download cisco 3845 ios

ROMmon Recovery for the Cisco 3600/3700/3800 Series Routers.

This page explains how to recover a Cisco 3600/3700/3800 Series Router stuck in ROMmon, rommon# > prompt.

Prerequisites.

Requirements.

There are no specific prerequisites for this document.

Components Used.

This document is not restricted to specific software and hardware versions.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Conventions.

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

Look for a Valid Image in Flash.

First issue the dev command in order to see which devices are available on your router:

Next, issue the dir [device ID] command for each Flash or PCMCIA device available, and then look for a valid Cisco IOS ® software image:

Try to boot from that image. If the file is valid, this brings you back to normal operation mode:

If none of the files are valid, you have to download a new one that uses one of these procedures:

Use Another Router to Get a Valid Cisco IOS Software Image into the PCMCIA Card.

In the event that you have a similar router, or at least one other router which has a compatible PCMCIA Flash card filesystem, you can also use that Flash card in order to recover the router. Refer to PCMCIA Filesystem Compatibility Matrix and Filesystem Information for more information.

If both routers are identical, or same series, you can use the Flash card from the other router in order to boot the one you want to recover.

3600/3700/3800 series routers run their Cisco IOS software from dynamic RAM (DRAM), so you can remove a PCMCIA card while the router runs.

If both routers are different but have a compatible PCMCIA Flash card filesystem, you can use the other router to load a Cisco IOS Software image into a Flash card, which you can then move to the router you try to recover.

From the router that works, copy the image into the PCMCIA card.

Insert the PCMCIA card into the router in ROMmon mode and issue the boot command:

Once the router is up and runs you can copy the image to Flash and set the boot variable so that the router boots through this new image everytime it is rebooted.

Note: Refer to Software Upgrade Procedure for more information.

Download Using Xmodem from ROMmon.

You can also download a new Cisco IOS Software through the console port through the use of Xmodem. Refer to Xmodem Console Download Procedure Using ROMmon for more information.

Download Using tftpdnld ROMmon command (Cisco 3800 only)

You can also download the Cisco IOS software when you use the tftpdnld command from TFTP server when the router is in ROMmon mode. This procedure is explained in detail in How to Download a Software Image via TFTP Using the tftpdnld ROMMON Command.

VPN AIM for the Cisco 1841, 2800 and 3800 Series Integrated Services Routers.

The VPN Advanced Integration Module (AIM) for the Cisco ® 1841 Integrated Services Router and Cisco 2800 and 3800 Series Integrated Services Routers optimizes the Cisco Integrated Services Router platforms for virtual private networks in both IP Security (IPSec) and Secure Sockets Layer (SSL) Web and VPN deployments.

Figure 1. Integrated Services Router with the "AIM-VPN/SSL" Module.

Table 1. Supported Modules and Features, by Platform.

Module Part Numbers.

Cisco 2801, 2811, 2821, 2851.

AES and Triple Data Encryption Standard (3DES)

WebVPN SSL Encryption.

IPv6 Cryptography in Hardware.

Table 2. Supported Features of Cisco IPsec and SSL VPN AIM.

The Cisco IPsec and SSL VPN AIM fits in any open AIM slot in the Cisco Integrated Services Router.

The Cisco IPsec and SSL VPN AIM supports the Cisco 1841 and the Cisco 2800, 3700, and 3800 Series.

An AIM slot for the Cisco 1841 and the Cisco 2800, 3700, and 3800 Series is required.

IPSec Encryption Supported.

All modules support IPSec DES and 3DES; Authentication: Rivest, Shamir, and Adelman (RSA) and Diffie Hellman; data integrity: Secure Hash Algorithm 1 (SHA-1) and Message Digest Algorithm 5 (MD5); and DES, 3DES, and AES key sizes: AES128, AES192, and AES256.

Hardware SSL Encryption Supported.

Only the Cisco IPsec and SSL VPN AIM in the Cisco 1841 and the Cisco 2800, 3700, and 3800 Series supports SSL VPN encryption.

IPSec Hardware-Based Compression.

The Cisco IPsec and SSL VPN AIM uses Layer 3 IPPCP compression.

The Cisco IPsec and SSL VPN AIM uses the Cisco IOS Software with the Advanced Security, Advanced IP, or Advanced Enterprise feature set.

Number of Encryption Modules per Router.

The Cisco IPsec and SSL VPN AIM uses one encryption module per router.

Minimum Cisco IOS Software Version Required.

The Cisco IPsec and SSL VPN AIM requires Cisco IOS Software Version 12.4(9)T or higher.

Maximum Number of IPSec Encrypted Tunnels.

The Cisco IPsec and SSL VPN AIM supports up to 800 tunnels on the Cisco 1841, up to 1500 tunnels on the Cisco 2800 Series, and up to 2000 tunnels on the Cisco 3800 Series. The Maximum Tunnel Scalability test is done with no data passing over the tunnels to only determine maximum number. For site-to-site design, Cisco recommends you consult with your Cisco account team or a Cisco authorized reseller and also review the Cisco DMVPN Design Guide at:
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a008075ea98.pdf.

Maximum Number of Cisco IOS WebVPN SSL VPN Users with VPN and SSL AIM.

Only the Cisco IPsec and SSL VPN AIM supports Cisco IOS SSL VPN. On the Cisco 1841 and 2801, it supports 50 users; on the Cisco 2811 and 2821, it supports 100 users; on the Cisco 2851, it supports 150 users; on the Cisco 3725 and 3745, it supports 150 users; and on the Cisco 3825 and 3845, it supports 200 users. The Cisco IOS WebVPN SSL VPN requires the purchase of a user license. (All supported platforms include a two-user demo license at no additional cost.)

The Cisco IPsec and SSL VPN AIM supports the IPSec Internet Key Exchange (IKE): RFCs 2401 to 2410, 2411, and 2451.

Table 3. Features and Benefits of the Cisco IPsec and SSL VPN AIM.

High Overhead IPSec Processing from the Main Processor.

Reserves critical processing resources for other services such as routing, firewall, and voice.

Allows Cisco IPSec configuration monitoring and can be integrated into a variety of VPN management solutions.

Certificate Support to Facilitate Automatic Authentication using Digital Certificates.

Scales encryption use for large networks requiring secure connections between multiple sites.

Easy Integration of VPN Modules into Existing Cisco 1841 and Cisco 2800, 3700, and 3800 Series Routers.

Significantly reduces system costs, management complexity, and deployment effort compared to multiple-device solutions.

Confidentiality, Data Integrity, and Data Origin Authentication through IPSec.

Facilitates secure use of public switched networks and the Internet for WANs.

Cisco IOS SSL VPN.

Allows businesses to securely and transparently extend their networks to any Internet-enabled location using SSL VPN; the Cisco IOS SSL VPN supports clientless access to applications such as HTML-based intranet content, e-mail, network file shares, and Citrix and to the Cisco SSL VPN Client, enabling full network access remotely to virtually any application.

Cisco IPsec and SSL VPN AIM provides hardware support for IPSec Layer 3 IPPCP and can compress a packet before encryption. This allows for higher throughput for Wide Area Networks (WAN) links.

Cisco IPsec and SSL VPN AIM Performance.

• The Cisco 1841 Series Module (AIM-VPN/SSL-1) can provide hardware-based IPSec encryption services of 25 and 95 Mbps in the Cisco 1841 (IPSec Internet mix [IMIX] and 1400-byte packets).

• The Cisco 2800 Series Module (AIM-VPN/SSL-2) can provide hardware-based IPSec encryption services of 30 and 90 Mbps in the Cisco 2801, 35 and 100 Mbps in the Cisco 2811, 90 and 125 Mbps in the Cisco 2821, and 100 and 150 Mbps in the Cisco 2851 (IPSec IMIX and 1400-byte packets).

• The Cisco 3800 Series Module (AIM-VPN/SSL-3) can provide hardware-based IPSec encryption services of 160 and 185 Mbps in the Cisco 3825 and 190 and 210 Mbps in the Cisco 3845 (IPSec IMIX and 1400-byte packets).

• The Cisco 1841 Series Module (AIM-VPN/SSL-1) c can provide hardware-based SSL VPN encryption of 5 Mbps with a Maximum of 50 Users. 1.

• The Cisco 2800 Series Module (AIM-VPN/SSL-2) can provide hardware-based SSL VPN encryption of 5Mbps with a Max of 50 users in the Cisco 2801, 5 Mbps with a Max of 75 users in the 2811, 10 Mbps with a Max of 100 users in the Cisco 2821, and 14 Mbps with a Max of 150 users in the Cisco 2851 routers.

• The Cisco 3800 Series Module (AIM-VPN/SSL-3) can provide hardware-based SSL VPN encryption of 20 Mbps with a Max of 175 Users in the Cisco 3825, and 26 Mbps with a Max of 200 Users in the Cisco 3845 routers. 2.

• The Cisco IPsec and SSL VPN AIM offloads the SSL encryption processing, allowing improved SSL VPN performance.

• The Cisco IOS SSLVPN is the first router-based solution that offers SSL VPN remote-access connectivity integrated with security and industry-leading routing features on a converged data, voice, and wireless platform.

• SSL VPN is compelling because the security is transparent to the end user and easy for IT personnel to administer. Using only a Web browser, companies can extend their secure enterprise networks to any Internet-enabled location, including home computers, Internet kiosks, and wireless hotspots, thereby facilitating higher employee productivity and protecting corporate data while providing transient partner and consultant network access.

• Cisco IOS SSL VPN supports both clientless and full-network-access SSL VPN capabilities.

• DES, 3DES, and AES-the National Institute of Standards and Technology (NIST) created AES as a Federal Information Processing Standard (FIPS) publication to replace DES, IPSec and IKE. AES has a variable key length; the algorithm can specify a 128-bit key (default), a 192-bit key, or a 256-bit key. For details about AES, refer to http://csrc.nist.gov/encryption/aes/ .

• IPSec-this protocol uses encryption technology to provide data confidentiality, integrity, and authenticity between participating peers in a private network. Cisco provides full Encapsulating Security Payload (ESP) and authentication header support.

• IKE-Using the Internet Security Association Key Management Protocol (ISAKMP) or Oakley, IKE provides security association management. IKE authenticates each peer in an IPSec transaction, negotiates security policy, and handles the exchange of session keys.

• Certificate management-Cisco fully supports the X509.V3 certificate system for device authentication and the Simple Certificate Enrollment Protocol (SCEP), a protocol for communicating with certificate authorities. Several vendors, including Verisign, Entrust Technologies, and Microsoft, support Cisco SCEP, and their products can operate with Cisco devices.

• RSA signatures and Diffie-Hellman-RSA and Diffie-Hellman are used every time an IPSec tunnel is established to authenticate the IKE security

association. Diffie-Hellman is used to derive the shared secret encryption key for the protection of data across the IKE security association, including the negotiation of the IPSec policy to be used.

• Enhanced security-Hardware-based cryptography offers several security advantages over software-based solutions, including enhanced protection of keys.

Latest Cisco 3745 IOS image For Gns3.

IOS image is software or Operating System used in most Cisco routers and switches. IOS image support different packages like routing, switching and inter-networking etc. You can use these IOS images with GNS3. Gns3 is one of the famous network simulator and its hot feature is that it can run the real Cisco IOS image, as compare to other network simulator like packet-tracer which perform all functions base on programming. If you are beginner then learn more here:Cisco Switch Basic Configuration, how to use or configure GNS3.

Remember only the c7200 series ios images get newer IOS images. According to Cisco all other platforms are now "end of life", but you can used these older ios images as well with Gns3.

Gns3 3745 IOS image Details.

Cisco 3700 Series are the multi-service routers provide LAN/WAN connectivity, new high-density service modules, and support for multiple advanced integration modules. You can use NM-16ESW module with this 3745 IOS, which will enable the switching functionality in GNS3. In this way you will be able to perform different switching labs with GNS3 like Vlans, inter-vlan (Router on stick), VTP (vlan trunking protocol), different multi-layer functionality etc. learn more about Layer 3 Switching vs Routing.

From here you can download Cisco 3745 IOS image for your GNS3 and perform different GNS3 labs with this IOS. Remember this IOS is only for informational, practice purposes and for GNS3 used. If you need the IOS for your real hardware then it is better to Contact Cisco for latest and best IOS for your device. Following is the details and recommended setting of Gns3 3745 IOS image for your GNS3 setup. This Image was tested with Gns3 1.1 and i hope this will also work fine with the latest GNS3 version as well.

Clientless SSL VPN (WebVPN) on Cisco IOS with SDM Configuration Example.

Clientless SSL VPN (WebVPN) allows a user to securely access resources on the corporate LAN from anywhere with an SSL-enabled Web browser. The user first authenticates with a WebVPN gateway which then allows the user access to pre-configured network resources. WebVPN gateways can be configured on Cisco IOS ® routers, Cisco Adaptive Security Appliances (ASA), Cisco VPN 3000 Concentrators, and the Cisco WebVPN Services Module for the Catalyst 6500 and 7600 Routers.

Secure Socket Layer (SSL) Virtual Private Network (VPN) technology can be configured on Cisco devices in three main modes: Clientless SSL VPN (WebVPN), Thin-Client SSL VPN (Port Forwarding), and SSL VPN Client (SVC) mode. This document demonstrates the configuration of theWebVPN on Cisco IOS routers.

Note: Do not to change either the IP domain name or the host name of the router as this will trigger a regeneration of the self-signed certificate and will override the configured trustpoint. Regeneration of the self-signed certificate causes connection issues if the router has been configured for WebVPN. WebVPN ties the SSL trustpoint name to the WebVPN gateway configuration. Therefore, if a new self-signed certificate is issued, the new trustpoint name does not match the WebVPN configuration and users are unable to connect.

Note: If you run the ip https-secure server command on a WebVPN router that uses a persistent self-signed certificate, a new RSA key is generated and the certificate becomes invalid. A new trustpoint is created, which breaks SSL WebVPN. If the router that uses the persistent self-signed certificate reboots after you run the ip https-secure server command, the same issue occurs.

Refer to Thin-Client SSL VPN (WebVPN) IOS Configuration Example with SDM in order to learn more about the thin-client SSL VPN.

Refer to SSL VPN Client (SVC) on IOS with SDM Configuration Example in order to learn more about the SSL VPN Client.

SSL VPN runs on these Cisco Router platforms:

Cisco 870, 1811, 1841, 2801, 2811, 2821 and 2851 series routers.

Cisco 3725, 3745, 3825, 3845, 7200 and 7301 series routers.

Prerequisites.

Requirements.

Ensure that you meet these requirements before you attempt this configuration:

An advanced image of Cisco IOS Software Release 12.4(6)T or later.

One of the Cisco router platforms listed in the Introduction.

Components Used.

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

Cisco 3825 router.

Advanced Enterprise software image - Cisco IOS Software Release 12.4(9)T.

Cisco Router and Security Device Manager (SDM) - version 2.3.1.

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. The IP addresses used in this example are taken from RFC 1918 addresses which are private and not legal to use on the Internet.

Network Diagram.

This document uses this network setup:

Conventions.

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

Preconfiguration Tasks.

Before you begin, complete these tasks:

Configure a host name and domain name.

Configure the router for SDM. Cisco ships some routers with a preinstalled copy of SDM.

If the Cisco SDM is not already loaded on your router, you can obtain a free copy of the software from Software Download (registered customers only) . You must have a CCO account with a service contract. For detailed information on the installation and configuration of SDM, refer to Cisco Router and Security Device Manager.

Configure the correct date, time, and time zone for your router.

Configure WebVPN on Cisco IOS.

You can have more than one WebVPN gateway associated with a device. Each WebVPN gateway is linked to only one IP address on the router. You can create more than one WebVPN context for a particular WebVPN gateway. To identify individual contexts, provide each context with a unique name. One policy group can be associated with only one WebVPN context. The policy group describes which resources are available in a particular WebVPN context.

Complete these steps in order to configure WebVPN on Cisco IOS:

Step 1. Configure the WebVPN Gateway.

Complete these steps in order to configure the WebVPN Gateway:

Within the SDM application, click Configure , and then click VPN .

Expand WebVPN , and choose WebVPN Gateways .

The Add WebVPN Gateway dialog box appears.

Enter values in the Gateway Name and IP Address fields, and then check the Enable Gateway check box.

Check the Redirect HTTP Traffic check box, and then click OK .

Click Save , and then click Yes to accept the changes.

Step 2. Configure the Resources Allowed for the Policy Group.

In order to make it easier to add resources to a policy group, you can configure the resources before you create the policy group.

Complete these steps in order to configure the resources allowed for the policy group:

Click Configure , and then click VPN .

Choose WebVPN , and then click the Edit WebVPN tab.

Note: WebVPN allows you to configure access for HTTP, HTTPS, Windows file browsing through the Common Internet File System (CIFS) protocol, and Citrix.

The Add WebVPN Context dialog box appears.

Expand WebVPN Context , and choose URL Lists .

The Add URL List dialog box appears.

Enter values in the URL List Name and Heading fields.

Click Add , and choose Website .

This list contains all the HTTP and HTTPS Web servers that you want to be available for this WebVPN connection.

In order to add access for Outlook Web Access (OWA), click Add , choose E-mail , and then click OK after you have filled in all the desired fields.

In order to allow Windows file browsing through CIFS, you can designate an NetBIOS Name Service (NBNS) server and configure the appropriate shares in the Windows domain in order.

From the WebVPN Context list, choose NetBIOS Name Server Lists .

The Add NBNS Server List dialog box appears.

Enter a name for the list, and click Add .

The NBNS Server dialog box appears.

If applicable, check the Make This the Master Server check box.

Click OK , and then click OK .

Step 3. Configure the WebVPN Policy Group and Select the Resources.

Complete these steps in order to configure the WebVPN policy group and select the resources:

Click Configure , and then click VPN .

Expand WebVPN , and choose WebVPN Context .

Choose Group Policies , and click Add .

The Add Group Policy dialog box appears.

Enter a name for the new policy, and check the Make this the default group policy for context check box.

Click the Clientless tab located at the top of the dialog box.

Check the Select check box for the desired URL List.

If your customers use Citrix clients that need access to Citrix servers, check the Enable Citrix check box.

Check the Enable CIFS , Read , and Write check boxes.

Click the NBNS Server List drop-down arrow, and choose the NBNS server list that you created for Windows file browsing in Step 2.

Step 4. Configure the WebVPN Context.

In order to link the WebVPN gateway, group policy, and resources together, you must configure the WebVPN context. In order to configure the WebVPN context, complete these steps:

Choose WebVPN Context , and enter a name for the context.

Click the Associated Gateway drop-down arrow, and choose an associated gateway.

If you intend to create more than one context, enter a unique name in the Domain field to identify this context. If you leave the Domain field blank, users must access the WebVPN with https:// IPAddress . If you enter a domain name (for example, Sales), users must connect with https:// IPAddress /Sales .

Check the Enable Context check box.

In the Maximum Number of Users field, enter the maximum number of users allowed by the device license.

Click the Default Group policy drop-down arrow, and select the group policy to associate with this context.

Click OK , and then click OK .

Step 5. Configure the User Database and Authentication Method.

You can configure Clientless SSL VPN (WebVPN) sessions to authenticate with Radius, the Cisco AAA Server, or a local database. This example uses a local database.

Complete these steps in order to configure the user database and authentication method:

Click Configuration , and then click Additional Tasks .

Expand Router Access , and choose User Accounts/View .

Click the Add button.

The Add an Account dialog box appears.

Enter a user account and a password.

Click OK , and then click OK .

Click Save , and then click Yes to accept the changes.

Results.

The ASDM creates these command-line configurations:

ausnml-3825-01.

Verify.

Use this section to confirm that your configuration works properly.

Procedure.

Complete these procedures in order to confirm your configuration works properly:

Test your configuration with a user. Enter https:// WebVPN_Gateway_IP_Address into an SSL-enabled Web browser; where WebVPN_Gateway_IP_Address is the IP address of the WebVPN service. After you accept the certificate and enter a user name and password, a screen similar to this image should appear.

Check the SSL VPN session. Within the SDM application, click the Monitor button, and then click VPN Status . Expand WebVPN (All Contexts) , expand the appropriate context, and choose Users .

Check error messages. Within the SDM application, click the Monitor button, click Logging , and then click the Syslog tab.

View the running configuration for the device. Within the SDM application, click the Configure button, and then click Additional Tasks . Expand Configuration Management , and choose Config Editor .

Commands.

Several show commands are associated with WebVPN. You can execute these commands at the command-line interface (CLI) to show statistics and other information. For detailed information about show commands, refer to Verifying WebVPN Configuration.

Note: The Output Interpreter Tool (registered customers only) (OIT) supports certain show commands. Use the OIT to view an analysis of show command output.

Troubleshoot.

Use this section to troubleshoot your configuration.

Note: Do not interrupt the Copy File to Server command or navigate to a different window while the copying is in progress. Interruption of the operation can cause an incomplete file to be saved on the server.

Note: Users can upload and download the new files using the WebVPN client, but the user is not allowed to overwrite the files in the Common Internet File System (CIFS) on WebVPN using the Copy File to Server command. The user receives this message when the user attempts to replace a file on the server:

Procedure.

Complete these steps in order to troubleshoot your configuration:

Ensure clients disable pop-up blockers.

Ensure clients have cookies enabled.

Ensure clients use Netscape, Internet Explorer, Firefox, or Mozilla Web browsers.

Commands.

Several debug commands are associated with WebVPN. Refer to Using WebVPN Debug Commands for detailed information about these commands.

Note: The use of debug commands can adversely impact your Cisco device. Before you use debug commands, refer to Important Information on Debug Commands.

Internet & Network Software › cisco 2600 ios.

More information about Internet & Network Software.