

# Cisco Virtual Wireless Controller Deployment Guide

**Document ID: 113677**

Introduction

Prerequisites

Virtual Controller Support

Virtual WLAN Controller Unsupported Features

Single Virtual Controller Resource Requirement

Suggested Hardware Recommendations for Hosting Cisco Virtual Controllers

AP Requirement

Components Used

Topology

Conventions

Release Notes

Virtual Controller Installation

Virtual Controller Virtual Interfaces

Switch Interface Configuration Connected to UCS Server

VMware Promiscuous Mode Definition

Virtual Controller Settings

Virtual Controller Console Port

Start up the vWLC

Virtual Controller Management with Cisco Prime 1.2

Upgrade the Virtual Controller

Troubleshooting

AP Considerations

Time is Incorrect

SSC Hash

Related Information

## Introduction

Prior to release 7.3, wireless LAN (WLAN) controller software ran on dedicated hardware you were expected to purchase. The Virtual Wireless LAN Controller (vWLC) runs on general hardware under an industry standard virtualization infrastructure. The vWLC is ideal for small and mid-size deployments with a virtual infrastructure and require an on-premises controller. Distributed branch environments can also benefit with a centralized virtual controller with fewer branches required (up to 200).

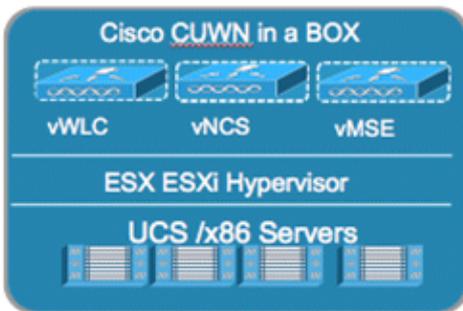
vWLCs are not a replacement of shipping hardware controllers. The function and features of the vWLC offer deployment advantages and benefits of controller services where data centers with virtualization infrastructure exist or are considered.

Advantages of the vWLC:

- Flexibility in hardware selection based on your requirements.
- Reduced cost, space requirements, and other overheads since multiple boxes can be replaced with single hardware running multiple instances of controllers, network management devices (NCS) and other servers (ISE, MSE, VSG / firewall).
- Independent and mutually exclusive instances allow administrators to use multiple virtual controllers to manage different campuses (or even to manage multiple customer sites) using the same hardware.
- Enable features provided by the virtualization software, including High Availability, failover protection, and ease of migration.

VMware benefits with the vWLC:

- **vSphere:** A virtualization infrastructure package from VMware, which includes ESX/ESXi hypervisor, vMotion, DRS, HA, Fault Tolerance, vSphere Distributed Switch, and more.
- **vCenter Server:** The VMware vCenter Server (formerly VMware VirtualCenter) provides a scalable and extensible platform that forms the foundation for virtualization management:
  - ◆ Centralized control and visibility at every level of virtual infrastructure
  - ◆ Pro-active management with vSphere
  - ◆ Scalable and extensible management platform with a broad partner ecosystem



## Prerequisites

### Virtual Controller Support

- Platform: AIR-CTVM-K9
- Hardware: Cisco UCS, UCS Express, HP and IBM servers
- VMware OS: ESX/ESXi 4.x/5.x
- FlexConnect Mode: central and local switching
- Licensing: Node locked licenses to UDI (eval 60 days)
- Maximum number of access points (APs): 200
- Maximum number of Clients: 3000
- Maximum number of sites up to 200
- Throughput performance up to 500 Mbps per virtual controller
- Management with Cisco Prime Infrastructure 1.2 and above

### Virtual WLAN Controller Unsupported Features

- Data DTLS
- OEAP (no data DTLS)
- Rate Limiting
- Internal DHCP server
- Mobility/Guest Anchor
- Multicast-Unicast mode
- PMIPv6
- Outdoor Mesh Access Points; an Outdoor AP with FlexConnect mode will work

### Single Virtual Controller Resource Requirement

- CPU: 1 virtual CPU
- Memory: 2 GB
- Disk Space: 8 GB
- Network Interfaces: 2 or more virtual Network Interface cards (vNICs)

# Suggested Hardware Recommendations for Hosting Cisco Virtual Controllers

- UCS R210–2121605W Rack Mount Server (2 RU):
  - ◆ 2 \* Intel Xeon CPU X5670 @ 2.93 GHz
  - ◆ 16 G memory
- IBM x3550 M3 Server:
  - ◆ 2 \* Intel Xeon 5600 series processors with 4 cores each and each core capable of doing hyper threading which gives you 16 CPUs in total @3.6 GHz
  - ◆ 12G memory
- ISR G2 Services Ready Engine (SRE) using UCS Express (Stretch goal):
  - ◆ SRE 700: Single Core Intel Core Duo 1.86 GHz with 4 GB memory
  - ◆ SRE 900: Dual Core Intel Core Duo 1.86 GHz with 4 GB memory (upgradable to 8 GB)

## AP Requirement

- All 802.11n APs with required software version 7.3 are supported.
- APs will be operating in FlexConnect mode only.
- AP autoconvert to FlexConnect is supported on controller.
- New APs ordered will ship with 7.3 software from manufacturing.
- Existing APs must be upgraded to 7.3 software before joining a virtual controller.

**Note:** The Virtual Controller in release 7.3 uses Self Signed Certificates (SSC) as against the Manufacturing Installed Certificates (MIC) in the traditional controller. The AP will be able to validate the SSC certificate provided by the virtual controller before joining. See AP Considerations in the Troubleshooting section for more details.

## Components Used

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

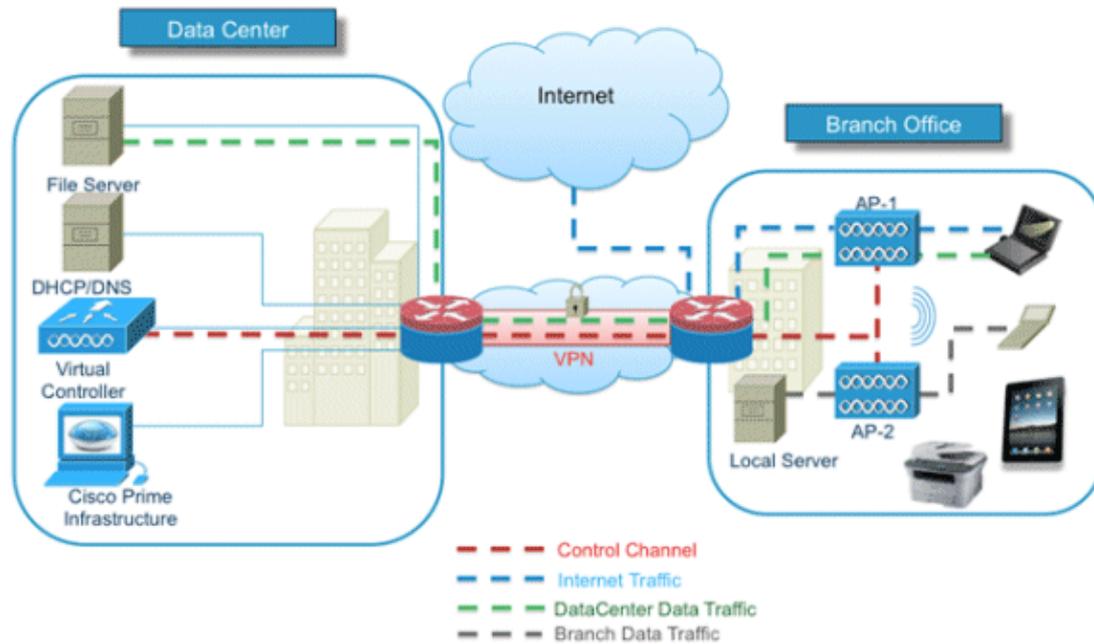
- Cisco Catalyst Switch
- Wireless LAN Controllers Virtual Appliance
- Wireless LAN Controller 7.3 Software
- Cisco Prime Infrastructure 1.2
- 802.11n Access Points in FlexConnect Mode
- DHCP server
- DNS Server
- NTP
- Wireless Client Laptop, Smartphone, and Tablets (Apple iOS, Android, Windows, and Mac)

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.

## Topology

In order to properly implement and test the Cisco vWLC, a minimal network setup is required, similar to the diagram shown in this section. You need to simulate a location with a FlexConnect AP in a centrally switched deployment, and/or with the addition of local and remote sites with local DHCP (better if there is also a DNS

and local access to Internet).



## Conventions

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

## Release Notes

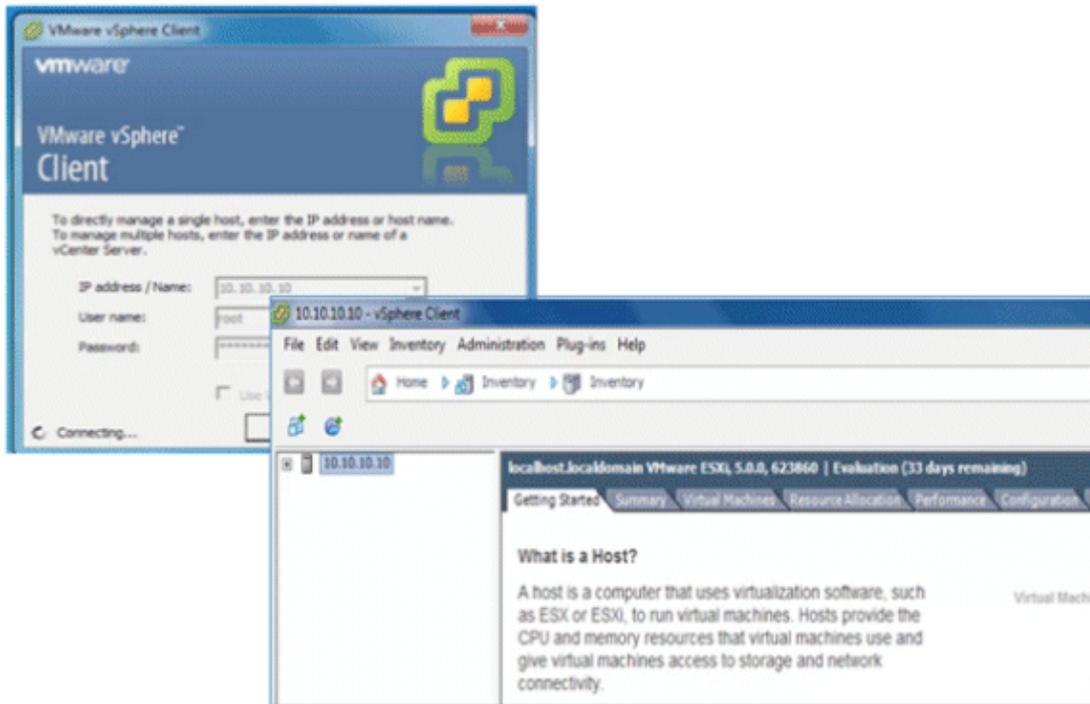
Cisco Unified Wireless Network (CUWN) 7.3 Release Notes contain important information about this release. Log in to Cisco.com for the latest release notes before loading and testing software.

## Virtual Controller Installation

For deployment and management of the vWLC, you will need to download any of these VMware suites to the workstation:

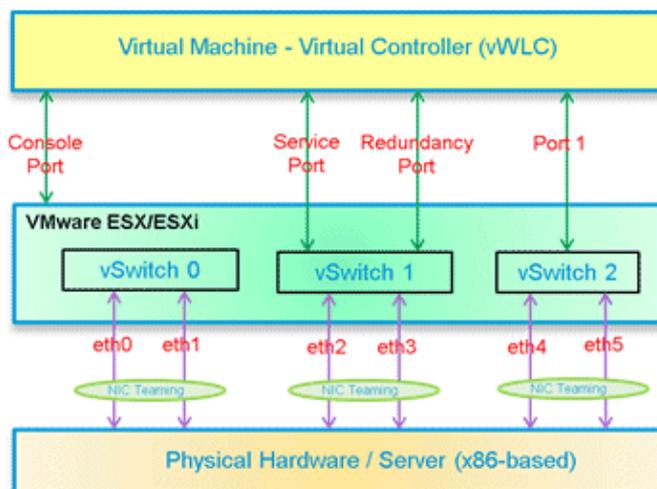
- Single ESXi server management – Use VMware vSphere Client.
- Multiple ESXi servers requires vCenter – Advance features are also tied with vCenter which needs separate licenses (vMotion, and so on).

Start the **VMware vSphere Client**, and log in to the ESXi server.



## Virtual Controller Virtual Interfaces

- Management Interface
- Virtual Interface
- Dynamic Interface
- AP Manager Interface



## Switch Interface Configuration Connected to UCS Server

This section provides a sample configuration of the Cisco Catalyst interface connection to the ESXi server for the virtual switch as trunk interface. The management interface can be connected to an access port on the switch.

```
interface GigabitEthernet1/1/2
description ESXi Management
switchport access vlan 10
switchport mode access
!
```

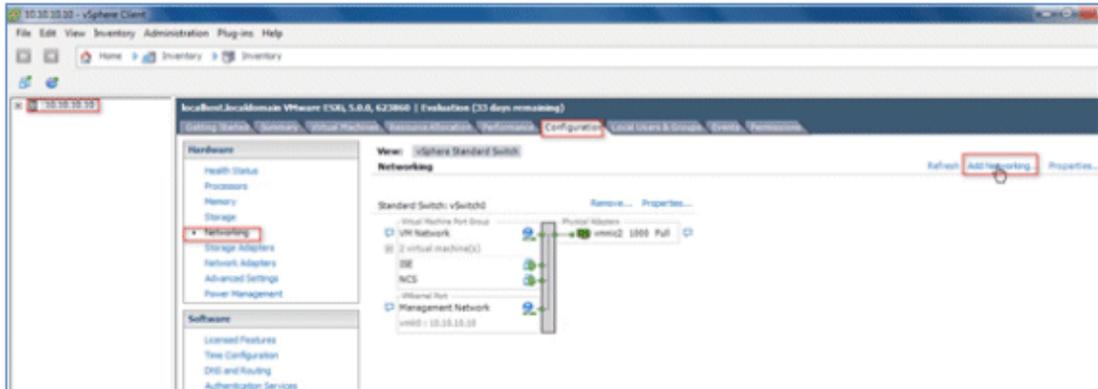
```

interface GigabitEthernet1/1/3
description ESXi Trunk
switchport trunk encapsulation dot1q
switchport mode trunk
end

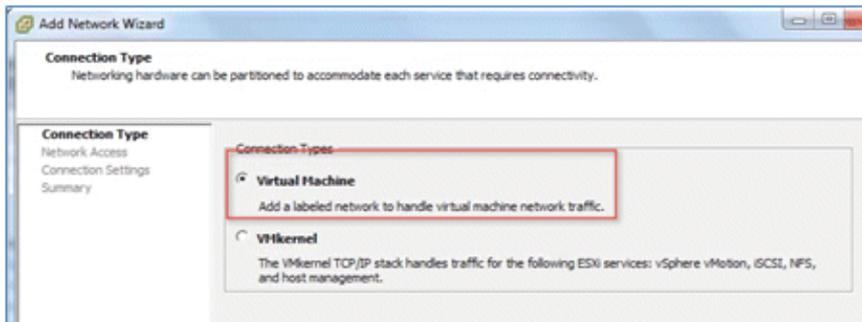
```

Complete these steps:

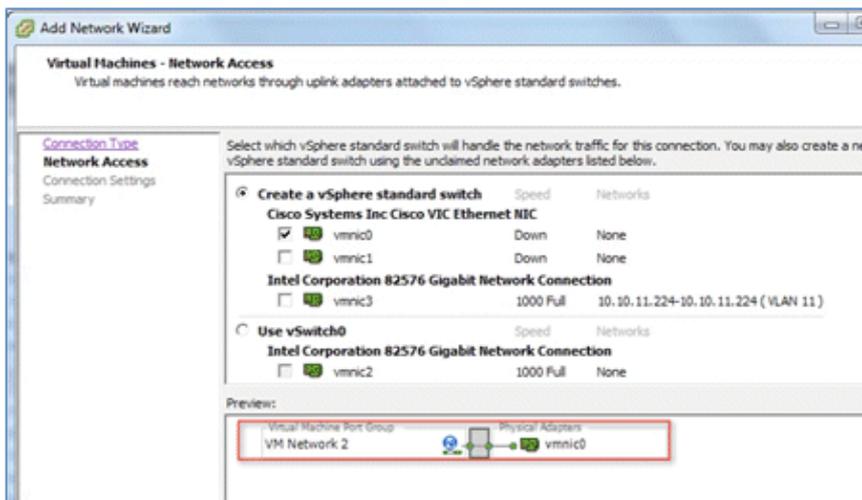
1. Create two separate virtual switches in order to map to the virtual controller Service and Data Port. Go to **ESX > Configuration > Networking**, and click **Add Networking**.



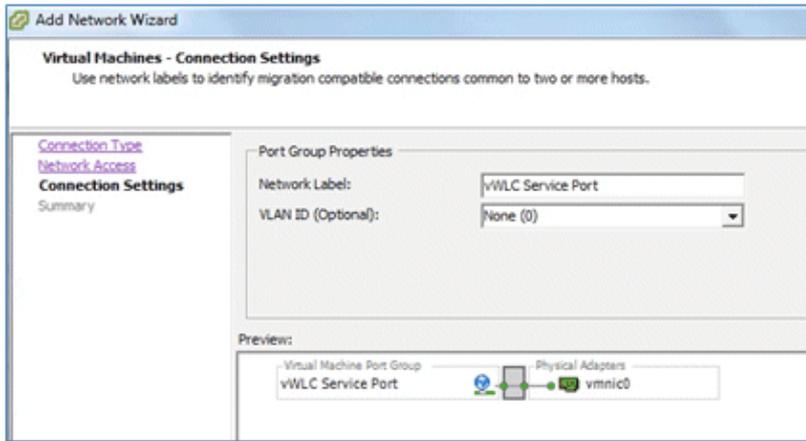
2. Select **Virtual Machine**, and click **Next**.



3. Create a vSwitch and assign a physical NIC in order to connect the vWLC service port. The service port does not have to be connected to any part of the network (typically disconnected/unused). As a result, any NIC (even disconnected) can be used for this vSwitch.

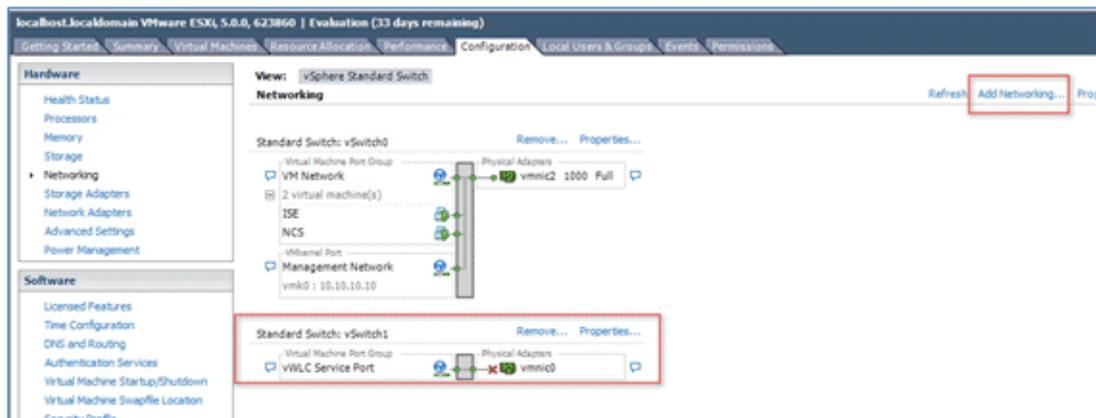


4. Click **Next**.
5. Provide a label (in this example, **vWLC Service Port**).
6. Select **None (0)** for VLAN ID as the service port is typically an access port.



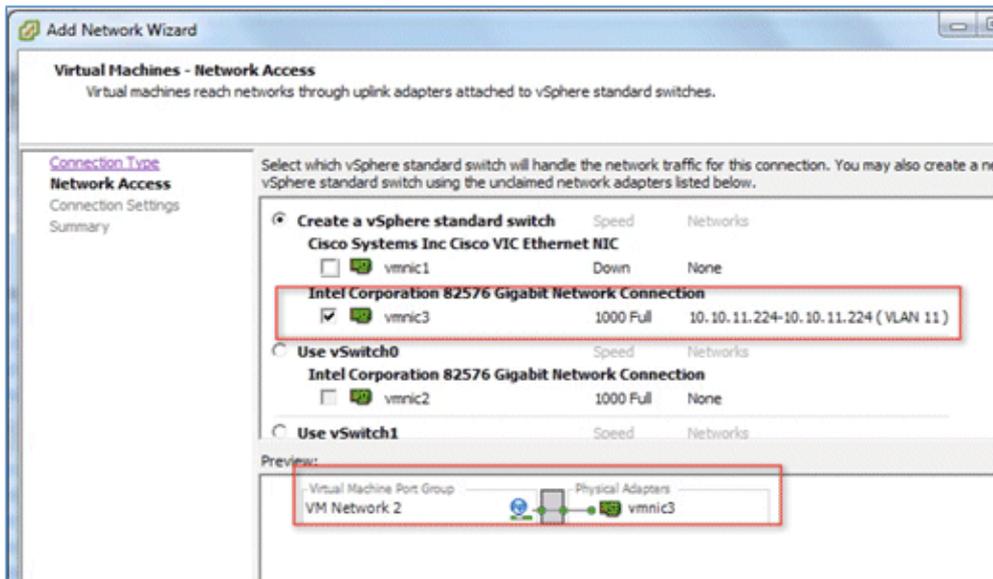
7. Click **Next**.

8. Here, you see vSwitch1 is created for vWLC Service Port. Click **Add Networking** in order to repeat for the Data Port.



9. For the new vSwitch, select the physical NIC(s) connected on a trunk port if there are multiple NICs / portgroup assigned to an etherchannel on the switch.

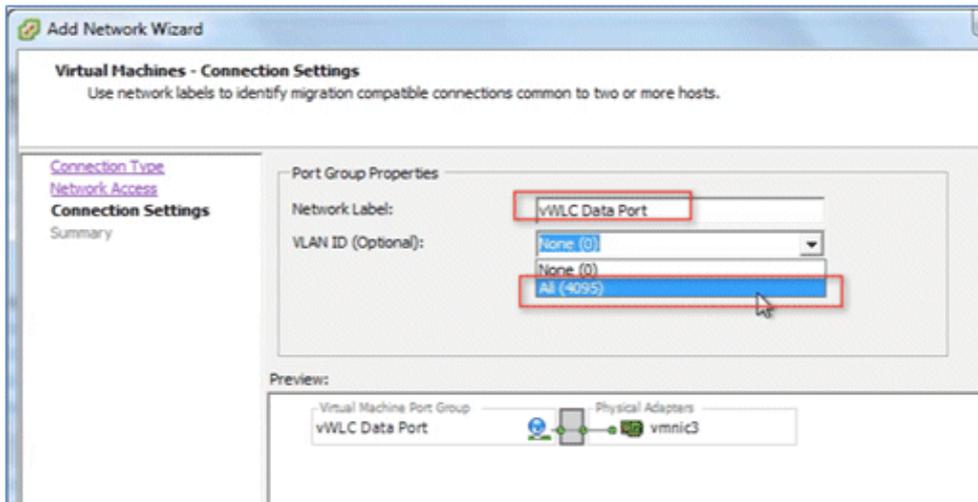
10. Add the NIC.



11. Click **Next**.

12. Provide a label (in this example, **vWLC Data Port**).

13. For VLAN ID, select **ALL(4095)** since this is connected to a switch trunk port.



14. Click **Next** until you complete the steps to add the vSwitch.

## VMware Promiscuous Mode Definition

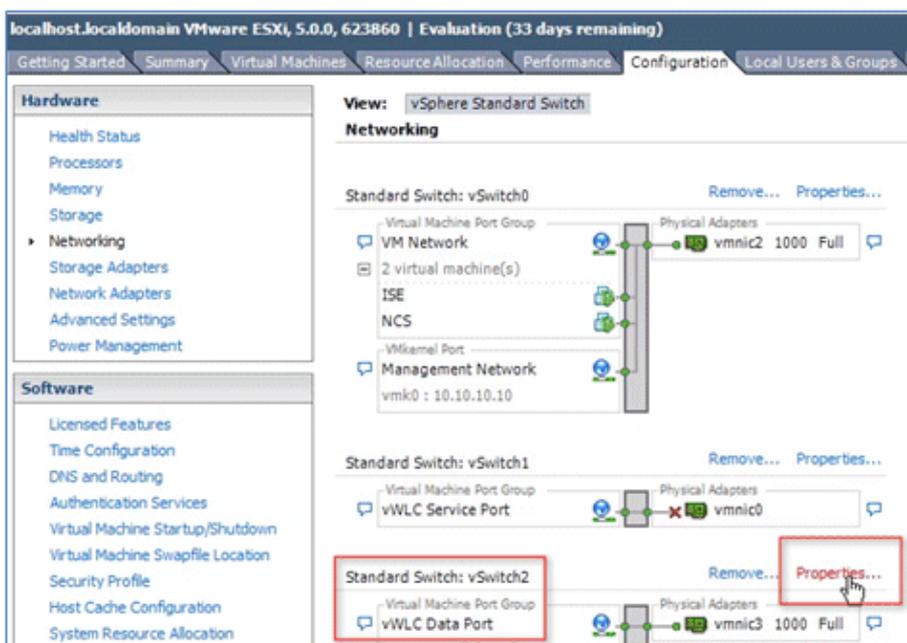
Promiscuous mode is a security policy which can be defined at the virtual switch or portgroup level in vSphere ESX/ESXi. A virtual machine, Service Console, or VMkernel network interface in a portgroup which allows the use of promiscuous mode can see all network traffic traversing the virtual switch.

By default, a guest operating system's virtual network adapter only receives frames that are meant for it. Placing the guest's network adapter in promiscuous mode causes it to receive all frames passed on the virtual switch that are allowed under the VLAN policy for the associated portgroup. This can be useful for intrusion detection monitoring or if a sniffer needs to analyze all traffic on the network segment.

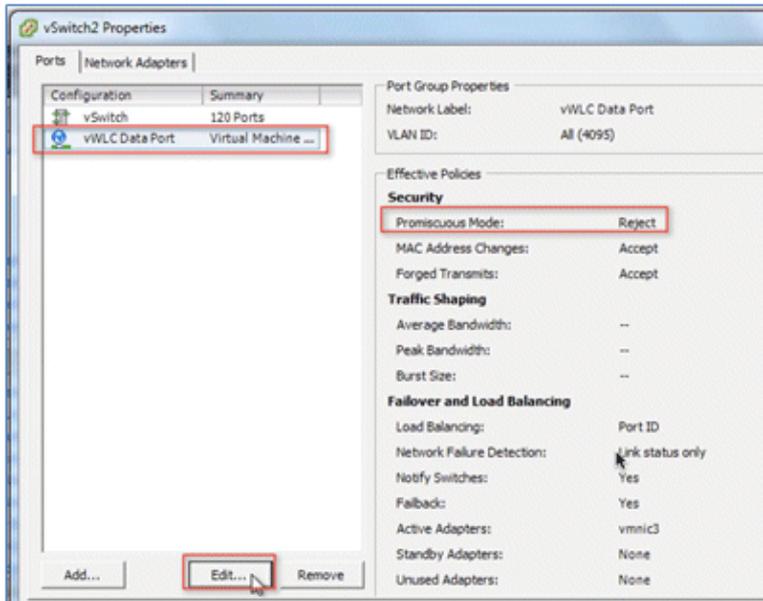
The vWLC Data Port requires the assigned vSwitch to accept Promiscuous mode for proper operations.

Complete these steps:

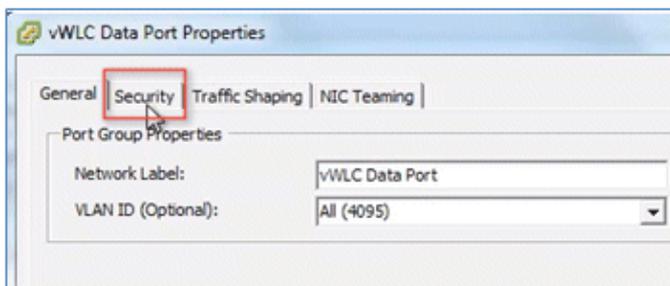
1. Locate vSwitch2 (assigned for vWLC Data Port), and click **Properties**.



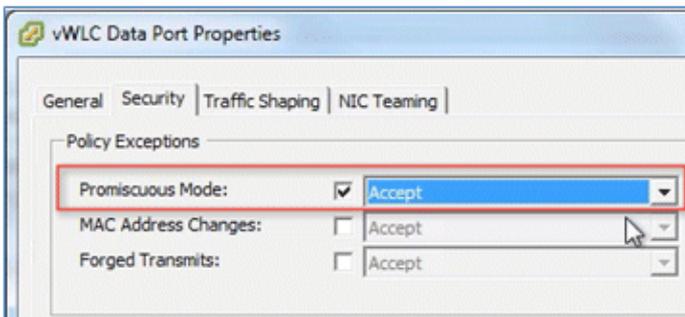
2. Select the VMNet assigned to the vWLC Data Port (note that the default Security Promiscuous Mode is set to Reject), and click **Edit**.



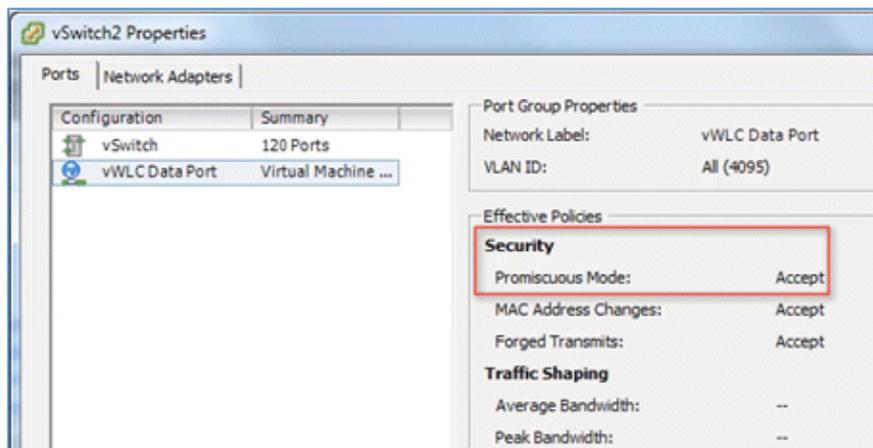
3. In the Properties window, select the **Security** tab.



4. Check the box for **Promiscuous Mode**, choose **Accept** from the drop-down list, and click **OK**.



5. Confirm the change, and click **Close**.

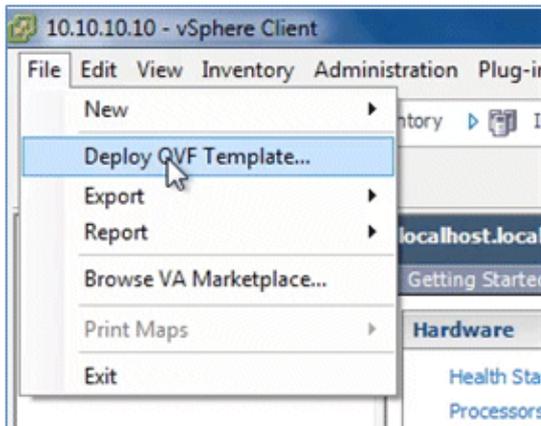


The virtual controller software is posted as an .ovf package in the Cisco software center. You can download the .ova/.ovf package and install to any other virtual application. The software comes with a free 60-day evaluation license. After the VM is started, the evaluation license can be activated and a purchased license can be automatically installed and activated later.

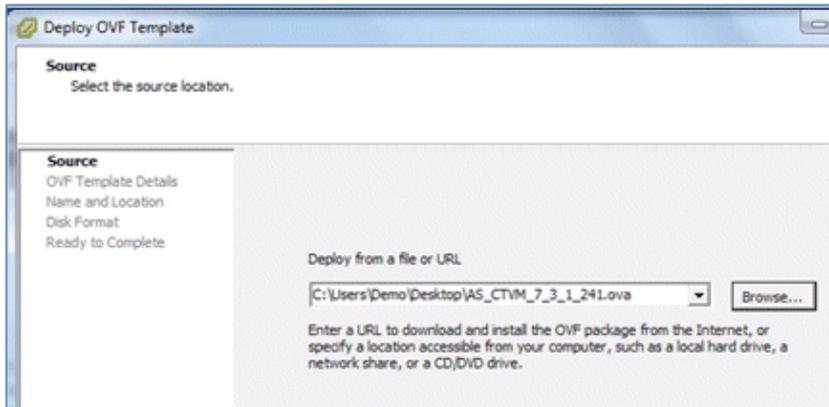
6. Download the virtual controller OVA image to the local disk.



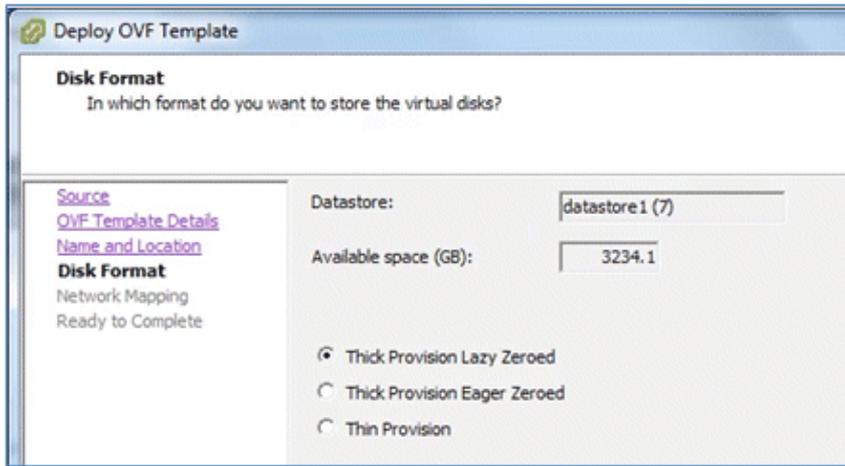
7. Go to **ESX > File > Deploy OVF Template** in order to start the installation.



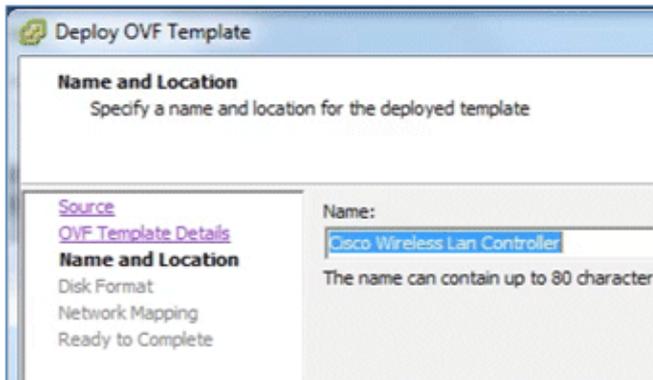
8. Browse to the location of the OVA file (downloaded from Cisco site), and click **Next**.



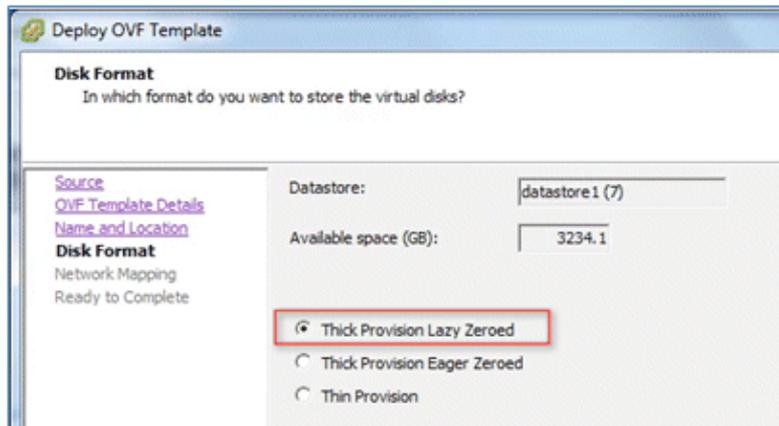
9. Click **Next**.



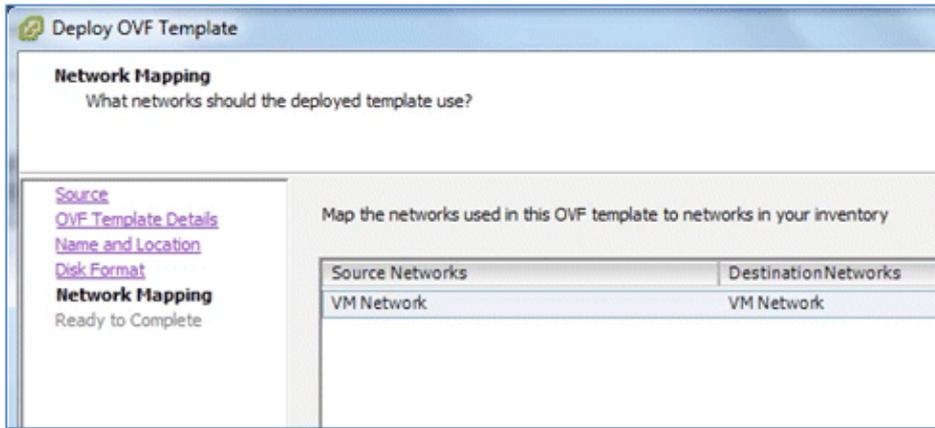
10. Provide a name for the vWLC or accept the default, and click **Next**.



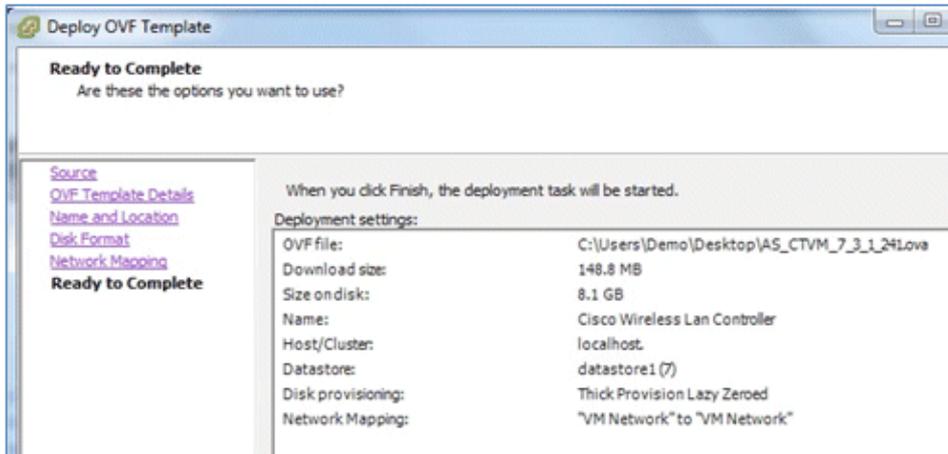
11. Accept the default **Thick Provision Lazy Zeroed** setting, and click **Next**.



12. Accept the Network Mapping default, and click **Next**.



13. Confirm the Deployment settings, and click **Finish** in order to begin installation.



14. Click **Close** when Deployment is complete.



Two important things to note regarding upgrading virtual controllers:

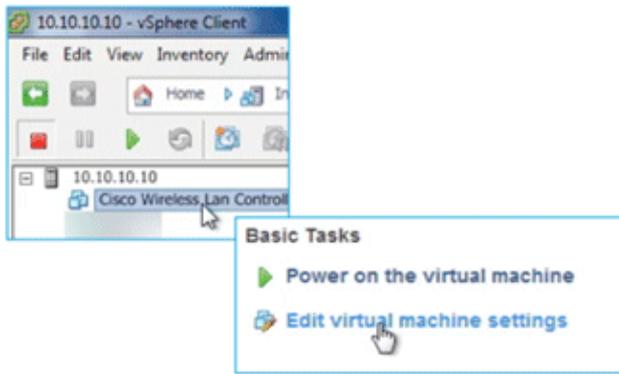
- The OVA image is needed only for first time installation.
- The .AES image can be subsequently used for upgrading/downgrading.

## Virtual Controller Settings

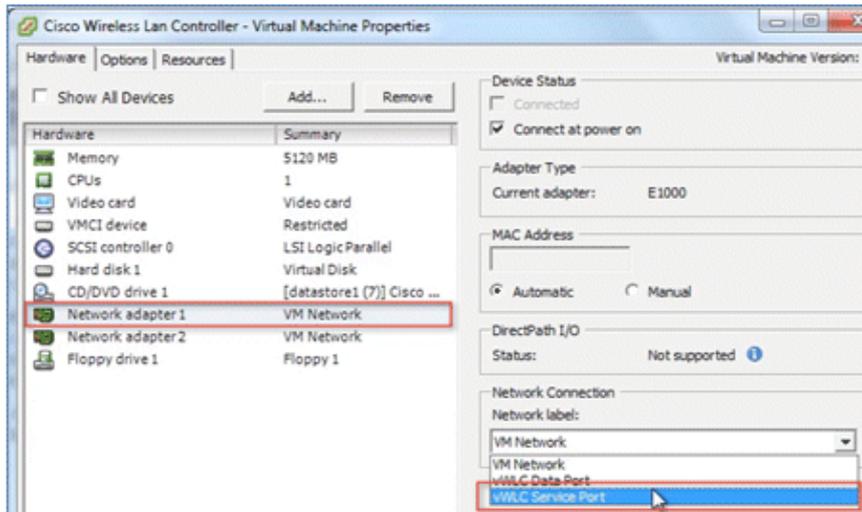
After creating the virtual controller, configure the virtual machine settings to map networking and add a virtual serial console.

Complete these steps:

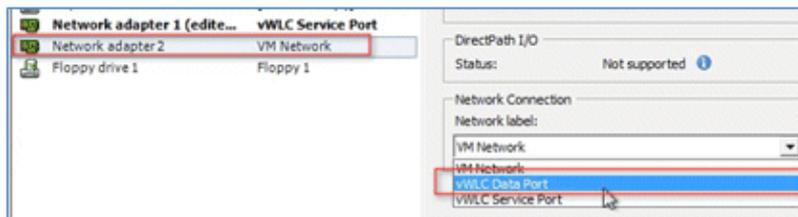
1. Select the vWLC, and click **Edit virtual machine settings**.



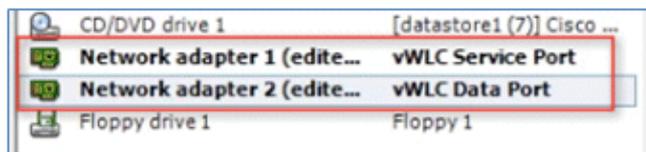
2. Select **Network adapter 1** to **vWLC Service Port** (vSwitch created in ESX networking).



3. Map **Network adapter 2** to **vWLC Data Port**.



4. Confirm the correct mapping.



## Virtual Controller Console Port

The console port gives access to the console prompt of the WLC. As a result, the VM can be provisioned with serial ports in order to connect to these. In the absence of serial ports, the vSphere Client Console is connected to the console on the vWLC.

VMware ESXi supports a virtual serial console port that can be added to the vWLC VM. The serial port can be accessed in one of these two ways:

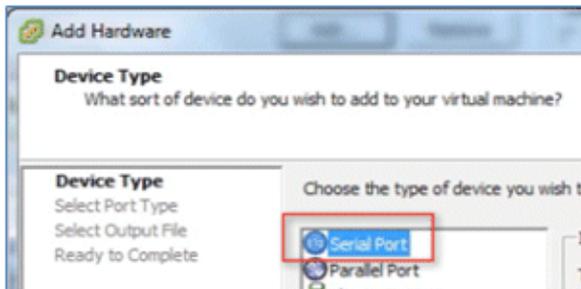
- **Physical Serial Port on the Host:** The vWLC's virtual serial port is mapped to the hardware serial port on the server. This option is limited to the number of physical serial port(s) on the host. If in a multi-tenant vWLC scenario, this may not be ideal.
- **Connect via Network:** The vWLC's virtual serial port can be accessed using Telnet session from a remote machine to a specific port allocated for the VM on hypervisor. For example, if the hypervisor's IP address is 10.10.10.10 and the port allocated for a vWLC VM is 9090, using "telnet 10.10.10.10 9090", just like accessing a physical WLC's console using a Cisco terminal server, the vWLC's serial console can be accessed.

Complete these steps:

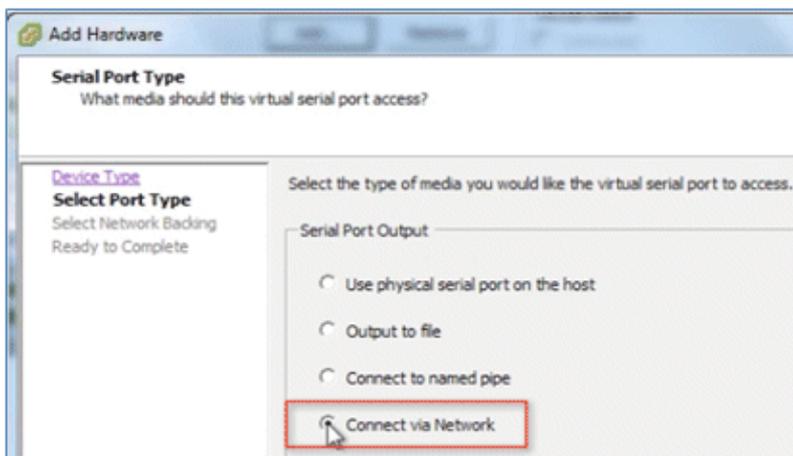
1. On the vWLC **Hardware** tab, click **Add**.



2. On the vWLC **Hardware** tab, click **Add**.

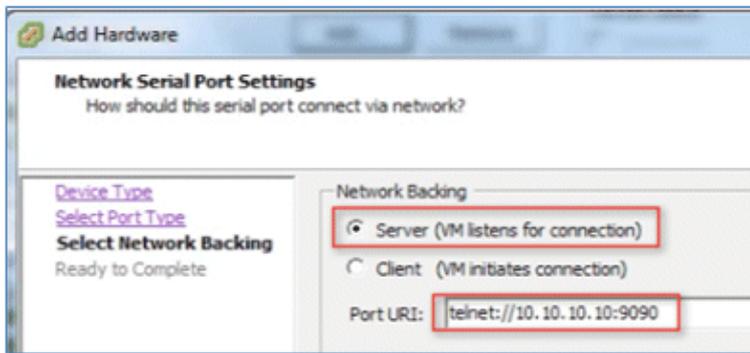


3. In this example, choose **Connect via Network**, and click **Next**.

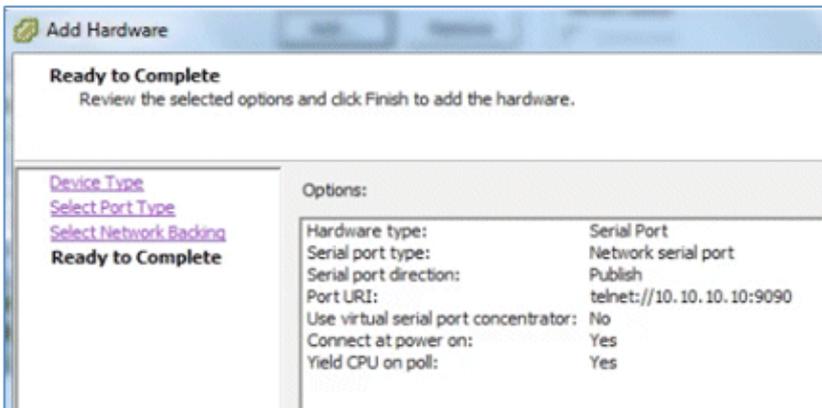


4. Go to **Select Network Backing**:

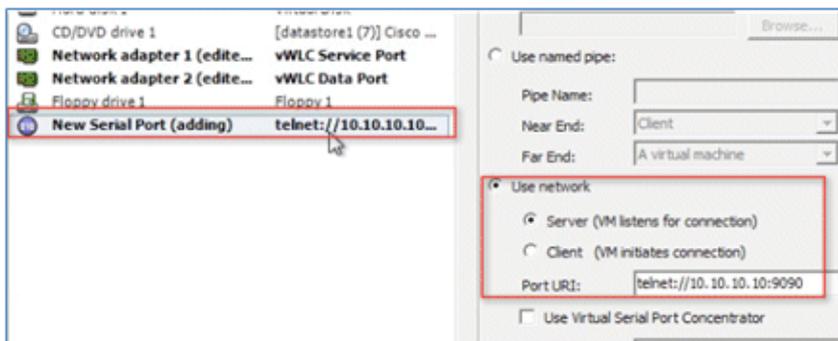
- ◆ For Network Backing, choose **Server (VM listens for connection)**.
- ◆ For Port URI, enter **telnet://<host>:<port>** (for example, telnet://10.10.10.10:9090).



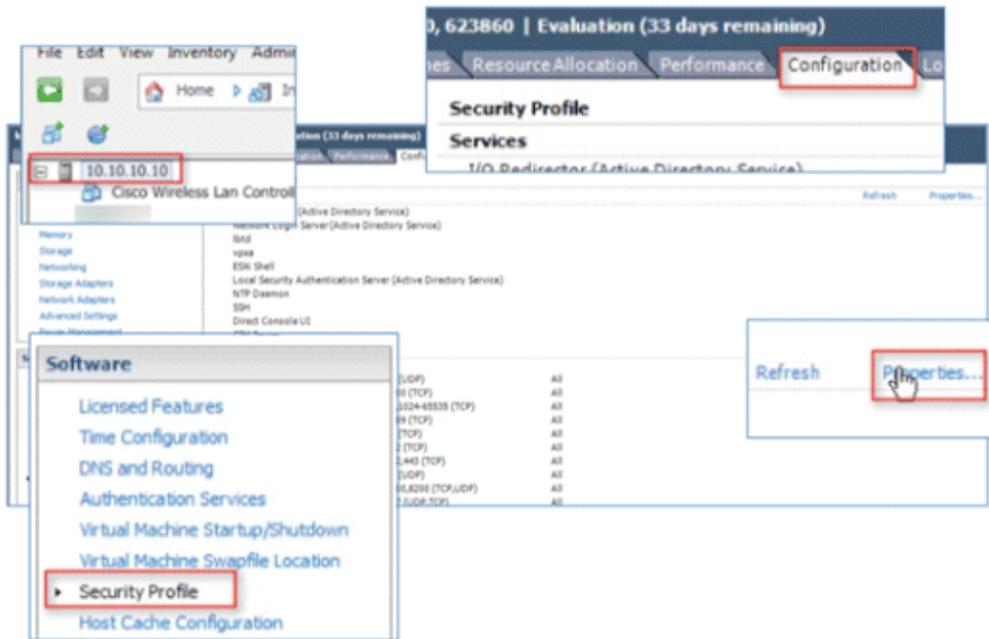
5. Click **Next** in order to review the Options, and click **Finish**.



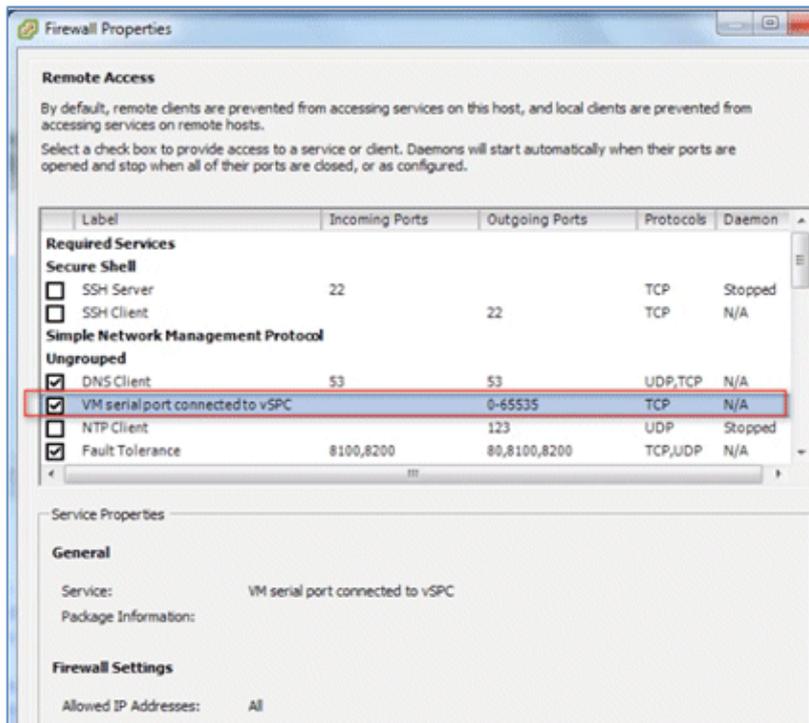
6. Click **OK** in order to complete the configured settings.



In order to enable for the serial via network, ESX must be configured to allow for such requests.  
 7. Navigate to the ESX, click the **Configuration** tab, go to **Software > Security Profile**, and click on **Properties**.



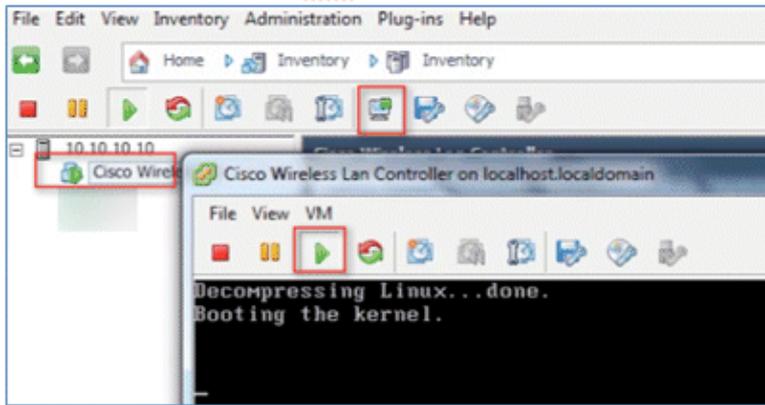
8. In the **Firewall Properties** window, select **VM serial port connected to vSPC**, and click **OK**.



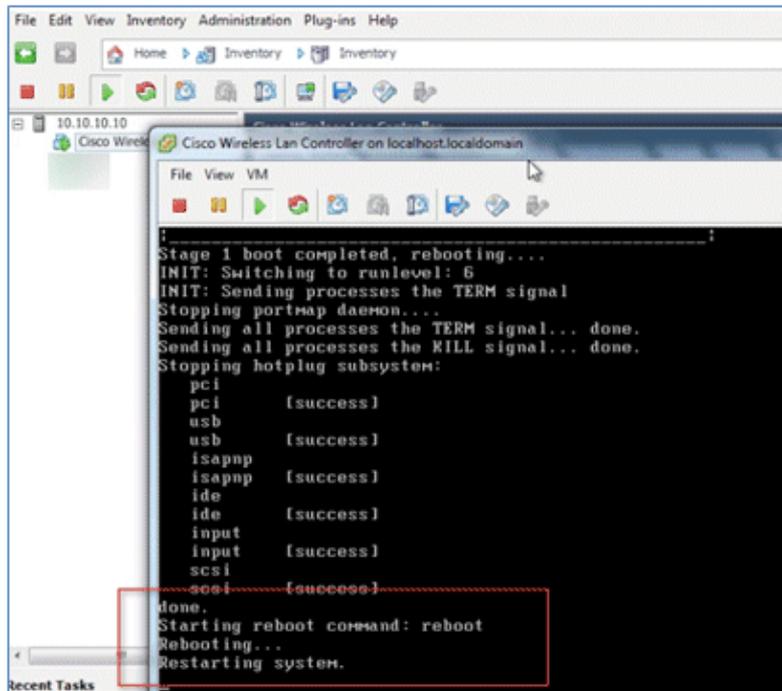
## Start up the vWLC

Complete these steps:

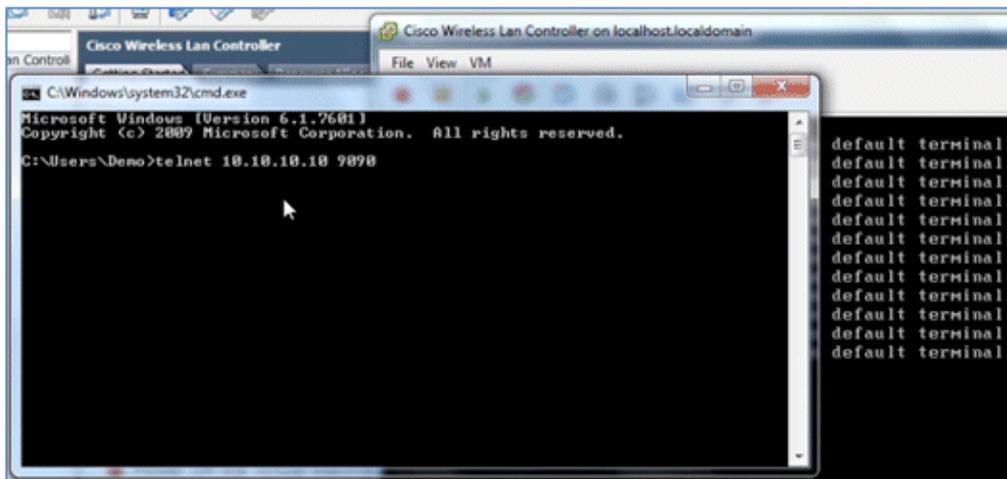
1. Start the vWLC, and select the console in order to observe the first-time installation process.



2. Monitor the progress until the VM console shows that the vWLC has restarted (this is automatic).



3. Open a Telnet session to the vWLC as shown here:



4. The Telnet session will now manage the console to the vWLC.

```

Telnet 10.10.10.10
Cisco Bootloader (Version 7.3.1.241)

.o88b. d888888b .d8888. .o88b. .d88b.
d8P Y8 '88' 88' YP d8P Y8 .8P Y8.
8P   88   88   '88. 8P   88   88
8b   88   88   'Y8b. 8b   88   88
Y8b d8 .88. db 8D Y8b d8 '8b d8'
'Y88P' Y888888P '8888Y' 'Y88P' 'Y88P'

Booting Primary Image...
Press <ESC> now for additional boot options...
Booting 'Primary image'

```

**Note:** Only one mode of console can be operational at any time, such as a VM console (by key-interrupt at startup) or serial console (physical/network). It is not possible to maintain both at the same time.

- Continue to wait until the vWLC has come online fully and prompts you to start the configuration tool wizard.

```

Telnet 10.10.10.10
Starting Ethernet-over-IP: ok
Starting DTLs server: enabled in CAPWAP
Starting CleanAir: ok
Starting WIPS: ok
Starting SSHPM LSC PROU LIST: ok
Starting RRC Services: ok
Starting SXP Services: ok
Starting FMC HS: ok
Starting IPv6 Services: ok
Starting Config Sync Manager : ok
Starting Hotspot Services: ok
Starting Management Services:
  Web Server: CLI: ok
  Secure Web: Web Authentication Certificate not found (error). If you cannot a
ccess management interface via HTTPS please reconfigure Virtual Interface.
  License Agent: ok

<Cisco Controller>

Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup

Would you like to terminate autoinstall? [yes]:

```

- Configure the management interface address / mask / gateway. Configure Management Interface VLAN ID if tagged. Continue with the remainder.

```

Telnet 10.10.10.10
System Name [Cisco_08:5b:c2] (31 characters max):
AUTO-INSTALL: no interfaces registered.
AUTO-INSTALL: process terminated -- no configuration loaded
vWLC
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (3 to 24 characters): *****
Re-enter Administrative Password : *****

Service Interface IP Address Configuration [static][DHCP]:
Management Interface IP Address: 10.10.11.20
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.11.1
Management Interface VLAN Identifier (0 = untagged): 11
Management Interface Port Num [1 to 1]: 1
Management Interface DHCP Server IP Address: 10.10.10.1

Virtual Gateway IP Address: 1.1.1.1

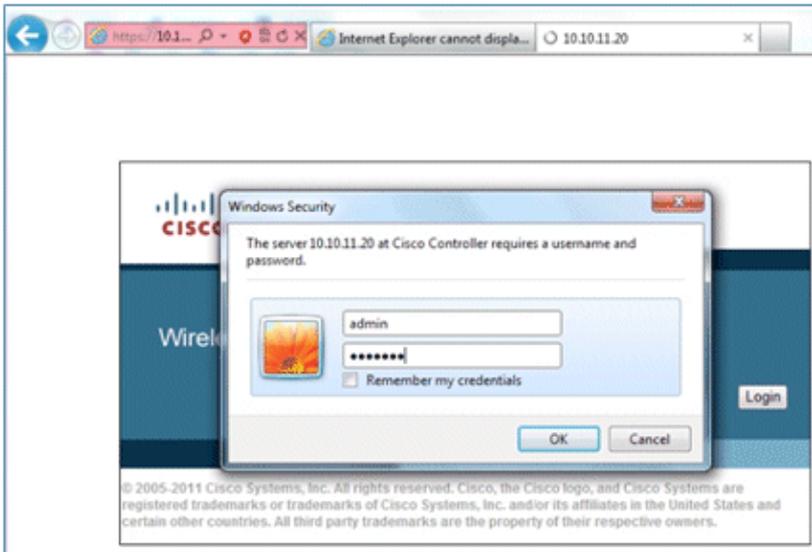
Mobility/RF Group Name: demo

Network Name (SSID):

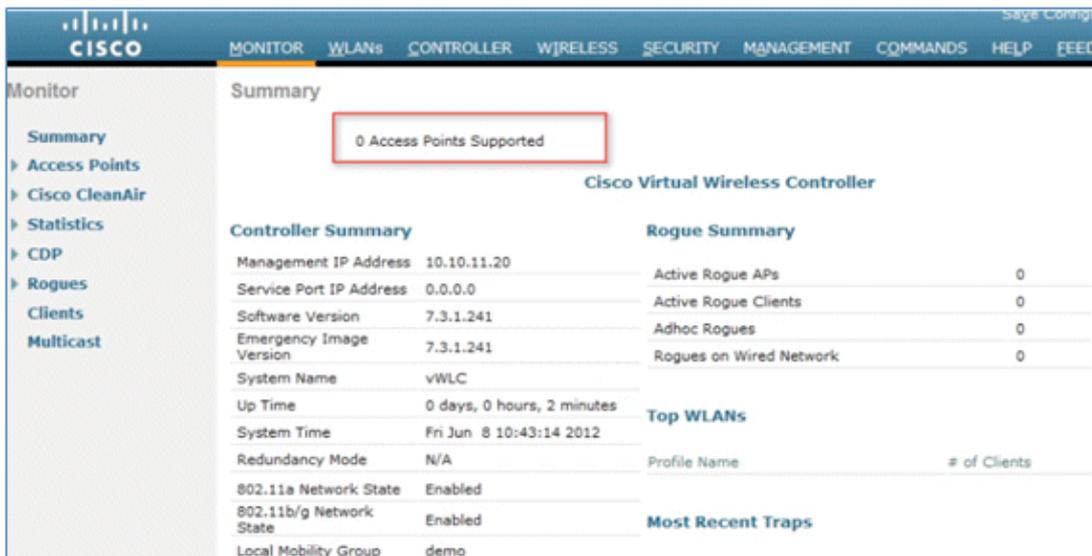
```

- Similar to all network device(s), configuring the NTP is crucial. The virtual controller must have the correct clock as it is possible to have an incorrect clock on the ESX host, or from manual

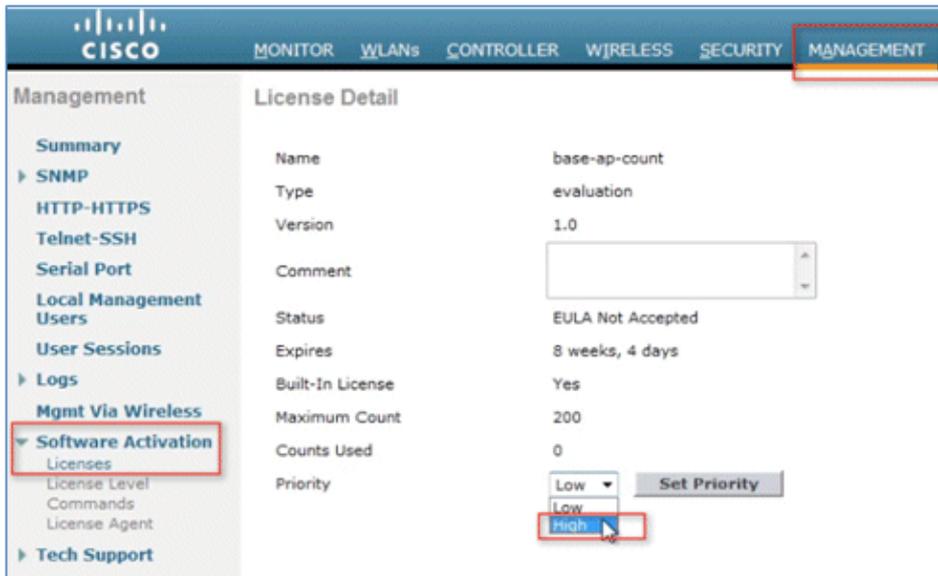




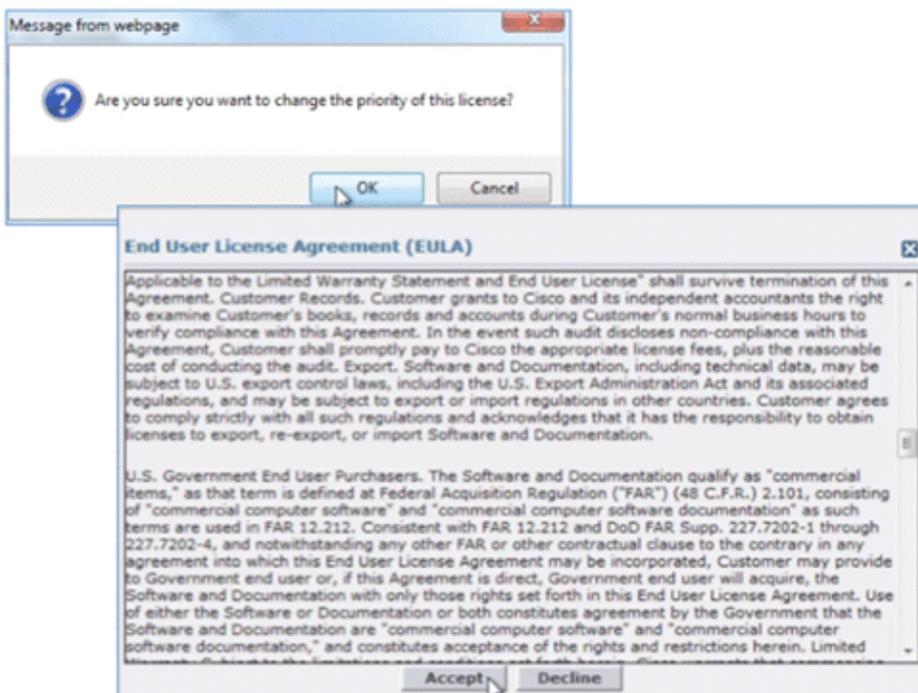
12. Initially, there are 0 (zero) Access Points Supported. Enable the evaluation license in order to allow the AP to join.



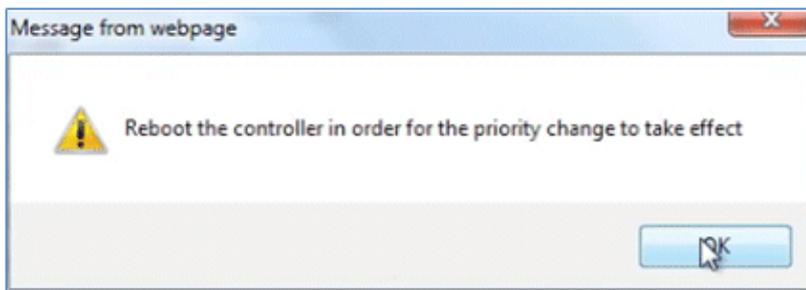
13. Go to **Management > Software Activation > Licenses**. Select **base-ap-count**, and set the Priority to **High**.



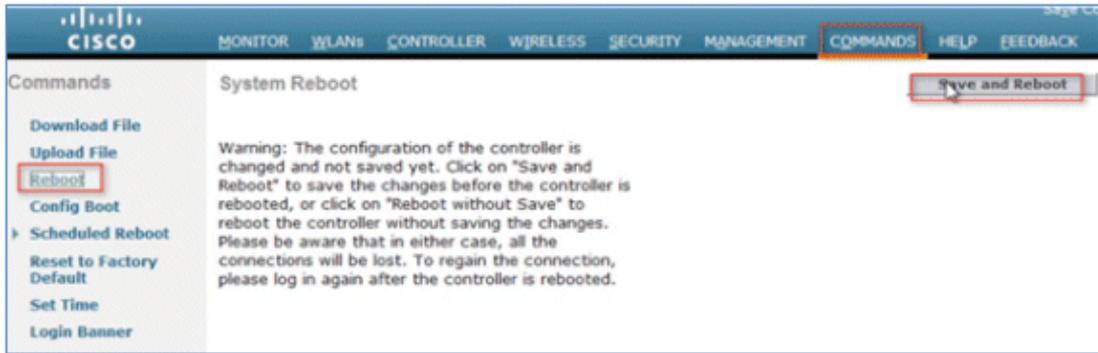
14. Click **OK**, and **Accept** the EULA in order to continue.



15. Click **OK**, and reset the vWLC in order for the evaluation license to take effect.



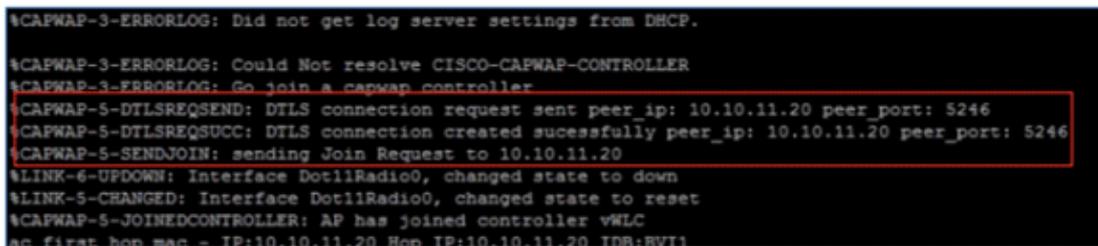
16. Reboot the vWLC.



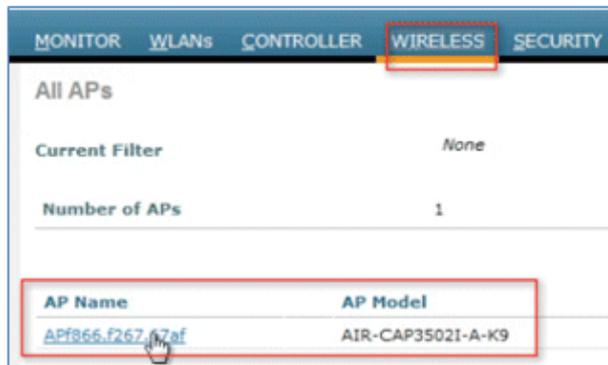
17. Log back in to the vWLC, and note that the 200 APs are now supported with the evaluation license enabled.



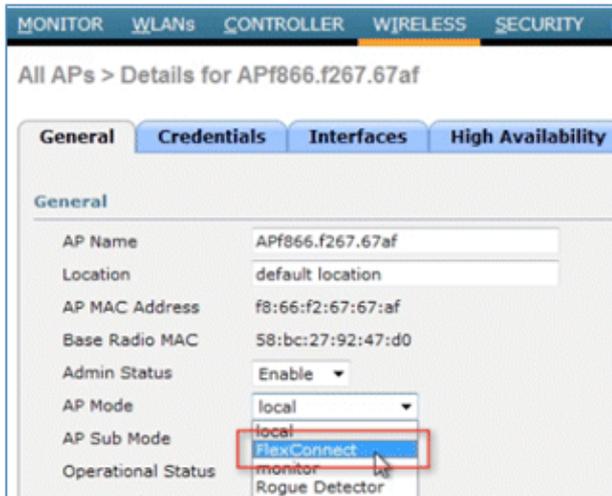
18. Connect an AP, and monitor for the join message to occur.



19. From the browser, go to **WIRELESS** and confirm that the AP has joined.



20. Click the AP, and change the AP Mode to **FlexConnect**. Only FlexConnect is supported (central and local switching) in the 7.3 release.



21. It may be useful to consider using the autoconvert function of the controller (for example, any mode AP joining the vWLC will be converted automatically to FlexConnect). Issue this command in order to implement:

```
(Cisco Controller) > config ap autoconvert flexconnect enable
```

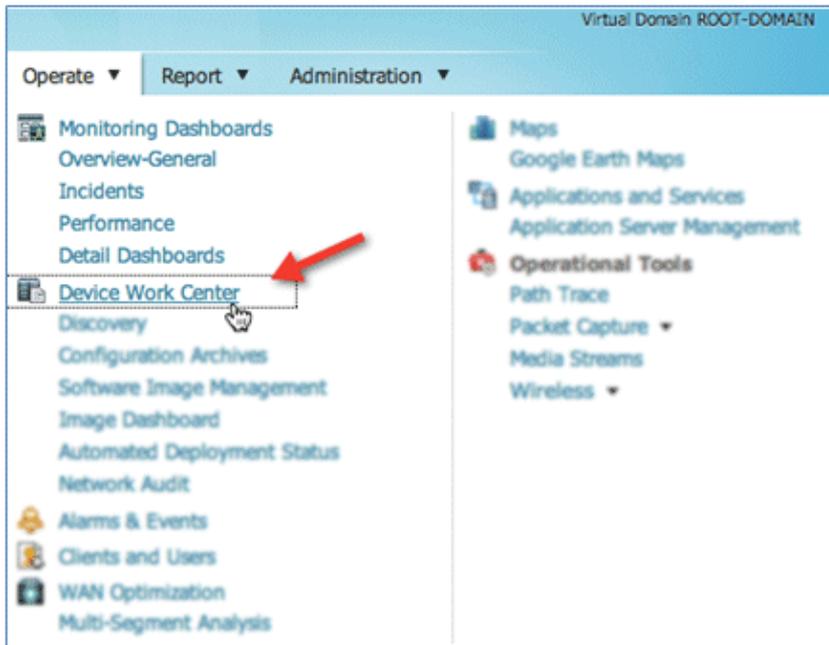
## Virtual Controller Management with Cisco Prime 1.2

Cisco Prime Infrastructure version 1.2 is the minimum release required to centrally manage one or more Cisco Virtual Controller(s). Management for the Cisco Virtual Controller is no different than legacy physical controllers in comparison to Cisco WCS or NCS. Cisco Prime Infrastructure 1.2 provides configuration, software management, monitoring, reporting, and troubleshooting of virtual controllers. Refer to Cisco Prime Infrastructure documentation as required for administrative and management support.

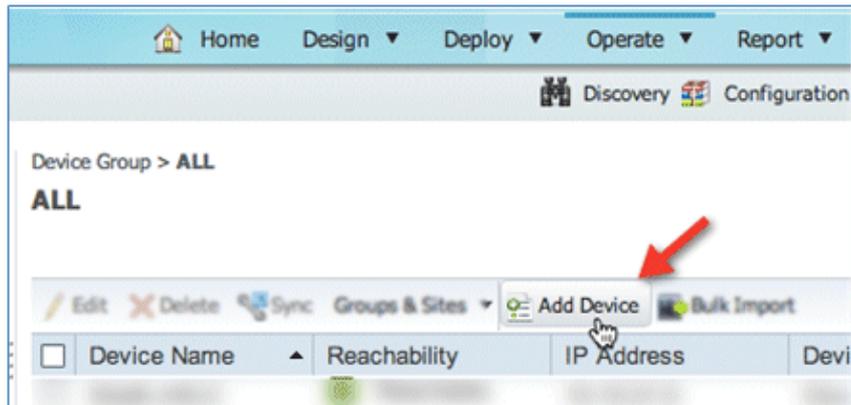
1. Log in to Cisco Prime Infrastructure server as **root**. By default, the management view selection is Lifecycle Theme, which is new beginning with release version 1.2. The Classic Theme (shown later) will be more familiar to administrators who have been working in Cisco WCS and NCS.



2. Go to **Operate > Device Work Center**.



3. In Device Work Center, click **Add Device**.



4. Enter the IP Address and SNMP Community string (Read/Write). By default, the SNMP RW for the controller is Private. Click **Add**.

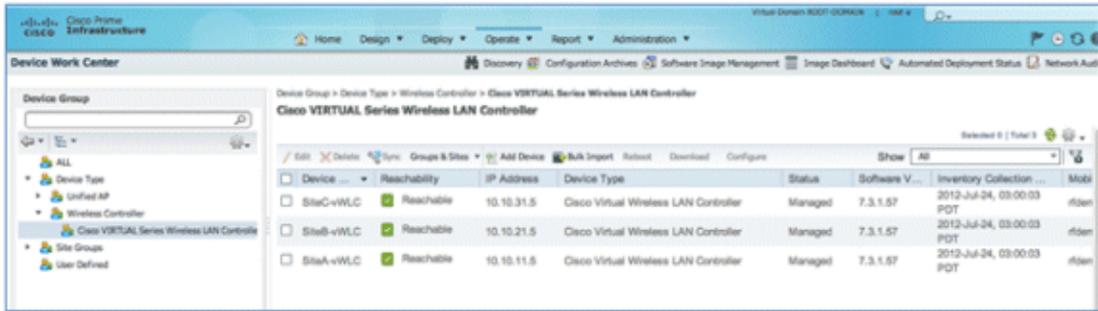
5. Cisco Prime Infrastructure will discover and synchronize with the virtual controller. Click refresh in order to update the screen.

Device Name	Reachability	IP Address	Device Type	Collection Status
SiteB-vWLC	Reachable	10.10.21.5	Cisco Virtual Wir...	Managed
SiteC-vWLC	Reachable	10.10.31.5	Cisco Virtual Wir...	Managed
	Unknown	10.10.11.5		Synchronizing

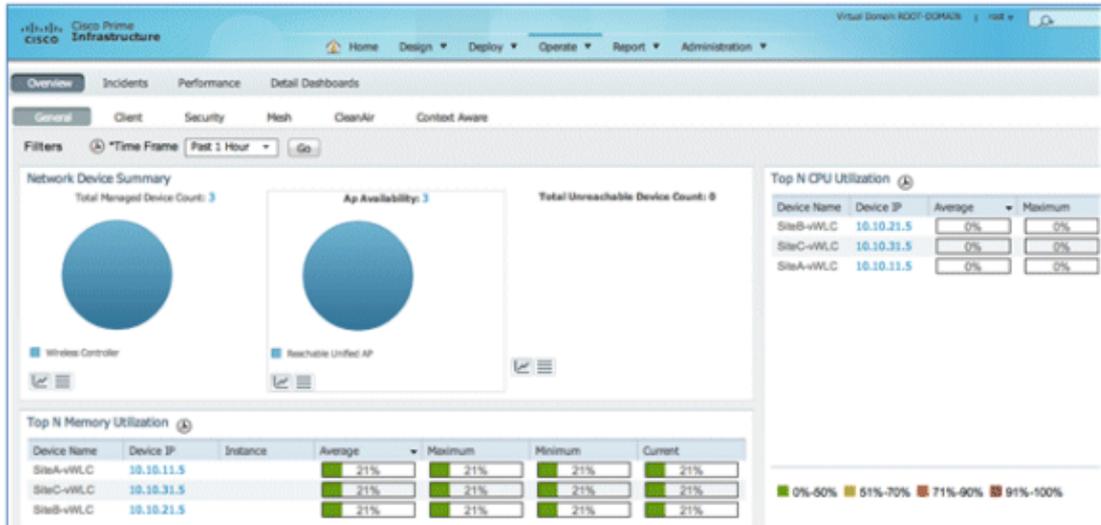
6. When the virtual controller is discovered, it is listed as Managed and Reachable (shown in green). Add any other virtual controller(s) at this point, if available.

Device Name	Reachability	IP Address	Device Type	Collection Status
SiteA-vWLC	Reachable	10.10.11.5	Cisco Virtual Wireless LAN Co...	Managed
SiteB-vWLC	Reachable	10.10.21.5	Cisco Virtual Wireless LAN Co...	Managed
SiteC-vWLC	Reachable	10.10.31.5	Cisco Virtual Wireless LAN Co...	Managed

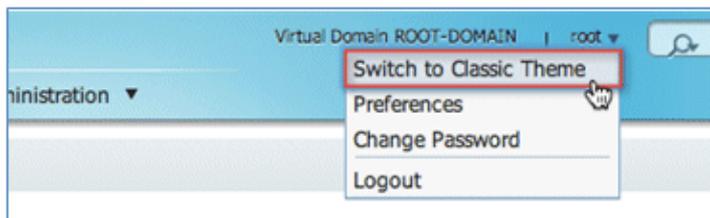
7. The new controller will be listed in **Device Type > Cisco VIRTUAL Series Wireless LAN Controller**.



8. Navigate to Home for a Summary view (in Lifecycle Theme) of the devices being managed.



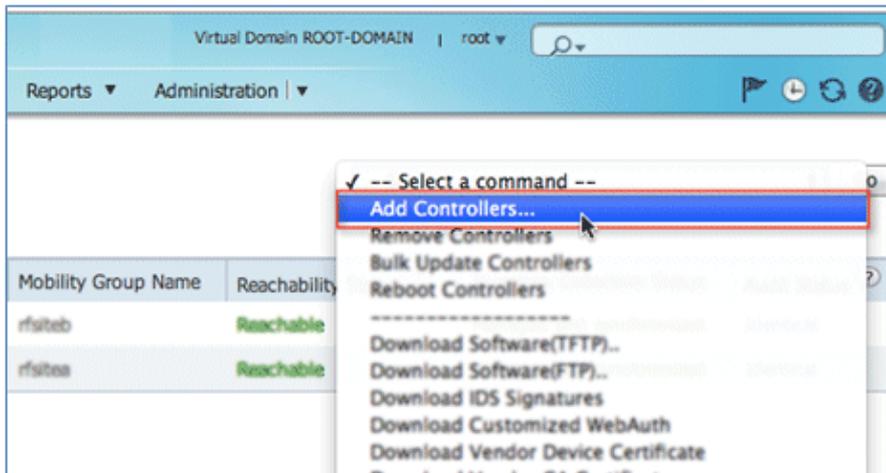
9. For the remainder of this guide, the Classic Theme is used to perform similar task of adding the virtual controller, as well as updating the system image. Go to and select **Switch to Classic Theme**.



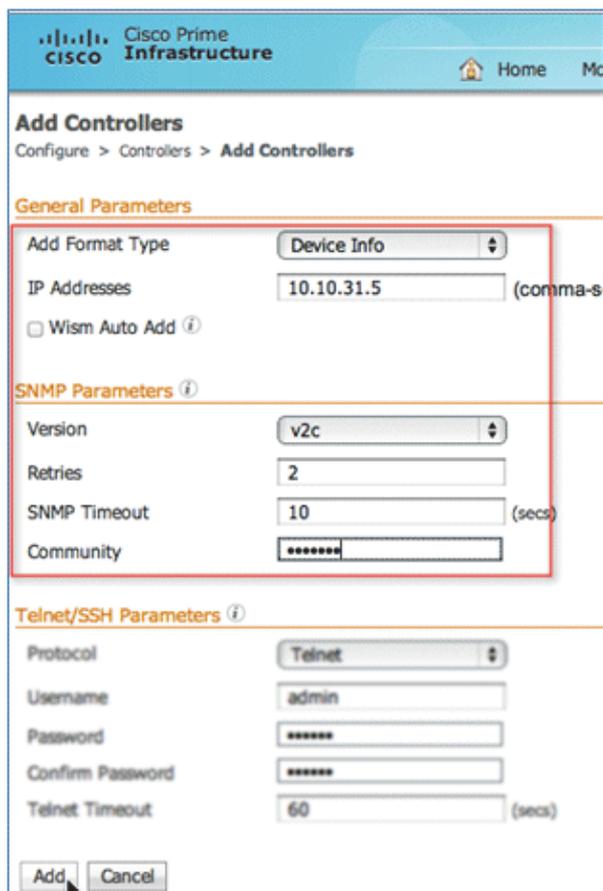
10. Go to **Configure > Controllers**.



11. In order to add a new virtual controller, select **Add Controllers...** from the Select a command drop-down list.



12. Enter the IP Address, Read/Write SNMP Community string, and click **Add**.



13. Cisco Prime Infrastructure will display this notification:



14. Go to **Configure > Controllers**. The virtual controller will be listed as Reachable once it has been successfully discovered and added. Otherwise, and as shown above, the device will appear in the Unknown Device page if it was not discovered successfully.

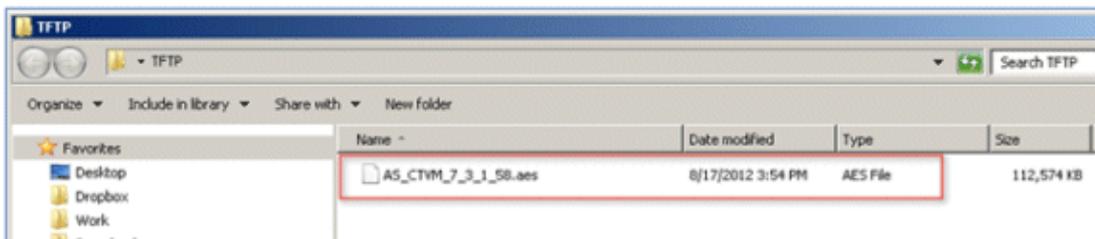
IP Address	Device Name	Device Type	Location	SW Version	Mobility Group Name	Reachability Status
10.10.31.5	SiteC-vWLC	VWLC		7.3.1.57	rfSiteC	Reachable
10.10.21.5	SiteB-vWLC	VWLC		7.3.1.57	rfSiteB	Reachable
10.10.11.5	SiteA-vWLC	VWLC		7.3.1.57	rfSiteA	Reachable

## Upgrade the Virtual Controller

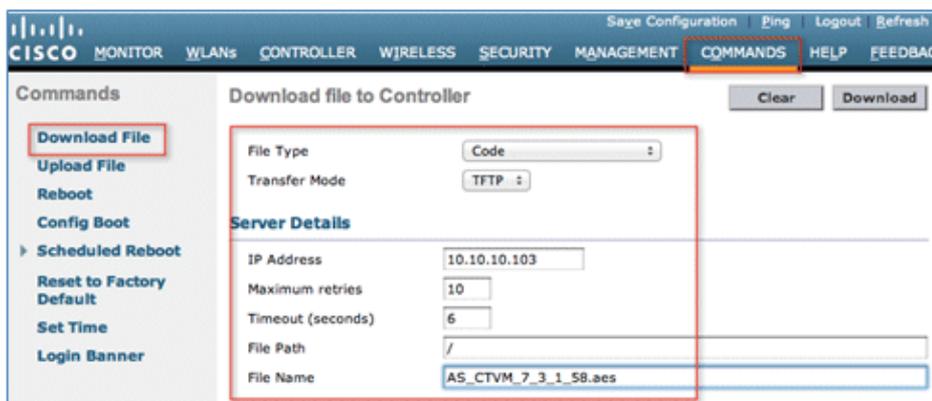
In the early steps of installation, the Cisco Virtual Controller initially required an OVA file for new virtual appliance creation. However, maintaining virtual controller features and software upgrades require a common AES file downloadable from the Cisco website.

Complete these steps:

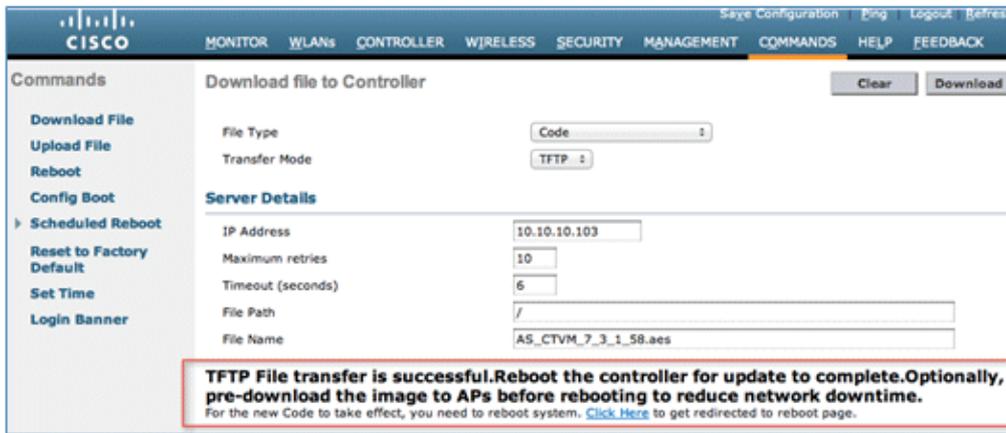
1. Download the AS\*7\_3\*aes file to a target host (for example, the TFTP/FTP server).



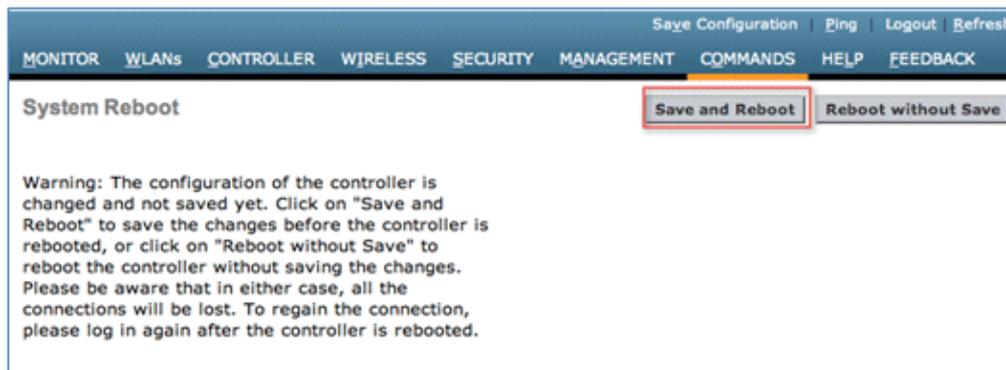
2. Just as for legacy controllers, go to the web GUI of the controller > **COMMANDS** > **Download File**. Select the File Type, Transfer Mode, IP Address, File Path, and File Name (.aes file). Click **Download** in order to start the process.



3. When the process has completed successfully, you are prompted to Reboot in order for the new software image to take effect. Click the link to the Reboot Page in order to continue.



4. Click **Save and Reboot**.



5. Cisco Prime Infrastructure can also be useful for upgrading one virtual controller or many virtual controllers at the same time. Go to **Configure > Controllers**. Select (check box) one or more virtual controllers. Select **Download Software (TFTP)** from the command drop-down list. This example uses TFTP mode for image upgrade.



6. Provide the Download Type, TFTP server (new if using external), IP Address, File Path, and Server File Name (which is the .aes file type). Click **Download**.

**Download Software to Controller**  
 Configure > Controllers > Download Software to Controller

Some TFTP servers may not support files larger than 32 MB.

Controller IP Address	Current Software Version
10.10.11.5	7.3.1.57
10.10.21.5	7.3.1.57
10.10.31.5	7.3.1.57

**Download Type**

Download Type (i)  Now (i)  Scheduled

**TFTP Servers**

File is located on (i)  Local machine  TFTP server

Server Name:

External TFTP Server:

Server IP Address:

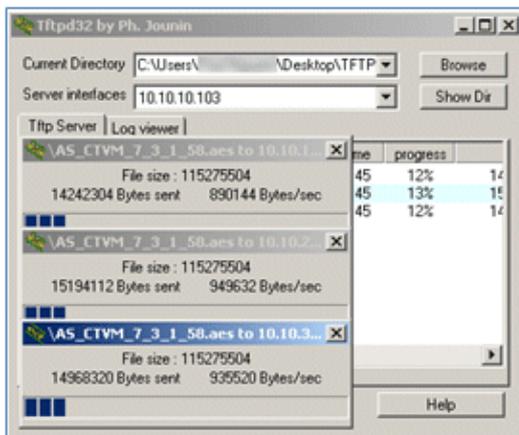
Maximum Retries:

Timeout:  (secs)

File Path:

Server File Name:

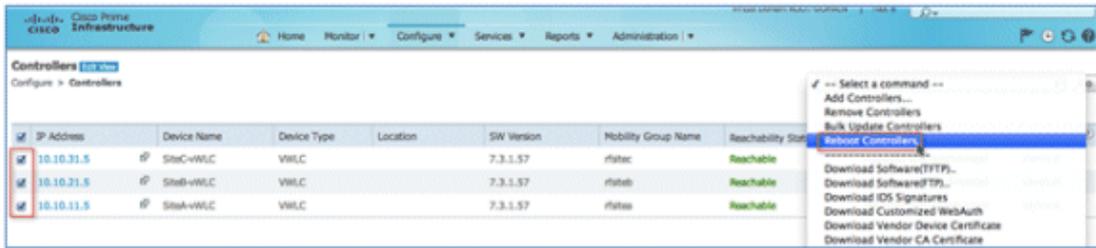
7. This screen is an example of the AES image being transferred to the virtual controllers:



8. Cisco Prime Infrastructure will update the status until the software has transferred successfully.

Controller IP Address	Current Software Version	Operation Status	Details
10.10.31.5	7.3.1.57	TRANSFER_SUCCESSFUL	TFTP File transfer is successful. Reboot the controller for update to complete. Optionally, pre-download the image to APs before rebooting to reduce network downtime.
10.10.21.5	7.3.1.57	TRANSFER_SUCCESSFUL	TFTP File transfer is successful. Reboot the controller for update to complete. Optionally, pre-download the image to APs before rebooting to reduce network downtime.
10.10.11.5	7.3.1.57	TRANSFER_SUCCESSFUL	TFTP File transfer is successful. Reboot the controller for update to complete. Optionally, pre-download the image to APs before rebooting to reduce network downtime.

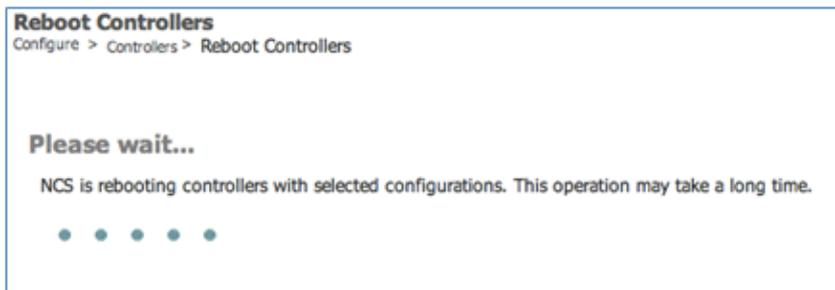
9. Similar to the experience directly from the controller, a reboot is required when the transfer is complete. In Cisco Prime Infrastructure, go to **Configure > Controllers**, and select the virtual controller(s). Select **Reboot Controllers** from the Select a command... drop-down list.



10. Cisco Prime Infrastructure will prompt for reboot parameters such as save configuration, and so forth. Click **OK**.



11. Cisco Prime Infrastructure will notify the administrator that the virtual controllers are being rebooted.



12. When complete, Cisco Prime Infrastructure will provide the results of the process.

**Reboot Controllers Result**  
Configure > Controllers > Reboot Controllers Result

IP Address	Reboot Controller	Save Config to Flash	Reboot APs	Swap AP Image
10.10.31.5	✓	✓	✗	✗
10.10.21.5	✓	✓	✗	✗
10.10.11.5	✓	✓	✗	✗

## Troubleshooting

### AP Considerations

Known Issue: AP(s) not joining vWLC – The AP must get the hash entry from a legacy controller before it joins a vWLC.

- An AP must be at software version 7.3.1.35 and above to successfully join a virtual controller. Virtual controllers use SSC in order to validate an AP before joining.
- An AP at version 7.3 can validate the SSC certificate provided by the virtual controller.
- After successful certificate validation, an AP will check the hash key of the virtual controller in the list of stored keys in flash. If it matches the stored hash, validation is passed and the AP moves to the RUN state. If hash validation fails, it will disconnect from the controller and restart the discovery process.

- The hash validation, which is an extra authorization step, will be performed only if the AP is joining a virtual controller. There will be a knob to turn on/off hash key validation.
- By default, hash validation is enabled, which means that the AP needs to have the virtual controller hash key in its flash before it can successfully complete association with the virtual controller. If the knob is turned off, the AP will bypass the hash validation and move directly to the RUN state.
- The hash key can be configured in the controller mobility configurations, which gets pushed to all the APs which are joined. The AP will save this configuration until it successfully associates to another controller. After which, it inherits the hash key configuration from the new controller.
- Typically, APs can join a traditional controller, download the hash keys, and then join a virtual controller. However, if it is joined to a traditional controller, the hash validation knob can be turned off and it can join any virtual controller. The administrator can decide to keep the knob on or off

This information is captured in Cisco bug ID CSCua55382.

### Exceptions:

- If the AP does not have any hash key in its flash, it will bypass the hash validation, assuming that it is a first time installation.
  - ◆ In this case, the hash validation is bypassed irrespective of whether the hash validation knob is on/off.
  - ◆ Once it successfully joins the controller, it will inherit the mobility group member hash configuration (if configured in the controller). After which, it can join a virtual controller only if it has a hash key entry in its database.
- Clearing the AP configuration from the controller or on the AP console will result in the erasing of all the hash keys. After which, the AP joins the virtual controller as if it is a first time installation.
  - ◆ AP> test capwap erase
  - ◆ AP> test capwap restart

### Time is Incorrect

- At initial install, it is possible that the time may be skewed or not properly synced. As a result, the AP may not be able to join properly. In this instance, check the SSC validity time stamp in order to ensure that it is correct. NTP is always recommended going forward.

```
(Cisco Controller) >show certificate ssc
SSC Hash validation..... Enabled.

SSC Device Certificate details:

Subject Name :
  C=US, ST=California, L=San Jose, O=Cisco Virtual Wireless LAN Controller,
  CN=DEVICE-vWLC-AIR-CTVM-K9-000C29085BB8, MAILTO:support@vwlc.com

Validity :
          Start : 2012 Jun 8th, 17:52:46 GMT
          End   : 2022 Apr 17th, 17:52:46 GMT

Hash: b7b60436202e830802be1e8931d539b67b2537
```

### SSC Hash

- The AP is a new AP with 7.3 and does NOT have hash can join virtual WLC readily:

```
ap#show capwap client config
```

- The AP may have an older SSC hash, either from an old installation or joining other controllers. It is possible to configure the WLC to not validate SSC, allow APs to join the vWLC, then re-enabling the validation again.

```
(Cisco Controller) >configure certificate ssc hash validation disable
```

- Perform the **test capwap** <erase/restart> command in order to clear AP capwap settings and initiate join process.

```
APf866.f267.67af#test capwap erase
APf866.f267.67af#test capwap restart
restart capwap
APf866.f267.67af#
*Jun  9 12:27:22.469: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
 10.10.11.20:5246
*Jun  9 12:27:22.525: %WIDS-6-DISABLED: IDS Signature is removed and disabled.
*Jun  9 12:27:22.529: %LWAPP-3-CLIENTERRORLOG: LWAPP LED Init: incorrect led
  state 255
*Jun  9 12:27:22.897: Starting Ethernet promiscuous mode
*Jun  9 12:27:32.903: %CAPWAP-3-ERRORLOG: Go join a capwap controller
*Jun  9 12:27:23.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent
 peer_ip: 10.10.11.20 peer_port: 5246
*Jun  9 12:27:23.276: %CAPWAP-5-DTLSREQSUCC: DTLS connection created
 successfully peer_ip: 10.10.11.20 peer_port: 5246
*Jun  9 12:27:23.276: %CAPWAP-5-SENDJOIN: sending Join Request to 10.10.11.20
```

- As part of the mobility configuration, if there is a virtual controller in the network, the administrator needs to add a hash key of the virtual controller in all the peer controllers. If adding another peer controller, the consideration is to add the hash (shown in the SSC output above) to the mobility group member.

```
(Cisco Controller) >config mobility group member add 10.10.11.30
(Cisco Controller) >config mobility group member hash 10.10.11.30
bd7bb60436202e830802be1e8931d539b67b2537
```

## Related Information

- [FlexConnect Feature Matrix](#)
- [Cisco LAP Documentation](#)
- [Flex 7500 Wireless Branch Controller Deployment Guide](#)
- [Technical Support & Documentation – Cisco Systems](#)

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2012 – 2013 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Sep 04, 2012

Document ID: 113677

---

## Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>