

VPN Client Auto-Update Feature with VPN 3000 Concentrator Configuration Example

Document ID: 100248

Introduction

Prerequisites

Requirements

Components Used

Conventions

Configure the VPN Client Auto-Update Feature

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document describes how to configure the Cisco VPN Client auto-update feature in the Cisco VPN 3000 Concentrator with Update Server.

Note: These auto-update features are not supported on the Cisco Routers and Cisco Security Appliances (PIX/ASA).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Cisco VPN Client version 4.6 and later.

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

Conventions

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

Configure the VPN Client Auto-Update Feature

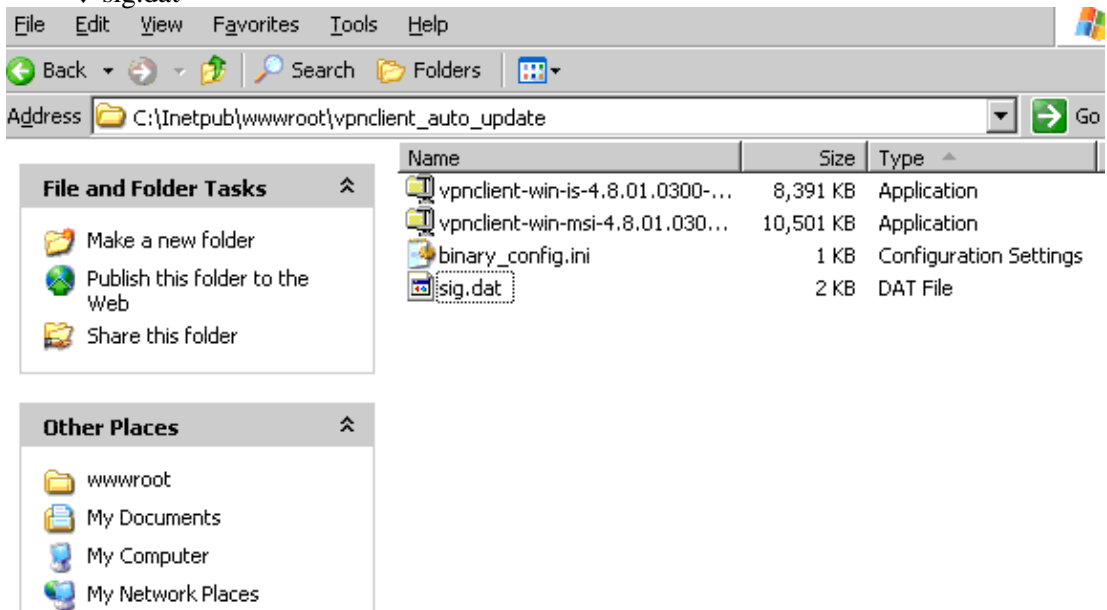
1. Download the update package to a folder on your Update Server.

You can download the update package from the Cisco software download page (registered customers only) . The package contains these files:

- ◆ vpnclient-win-is-<version>-k9.exe For the Installshield.
- ◆ vpnclient-win-msi-<version>-k9.exe For the MSI install.

◆ binary_config.ini

◆ sig.dat



Note: Refer to Getting the Updated Software from Cisco Systems for more information on various objects.

2. Create a text file that contains this text:

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

[Oem]
FileName=oem.zip
MaxSize=10000

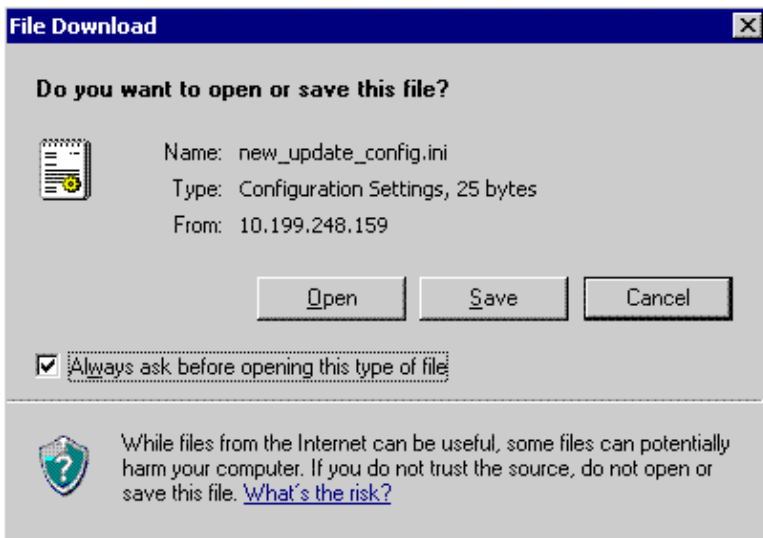
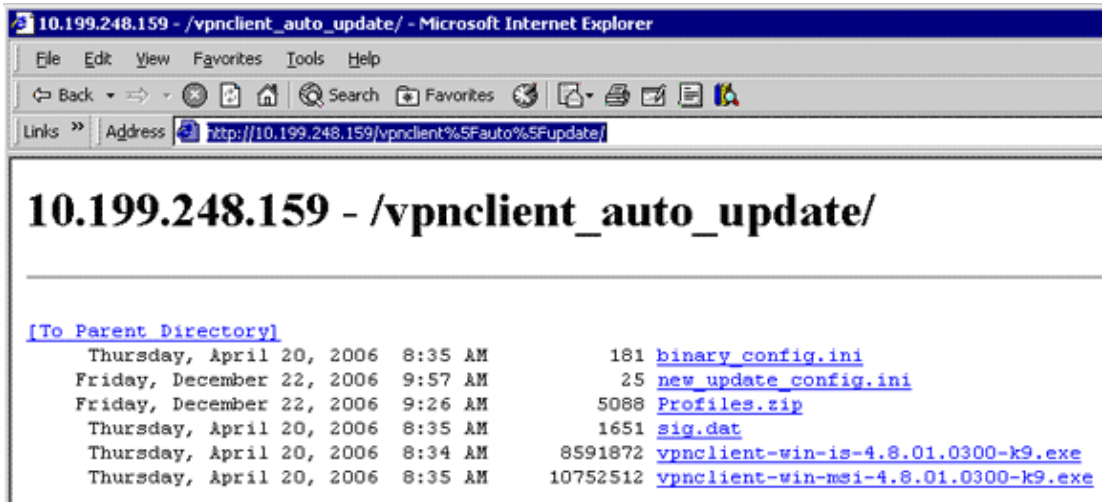
[Transform]
Filename=transform.zip
MaxSize=12000

[Autoupdate]
Required=1
```

Refer to Creating the New Update Configuration File for more information about the values in this file.

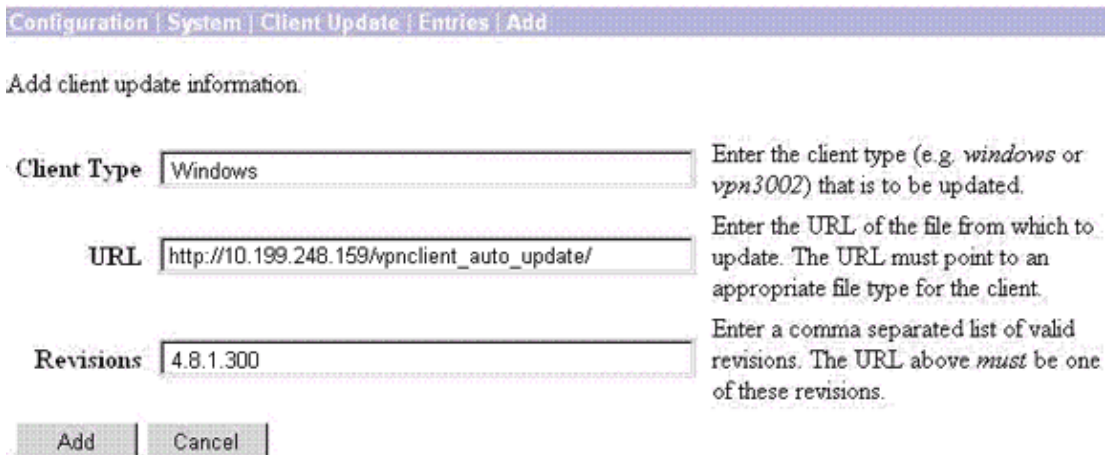
3. Name the file *new_update_config.ini*, and save it to the same web folder.
4. Create a profiles.zip folder where all the updated PCF files are stored. Refer to Creating the Profile Distribution Package for more information.
5. Make sure that the web folder is accessible by the VPN Client when it is connected to the VPN server.

In order to test this accessibility, connect the VPN Client, open a web browser, and explore the URL where the auto-update files are located. Make sure that all files can be downloaded. If you are unable to access the web folder or download a file, you must configure the MIME settings (or equivalent) and appropriate permissions for your web or update server. If you are unable to configure this, contact technical support for your web server for further assistance.



6. On the VPN Concentrator, go to **Configuration > System > Client Update > Entries**, and add this client update information:

- ◆ **Client Type** = Windows
- ◆ **URL** = http://10.199.248.159/vpnclient_auto_update/ (for example)
- ◆ **Revisions** = 4.8.1.300



7. Go to **Configuration > System > Client Update > Enable**, and check the **Enable** check box in order to enable the Client Update feature.

Check the box to enable Client Update functionality.

Enabled

8. Click **Add** or **Apply**.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for VPN
Service Providers: VPN Service Architectures
Service Providers: Network Management
Virtual Private Networks: General

Related Information

- [Cisco VPN Client Support Page](#)
- [IPSec Negotiation/IKE Protocols](#)
- [Cisco VPN 3002 Hardware Clients](#)
- [Cisco VPN 3000 Series Concentrators](#)
- [Cisco VPN 3000 Series Concentrator Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Dec 11, 2007

Document ID: 100248