on the lock icon at the top left corner of the Cisco Systems VPN Client main window and choose **About VPN Client**.

Step 6 In the URL field, enter the URL that contains the notification.

To activate the Launch button on the VPN Client Notification, the message must include the protocol HTTP or HTTPS and the server address of the site that contains the update. The message can also include the directory and filename of the update, for example, <http://www.oz.org/upgrades/clientupdate>. If you do not want to activate the Launch button for the remote user, you do not need to include a protocol in the message.

Step 7 In the Revisions field, enter a comma separated list of client revisions that do not need the update because they are already using the latest software. For example, the value 4.0 (Rel) , 4 . 0 . 3 identifies the releases that are compliant; all other VPN Clients need to upgrade.

Step 8 Click **Add**.

The Notification dialog box appears when the remote user first connects to the VPN device or when the user clicks the Notifications button on the Connection Status dialog box. When the notification pops up, on the VPN Client, click **Launch** on the Notification dialog box to open a default browser and access the URL containing the update.

Updating the VPN Client Software Automatically on Windows 2000 and Windows XP Systems

The VPN Client for Windows 2000 and Windows XP software can securely download updates and new versions automatically through a tunnel from a VPN 3000 Concentrator or other VPN server that can provide notifications.

With this feature, called *autoupdate*, users do not need to uninstall an old version of the software, reboot, install the new version, and then reboot again. Instead, an administrator makes updates and profiles available on a web server and when a remote user starts up the VPN Client, the software detects that a download is available and automatically gets it.

If a new version requires reboots (during a major upgrade), the remote user has to reboot only twice, when the program uninstalls the old version and when download completes. If the new version does not require a reboot, as in a minor update, autoupdate notifies users that they do not need to reboot. Also, if a user interrupts the download by disconnecting the VPN Client and then later reconnects, the download resumes at the point where it was interrupted.

Managing Autoupdates

This section explains the manager tasks needed to automatically update VPN Client software. Generally, an administrator is responsible for performing the following tasks:

- Setting up a web server to contain the download packages, called the *update server*. The packages contain update-x.x.xx.xxxx-minor/major-K9 files, provided by Cisco Systems. This procedure outline assumes that you already know how to set up web servers and does not include instructions for doing so.
- Enabling the VPN Concentrator to perform autoupdates.
- Obtaining the latest version package from Cisco.
- Creating the profile bundle—a package containing new or revised profiles (.pcf files) (optional).
- Changing the version information file (new_update_config.ini) (optional).
- Creating oem zip packages and enter the names of these packages into the new_update_config.ini file (optional).



Note

VPN Client automatic updating does not support Windows Vista.

Prerequisite

Remote users must have the VPN Client for Windows 4.6 or greater installed on their PCs to use the automatic update feature.

Enabling Client Update for Automatic Updates

The procedure for configuring Client Update on the VPN Concentrator for automatic updating VPN Client software is a subset of the notification feature described in the section “[Enabling Client Update \(All Client Types\)](#).” For detailed information about how to configure Client Update, you should read the Client Update section of *Cisco VPN 3000 Series Concentrator Reference, Vol. I: Configuration*.

For information about how to configure Client Update on a Cisco ASA Series 5500 Adaptive Security Appliance using ASDM, see [Configuring Client Software Update Using ASDM, page 2-13](#). To use the command-line interface to do this, see [Configuring Client Software Update Using ASDM, page 3-9](#).

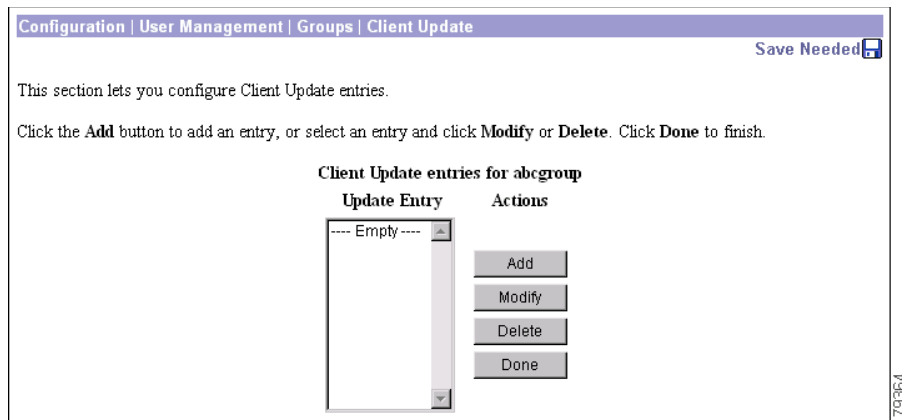
To enable Client Update on the VPN 3000 Series Concentrator, use the procedure in the section “[Enabling Client Update \(All Client Types\)](#).”

You may want to create a group especially for autoupdate; use the following procedure.

-
- Step 1** To enable Client Update at the VPN group level, go to Configuration | User Management | Groups.

- Step 2** To add a new group especially for automatic updates, click **Add** and enter the name of the group. Then click **Apply**. The new group appears in the Current list. Now you can select the group and modify it for Client Update.
- Step 3** Next too modify a group in the Current list for Client Update, select the group and click **Client Update**. The manager displays the Client Update screen.

Figure 6-1 VPN Concentrator Client Update Screen



- Step 4** When you get to the Client Update | Entries | Add or Modify screen, enter information into the fields as follows:
- Enter the Client Type information. Since autoupdate runs only on Windows 2000 and Windows XP, all other client types update manually. So for example, enter WinNT. This choice automatically updates Windows 2000 and Windows XP users, while Windows NT users get notified and can get an update manually from the update server.
 - In the URL field, enter the URL of the update server that contains the update download package and the notification. The URL must contain **http://**; for example, http://update_server_engineering.
 - Enter the revision for this autoupdate; for example, update-4.6.
- Step 5** Click **Add** or **Apply**.

When the VPN Client software gets the notification, it launches the autoupdate program and gives it the location from which to download the updated version and profiles (if there are any).

Getting the Updated Software from Cisco Systems

The installation package that the VPN Client software downloads from the update server can be either a completely new release (a full install) or an update. A new (major) release has a name in the form update-x.x.xx.xxxx-major-K9.zip and a minor release has a name in the form update-x.x.xx.xxxx.-minor-K9.zip. You can download the latest VPN Client software from the following location:

<http://www.cisco.com/cgi-bin/tablebuild.pl/updates>

Each full release of the VPN Client for Windows software requires the following objects:

- `vpnclient-win-msi-x.x.int_x-k9.exe`—the Microsoft installation file; for example, `vpnclient-win-msi-5.0.04.0300-k9.exe` or `vpnclient-win-msi-5.0.4rel-k9.exe`—VPN Client Software for 2000/XP/Vista - Microsoft Installer, or `vpnclient-win-msi-5.0.04.0300-k9-jp_wohelp.exe`—Japanese VPN Client Software for 2000/XP/Vista without online help - Microsoft Installer.
- `update-5.0.04.0300-major-K9.zip`—Windows AutoUpdate Component Zip File.
- ReadMe File for 5.0.04.0300.
- `sig.dat`—a signature file containing a signature of `binary.zip` and the MSI installation file. This file is used for the verification process to ensure that these files have not been tampered with. When autoupdate finishes downloading the update, it deletes this file.
- `binary_config.ini`—a configuration file listing the version available on the update server. Autoupdate uses this file to determine whether it needs to go get the update. If the last major version number (for example, 5.0.4.0300) in this file is greater than the current version, autoupdate downloads a full install. If not, then autoupdate looks at the version field. If the version number is greater than the current version (for example, 4.6.1.1) on the PC, autoupdate downloads an update. In any case, after autoupdate finishes downloading the update package, it deletes this file.
- `new_update_config.ini`—this optional configuration file is used by the autoupdate program to determine what custom settings to download. An administrator who is adding profiles and oem packages to an update must enter the names of the files that contain new or updated profiles and oem packages into this file. Once autoupdate has completed the update, this file becomes `update_config.ini` on the user's system.

Of these objects, an administrator is responsible only for updating the `new_update_config.ini` file when distributing new or updated profiles. You must not modify the other files in the package. Cisco supplies these files and they are secured by the signature in the `sig.dat` file.

Creating the New Update Configuration File

When distributing new or modified profiles, the administrator must enter information into the `new_update_config.ini` file. This file has the same structure as a standard configuration file (see “[File Format for All Profile Files](#)” section on page 5-2). Following is a sample `new_update_config.ini` file.

```
[Update]
Version=1
FileName=profiles.zip
MaxSize=7000

[Oem]
FileName=oem.zip
MaxSize=10000

[Transform]
Filename=transform.zip
MaxSize=12000

[Autoupdate]
Required=1
```

`new_update_config.ini` File Keywords and Values

Table 6-1 describes each part of the `new_update_config.ini` file.

Table 6-1 *new_update_config.ini* File Parameters

| Keyword | Description | Value |
|--------------|--|---|
| [Update] | Required keyword to identify update information. | Keep exactly as shown. |
| Version= | Version number of the update package. The administrator can use this parameter to track updates by incrementing the value each time there is a new version of this file. | Enter a value 0 or greater. |
| Filename= | Name of the zip file containing profiles to update or install | Enter the filename (string.zip) Example: newprofile.zip |
| MaxSize= | Size in bytes of the profile file plus 5000 bytes. This places a limit on how large the file can be. | Enter the size of the file plus 5000 bytes. Example: 10000 |
| MaxSize= | Size in bytes of the oem file plus 5000 bytes. This places a limit on how large the file can be. | Enter the size of the file plus 5000 bytes. Example: 12000 |
| [Transform] | Optional keyword to identify oem information for MSI installation. | Keep exactly as shown. |
| FileName= | Name of the zip file containing transform information to update or install an update to the MSI installation program. | Enter the filename (string.zip). Example: newtransform.zip |
| MaxSize | Size in bytes of the transform file plus 5000 bytes. This places a limit on how large the file can be. | Enter the size of the file plus 5000 bytes. Example: 14000 |
| [Autoupdate] | Keyword to identify the autoupdate section. | Keep exactly as shown. |
| Required= | Indicates whether the update or profile update is required. | Enter either 0 or 1. 0 = not required 1 = required |

**Note**

The transform within the zip file for modifying an MSI installation must be named oem.mst.

Creating the Profile Distribution Package

To automatically distribute new or updated profiles, use the following procedure:

- Step 1** Create the new profile files or modify your current profile files. For information on how to create and modify individual profiles (.pcf files), see [Creating Connection Profiles, page 5-23](#).
- Step 2** Create a zip file containing the updated profiles; for example, name it profiles.zip.

- Step 3** Enter the name of this .zip file into the new_update_config.ini file and increment the version number under the [Update] section of this file.



Note Although you do not need to update the VPN Client to update the profiles, the update server must also contain all of the required Cisco distributed update files for the VPN Client to accept the new profiles.

- Step 4** Copy the new_update_config.ini and the zip file containing the new profiles onto the update server.

How Automatic Update Works

This section provides information for administrators that want to understand more about how this feature works. This is a high-level overview of the autoupdate feature.

The automatic update feature (*autoupdate*) comprises three processes:

- autoupdate.exe—detects that an update package is on the update server and goes out and retrieves it
- autoinstall.exe—installs the update package
- autoupdategui.exe—handles notifications to the remote user and user responses to notifications

This is what happens:

- A remote user starts up the VPN Client and establishes a tunnel
- The VPN Client software gets the URL of the site containing the update package
- The VPN Client software starts the autoupdate.exe program and gives it the URL for the update package
- Autoupdate determines if an update is necessary by comparing the version information to the one that exists on the VPN Client PC.
- If the update package is later than the one on the PC, autoupdate downloads the update package.
- Autoupdate then lets the remote user know that the update package is available
- The remote user accepts or rejects the update package
- If the remote user accepts the update package, autoupdate verifies the integrity of the update
- Autoupdate unzips the update package then installs it
- If there are any errors, autoupdate or autoinstall logs them in the autoupdate.log and autoinstall.log files found in the Updates folder of the VPN Client folder.

