

Upgrading the VPN 3002 Hardware Client from a VPN 3000 Series Concentrator

Document ID: 14098

Introduction

Prerequisites

- Requirements
- Components Used
- Network Diagram
- Conventions

Configure the Headend for the VPN 3002 Hardware Client Upgrade

Verify

Troubleshoot

- Troubleshoot Procedure

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

Note: The Cisco VPN 3000 Concentrator Series includes the VPN 3005, 3015, 3030, 3060, and 3080. It does not include the VPN 3002 Hardware Client.

The VPN 3002 Hardware Client software can be upgraded through a push from a headend Cisco VPN 3000 series concentrator, rather than upgrading it manually from the VPN 3002 Hardware Client GUI. This works well in large environments where multiple VPN 3002 Hardware Clients are used. Because only one change needs to be made on the headend VPN 3000 Series Concentrator, rather than visiting each VPN 3002 Hardware Client individually.

The VPN 3002 Hardware Client is notified of the pending software upgrade through an Internet Security Association and Key Management Protocol (ISAKMP) message upon connecting back to the headend. The message contains the TFTP server address. This holds the software and the filename it should use.

Currently only the VPN 3002 Hardware Client is upgraded automatically. The client type is defined in the VPN 3000 series as **vpn3002** without adding any extra characters to this type.

When you configure the headend VPN 3000 Concentrator, you need the revision level of the software that is loaded in the VPN 3002 Hardware Client. This information is found between the two dashes in the file name.

For example, if the file name is **vpn3002-3.0.3.A-k9.bin**, then the revision (the part between the two dashes) is "3.0.3.A".

Note: Failure to properly set the revision level causes the VPN 3002 Hardware Client to go into an infinite upgrade loop.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

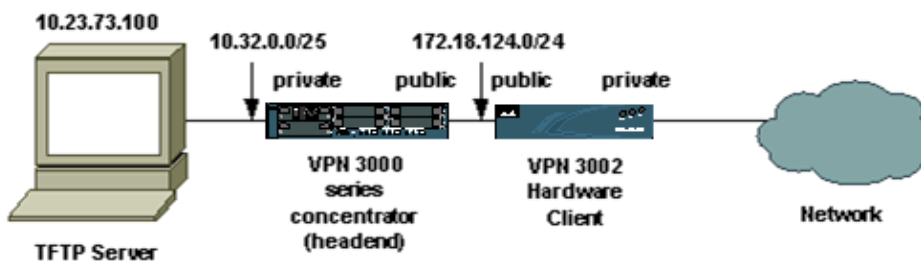
The information in this document is based on these software and hardware versions:

- Cisco VPN 3000 Series Concentrator (headend)
- Cisco VPN 3000 Series Concentrator software 3.0.3.A
- Cisco VPN 3002 Hardware Client

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.

Network Diagram

This document uses this network setup:



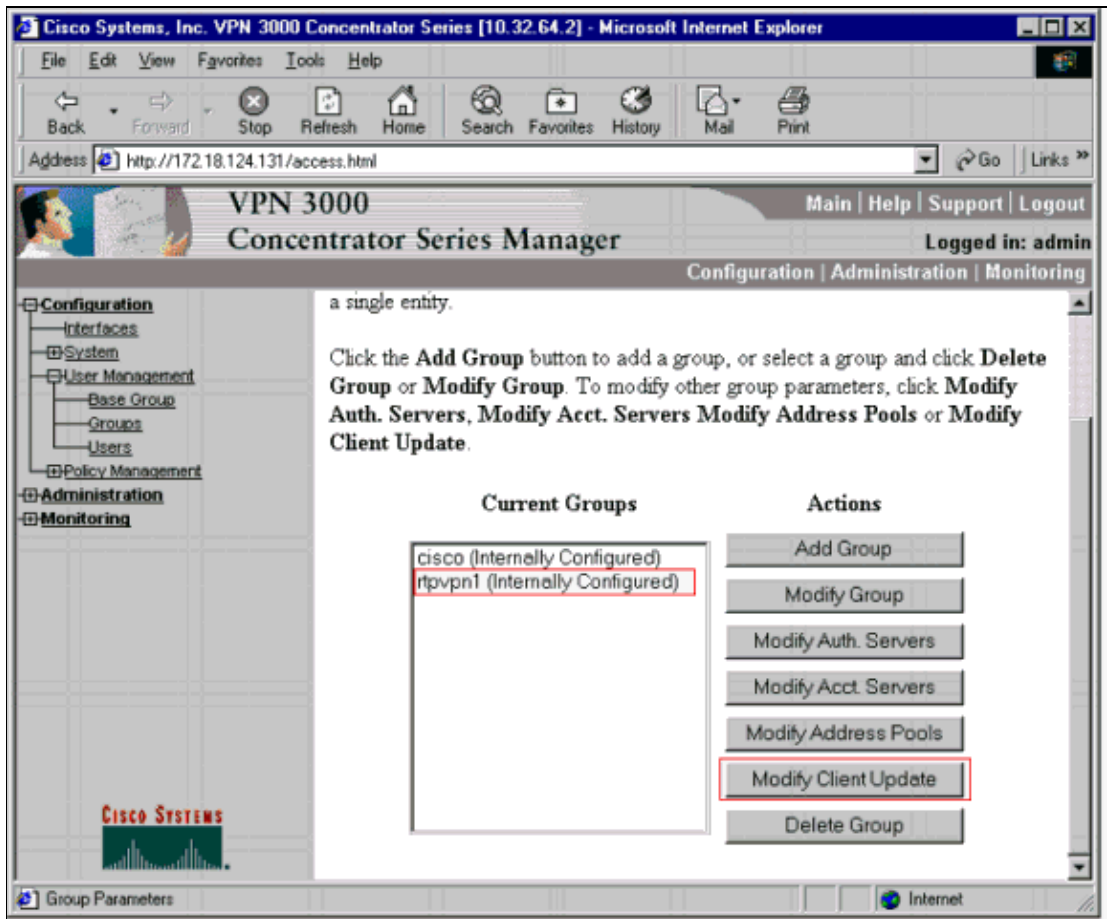
Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Configure the Headend for the VPN 3002 Hardware Client Upgrade

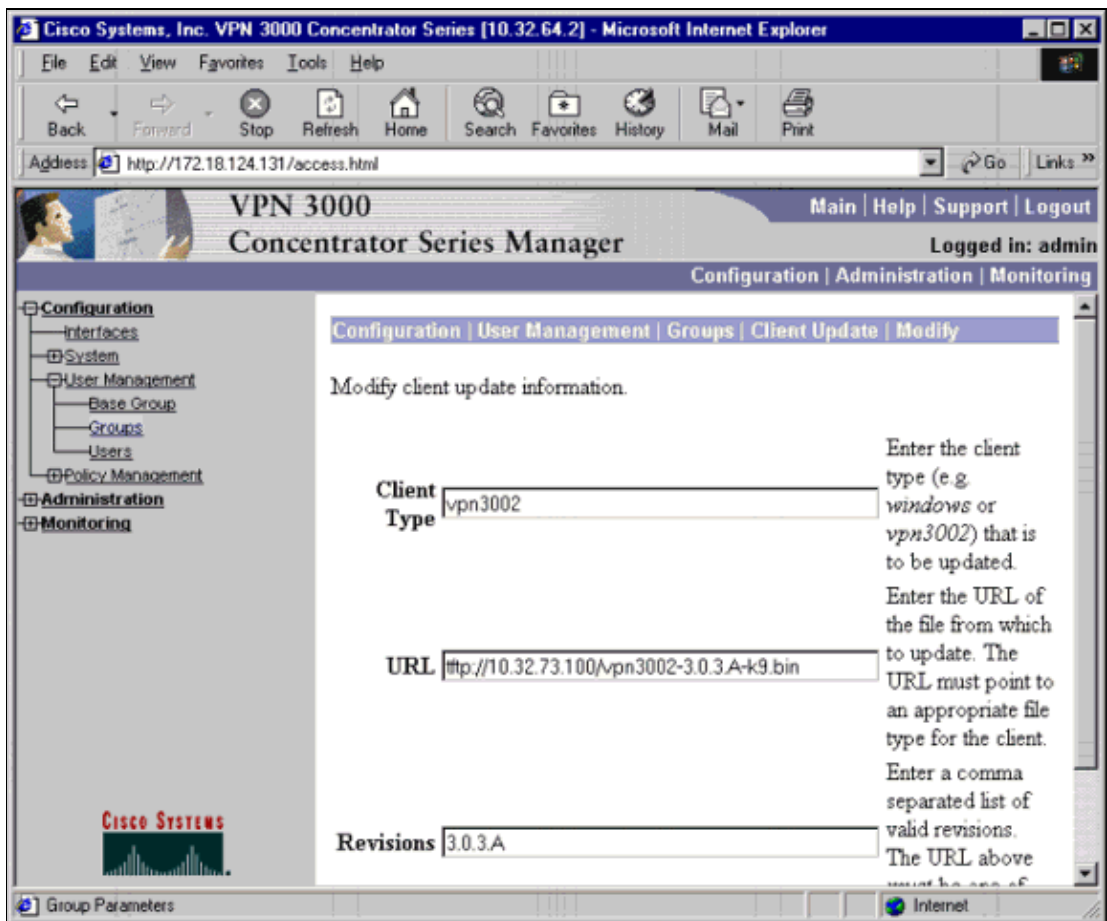
In this example, the VPN 3002 Hardware Client connects with the **rtpvpn1** group with a pool of 10.32.73.1–10.

1. Go to **Configuration > User Management > Groups**. Select **rtpvpn1 (Internally Configured)**.
2. Choose **Modify Client Update**.

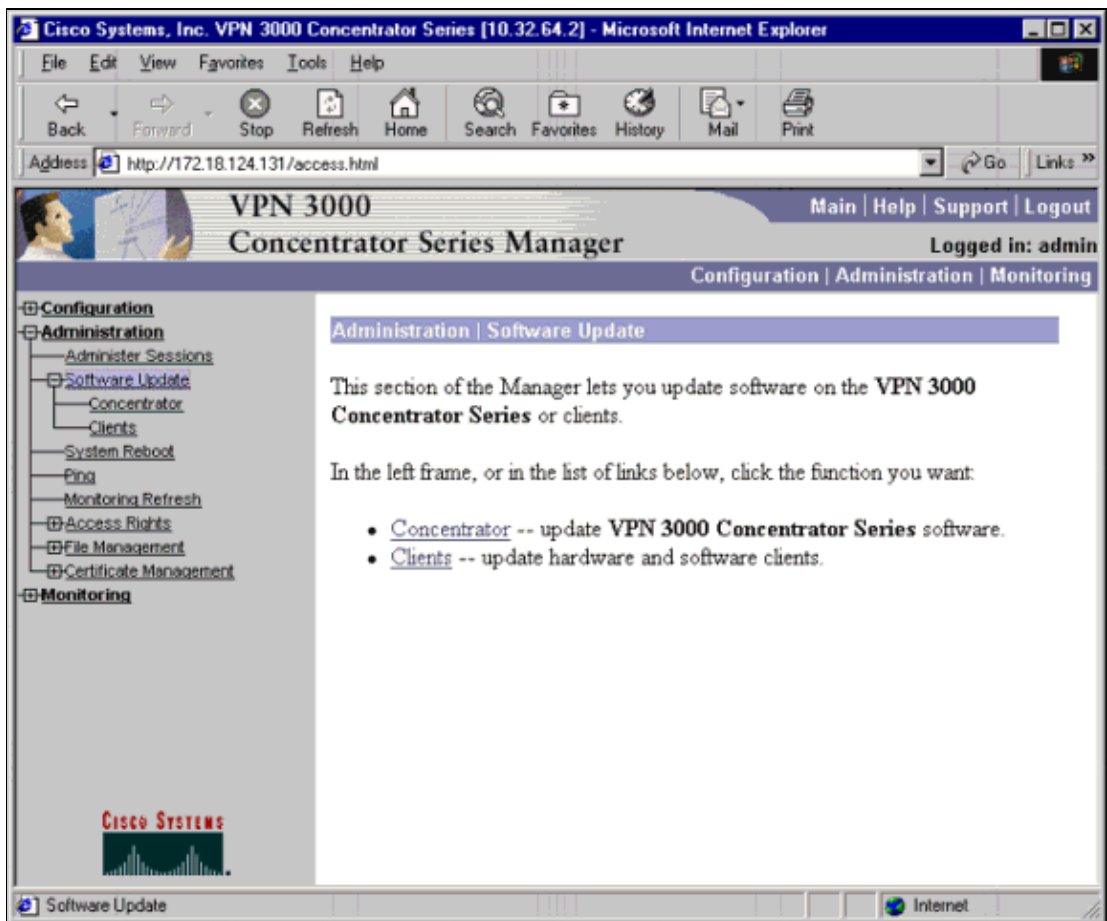


3. In the Client Update screen, choose **Add** to add a new client package.
4. On the next screen, enter **vpn3002** as the client type. Enter **tftp://{IP address of server}/{filename}** as the URL. Enter **3.0.3.A** as the revision.

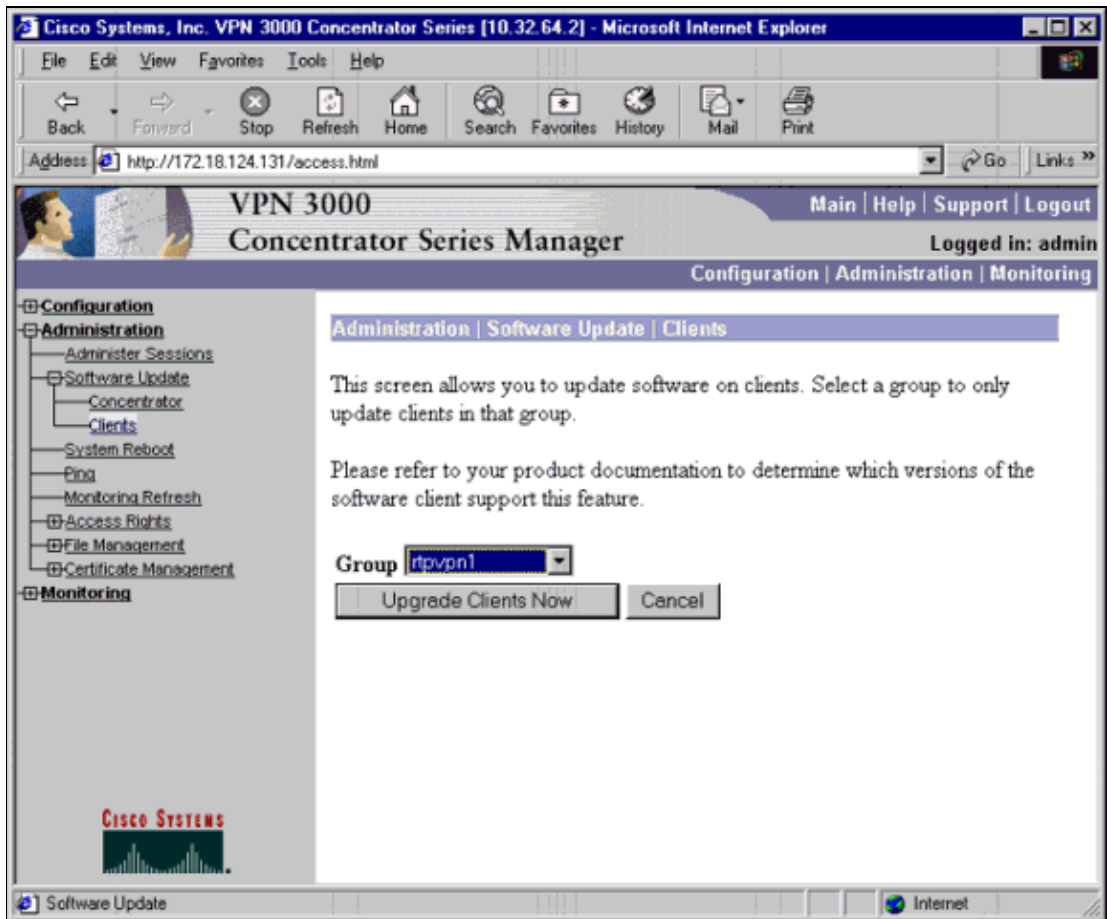
Note: The client type can *only* be **vpn3002**. The TFTP server *must* reside behind the VPN 3000 Concentrator. The VPN 3002 Hardware Client needs to use the VPN tunnel back to the headend concentrator in order to obtain the OS image file through TFTP. The TFTP server IP address *cannot* be the outside network of the public interface, or routed in such a way that it needs to pull the image through the outside interface without encryption.



5. Select **Apply**.
6. Notify the VPN 3002 Hardware Client about the upgrade by selecting **Administration > Software Update > Clients**.



7. Select the group. In this example, the group is **rtvpn1**.



8. Select **Upgrade Client Now**.
9. When the upgrade works, the VPN 3002 Hardware Client web interface shows that the new software is loaded. Check this by selecting **Administration > Software Update**.

Verify

There is currently no verification procedure available for this configuration.

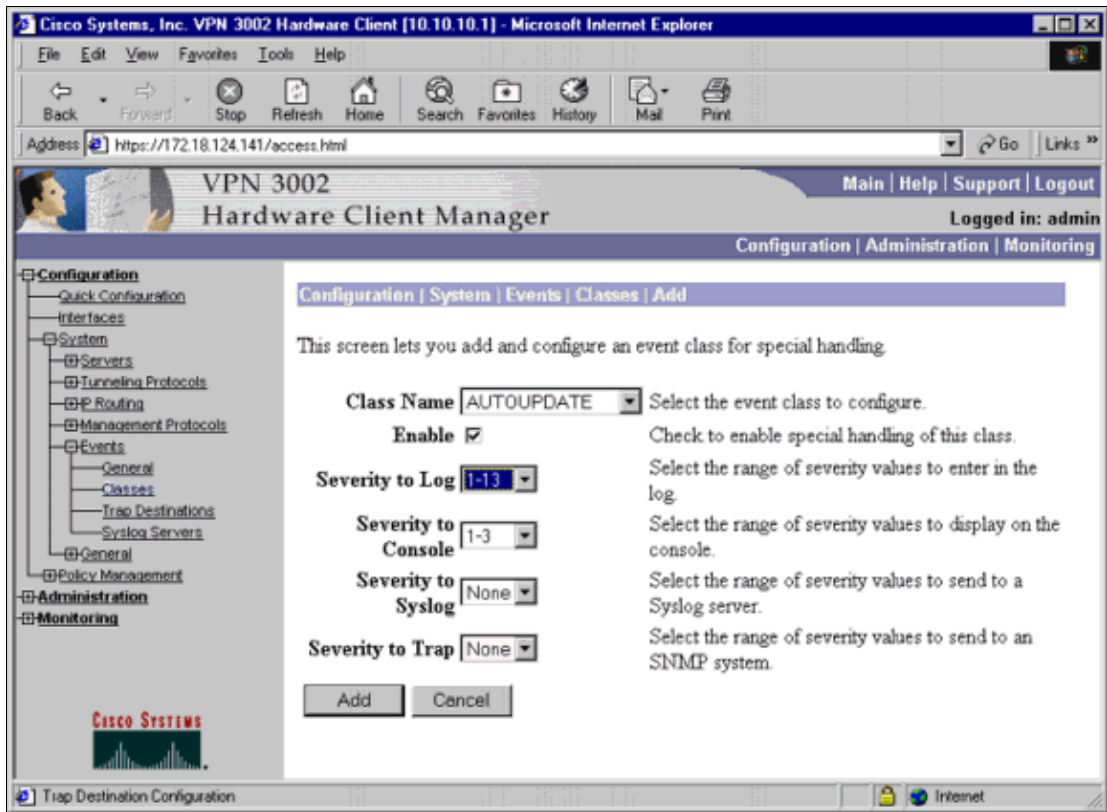
Troubleshoot

This section provides the information to troubleshoot your configuration.

Troubleshoot Procedure

If the upgrade does not work, debug should be added to the VPN 3002 Hardware Client.

1. Add the debug by selecting **Configuration > System > Events > Classes**. Add these settings.
 - ◆ Class Name: **AUTOUPDATE**
 - ◆ Severity to Log: **1-13**
 - ◆ Severity to Console: **1-3**



2. Retrieve the VPN 3002 Hardware Client event log by selecting **Monitoring > Event Log**.

On a successful upgrade, the event log shows this:

At the time of the upgrade:

```

52 06/15/2001 10:13:17.230 SEV=4 AUTOUPDATE/6 RPT=1
    Current version 3.0.2 does not match 3.0.3.A
53 06/15/2001 10:13:17.230 SEV=4 AUTOUPDATE/7 RPT=1
    Updating firmware to 3.0.3.A from 3.0.2
54 06/15/2001 10:13:17.230 SEV=4 AUTOUPDATE/12 RPT=1
    Update firmware will now begin using file
    vpn3002-3.0.3.A-k9.bin on server 10.32 .73.100 [0A204964]

```

After the upgrade

```

34 06/15/2001 10:10:00.900 SEV=4 AUTOUPDATE/5 RPT=1
    Current version 3.0.3.A is up to date

```

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 3000 Series Concentrator Support Page](#)
 - [Cisco VPN 3000 Series Client Support Page](#)
 - [IPSec Support Page](#)
 - [Technical Support – Cisco Systems](#)
-

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

Updated: Jul 24, 2007

Document ID: 14098
