Cisco Virtual Office Deployment Guide

Scope of Document

This deployment guide provides detailed information on configuring the Cisco® Virtual Office headend devices and ManageExpress® Virtual Office. It also presents the end-user provisioning process performed to deploy new Cisco Virtual Office spoke routers.

Please refer to the Cisco Virtual Office overview (http://www.cisco.com/go/cvo) for more information about the solution, its architecture, and all of its components.

Contents

Introduction

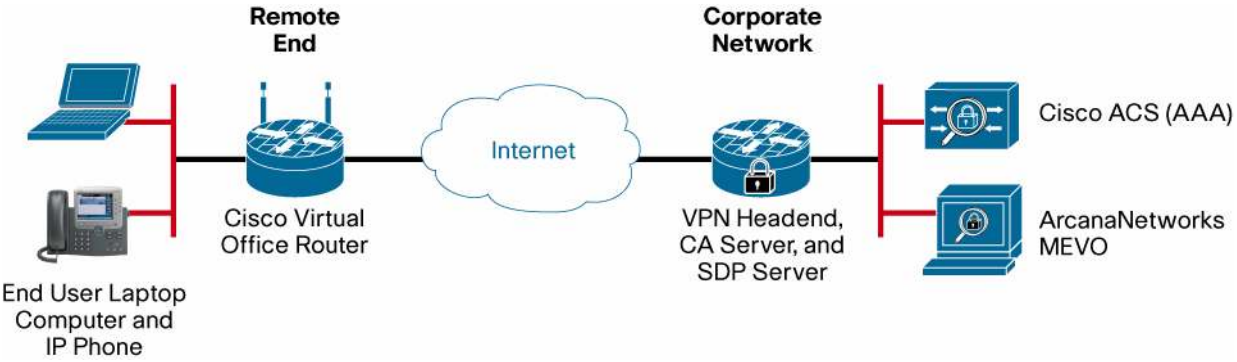
Cisco® Virtual Office is an end-to-end solution that provides an office-caliber end-user experience for employees working outside the traditional office environment, such as teleworkers or employees in a branch office. Integrating voice, video, wireless, and real-time data, Cisco Virtual Office offers the advantage of deployment with no need for administrator intervention, simplifying management and allowing rapid scaling. This document describes how to set up and configure Cisco Virtual Office using ArcanaNetworks ManageExpress Virtual Office (MEVO).

This document assumes a working knowledge of Cisco Virtual Office concepts. For more information and details about specific components of Cisco Virtual Office, please visit http://www.cisco.com/go/cvo.

Cisco Virtual Office Architecture

Figure 1 shows the basic Cisco Virtual Office architecture.

Figure 1. Cisco Virtual Office Architecture



Components on the corporate network or hub side include:

- VPN headend router serving as the VPN termination point
- Certificate authority (CA) server to issue certificates for both remote and headend routers
- Secure device provisioning (SDP) server for provisioning the remote routers
- Authentication, authorization, and accounting (AAA) server for device and user authentication: Typically a Cisco Secure Access Control Server (ACS)
- ArcanaNetworks MEVO on a Microsoft Windows 2008/2008R2 server for Cisco Virtual Office management and provisioning

Typical deployments on the remote side include:

- Cisco Virtual Office router: Typically a Cisco Integrated Services Routers Generation 2 (ISR G2)
- IP phone if voice is required
- Possibly a video endpoint
- Laptop computer for connecting to the corporate network; provided by the end user or employer

In a typical production environment, at least two headend devices are recommended on the corporate network side, for failover. One hub hosts the SDP server. A CA server, which can also be configured on one of the headends, is

also required. This document assumes that the CA and SDP servers are on the same VPN headend router, although they can be on a separate router (the SDP server must be on a router that runs Cisco IOS® Software).

On the remote-end side, a Cisco 880 Series ISR, Cisco 890 Series ISR, Cisco 1900 Series ISR, or Cisco 2900 Series ISR G2 (the platform is determined by the number of hosts that need to connect) is needed, with an optional IP phone depending on the needs of the customer.

Zero-Touch Deployment

One differentiating feature Cisco Virtual Office offers is zero-touch deployment. Initial setup of multiple home offices, remote offices, and branch offices is often a challenge. Cisco Virtual Office saves complete equipment upgrades and eliminates the need for preconfigured routers. In addition, the remote router can be provisioned and configured securely with minimal, nontechnical user intervention.

The setup begins at the corporate network, where a user account, User1 for example, is created on MEVO. When that user is approved for Cisco Virtual Office, the configuration for User1's router gets created automatically and stored in the MEVO database. The setup steps for provisioning at the corporate site end here; the rest of the provisioning and deployment occurs at the remote location.

At the remote location, the spoke router is shipped to the remote office with a default configuration from manufacturing that allows the router to get an IP address from DHCP. The spoke router is then connected to an ISP device through its WAN interface to obtain Internet connectivity. A laptop is connected behind the spoke router through one of its LAN interfaces. The end user (or perhaps an admin in the case of a branch deployment), User1, navigates to a provisioning URL (which connects to the SDP server) provided by the admin through the laptop connected to the remote router. User1 authenticates via a username and password prompt from the browser. The credentials are passed to the ACS, which checks to see if User1 is authorized to use/provision Cisco Virtual Office. If User1 is allowed to proceed with provisioning, the SDP router will find the configuration associated with User1 on MEVO and push it out to the remote router. After a few minutes, the remote router will get the full configuration and will be able to establish a VPN tunnel to the corporate headquarters or data center.

The remaining portion of this document focuses on the configuration of the CA and SDP servers, VPN headend router, and ArcanaNetworks' MEVO. Using this document, you should be able to fully configure the CA and SDP servers, VPN headend router, and ArcanaNetworks MEVO and deploy a remote router using the factory default configuration. Cisco Secure ACS policy configuration and the spoke router feature configuration are beyond the scope of this document.

Platforms and Images

For a complete list of supported and recommended platforms and images, please refer to the "Cisco Virtual Office Datasheet" under Deployment Models at http://www.cisco.com/go/cvo.

MEVO Requirements

ArcanaNetworks' MEVO must be installed on Microsoft Windows Server 2003, 2008, or 2008R2 (preferred). (See the ArcanaNetworks MEVO web site for a full list of system requirements: http://www.arcananet.com/mevo. The ArcanaNetworks' MEVO installation guide can be found on the ArcanaNetworks MEVO download page at http://downloads.arcananet.com/mevo . If you need a download account please contact: mevo-sales@arcananet.com.)

Setting Up Cisco Virtual Office

The following sections describe how to configure the management components, in the following order:

- Headend configuration

- CA server
- SDP server
- DMVPN headend

- ArcanaNetworks' MEVO

Headend Configuration

This section presents the configurations for the headend components of Cisco Virtual Office for the CA server, SDP server, and Dynamic Multipoint VPN (DMVPN).

The configurations in this section can be copied and pasted from the document to the headend routers after variables specific to each setup are replaced in the configurations. The variables appear here in the format **$variable_name$**. (ArcanaNetworks MEVO uses this same variable-naming convention.)

Note the values for variables set in the configuration templates here; you will need to enter them later in the ArcanaNetworks MEVO configuration.

These configurations assume that the CA and SDP servers are configured on the same router that is used as the DMVPN headend. If separate CA and SDP servers are being configured on a different router, simply paste the relevant configurations for the CA and SDP servers into the corresponding router.

Note: The following ports should be open on the corporate firewall, to allow for the Secure Device Provisioning (SDP) process, certificate enrollment process, and VPN tunnel establishment to complete:

1. HTTPS (TCP 443) – to the SDP server, used for provisioning
2. HTTP (TCP 8000, or any other port configured) – to the SDP server, for certificate enrollment
3. UDP 500 – to the DMVPN headend, for ISAKMP
4. UDP 4500 – to the DMVPN headend, for NAT-T
5. ESP (IP 50) – to the DMVPN headend, for IPSec

CA and SDP Server Configuration

The CA and SDP server configurations shown here allow the remote user to begin the Cisco Virtual Office provisioning process to securely establish a VPN tunnel to the hub routers. The CA and SDP server templates themselves come with ArcanaNetworks MEVO and do not need to be configured by the administrator. These configurations should be manually copied and pasted onto the CA and SDP server router; the CA and SDP router is not managed by ArcanaNetworks MEVO.

1. Configure the certificate server.

```
!!! Configure HTTP server required for Simple Certificate Enrollment Protocol (SCEP)
ip http server
ip http port $ca_http_port$  !! e.g. ip http port 8000

!!! Configure PKI server
crypto pki server cvo-cs
 database level complete
 database archive pkcs12 password $ca_password$
!! e.g. database archive pks12 password mypassword123

 issuer-name cn=cvo-cs,ou=cvo
 auto-rollover
 grant auto trustpoint cvo-pki
 no shut
```

1. Configure the AAA server for user authentication.

```
!!! Configure radius group
aaa new-model
aaa group server radius acs
 server-private $radius_server$ auth-port $auth_port$ acct-port $acct_port$ key $radius_key$
!! e.g. server-private 10.1.1.2 auth-port 1812 acct-port 1813 key mykey123

!!! Configure AAA lists
aaa authentication login sdp-acs group acs
aaa authorization network sdp-acs group acs
```

1. Configure the SDP server.

```
!!! Configure HTTPS server for SDP
ip http authentication aaa
ip http secure-server

!!! OpsXML server info
ip host OpsXML $OPSXML_ADDRESS$
!! e.g. ip host OpsXML 10.1.1.3
!!! The OpsXML IP address is usally the same IP address as the MEVO server.

!!! Configure SDP Registrar
crypto provisioning registrar
 pki-server cvo-cs

!!! Get the spoke config from MEVO
 template config http://OpsXML/mevo/Configs/$n_Bootstrap.cfg
 !!! The $n in $n_Bootstrap.cfg below refers to the username for the user/device associated with the config.  e.g. user johndoe would have config johndoe_Bootstrap.cfg associated with him.

 template username <username> password 0 <password>
!!! template username/password is a Windows local or domain account on the MEVO server with access with READ access to: .\Program Files (x86)\ArcanaNetworks\OpsXML\MeVoIP\ME_VO\Configs;
!! e.g. template username Administrator password 0 mypassword123

!!! AAA lists
 authentication list sdp-acs
 authorization list sdp-acs

!!! Custom SDP templates
 template http welcome http://OpsXML/mevo/sdp/2-sdp_welcome.html
 template http completion http://OpsXML/mevo/sdp/4-sdp_completion.html
 template http introduction http://OpsXML/mevo/sdp/3-sdp_introduction.html
 template http start http://OpsXML/mevo/sdp/1-sdp_start.html
 template http error http://OpsXML/mevo/sdp/sdp_error.html
```

```
!!! SDP templates come with MEVO by default and are displayed to end-users when
they are doing the SDP process
```

DMVPN Configuration

The DMVPN configuration for the hub router shown here must be copied and pasted onto the headend router manually; the headend router is not managed by ArcanaNetworks MEVO.

1. Configure the AAA server for device authorization (PKI-AAA, optional).

```
aaa new-model

!!! Configure radius group
aaa group server radius acs
 server-private $pkiaaa_server$ auth-port $pkiaaa_auth_port$ acct-port
$pkiaaa_acct_port$ key $pkiaaa_key$
!! e.g. server-private 10.1.1.2 auth-port 1812 acct-port 1813 key mykey123

!!! Configure AAA list for PKI-AAA
aaa authorization network pkiaaa group acs
!!! PKI-AAA adds security to the PKI infrastructure by validating certificates
using ACS
```

1. Configure public key infrastructure (PKI) trustpoint for Internet Security Association and Key Management Protocol (ISAKMP) authentication (if being used).

```
!!! PKI server info
ip host cvo-cs $SDP_ADDRESS$  !! e.g. ip host cvo-cs 10.2.2.1

!!! Create a trustpoint for PKI
crypto pki trustpoint cvo-pki
 enrollment url http://cvo-cs:$ca_http_port$
 !! e.g. enrollment url http://cvo-cs:8000
 serial-number
 ip-address none
 password none
 revocation-check crl
 auto-enroll 75
 authorization list pkiaaa
```

1. Authenticate and enroll the certificate.

```
crypto pki authenticate cvo-pki
!!! Type YES if prompted to accept the certificate
crypto pki enroll cvo-pki
```

1. Configure cryptography policies.

```
!!! ISAKMP
crypto isakmp policy 1
 encr $isakmp_encr$    !! e.g. encr aes 256
crypto isakmp keepalive 30 5
crypto isakmp nat keepalive 30
```

```
!!! IPSec
crypto ipsec transform-set t1 $ipsec_encr$ $ipsec_hash$
 !! e.g. crypto ipsec transform-set t1 esp-aes 256 esp-sha-hmac
 mode transport require
crypto ipsec profile cvo-profile
 set transform-set t1
```

1. Enable the DMVPN server.

```
!!! Enable multicast
ip multicast-routing (distributed) !(on ASR only)

!!! DMVPN tunnel
interface Tunnel0
 bandwidth $bandwidth$   !! e.g. bandwidth 2000
 ip address $pgw_tunnel_address$ $tunnel_subnet$
!! e.g. ip address 192.168.99.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip pim sparse-dense-mode
 ip nhrp authentication $nhrp_auth_key$  !! e.g. ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 ip nhrp network-id $nhrp_network_id$  !! e.g. ip nhrp network-id 12345
 ip nhrp redirect
 ip tcp adjust-mss 1360
 no ip split-horizon eigrp $eigrp_as$  !! e.g. ip split-horizon eigrp 99
 delay $delay$   !! e.g. delay 1000
 qos pre-classify
 tunnel source <OUTSIDE_INTERFACE_NAME>    !! e.g. tunnel source FastEthernet0
 tunnel mode gre multipoint
 tunnel key $tunnel_key$  !! e.g. tunnel key 12345
 tunnel protection ipsec profile cvo-profile
```

1. Enable routing.

```
!!! EIGRP for DMVPN
router eigrp $eigrp_as$  !! e.g. router eigrp 99
 no auto-summary
 network $pgw_tunnel_address$ 0.0.0.0        !! e.g. network 192.168.99.1 0.0.0.0

!!! Route Redistribution Example
ip access-list standard no_split_in
 permit 0.0.0.0
route-map no_split_in permit 10
 match ip address no_split_in
router eigrp $eigrp_as$!! e.g. router eigrp 99
 redistribute static route-map no_split_in
```

ArcanaNetworks' MEVO Configuration

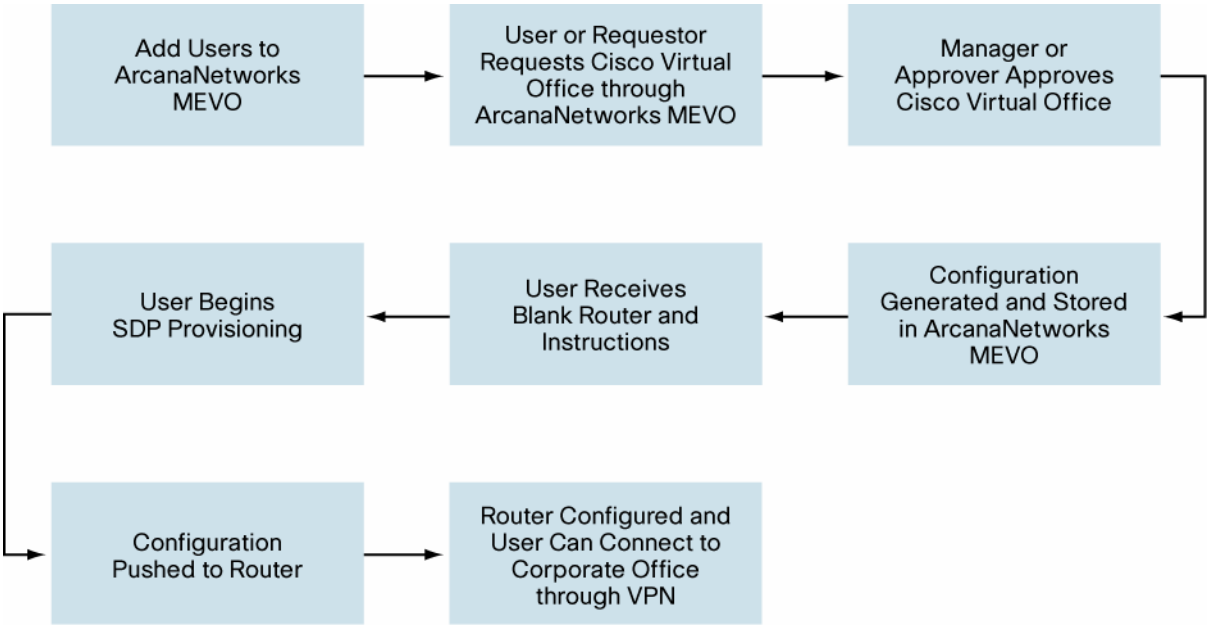
ArcanaNetworks' MEVO automatically generates configurations for the remote end devices and pushes configuration updates and Cisco IOS Software image upgrades.

Four roles are available in ArcanaNetworks MEVO:

- **User:** This role includes teleworkers, mobile workers, and individuals working at remote and branch offices. In the case of a branch-office deployment, the end user may also be the technician who configures the branch router for the office or the branch offices's name.
- **Approver:** This role approves or declines a user's request for Cisco Virtual Office in the typical Cisco Virtual Office deployment workflow.
- **Administrator:** This role configures and maintains ArcanaNetworks MEVO server. This role may also manage users, create requests, and approve requests. If the Administrator requests Cisco Virtual Office service on behalf of the user, a manager approval is not required.
- **User Administrator:** This role can be used to manage a group of users based on User Classes. This role does not have access to change the MEVO server configuration.This role can create requests, approve requests, and disconnect spokes..

Figure 2 shows the typical ArcanaNetworks MEVO workflow with Cisco Virtual Office.

Figure 2. Sample MEVO State Full Business Workflow with Cisco Virtual Office



An option to remove the end user from the approval process is also available. In this scenario, either the administrator or the user administrator requests Cisco Virtual Office service on behalf of the end user, eliminating the need for users to log into ArcanaNetworks MEVO to request Cisco Virtual Office. The steps after the request for Cisco Virtual Office are the same

The following sections describe the best practices for setting up ArcanaNetworks' MEVO for Cisco Virtual Office. All steps in the workflow shown in Figure 2 are covered; however, how a user obtains a router will differ depending on the customer.

Please refer to the ArcanaNetworks MEVO installation guide for instructions on installing ArcanaNetworks MEVO and to the ArcanaNetworks MEVO user guide for more detailed explanations of ArcanaNetworks MEVO components and functions. Both the ArcanaNetworks MEVO installation guide and user guide can be downloaded from the ArcanaNetworks MEVO download page at http://downloads.arcananet.com/mevo (after login). Please contact mevo-sales@arcananet.com if you need a download account.

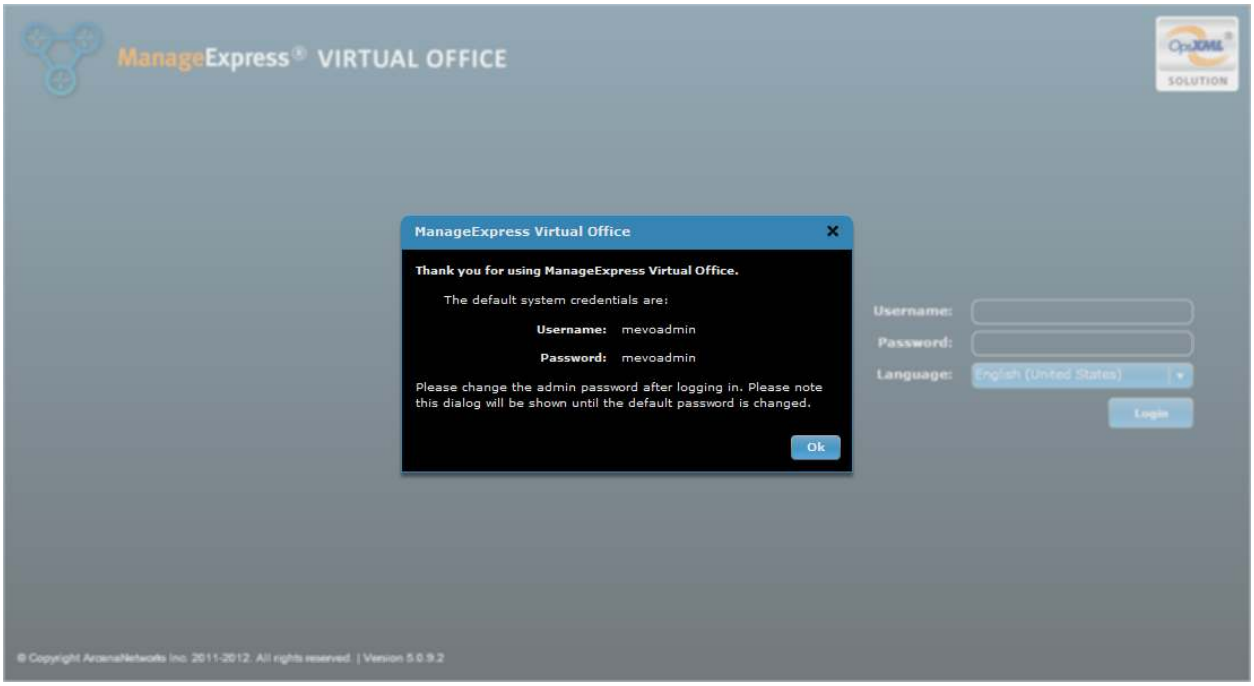
Administrator Tasks: Configuring ArcanaNetworks MEVO

This section describes the tasks needed to configure a newly installed instance of ArcanaNetworks' MEVO for Cisco Virtual Office. Many of the administrator tasks need to be performed only once. After the initial configuration, the administrator needs to do little except manage user accounts, assuming that the network addressing does not change.

Step 1: Logging In for the First Time

1. Open a browser and enter http://<ip-address-or-domain-name>/mevo to access the ArcanaNetworks MEVO GUI (Figure 3). (For example, enter http://cvoarcana.cisco.com/mevo).

Figure 3. MEVO GUI initial login screen.



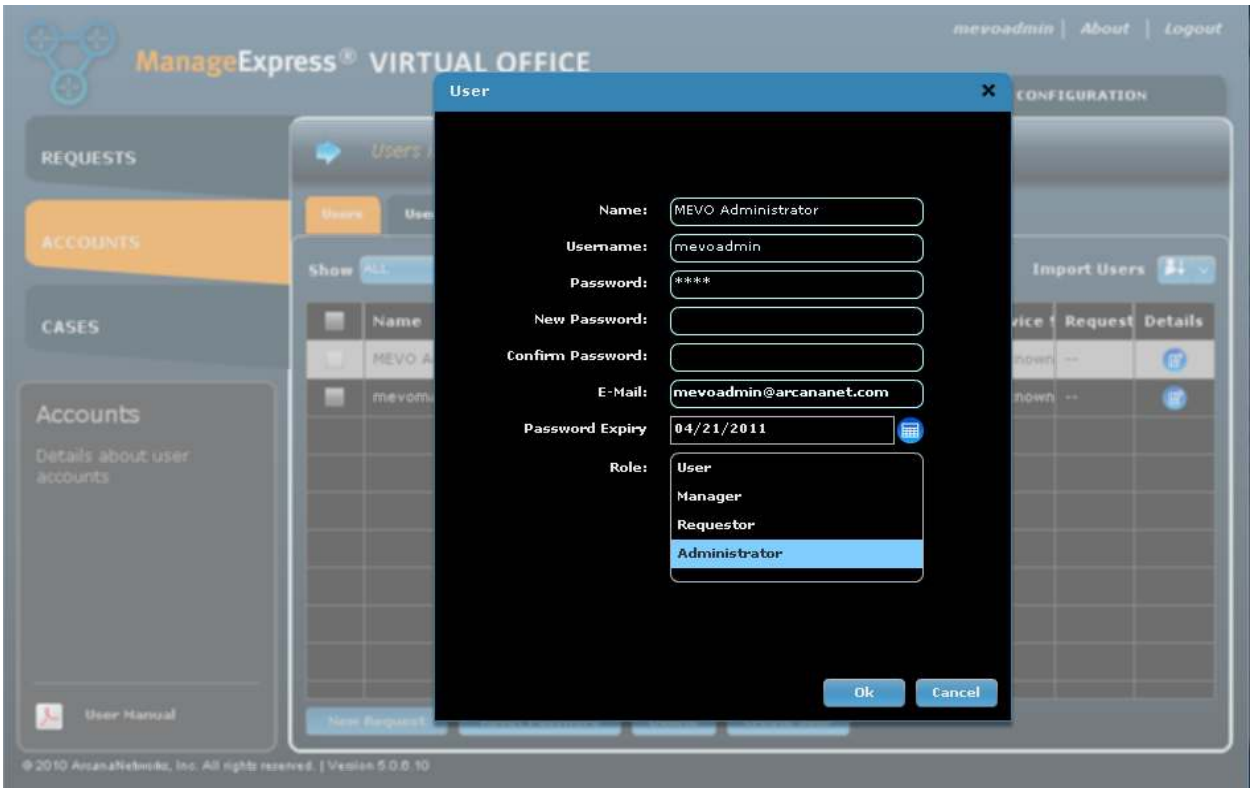
1.

2. Log in using the default credentials (username and password: mevoadmin and mevoadmin). Change the default password to a new password if this is the first time ArcanaNetworks MEVO is being used (Figure 4).

Figure 4. Login with username: mevoadmin and password: mevoadmin as default. Change the default password upon login.

3. Change the mevoadmin account password by clicking on the Accounts tab in the left column and then click the Users tab. Click the icon in the Details column for the MEVO Administrator account and set a new password and add an email address (Figure 5).

Figure 5. Change the default ArcanaNetworks MEVO admin credentials.

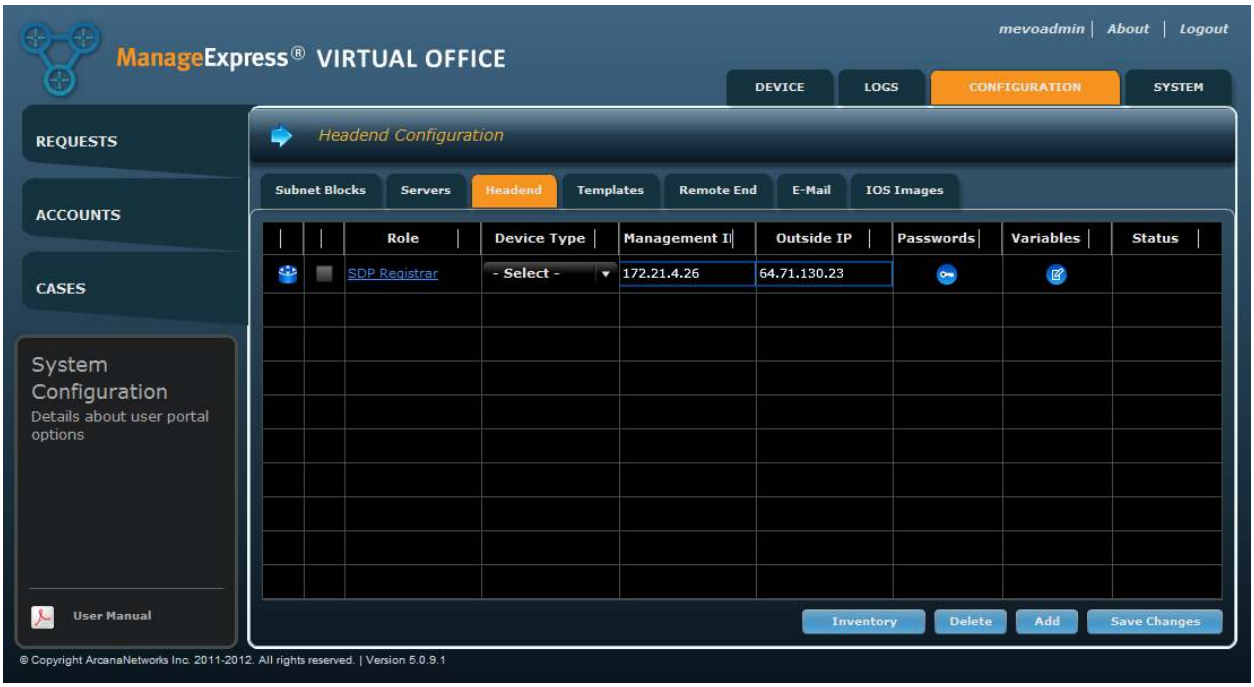


Step 2: Configuring the Headend

The Headend tab is used to configure service details. The router roles consist of Secure Device Provisioning Registrar, Primary and Secondary Gateways, and PKI- AAA. Primary and Secondary Gateways are part of DMVPN Clouds, of which there can be many added.

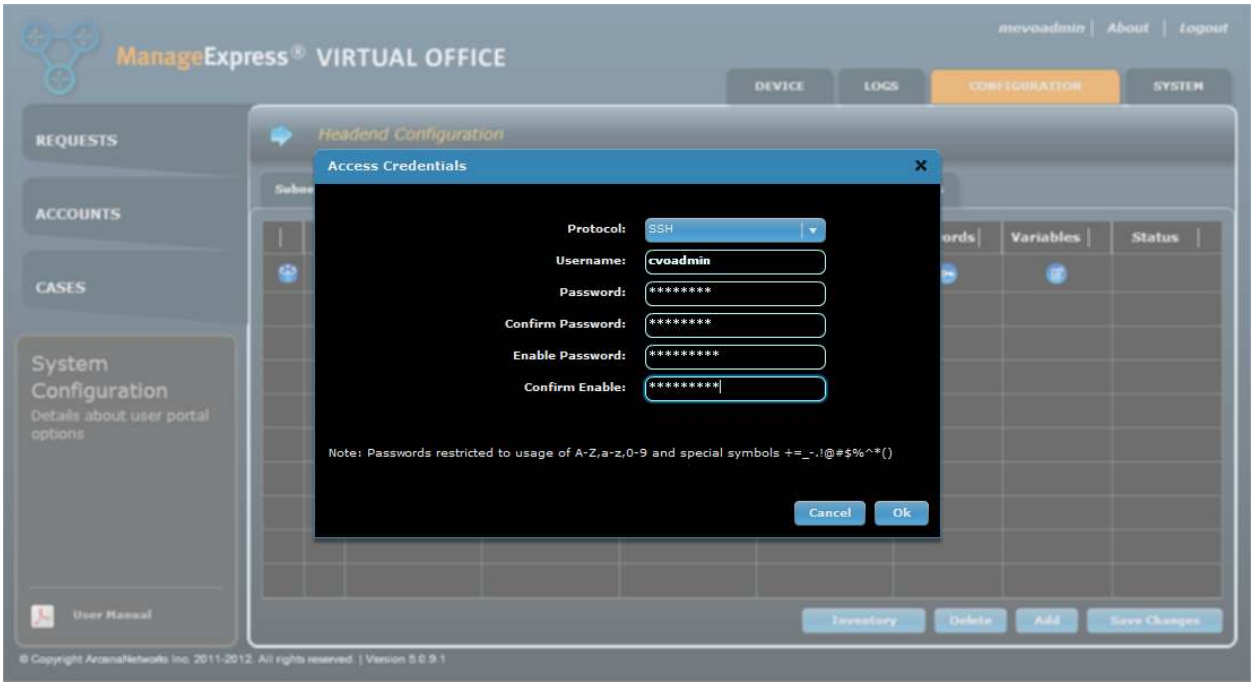
1. Go to the Configuration tab and click on the Headend sub-tab. For the SDP Registrar select the Device Type and enter the Management IP and Outside IP values (Figure 6).
   a. Device Type: For informational purposes only
   b. Management IP: IP address accessible from ArcanaNetworks MEVO
   c. Outside IP: IP address accessible from the Internet; end users will start the SDP process using this address.

Figure 6. Enter device type and IP addresses for SDP server.



1. Click the icon in the Passwords column and enter the access credentials to allow Secure Shell (SSH) Protocol access from MEVO to the SDP server (Figure 7).

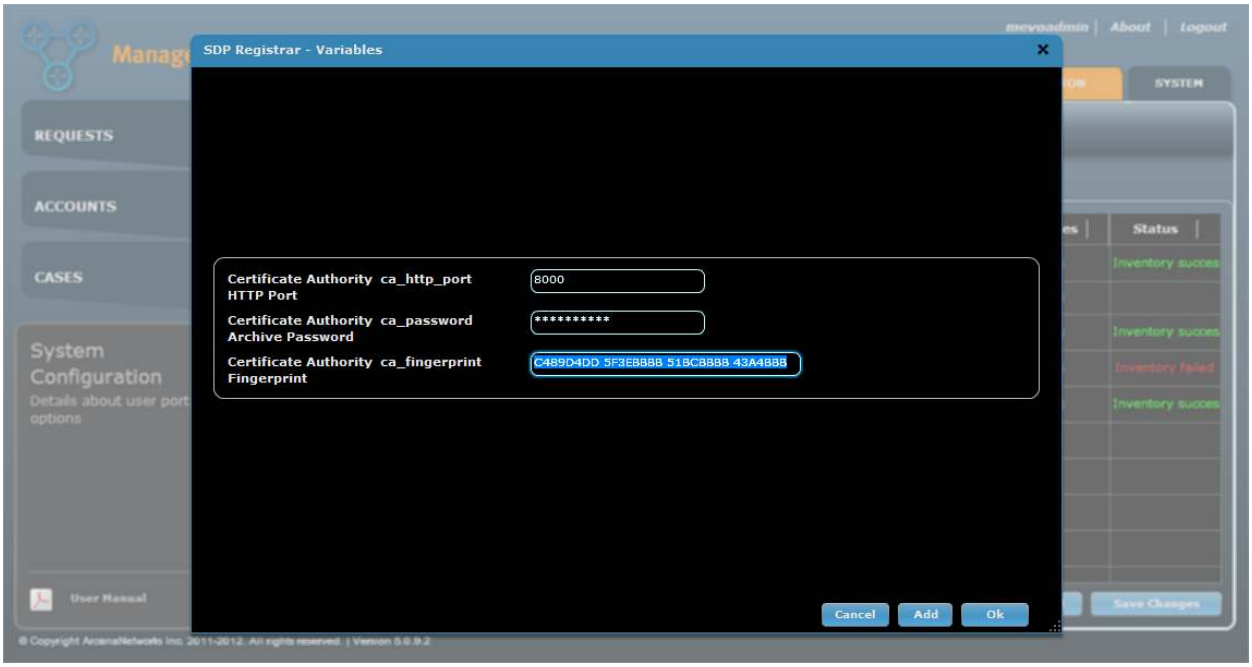
Figure 7. Enter access credentials for the SDP server.



If the SDP router has already been configured run the “Inventory” operation to populate the SDP information. The Certificate Authority HTTP Port will be automatically parsed and populated. The Archive Password will need to be manually configured after inventory completes. **It currently takes approximately 30 seconds before the user interface is updated after Inventory completes**.

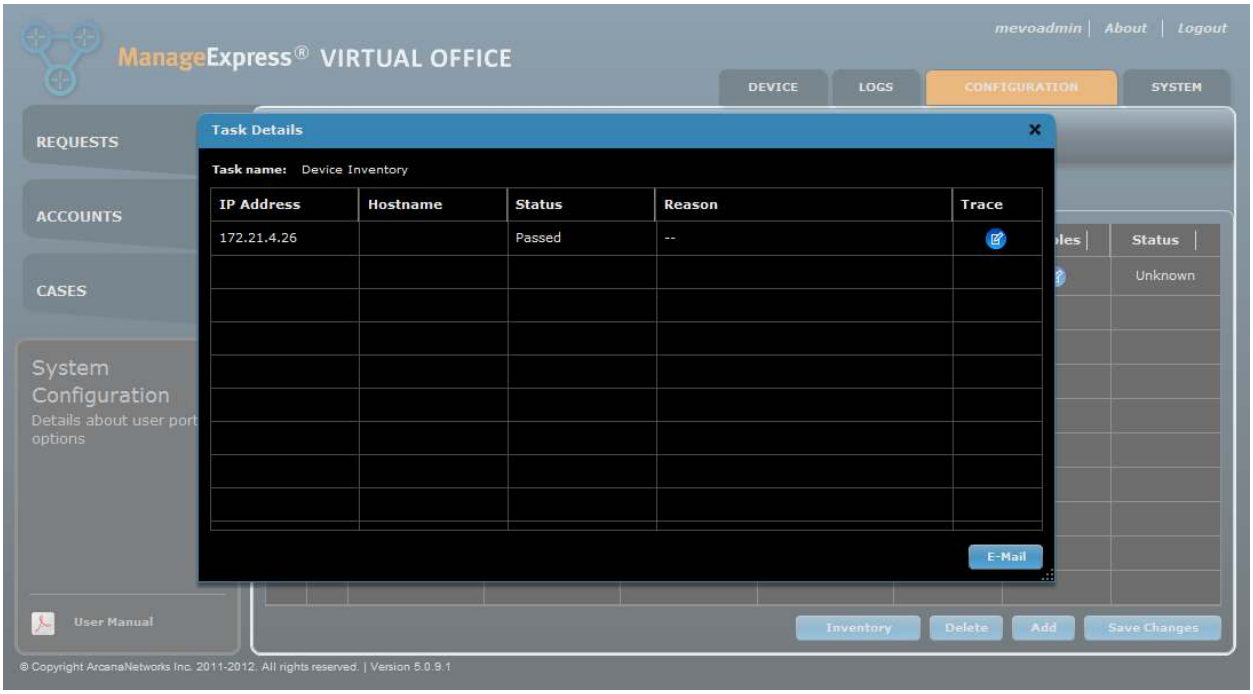
2. Click the icon in the Variables field and enter the Certificate Authority information as listed here. Click Ok when you are finished (Figure 8).
   a. Certificate Authority HTTP Port: HTTP port used for SCEP for certificate enrollment. This should be automatically populated after inventory completes, but should be verified.
   b. Certification Authority Archive Password: PKI server archive password; used locally on the SDP server only. **This password needs to be manually entered**.

Figure 8. Enter SDP Registrar Variables for the SDP server.



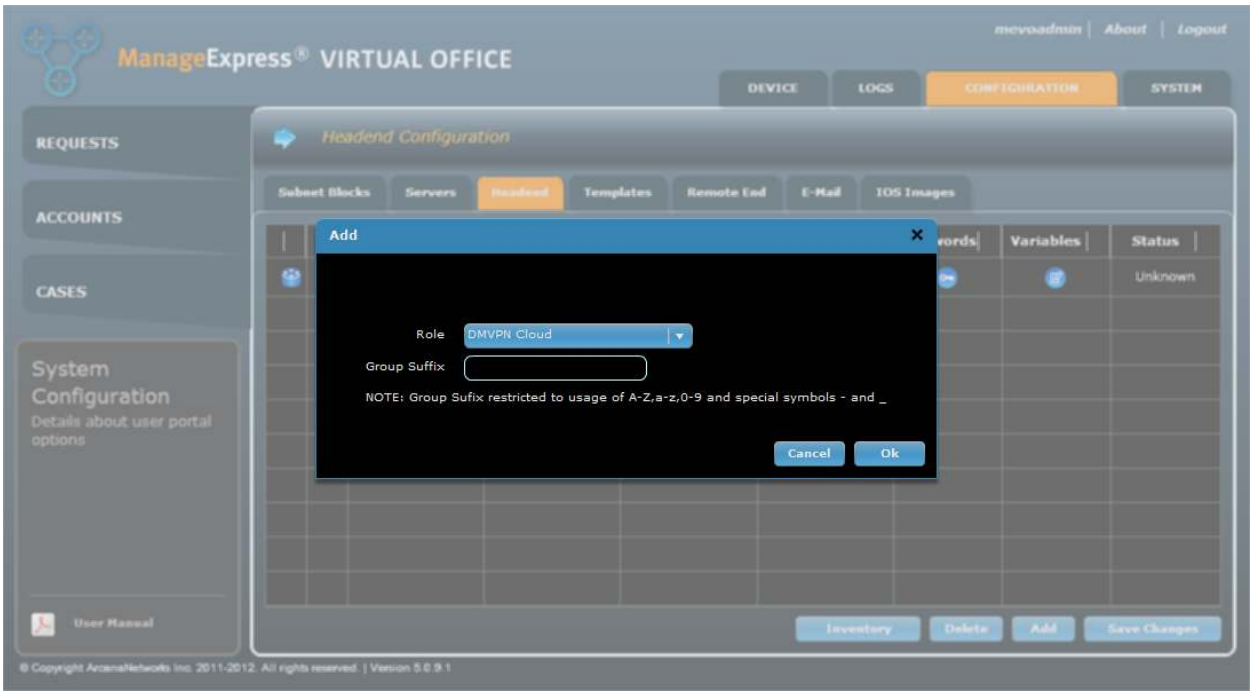
3. At the bottom right of the screen, click Save Changes. ArcanaNetworks MEVO will then try to use SSH or Telnet to reach the router. The resulting status will not affect provisioning (Figure 9).

Figure 9. MEVO tries to reach the router after SDP server is added. Status will show “Passed” if test is succesful.



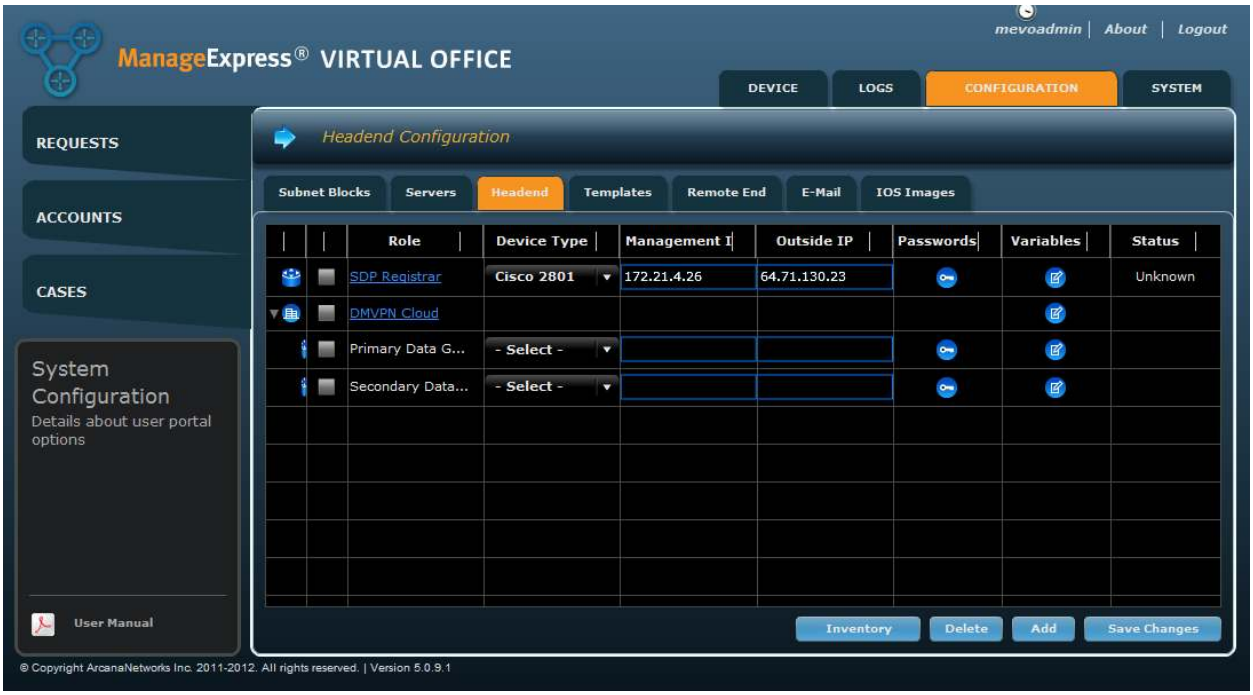
4. Click Add to add a new DMVPN cloud. No Group Suffix should be used for the first cloud (Figure 10).

Figure 10. Add a new DMVPN Cloud.



1. Enter Device Type, Management IP, and Outside IP values for the primary and secondary data gateways. If you do not need the secondary gateway, select it and click Delete (Figure 11).

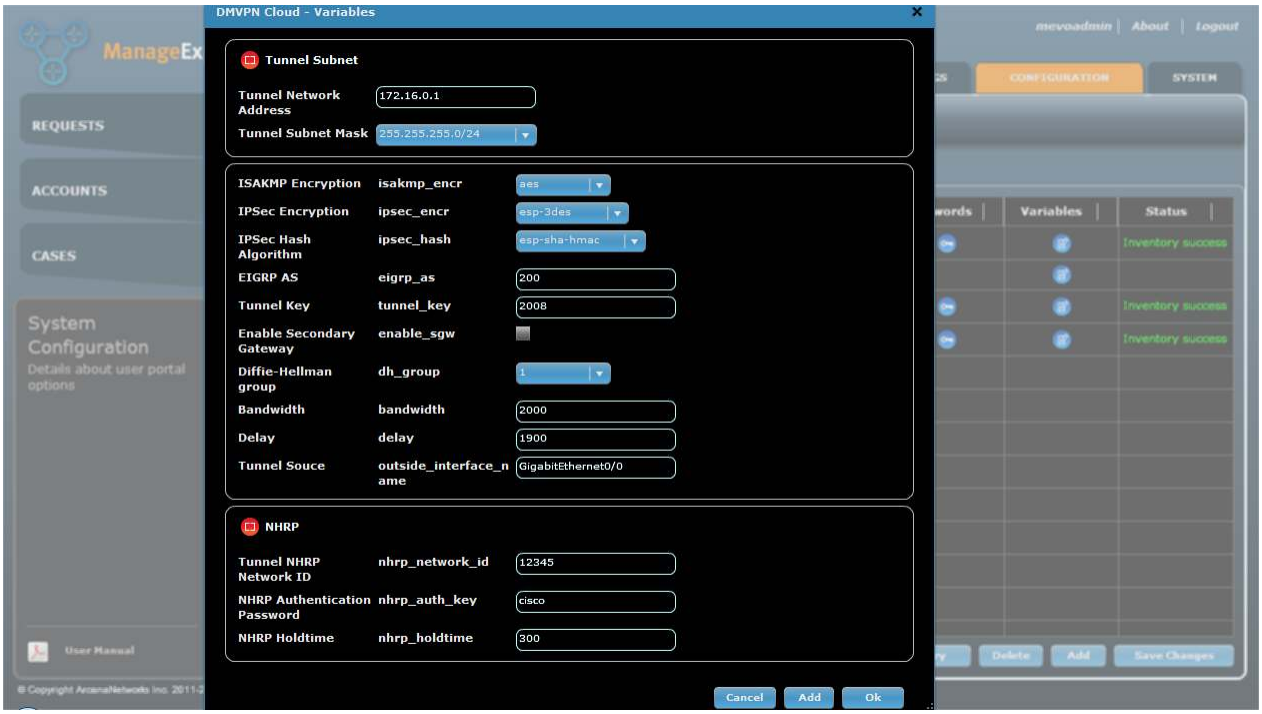
Figure 11. Enter device type and IP addresses for DMVPN Gateway(s).



1. For the DMVPN Cloud, click the icon in the Variables field and enter the information as listed below. These variables should match the configuration on the DMVPN hub (Figure 12). If the inventory operation is run for an existing headend, many of these values may be populated. **Passwords ALWAYS require manual entry. It is CRITICAL that all information be complete and verified as correct.**
   a. Tunnel Network Address: DMVPN multipoint generic routing encapsulation (mGRE) tunnel network address; these addresses will be passed to the spoke routers
   b. Tunnel Subnet Mask: DMVPN mGRE tunnel subnet mask
   c. ISAKMP Encryption, IPsec Encryption, IPsec Hash Algorithm, and Diffie-Hellman Group: Cryptographic policies; these policies should match on hubs and spokes
   d. EIGRP AS: Autonomous system (AS) number for Enhanced Interior Gateway Routing Protocol (EIGRP); this protocol is the preferred routing protocol for DMVPN
   e. Tunnel Bandwidth and Tunnel Delay: Parameters used by EIGRP for routing metrics
   f. Tunnel Key: DMVPN mGRE tunnel key; this value should match on hubs and spokes
   g. Enable Secondary Gateway: Check the box if a secondary gateway is used
   h. NHRP Network ID, Authentication Password, and Holdtime: Next-Hop Resolution Protocol (NHRP) parameters; **the authentication password should match on hubs and spokes**

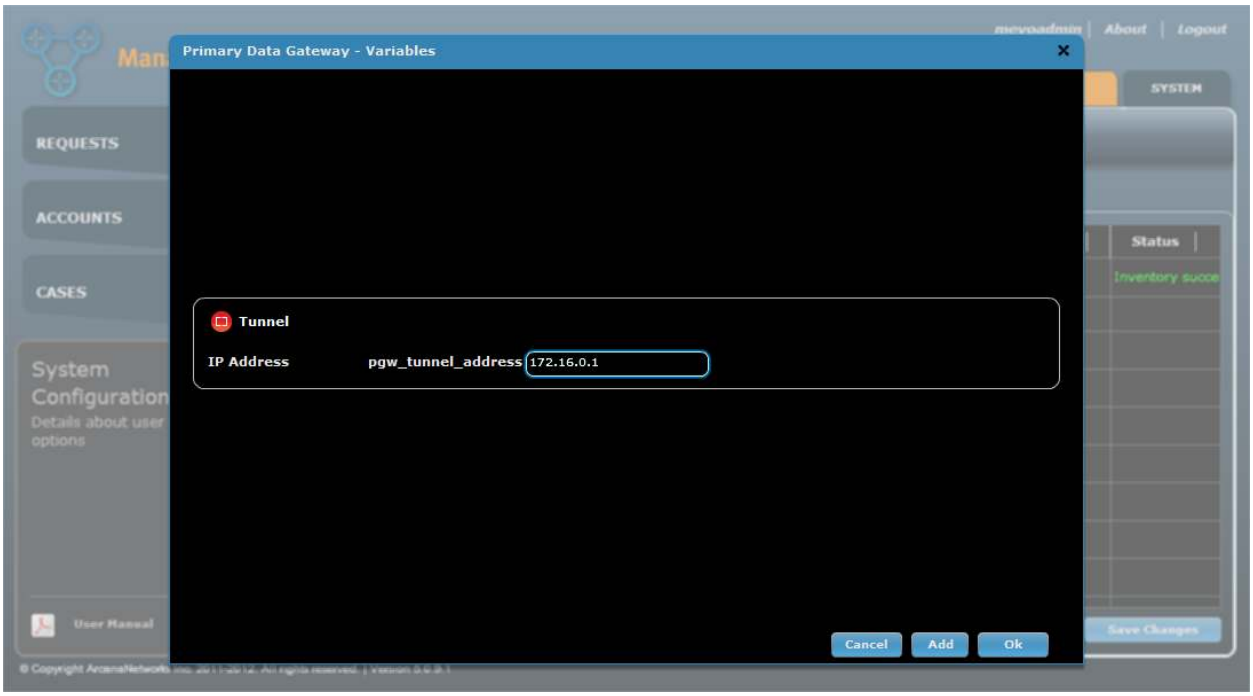
   When you are done, click Ok to save the settings.

Figure 12. Enter and save variables for the DMVPN cloud.



1. For Primary (and Secondary) Data Gateway, click the icon in the Variables field and enter the DMVPN mGRE tunnel IP addresses for each hub. Click Ok when done (Figure 13).

Figure 13. Enter a tunnel IP address for the Primary (and Secondary) Gateway.



1. Add a PKI-AAA server (optional).

   While optional, PKI-AAA is HIGHLY recommended. It provides the only means for MEVO to completely automate the disconnect process. With PKI-AAA MEVO can remove the spoke account used for authorizing the spoke certificate used to build the VPN tunnel, in addition to revocation checking. **Without PKI-AAA, certificate revocation is the sole means to prevent a device from establishing a vpn tunnel.**

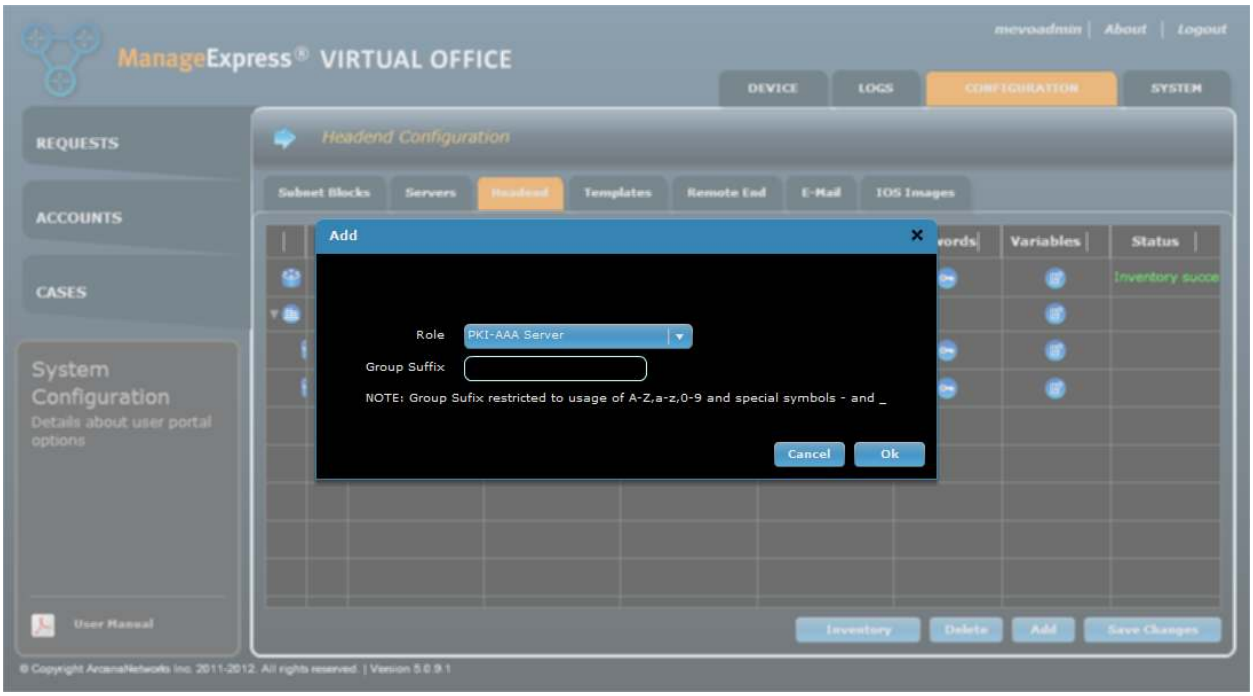
   Cisco ACS 5.3 is the preferred software version although ACS 4.x can still be used with a third party commerical SSH service. If you wish to use ACS 4.x please contact mevo-support@arcananet.com for more details on its configuration.

Note: The ACS 5.x API uses both SSH and FTP while ACS 5.3 can be configured to use the more secure option of SSH and HTTPS

   a. Click Add and select PKI-AAA Server from the Role drop-down menu.

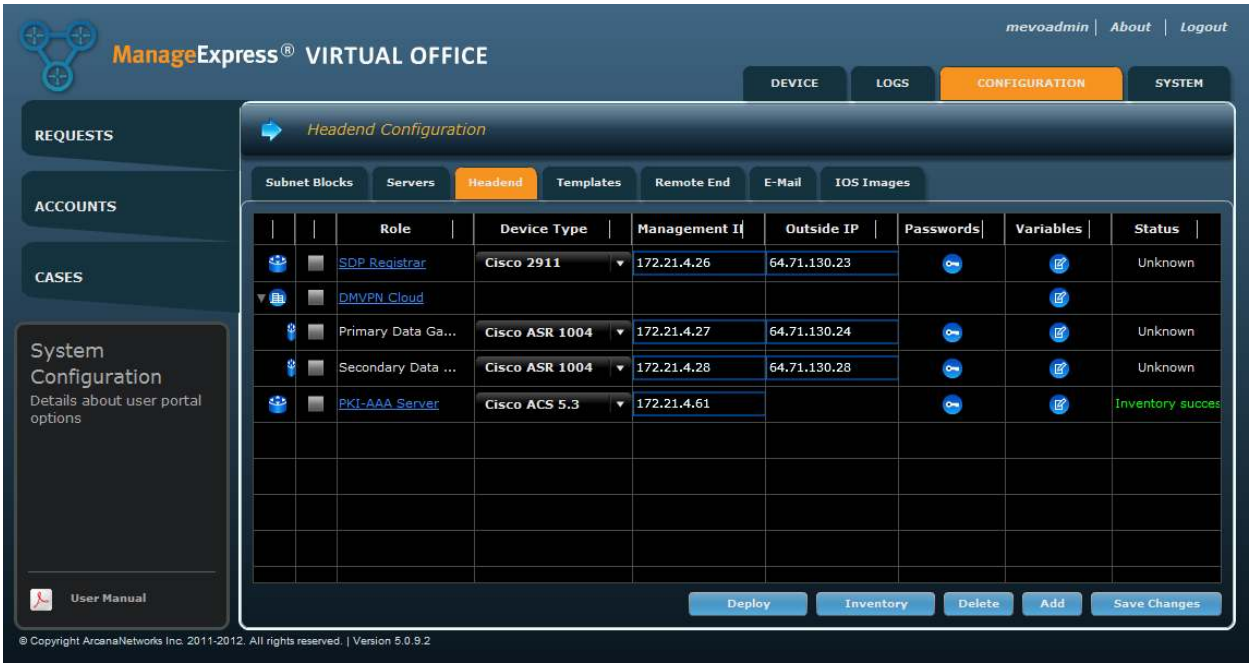
      Leave the Group Suffix field empty for the first PKI-AAA server (Figure 14).

Figure 14. Add a new PKI-AAA Server



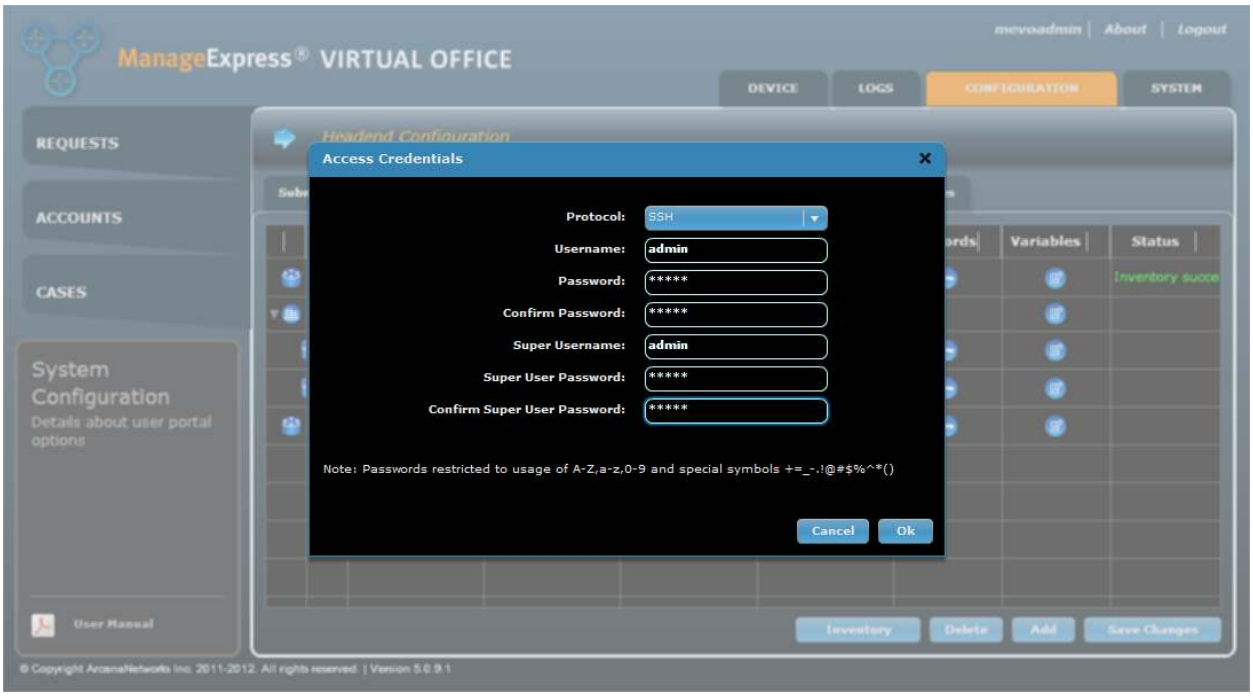
a. Select the Device Type (Cisco Access Control Server) and Management IP for the PKI-AAA server (Figure 15). The Cisco ACS 5.x option uses SSH and FTP for access and file copying. The Cisco ACS 5.3 option allows the ability to use SSH and HTTPS for access and file copying.

Figure 15. Enter device type and IP address for the PKI-AAA server.



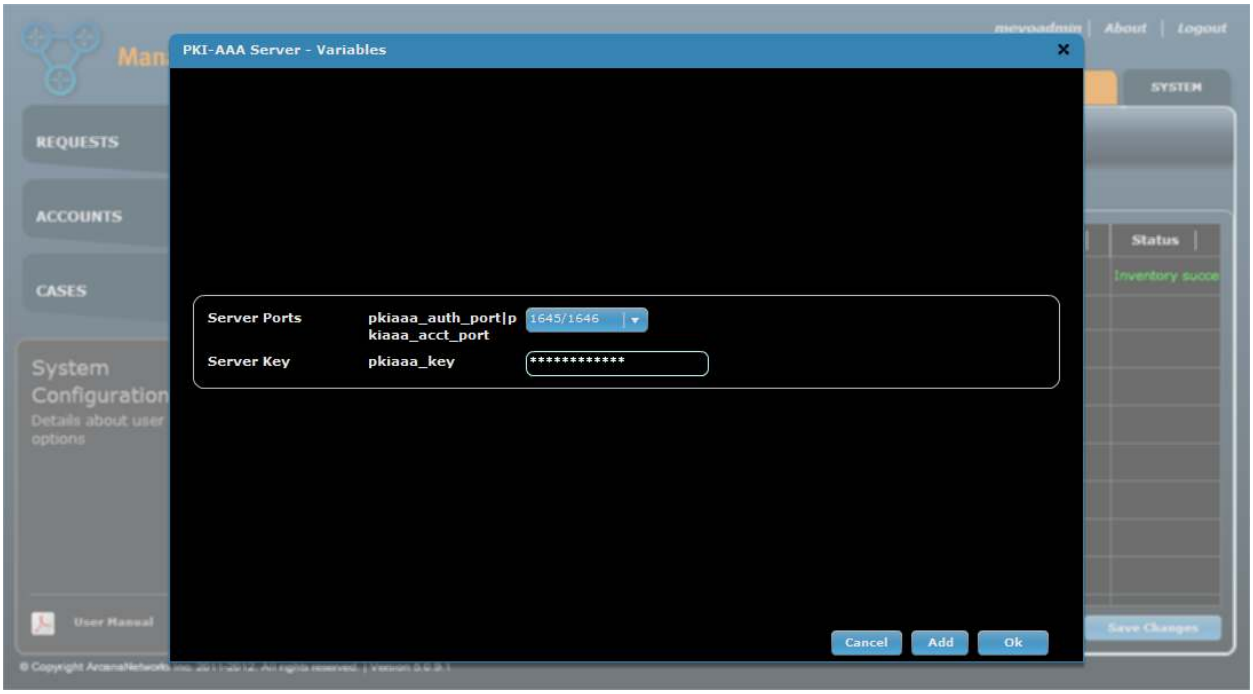
a. Click the icon in the Passwords field and enter the access credentials to allow Secure Shell (SSH) Protocol access to the PKI-AAA server. Click Ok when done (Figure 16).

Figure 16. Enter access credentials for the PKI-AAA server.



a. Click the icon in the PKI-AAA Variables field. Select the Server Ports from the drop-down menu, and enter the Server Key. Click Ok when done (Figure 17).

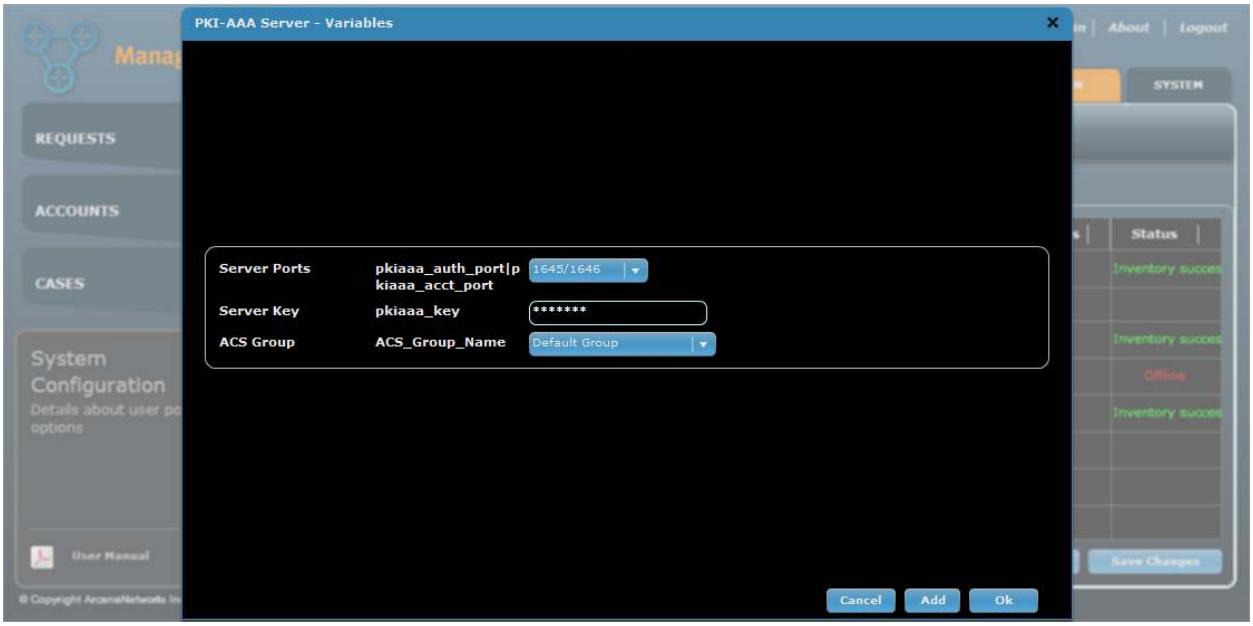
Figure 17. Enter PKI-AAA server variables.



b. Click Save Changes for the Headend configuration, and then put a check by the PKI-AAA Server and click on the Inventory button.

c. After successfully running an inventory on the ACS server you will need to go back into the PKI-AAA Server's Variables and select the appropriate "ACS Group" value (Figure 18). This is the group where MEVO will add the PKI-AAA device accounts.

Figure 18. Select the ACS Group from PKI-AAA server variables after running Inventory



1. Click Save Changes to save all headend settings.

Note: Status will not affect provisioning, but an Offline status generally means ArcanaNetworks MEVO cannot communicate with the headend, SDP server, or PKI-AAA server.

Step 3: Configuring ArcanaNetworks MEVO – Remote-End Variables

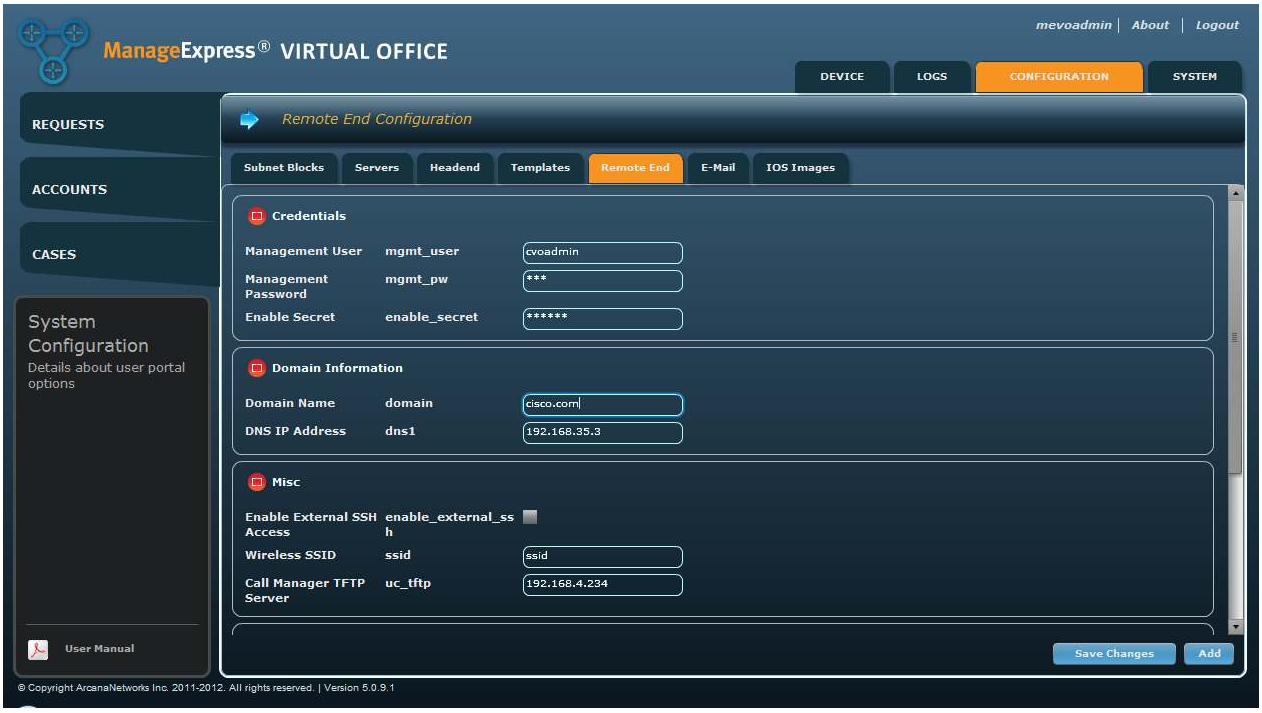
These are settings are used when generating the configurations for spoke routers are all required whether they will be immediately used or not.

1. Click Remote End and enter the information as listed here (Figure 19).
   a. Credentials for spoke routers: Management User, Management Password, and Enable Secret.
   b. Domain Information: Name and DNS IP Address. Enter the domain name in the format: <domain>.com|org|edu
   c. Miscellaneous: Enable External SSH Access to the spoke routers, Wireless SSID for an autonomous access point, and Cisco Unified Communications Manager TFTP Server for IP Phones.
   d. SNMP Read Community
   e. Time Settings: Time Zone, Enable Daylight Savings Time, and NTP IP Address

Note: All Remote-End Variables are required. If you are not using a variable, enter a placeholder value.

You can also add custom variables, such as an additional DNS server, by clicking on the "Add" button and filling in the required information. For more details, you can refer to the full User Guide available on the ArcanaNetworks download site: http://downloads.arcananet.com/mevo

Figure 19. Enter Remote End variables.

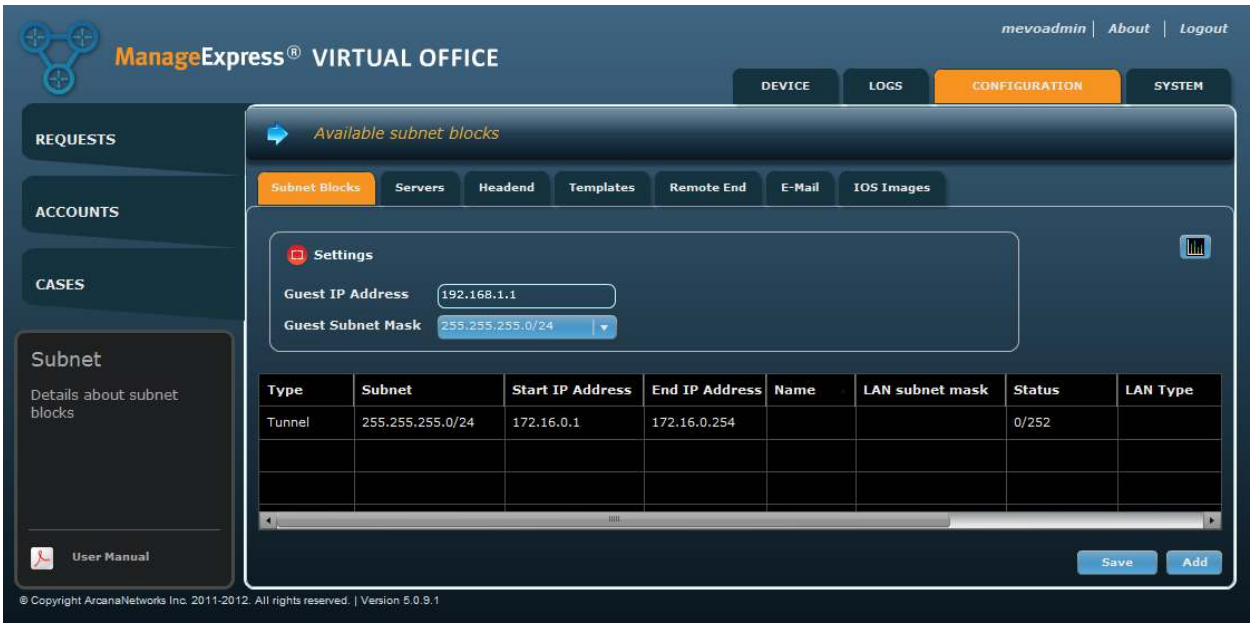


Step 4: Configuring Subnet Blocks

The Subnet Blocks tab is where you can add LANs that get allocated to spoke routers for use by end users via their User Class. There are various types of LANs that can be added, such as Data, Voice, etc., but for the purpose of getting started, adding a basic “default” type will be suggested here. For most cases, the default type is all that’s needed, unless more than one subnet per spoke is required. For more information on Subnet Blocks you can refer to the full User Guide available on the ArcanaNetworks download site: http://downloads.arcananet.com/mevo.

1. Choose Configuration > Subnet Blocks > Add to add a subnet block (Figure 20).

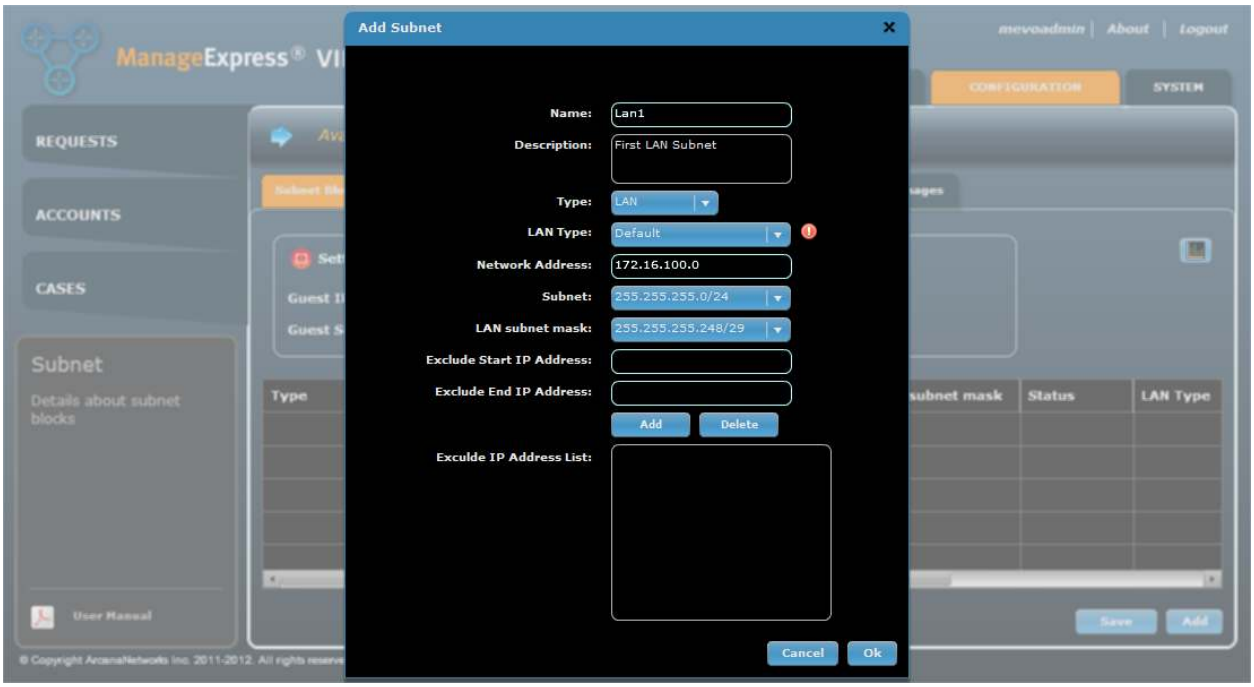
Figure 20. Add a subnet block.



Note: The Settings fields are for globally configuring the details for the guest networkthat bypasses the VPN on the spoke routers and is NAT'ed to the internet. The Tunnel subnet will be automatically populated from the DMVPN Cloud variables specified during Step 2.

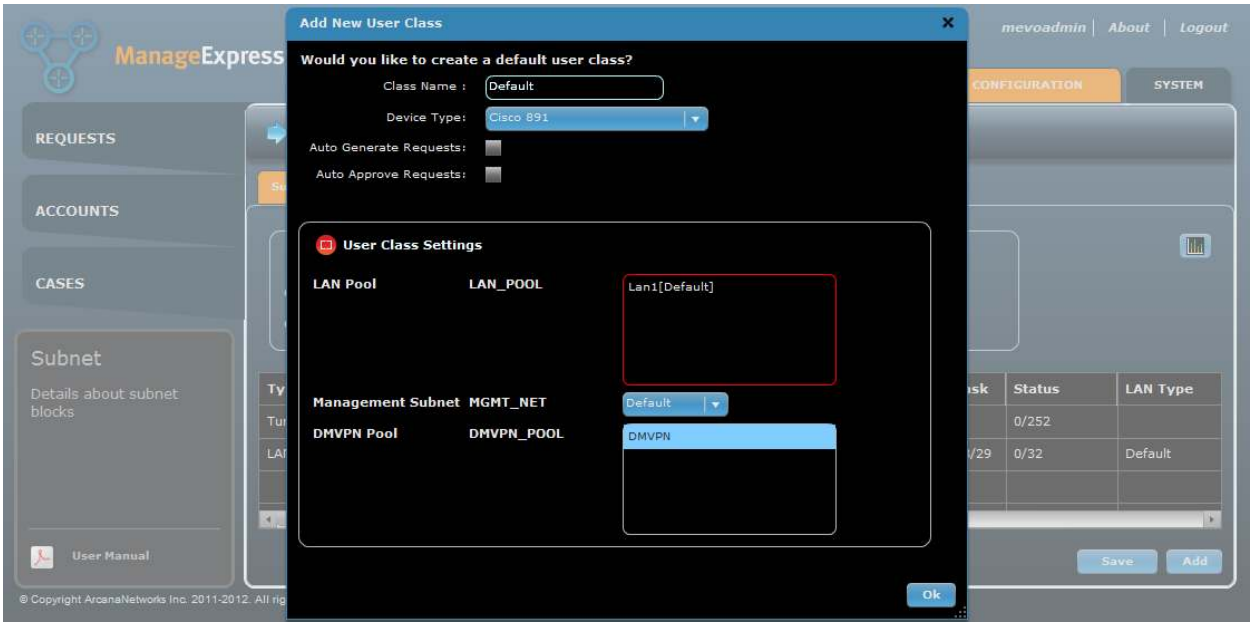
2. Click Add to configure a LAN subnet for the spoke routers. This LAN subnet should be network-routable and assigned uniquely to the Cisco Virtual Office spoke routers.
   a. In the Name field, enter the name of the subnet. This name should be uniquely defined. This name will be used as a key to be associated with a user class as discussed later in this document.
   b. The Type should be LAN, and the LAN Type should be left as **"Default".**
   c. In the Network Address field, enter the starting network address of your LAN subnet. Select the subnet size for this network from the Subnet drop-down menu. The range of IP addresses in the Network Address and Subnet fields will be automatically divided and assigned sequentially to each spoke based on the chosen LAN Subnet Mask.
   d. Enter any Subnet IP address ranges that should be excluded in the Exclude Start IP Address and Exclude End IP Address field and click Add to add them to the Exclude IP Address List. Click Delete to remove IP addresses from the Exclude IP Address List.
   e. Click Ok when you are finished (Figure 21).

Figure 21. Enter naming and IP addressing details to add a subnet.



3. Once the LAN is saved you will be prompted to create a default User Class. Leave the “Default” class name, select the appropriate Device Type and click on the name of your subnet block in LAN Pool and click on “Ok” (Figure 22). For a description of User Class see the “User Classes and Users” section in this document. For more detailed information about User Classes please refer to the full User Guide available from the ArcanaNetworks download site.

Figure 22. Add new Default User Class

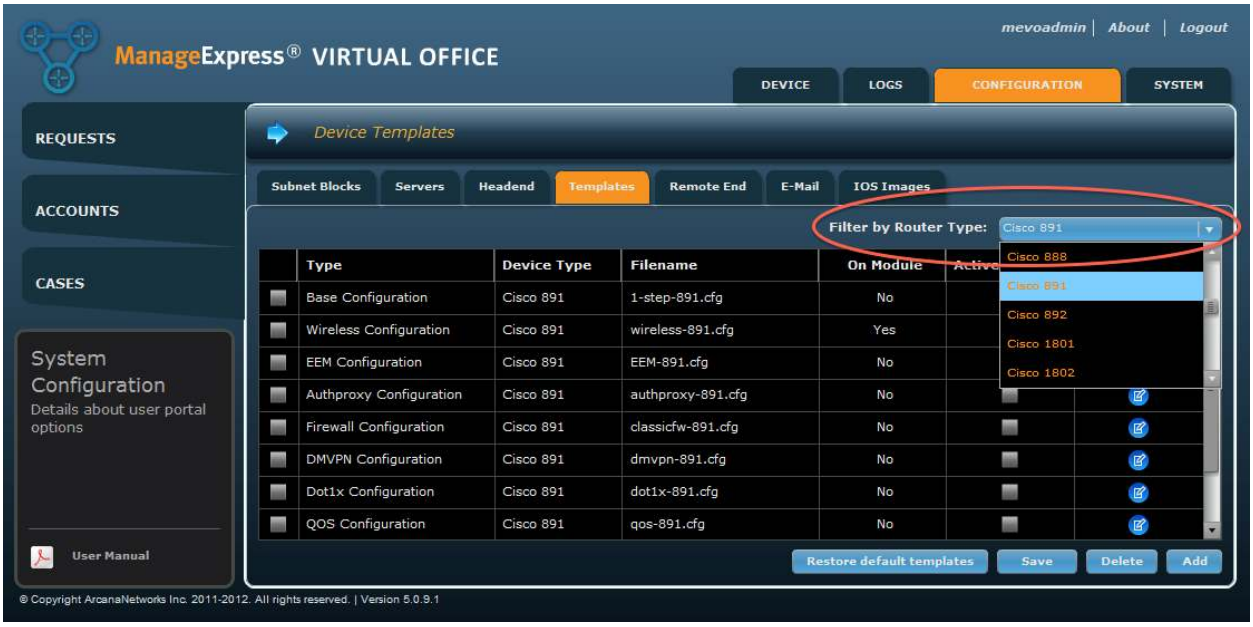


Step 5: Configuring ArcanaNetworks MEVO – Templates Selection

The Templates tab is used to set up configuration templates for the virtual office/spoke router. MEVO ships with default templates for the Cisco 881 and Cisco 891 ISRs,, in addition to several universal templates. You can also define your own templates by clicking on the “Add” button. For more information about templates, please refer to the MEVO User Guide on the ArcanaNetworks download site: http://downloads.arcananet.com/mevo.

1. Click on the Templates tab and choose the correct model from the Filter by Router Type dropdown. (Figure 24).

Figure 23. Choose a Router Type to select Templates for.

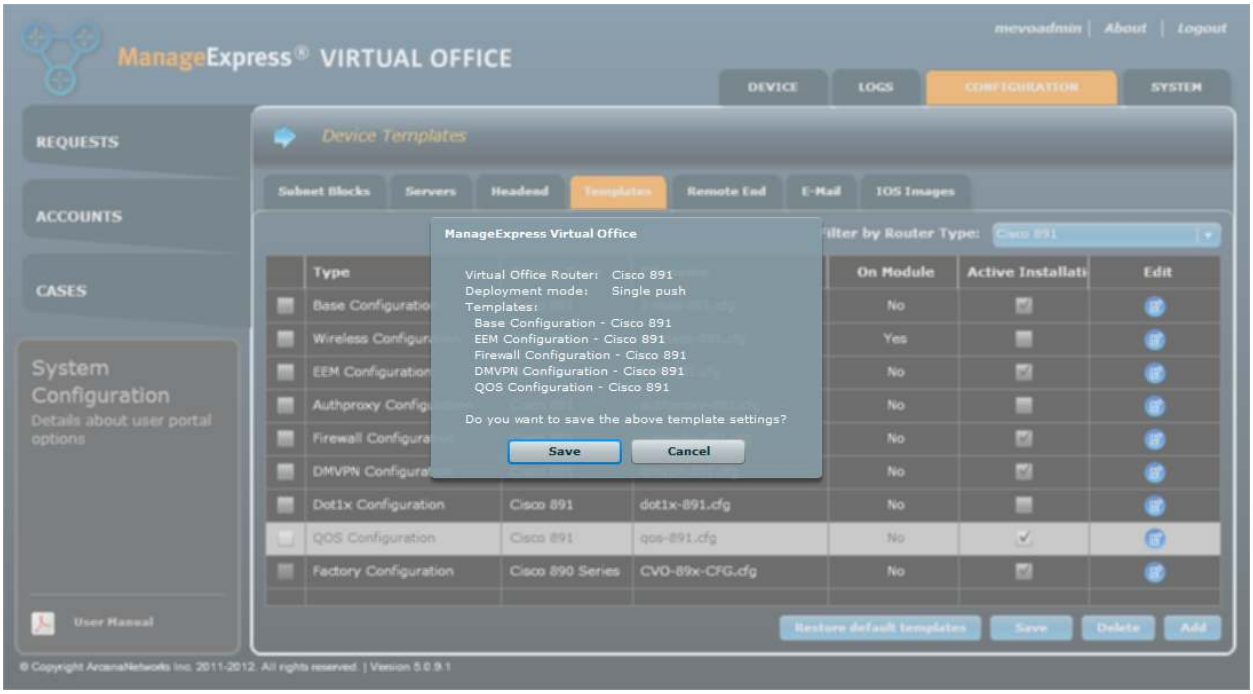


2. The minimum set of “Active” templates should be: Base, EEM, Firewall, DMVPN, , and Factory Configuration (Figure 25).

Figure 24. Select templates to be deployed to remote routers.

3. Save the Active templates for the selected router type by clicking on “Save”. Verify that the selected Templates are correct in the popup and click on “Save”. (Figure 26).

Figure 25. Verify the list of templates before clicking Save.

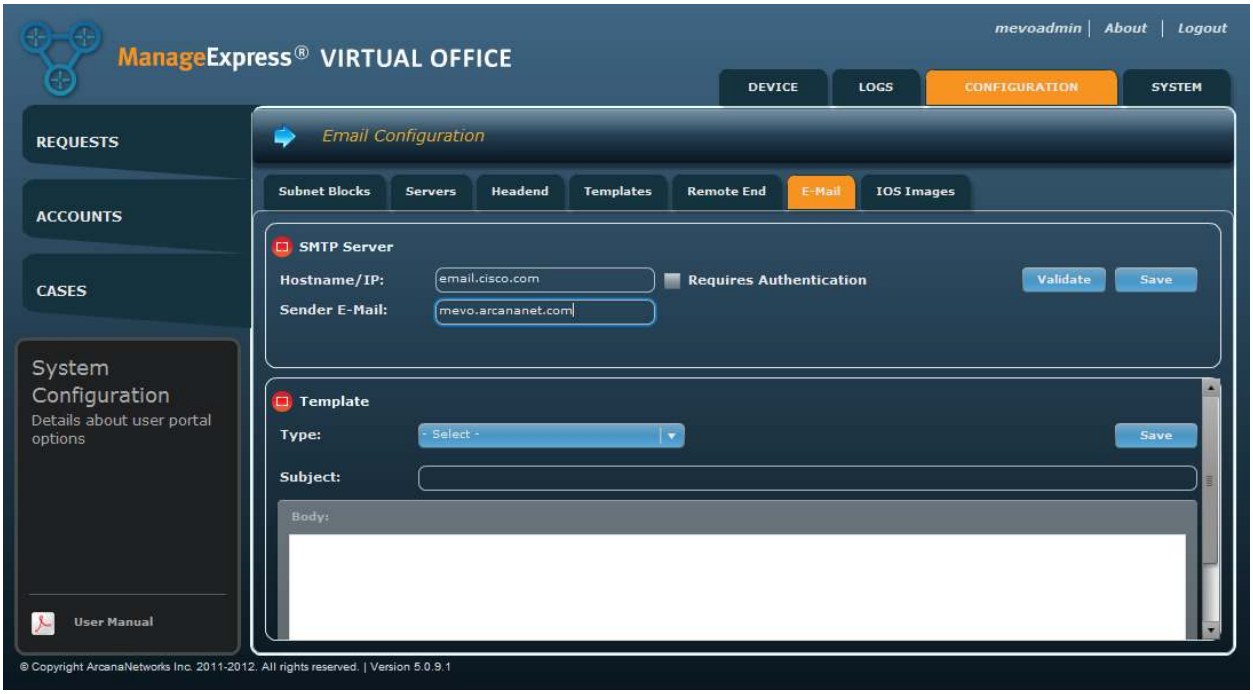


Step 6: Configuring Email

MEVO sends out customizable email notifications for certain system events. In order for notifications to be sent, MEVO requires that SMTP server information be configured. If desired, message templates can be customized.

1. Click Email and for the Simple Mail Transfer Protocol (SMTP) server, enter the hostname or IP address and the sender email address (Figure 27).

Figure 26. Configure email settings.



Administrator Tasks: User Classes and Users

MEVO uses the concept of user classes, allowing easy management of users with different configurations. There must be at least one user class, and each user can belong to one and only one class. User Classes are an essential part of managing disparate regions, network requirements, configurations, and remote end router types. User class specific variables can be used to customize the configuration templates for the different classes. For the purpose of getting started with MEVO the “Default” User Class that is created when adding your first LAN subnet should be sufficient. For more detailed information please refer to the full MEVO User Guide available from the ArcanaNetworks download site: http://downloads.arcananet.com/mevo.

A common example for requiring multiple user classes is a customer with employees divided between the East Coast and West Coast of the United States. In this case, the administrator may want to define two user classes, one for East Coast users and one for West Coast users, because the two groups may connect to different Cisco Unified Communications Manager clusters, etc. Another common example is a customer with employees who are using both Cisco 881 and 891 ISRs. In this case, the administrator may define two user classes, one for Cisco 881 ISR users and one for Cisco 891 ISR users, because the configurations on each type of platform may be slightly different. In addition to requiring a User Class, a spoke user must have an associated “Approver”. Hence, at least one user account with the special role of “approver” must be created prior to adding spoke users.

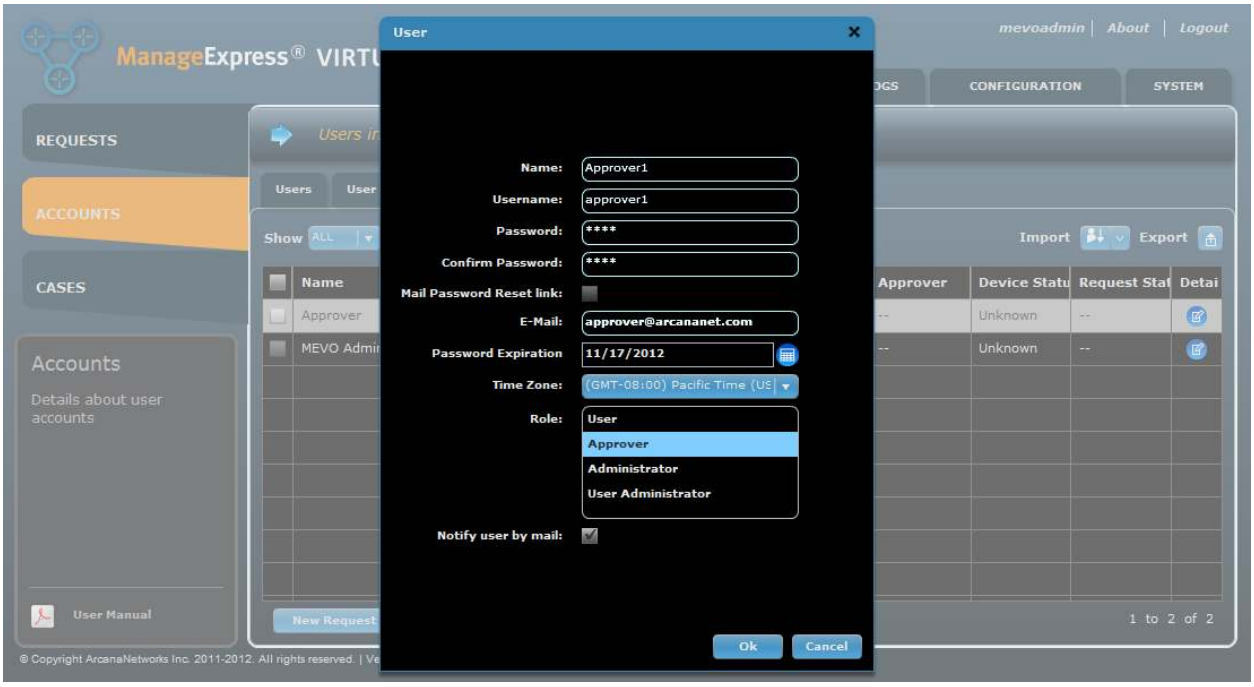
Note: “Users” in this section do not include Administrators or User Administrators which can be added at any time.

Adding User Accounts

1. You must first add an “Approver” privileged account before you can create a regular User. To add an individual user go to Accounts > Users and click on “Create User” at the bottom of the screen and enter the required

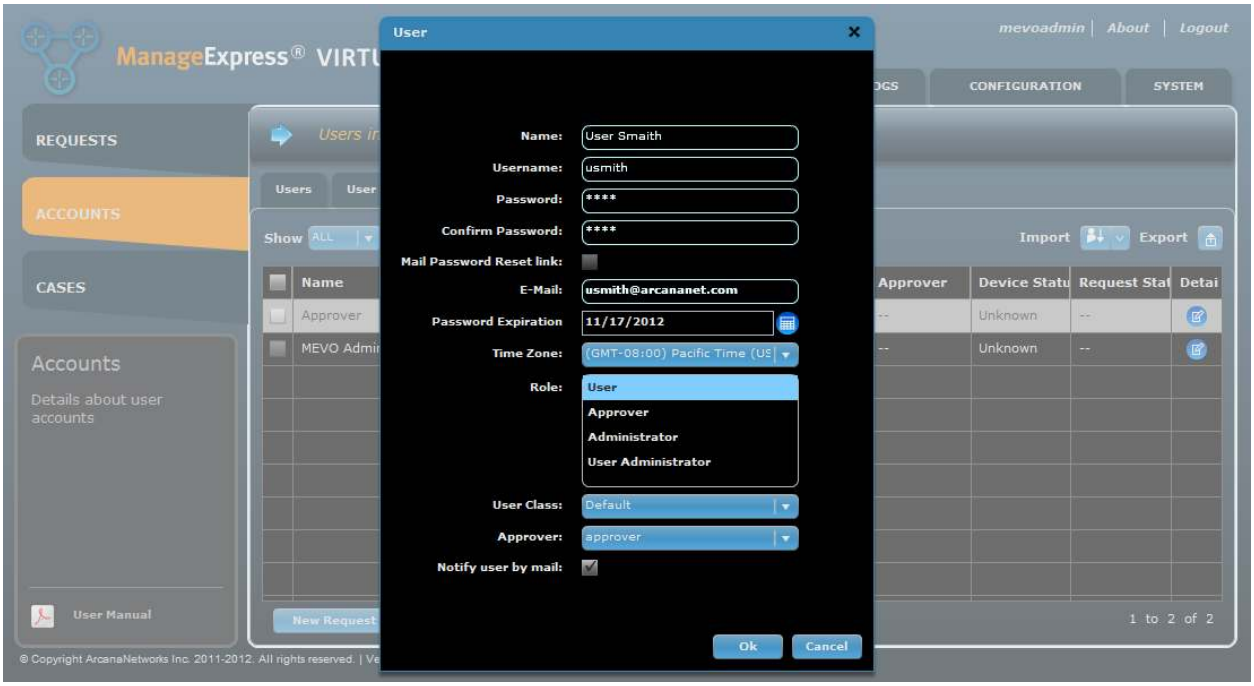
information. When you are finished, click Ok (Figure 28). The steps are the same regardless of the type of user being added. Simply be sure to add an Approver account prior to adding a normal user.

Figure 27. Adding an individual user manually.



2. After creating your “Approver” you can then add your regluar end user accounts used for Cisco Virtual Office provisioning (Figure 29). When the Role “User” is selected the default User Class created while adding the LAN Subnet and the Approver created in Step 1 will be automatically populated.

Figure 28. Adding an end user account



Note: MEVO has the ability to import Users in bulk from a CSV file, or add users transparently from an external authentication server to the MEVO database upon login. To learn how to import users from CSV or transparently, please refer the full User Guide available from the ArcanaNetworks MEVO download site: http://downloads.arcananet.com/mevo.

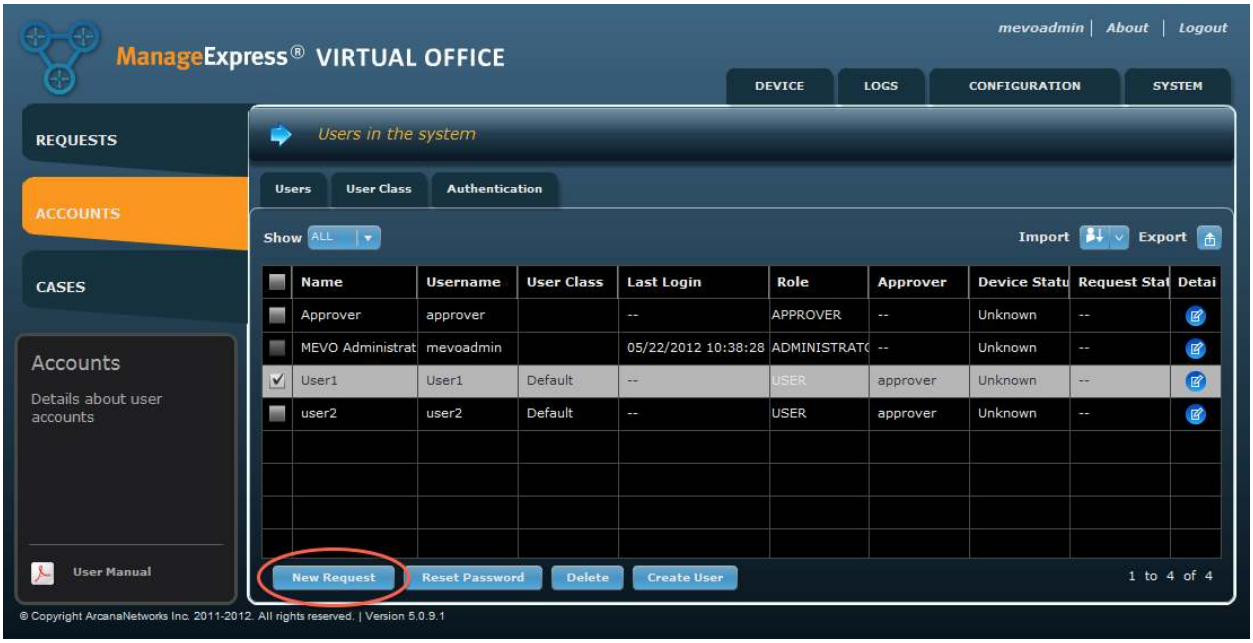
Requesting Cisco Virtual Office

MEVO provides several possible workflows for requesting and approving Cisco Virtual Office, ranging from end users signing up and submitting a request that is then approved, to the simplest method of an administrator requesting the service on behalf of a user. The administrator requested service workflow is covered here since it is the most direct and common method being used. For additional information on service request workflows please refer to the full MEVO User Guide on the ArcanaNetworks download site: http://downloads.arcananet.com/mevo.

Requesting Cisco Virtual Office on behalf of a user

1. Open a web browser, type the same URL as you entered when you first logged in (http://<ip-address-or-domain-name>/mevo), and log in with the admin credentials.
2. Go to the Accounts tab and select the Users tab. The admin will see the list of all users.
3. Select the user(s) that need Cisco Virtual Office and click New Request (Figure 29).

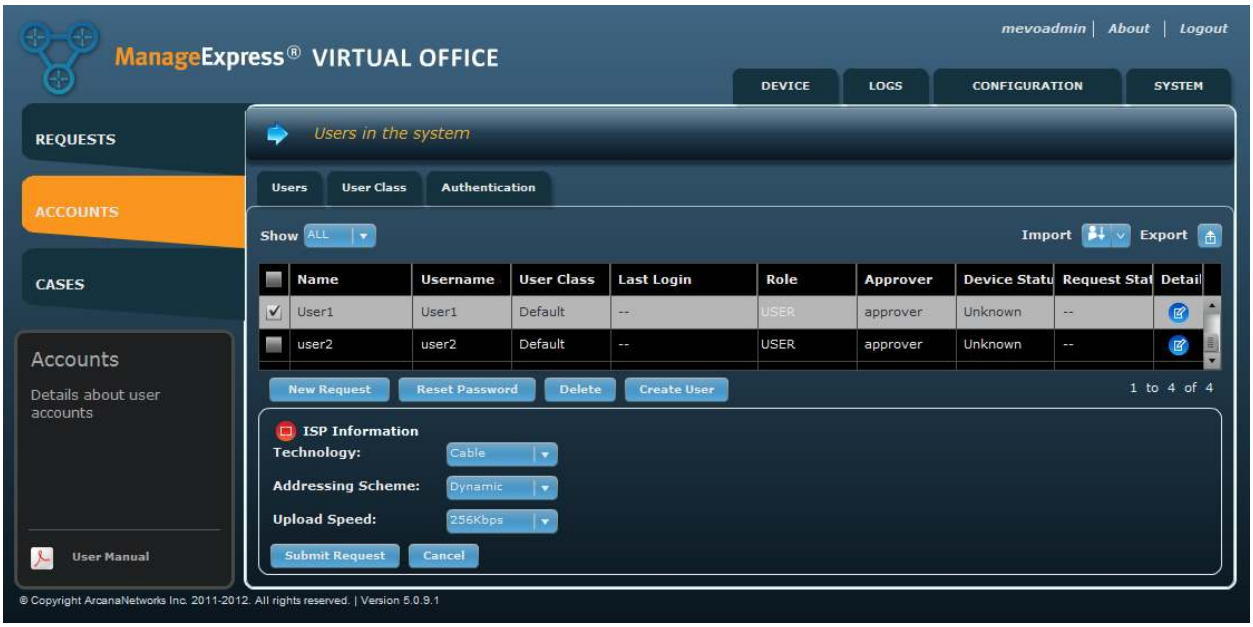
Figure 29. Create a New Request as Administrator.



4. Enter the ISP information: the Broadband, Addressing Scheme, and Upload Speed settings for the user. The admin should pick the average Upload Speed all users will have if adding more than one user at a time. Click Submit Request to submit the request.

Note: Upload Speed is used to adjust the QoS settings on the spoke router (Figure 30).

Figure 30. Enter ISP information for the end user(s).



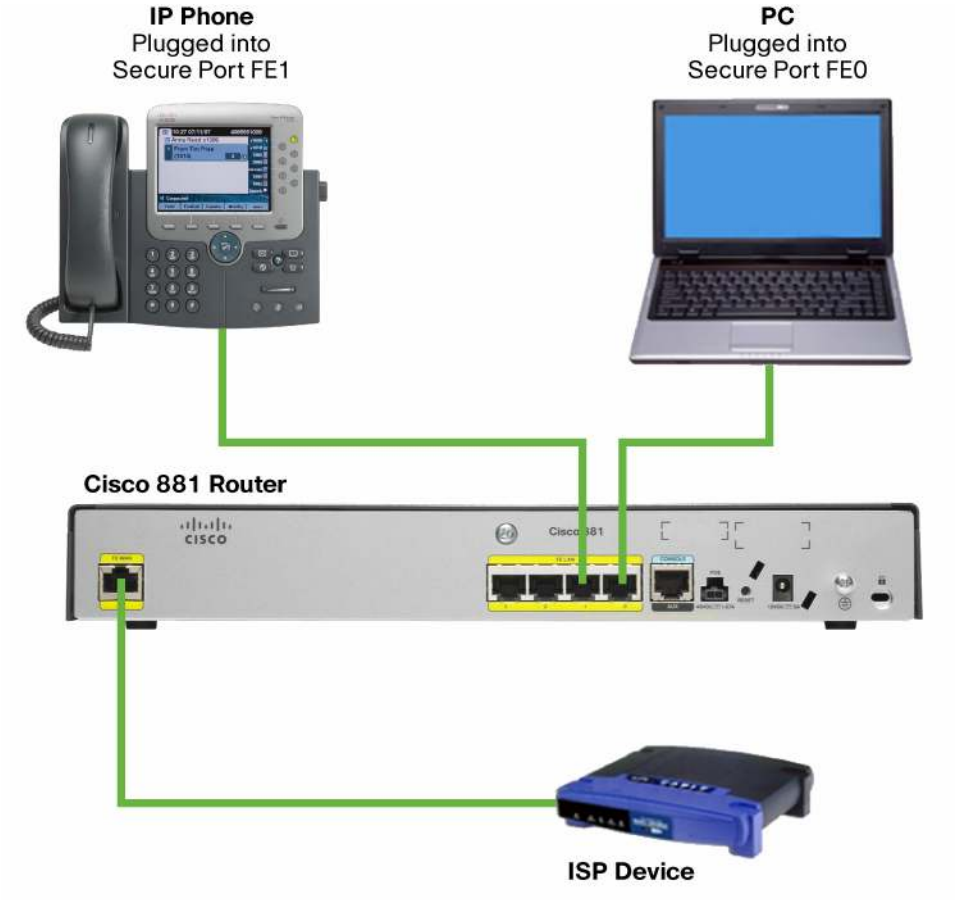
End-User Provisioning

This section describes the SDP process from the end-user's perspective and shows what needs to be done after the user receives the router at the remote location. Typically, the end user will receive a router with factory-default settings with instructions for setup and an email message to access the provisioning page (described in more detail in the steps that follow). In the case of a branch office or clinic, a technician or administrator at the branch office or clinic would most likely perform this process.

The steps presented here assume that an Internet connection is available with DHCP. Variations such as connection through DSL or a static IP address are also possible with a few modifications, but the basic steps performed by the end user remain the same.

1. Set up the router according to Figure 31.

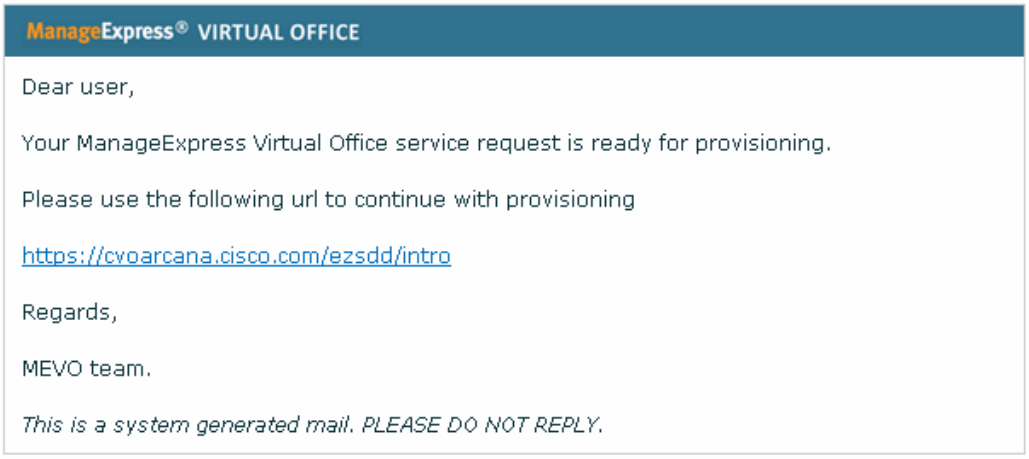
Figure 31. Router setup.



Routers ordered with the Cisco Virtual Office option come with a factory-default configuration that has DHCP enabled on the WAN side. After connecting according to the setup, you should have Internet connection through your PC.

1. After the configuration is generated on ArcanaNetworks MEVO, you will get an email message similar to the one shown in Figure 32 with a link to start the SDP process. Click the link to continue.

Figure 32. Sample email with link to start the SDP process for Cisco Virtual Office.

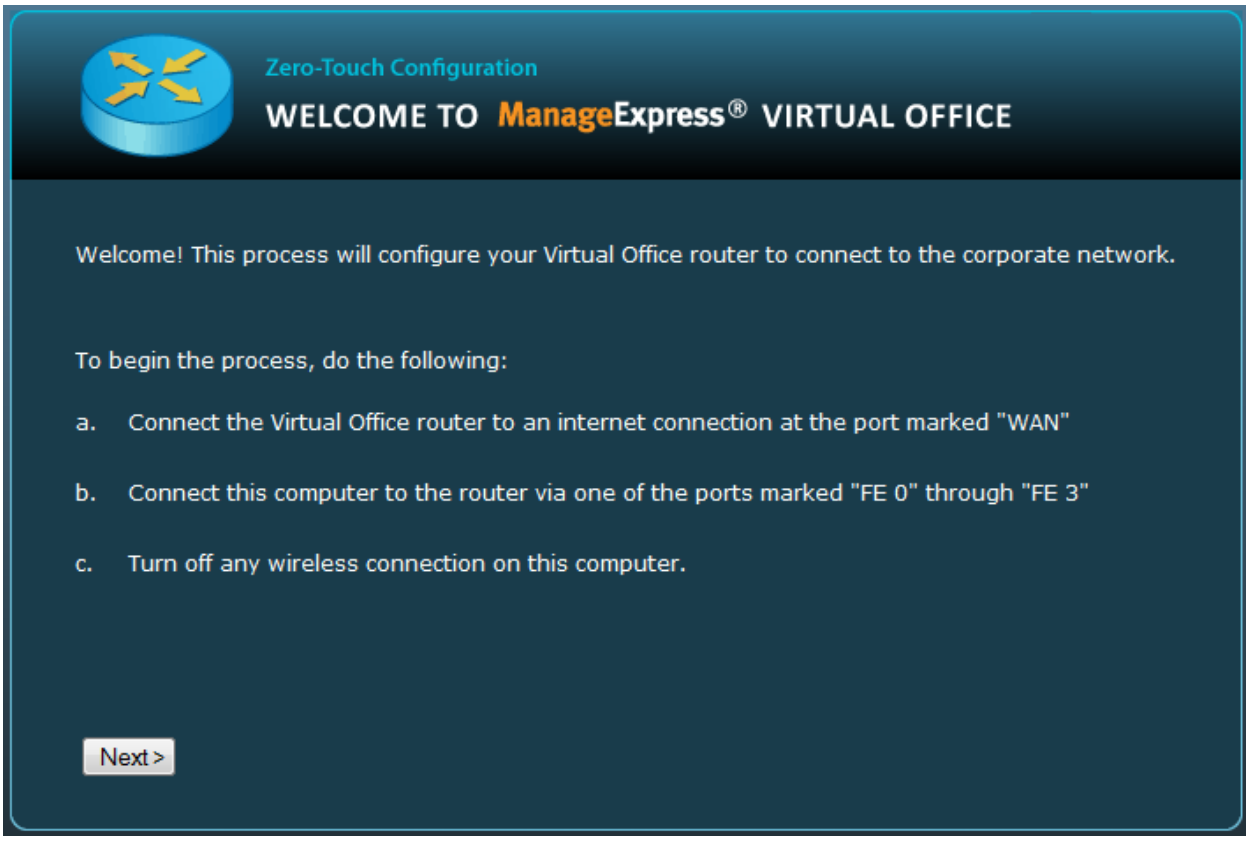


1. Enter the appropriate AAA credentials when the pop-up screen asks for user credentials (Figure 33).

Figure 33. User enters the appropriate AAA credentials to verify identity before the SDP process can start.

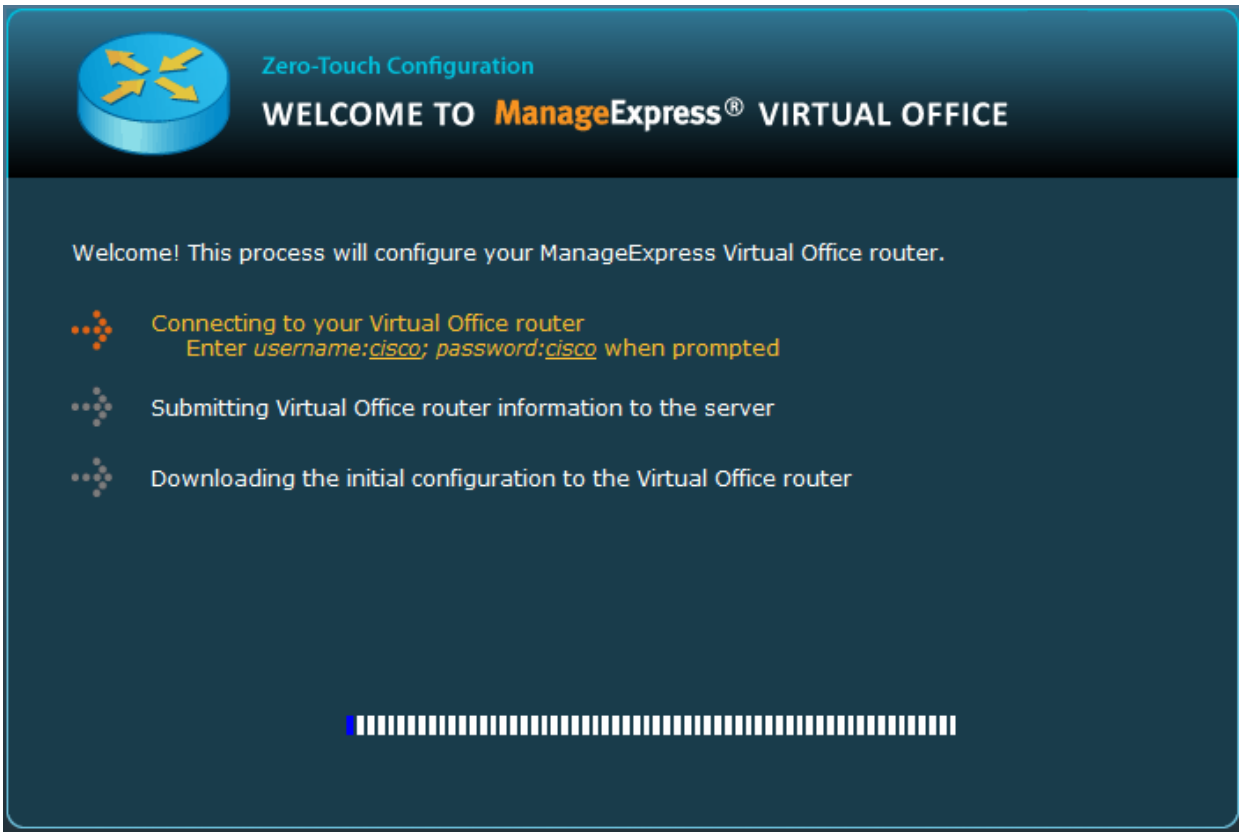
1. Click Next on the welcome screen to begin provisioning the router (Figure 34).

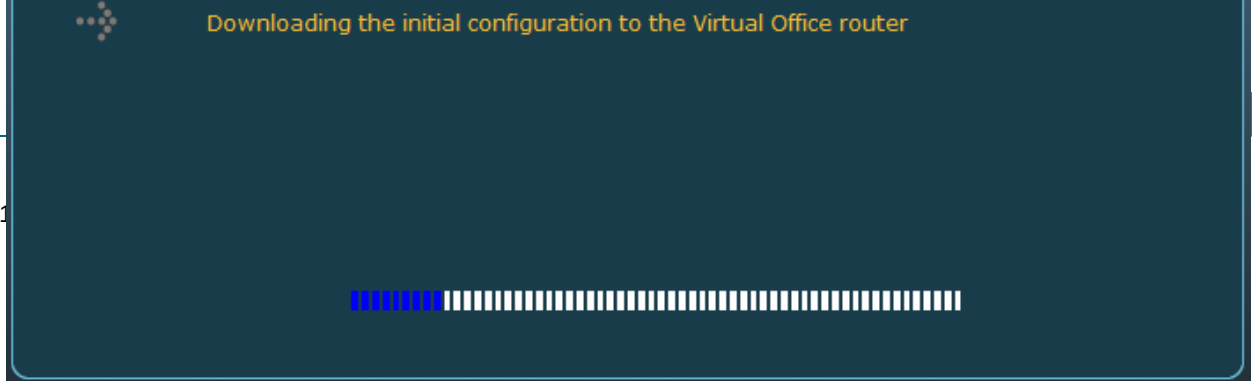
Figure 34. Welcome screen for Cisco Virtual Office's zero-touch router provisioning. User clicks "Next" button to begin.

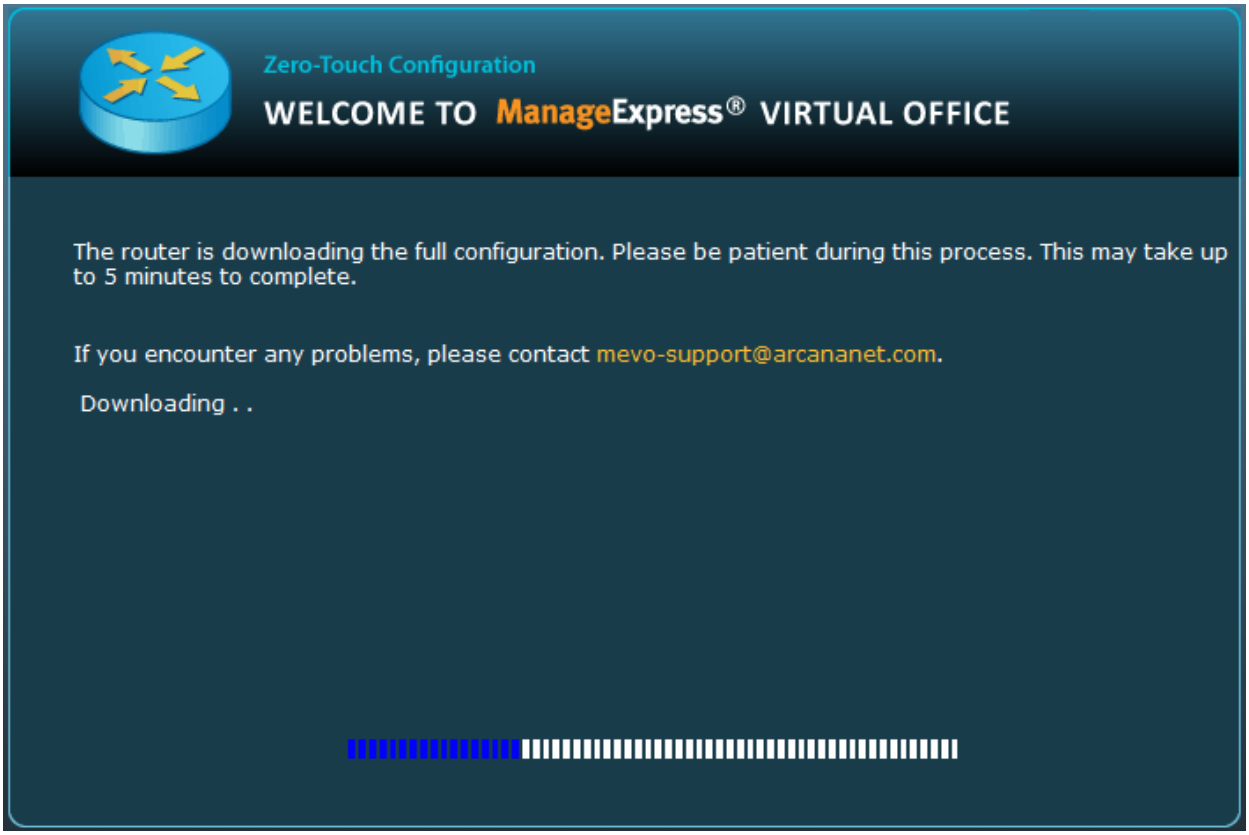


1. ArcanaNetworks MEVO will connect to the router to begin configuration (Figure 35).

Figure 35. ArcanaNetworks MEVO connects to the router to begin configuration.

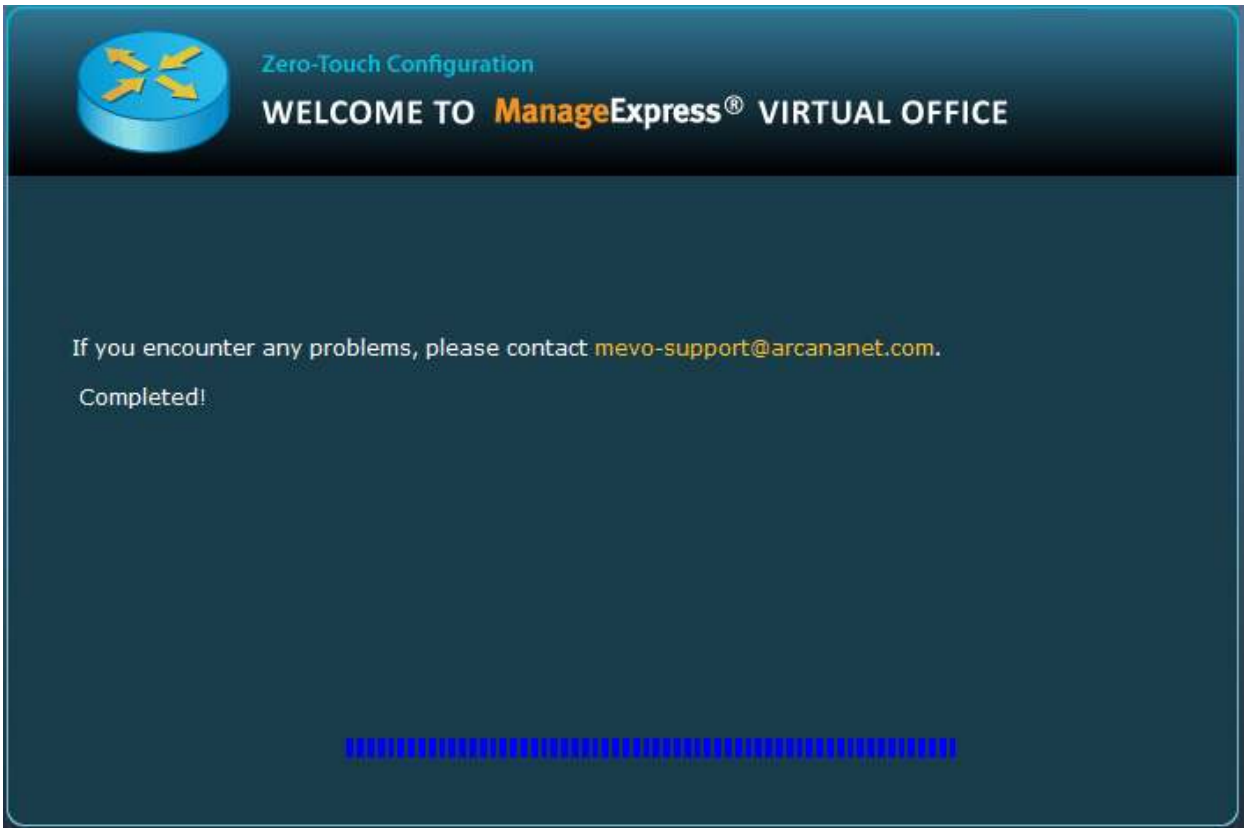






When the process is finished, the router is fully configured with access to the corporate network (Figure 37).

Figure 37. Once the router configuration push is complete, the user will be able to connect to the corporate network.



Appendix

Updating the Configuration

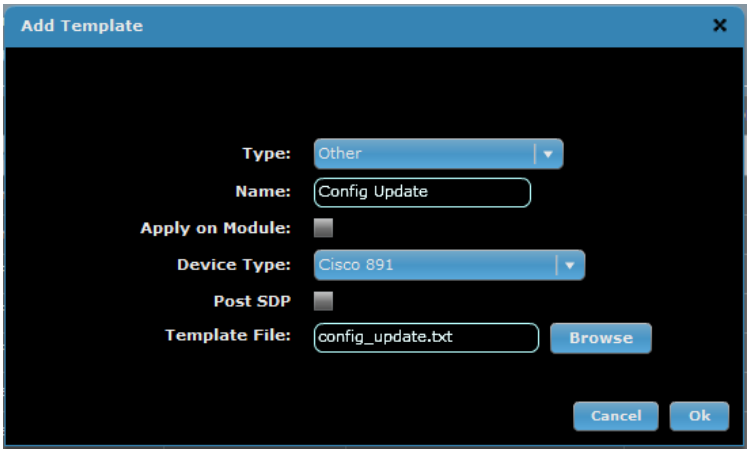
After a router is deployed and connected, the administrator can use the steps shown here to add a new configuration template to ArcanaNetworks MEVO and then push the configuration to the remote Cisco Virtual Office routers.

Step 1: Add a New Configuration Template to ArcanaNetworks MEVO.

Note: If you are only modifying an existing configuration template, go to Step 2 and make the changes (skip Steps 1 and 3).

1. Create a new configuration in a text file and save it.
2. Log into ArcanaNetworks MEVO and choose Configuration > Templates.
3. Click the Add button at the lower right and enter or select the information as listed here. When you are finished, click Ok (Figure A1).
   a. Type: Choose the type of configuration to be added: Authproxy, DMVPN, Dot1x, EEM, Base, Other, or Firewall. If you choose Other, provide a name for the configuration.
   b. Apply on Module: Select this option if the configuration is to go on a module within the router (for example, wireless configurations on the Cisco 881 ISR will need Apply on Module selected).
   c. Device Type: Choose the device platform on which the configuration is to be used. If the configuration is the same for all device types, choose Universal.
   d. Post SDP: Select the checkbox if the configuration is to be pushed after SDP is completed. In most cases, this option does not need to be selected.
   e. Template File: To upload the configuration file you created, click the Browse button and choose the file.

Figure A1. Add a template.

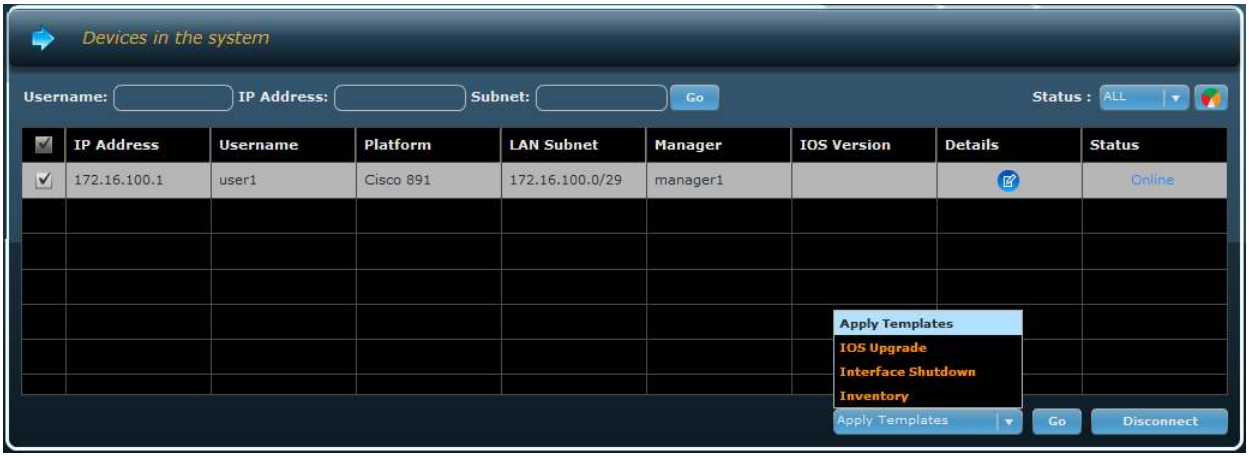


Step 2: Apply the Configuration Update to Deployed Routers

1. On the Device tab, select the devices that require a configuration update.
2. Choose Apply Templates and then click Go (Figure A2).

Note: Currently, only devices that are online can be updated.

Figure A2. Apply template

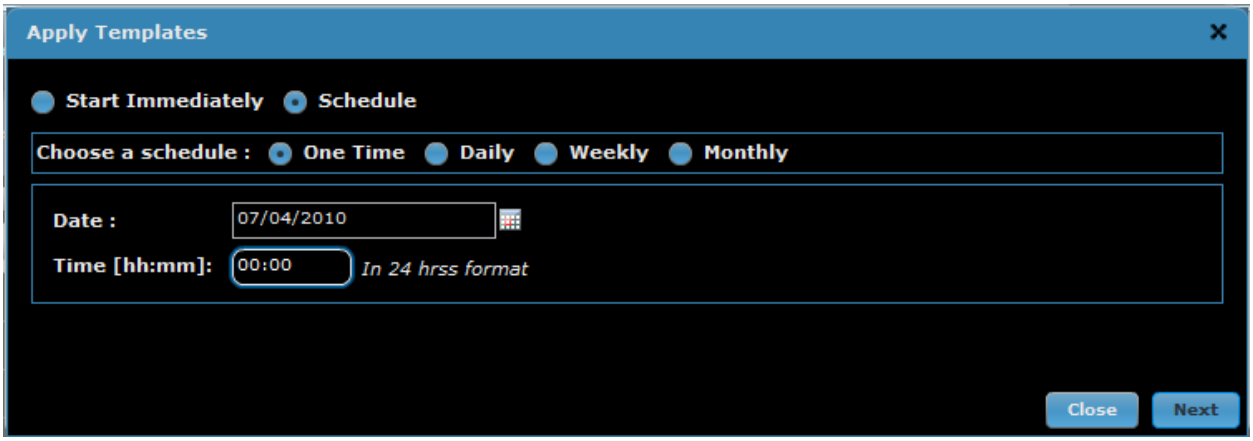


1. Select the configuration templates to be applied; then click Next.

Note: Base Configuration and EEM Configuration cannot be changed after provisioning.

1. To apply the configuration update immediately, select Start Immediately, or to select the date and time to apply the update, select Schedule. Click Next to complete the update or schedule (Figure A3).

Figure A3. Schedule time for template push.



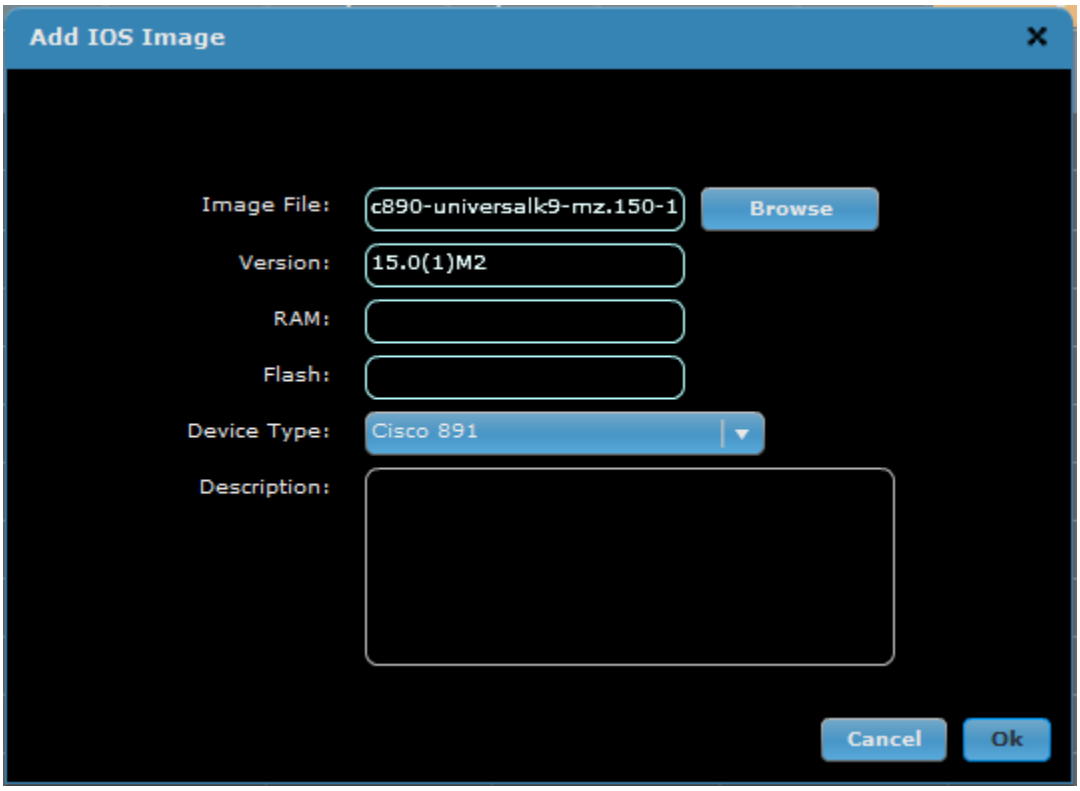
Updating the Image

This section describes how the administrator can add Cisco IOS Software router images to ArcanaNetworks MEVO and push the images to connected remote routers.

Step 1: Add a New Image to ArcanaNetworks MEVO

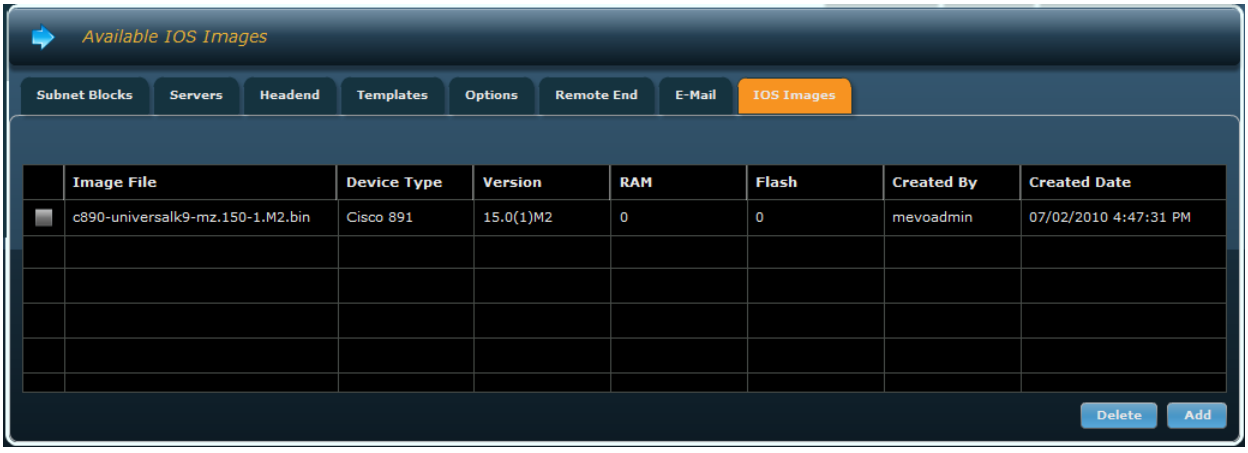
1. Log into ArcanaNetworks MEVO, choose Configuration > IOS Images, and click Add.
2. Browse to select the image file to be added, enter the image version, and select the device type. RAM, Flash, and Description are optional (Figure A4).

Figure A4. Add a new image toArcanaNetworks MEVO.



1. When you are done, click Ok to finish adding the image (Figure A5).

Figure A5. New IOS image added to ArcanaNetworks.



Step 2: Apply the Image Update to Deployed Routers

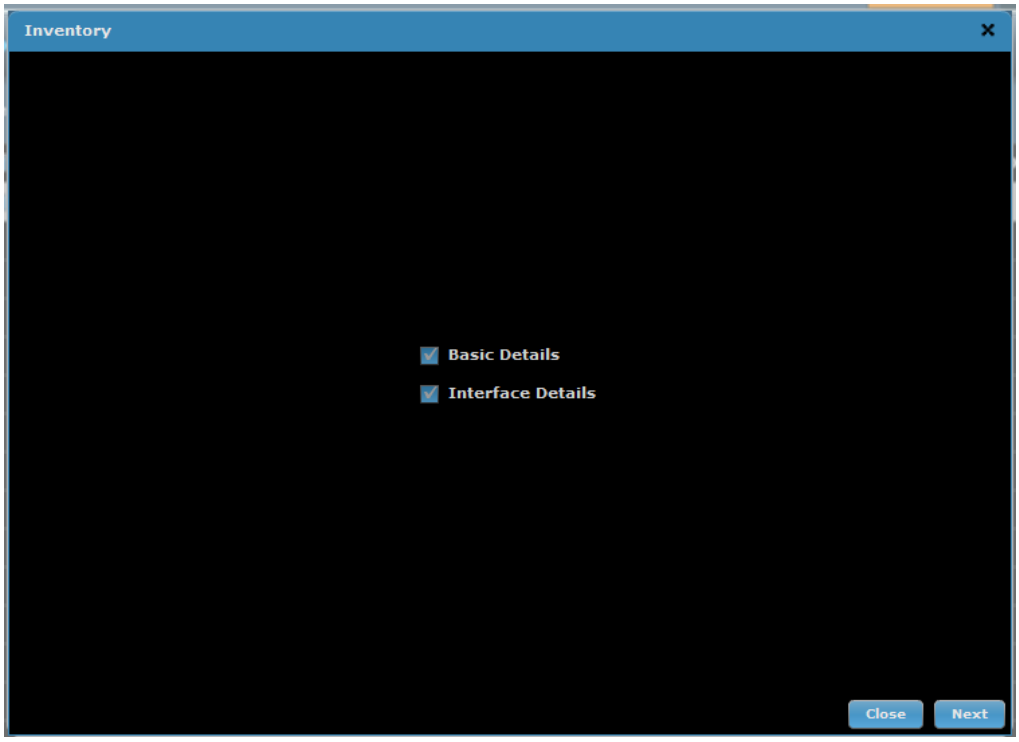
1. Under the Device tab in ArcanaNetworks MEVO, select the devices that require an image update.
2. At the bottom right, select IOS Upgrade and then click Go.

   If ArcanaNetworks MEVO asks for an inventory run, continue to Step 3; otherwise, skip to Step 4.

Note: Currently, only devices that are online can have image upgraded.

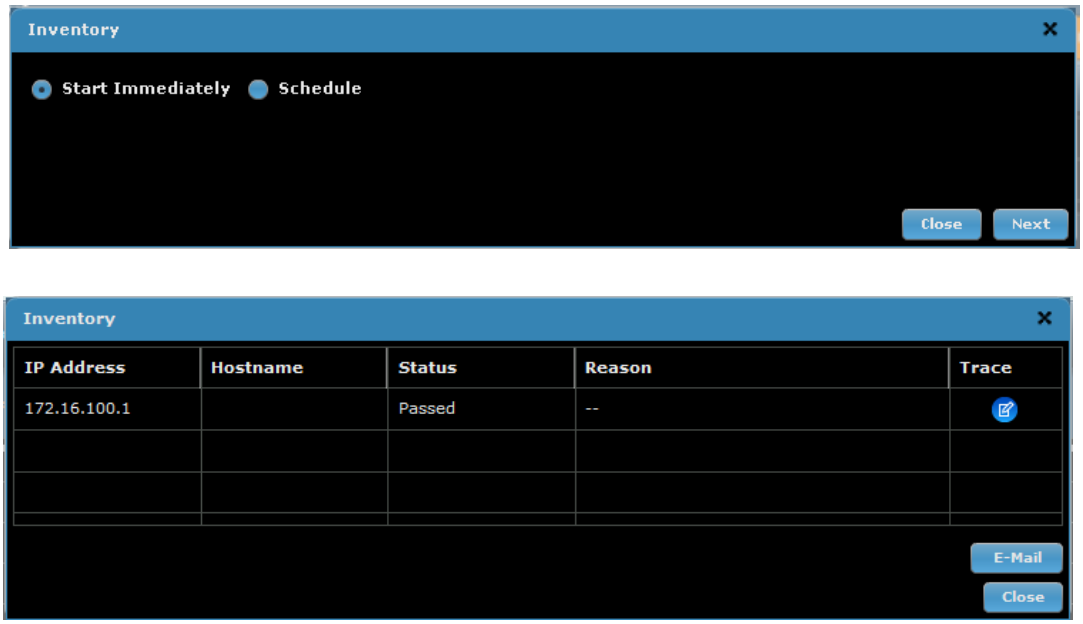
1. Run the inventory.
   a. Select the appropriate devices, select Inventory, and click Go.
   b. Basic Details and Interface Details should be checked automatically. Click Next to continue (Figure A6).

Figure A6. Select Inventory settings.



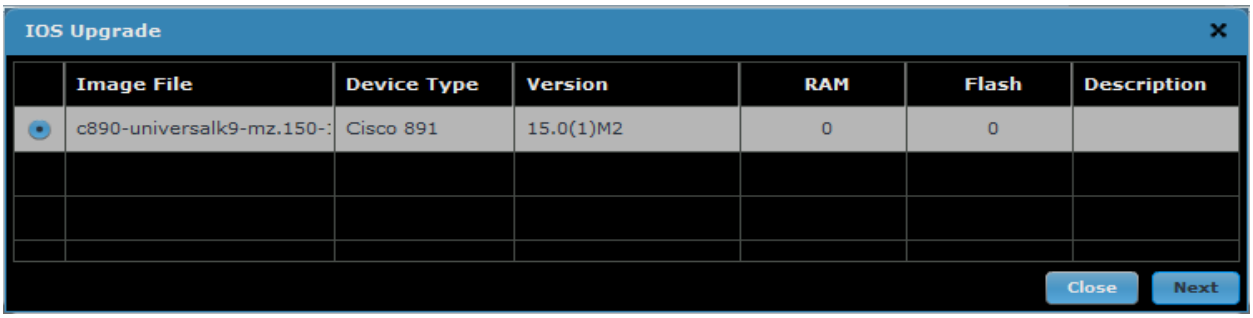
a. Select the Start Immediately button and click Next to complete the inventory run (Figure A7).

Figure A7. Schedule inventory or start immediately. Inventory will show status of “Passed” if successful.



1. Select the image to be pushed to the routers and click Next to complete the image update (Figure A8).

Figure A8. Select image for the image push.



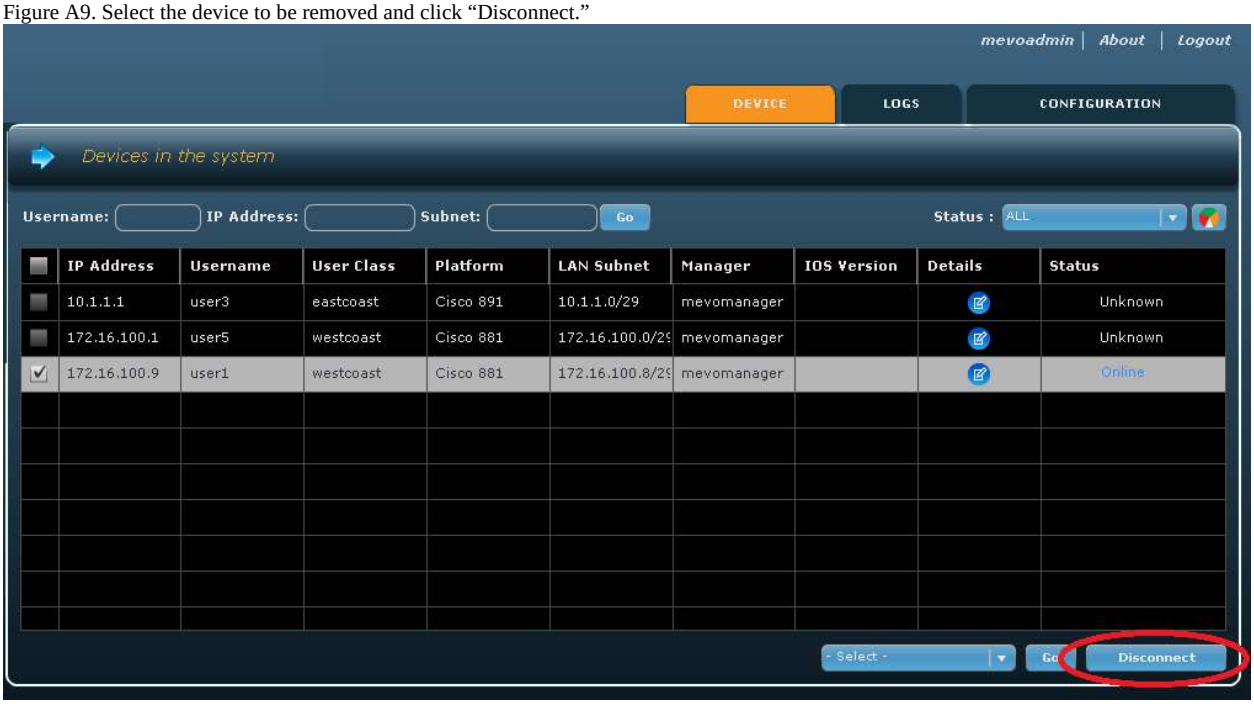
Disconnecting a Device and Removing a User

This section describes how the administrator can remove a spoke router that has already been provisioned and deployed.

1. Click the Device tab, and go to the chart view.
1. Select the device to be removed and click Disconnect to remove the device. ArcanaNetworks MEVO will use SSH to access that device and reload the router with the default configuration, thereby disconnecting the router from the network. ArcanaNetworks will also remove the device profile on the Cisco ACS for that device if PKI-AAA is enabled (Figure A9).

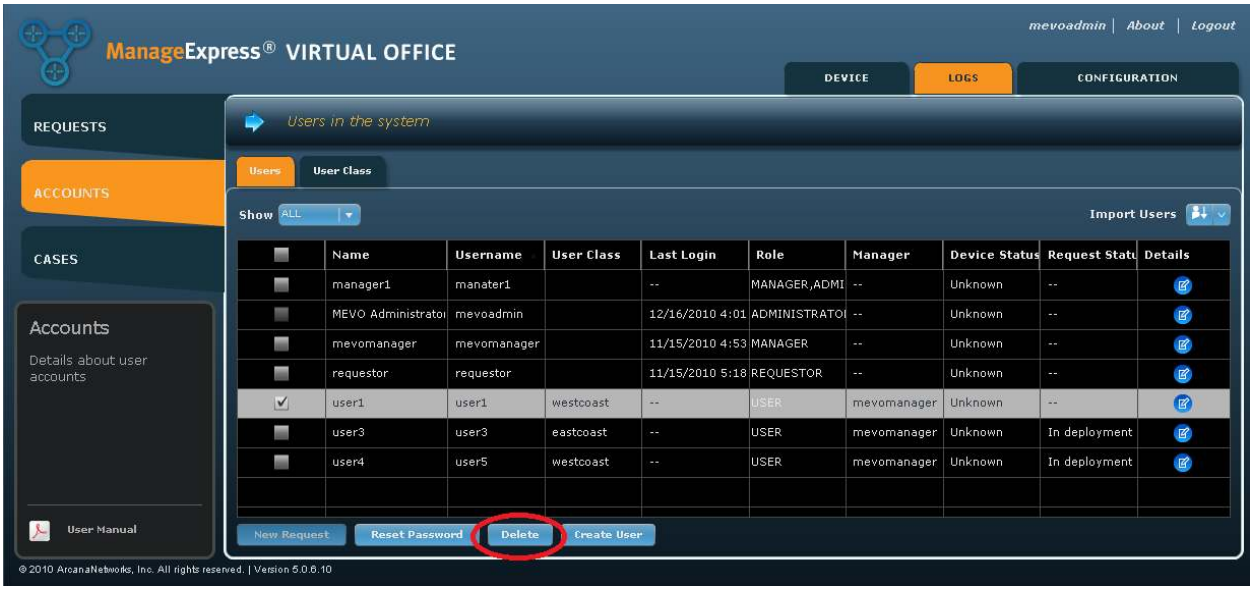
Note: The device must be online in order for it to be removed. If the device is not currently online, you can still remove the user (see step 3). ArcanaNetoworks currently removes the device profile automatically with Cisco ACS Version 5.0.

Figure A9. Select the device to be removed and click "Disconnect."



1. Delete the user associated with the device under the Accounts > Users page (Figure A10).

Figure A10. Delete the user associated with the removed device.



1. Remove the user profiles from the Cisco ACS.
2. Revoke the router certificate from the CA server.

   If you are using a Cisco IOS Software router as the CA server, use the following command:

   crypto pki server ***cs-label*** revoke ***certificate-serial-number***

For More Information

Cisco Virtual Office homepage

- http://www.cisco.com/go/cvo

Configure and Enroll a Cisco IOS Software Router to Another Cisco IOS Software Router Configured as a CA Server

- http://www.cisco.com/en/US/tech/tk583/tk372/technologies_configuration_example09186a0080210cdc.shtml

User Guide for the Cisco Secure Access Control System 5.1

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/user/guide/acsuserguide.html

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.**

Printed in USA C07-641108-00 1/11