

Cisco Virtual Office: Ongoing Management

Adding, Removing, and Changing a Remote Router's Configuration

Introduction

This white paper shows how Cisco® Virtual Office is managed on a day-to-day basis, from an IT administrator's perspective. The common tasks that the IT administrator will execute once Cisco Virtual Office is installed are:

1. Add new users and sites
2. Remove users and sites
3. Add data centers
4. Change/update configurations or Cisco IOS® Software for remote sites

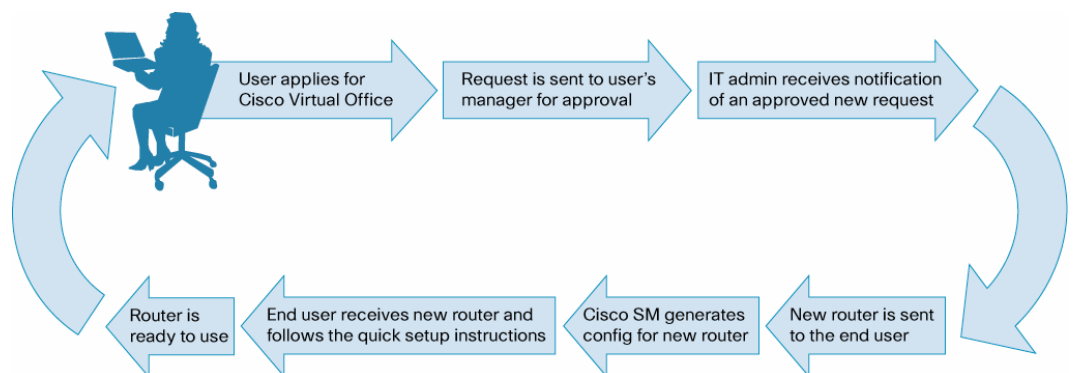
For information on how to manage the converged VPN and how to add new security features, visit <http://www.cisco.com/go/cvo> and look for "Converged VPN" and "Advanced Layered Identity."

Adding a New User or Remote Site to an Existing Cisco Virtual Office Deployment

To add a user to the VPN, you need to know the connection type and the IP address of the call manager cluster that the user is connected to.

A typical user deployment flow consists of the steps shown in Figure 1.

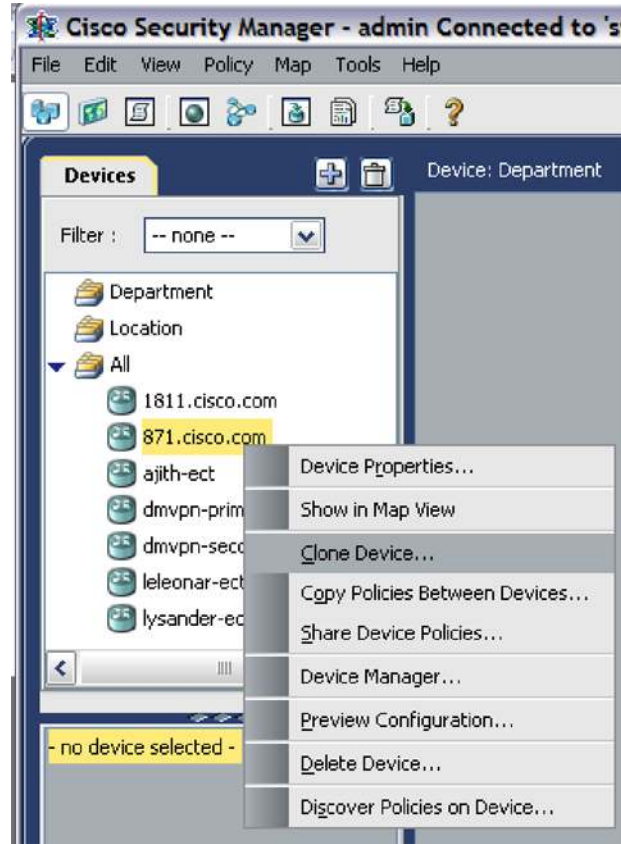
Figure 1. Steps in Adding a New User in Cisco Virtual Office



Briefly, the deployment process is as follows:

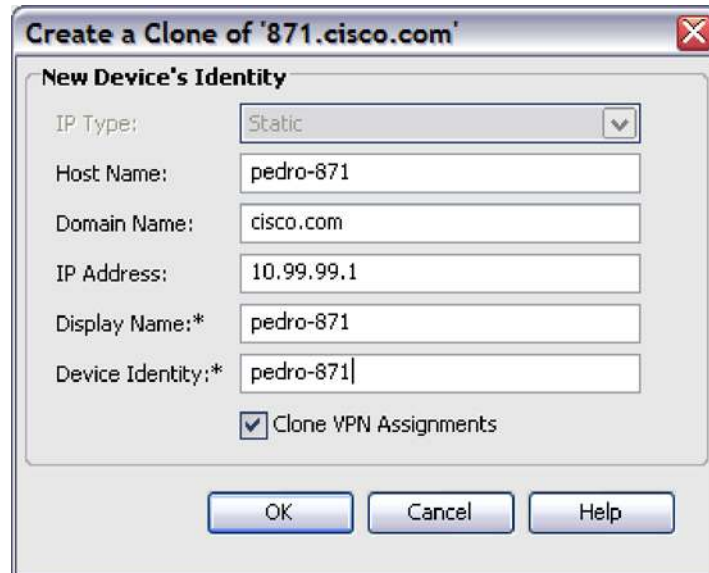
1. The user applies to the Cisco Virtual Office service and gives the admin his or her ISP information (DHCP, PPP over Ethernet, static).
2. The IT administrator receives the request, goes to Cisco Security Manager, and creates a device for the new user by cloning an existing one and keeping all the global policies (Figure 2). The administrator then makes Cisco Security Manager generate the full configuration file for the new user. Cisco Security Manager automatically stages it at the configuration engine and will be there waiting for a "Call Home" from the new Cisco 881/871/1811 Integrated Services Router (ISR).

Figure 2. Cloning a Device in Cisco Security Manager



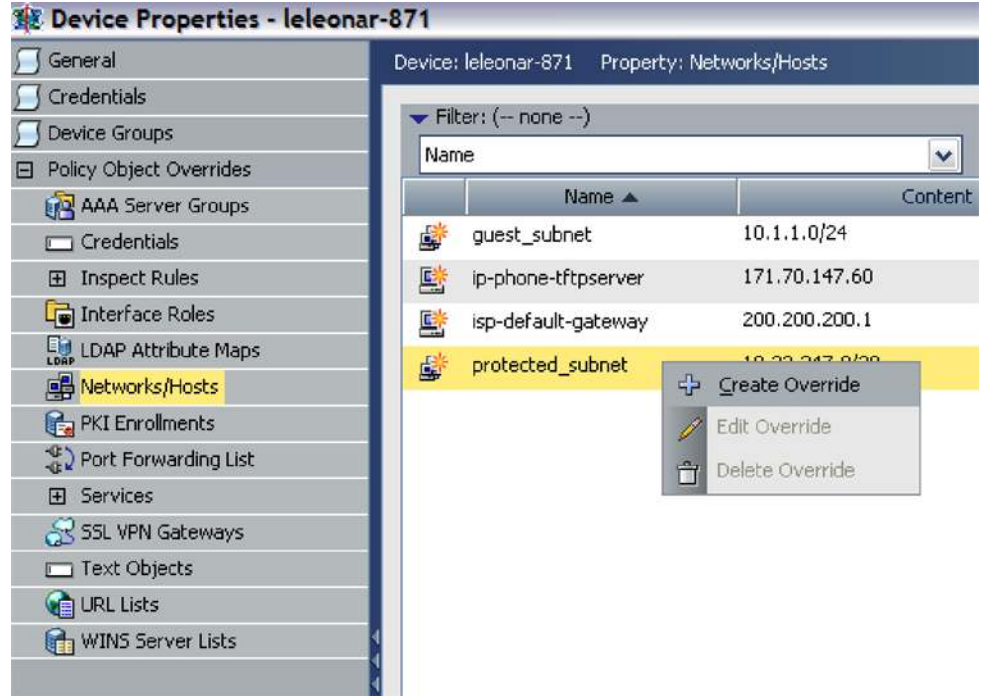
When cloning a device, enter the new host name (one that can uniquely identify the end user, such as the employee's user ID). In addition, the subnet identified by the LAN side protected IP address will be routable within the corporate network once the dynamic multipoint VPN (DMVPN) tunnel comes up. It must be unique per device (Figure 3).

Figure 3. Naming the Clone



For DMVPN spokes, edit the properties of the new device by double-clicking on the device, and add overrides for the networks that are different from the default ones. Each device needs to have its own unique subnet, which will be routable within the company network (Figure 4).

Figure 4. Creating an Override



The IT administrator also needs to add a public key infrastructure (PKI) profile for the new user in the Cisco Secure ACS authentication, authorization, and accounting (AAA) RADIUS (enter the fully qualified domain name [FQDN] of the router), as shown in Figure 5.

Figure 5. Configuring Cisco Secure ACS for a New Device Profile



User: pedro871-vpn.cisco.com

 Account Disabled

Supplementary User Info

Real Name

Description

User Setup

Password Authentication:

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

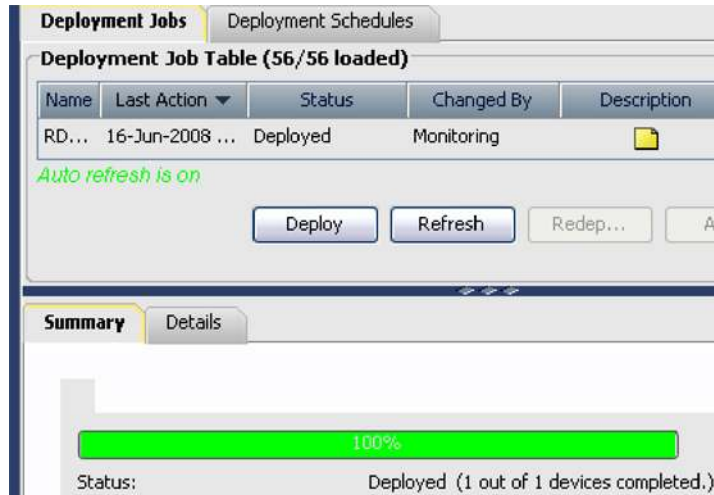
Password

Confirm Password

Cisco Security Manager: Submit and Deploy Job for New Router

- Cisco Security Manager current changes are seen only by the current user; changes need to be submitted to get committed so that other users can see them.
- Once Cisco Security Manager deploys a job, it sends the 871 full config to the configuration engine.
- Job status can be viewed from “tools > deployment manager” (Figure 6).

Figure 6. Displaying Job Status



If needed, go to the corporate DNS server and enter the `username.domainname.com` for the end-user router. This will make it easier to troubleshoot problems and allows the IT administrator to SSH to the user ID directly from anywhere in the corporate network.

Changing Configuration for One Device (or Remote Site), a Group, or All

To change one single device, click the device and navigate to the policy that needs to be changed. Then right-click the device and choose “Unshare Policy.” This will make the policy unique for that particular device, meaning that a change will affect only that device. After making and saving the changes, go to “File-Submit and Deploy,” identify this device from the list, and submit your job.

To change a shared policy, go to any device on Cisco Security Manager that has the shared policy and apply your changes. All of the other devices that share this policy will get the changes as well. Once the changes have been made, click “Submit and Deploy.” Cisco Security Manager will by default show all devices that share this policy, and when the job is submitted, it will connect to **the configuration engine** and configure a job change action for each individual device.

Removing a User or a Remote Site

To remove a device from the VPN, follow these steps:

1. Connect to Cisco Security Manager, click the device, and then click “Delete Device.”
2. SSH into the device. Copy the factory default to “startup config.” Delete the certificate from “NVRAM.” Reload the router.
3. Connect to your AAA. Remove the device profile for `username.domainname.com`
4. Revoke the PKI certificate (if needed).



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)