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).

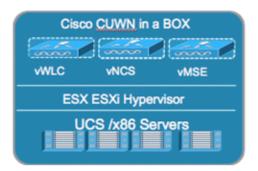
vWLCs are not a replacement of shipping hardware controllers. The function and features of the vWLC offer deployment advantages and benefits of controller services where data centers with virtualization infrastructure exist or are considered.

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:

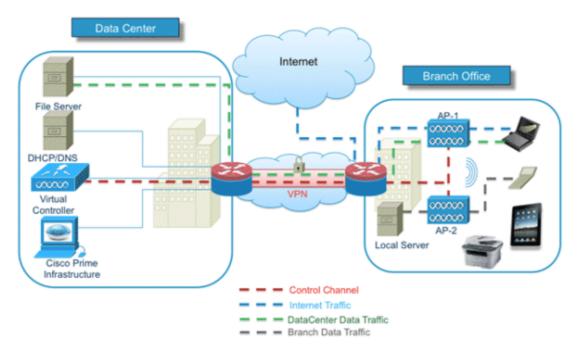
- Cisco Catalyst Switch
- Wireless LAN Controllers Virtual Appliance
- Wireless LAN Controller 7.3 Software
- Cisco Prime Infrastructure 1.2
- 802.11n Access Points in FlexConnect Mode
- DHCP server
- DNS Server
- NTP
- Wireless Client Laptop, Smartphone, and Tablets (Apple iOS, Android, Windows, and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

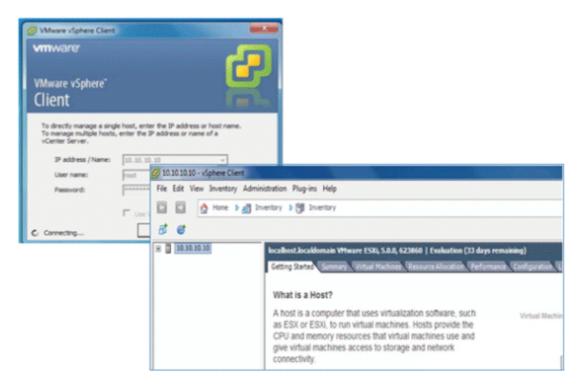
Cisco Unified Wireless Network (CUWN) 7.3 Release Notes contain important information about this release. Log in to Cisco.com for the latest release notes before loading and testing software.

Virtual Controller Installation

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

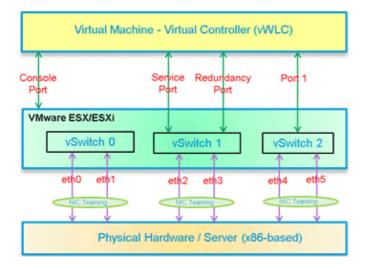
- Single ESXi server management Use VMware vSphere Client.
- Multiple ESXi servers requires vCenter Advance features are also tied with vCenter which needs separate licenses (vMotion, and so on).

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**.

🔗 10.30.20.00 - vSphere Clie			and a second
File Edit View Inventory	Administration Plug-ins Help		
1 1 1 1 1 1 mm 3	all Inventory > 15 Inventory		
× 🖉 10.10.10.10	the second se	1996, 5.8.8, 623060 Evaluation (23 days remaining) Defension, "Associationscience, "Automatica, Contemporary Statistical Science, Texas, "Association,	
	Hardware Helth Status	Vew: Signer Darlar Sont	Refeat Addinguing Popular.
	Processors Hensary Dongin • Tethologing Drongs Adapters Tethologing Advanced Settlogis Found Hanagement	Standard Sector Velocitid Remove Properties	
	Software Licensed Features The Carligatetion DHE and Routing Authentication Services	weet - 18.35.36.38	

2. Select Virtual Machine, and click Next.

Connection Type Networking hardware	can be partitioned to accommodate each service that requires connectivity.
onnection Type etwork Access onnection Settings ummary	Connection Types
	VHikemel The Wikemel TCP/IP stack handles traffic for the following ESN services: vSphere vMotion, ISCSI, NFS, and host management.

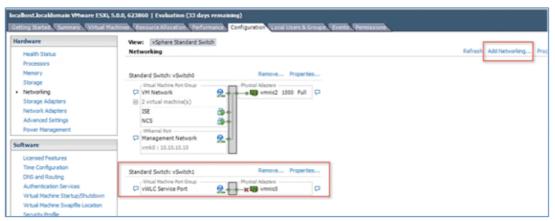
3. Create a vSwitch and assign a physical NIC in order to connect the vWLC service port. The service port does not have to be connected to any part of the network (typically disconnected/unused). As a result, any NIC (even disconnected) can be used for this vSwitch.

Virtual Machines - Net Virtual machines rea	twork Access ch networks through uplink adapters attached to vSph	ere standard s	witches.
Connection Type Network Access	Select which vSphere standard switch will handle the network traffic for this connection. You may also create a vSphere standard switch using the unclaimed network adapters listed below.		
Connection Settings Summary	Create a vSphere standard switch	Speed	Networks
Summary	Cisco Systems Inc Cisco VIC Ethern	et NIC	
	Vmnic0	Down	None
	🗆 🗐 vmnic1	Down	None
	Intel Corporation 82576 Gigabit Ne	twork Conne	ction
	🗆 💷 vmnic3	1000 Full	10.10.11.224-10.10.11.224 (VLAN 11)
	C Use vSwitch0	Speed	Networks
	Intel Corporation 82576 Gigabit Ne	twork Conne	ction
	🗆 🐻 vmnic2	1000 Full	None
	Preview:		
	Virtual Machine Port Group	Physical Adapter	
	VM Network 2	- 🔛 vmnic	:0

- 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.

Virtual Machines - Conn Use network labels to i	ection Settings dentify migration compatible connect	ions common to two or more hosts.
Connection Type letwork Access Connection Settings Jummary	Port Group Properties Network Label: VLAN ID (Optional):	VWLC Service Port None (0)
	Preview:	
	-Virtual Machine Port Group vWLC Service Port	Physical Adapters

- 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.

Virtual Machines - Nel Virtual machines rea	twork Access ch networks through uplink adapters attached to vSph	ere standard si	witches.
Connection Type Network Access	Select which vSphere standard switch will handle vSphere standard switch using the unclaimed ne		
Connection Settings Summary	• Create a vSphere standard switch	Speed	Networks
	Cisco Systems Inc Cisco VIC Ethern	et NIC	
	🗌 📟 vmnic1	Down	None
	Intel Corporation 82576 Gigabit Ne	twork Conne	ection
	🔽 📟 vmnic3	1000 Full	10.10.11.224-10.10.11.224 (VLAN 11)
	C Use vSwitch0	Speed	Networks
	Intel Corporation 82576 Gigabit Ne	twork Conne	ection
	🖂 🖾 vmnic2	1000 Full	None
	O Use vSwitch1	Speed	Networks
	Preview:		
	- Virtual Machine Port Group VM Network 2	Physical Adapter	

- 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.

Virtual Machines - Conne Use network labels to id	ction Settings entify migration compatible connections common to two or more	hosts.
Connection Type Network Access Connection Settings Summary	Port Group Properties Network Label: VLAN ID (Optional): None (0) Al (4095)	
	Preview:	£5
	vWLC Data Port 🧕 💿 ன vmn	

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.

Hardware	View: vSphere Standard Switch	
Health Status	Networking	
Processors		
Memory	Standard Switch: vSwitch0	Remove Properties
Storage	Virtual Machine Port Group	Physical Adapters
Networking	🖓 VM Network 🧕	🗣 🗣 🛛 🐯 vmnic2 1000 Full 📮
Storage Adapters	2 virtual machine(s)	
Network Adapters	ISE	+
Advanced Settings	NCS d	×+
Power Management	- VMkernel Port	
	🖓 Management Network 🧕	
oftware	vmk0 : 10.10.10.10	
Licensed Features		
Time Configuration		Remove Properties
DNS and Routing	Standard Switch: vSwitch1	
Authentication Services	Virtual Machine Port Group	Physical Adapters
Virtual Machine Startup/Shutdown	S Mice Service Port 2	
Virtual Machine Swapfile Location		
Security Profile	Standard Switch: vSwitch2	Remove Properties
Host Cache Configuration	- Virtual Machine Port Group	Physical Adapters
System Resource Allocation	🖓 vWLC Data Port 🧕 🧕	vmnic3 1000 Full 🖓

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

ts Network Adapte	rs		
Configuration vSwitch vWLC Data Port	Summary 120 Ports Virtual Machine		LC Data Port (4095)
		Effective Policies Security	
		Promiscuous Mode:	Reject
		MAC Address Changes:	Accept
		Forged Transmits:	Accept
		Traffic Shaping	
		Average Bandwidth:	-
		Peak Bandwidth:	-
		Burst Size:	-
		Failover and Load Balancing	
		Load Balancing:	Port ID
		Network Failure Detection:	Link status only
		Notify Switches:	Yes
		Falbad:	Yes
		Active Adapters:	vmnic3
		Standby Adapters:	None
Add	Edit N Remove	Unused Adapters:	None

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

	· long · l	
Seneral Security Traffic Sh	aping NIC Teaming	
Port Group Properties		
Network Label:	vWLC Data Port	

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

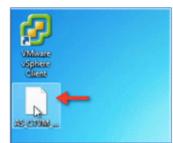
eneral Security Traffic Shap	oing NIC	C Teaming	
Policy Exceptions			
		-	
Promiscuous Mode:	•	Accept	
Promiscuous Mode: MAC Address Changes:		Accept Accept	æ

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

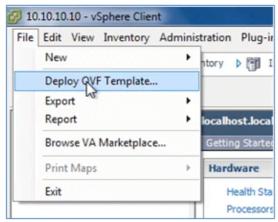
rts Network Adapters			
Configuration	Summary	Port Group Properties	
vSwitch	120 Ports	Network Label:	vWLC Data Port
👷 vWLC Data Port	Virtual Machine	VLAN ID:	All (4095)
		Security	
		Security Promiscuous Mode:	Accept
			Accept
		Promiscuous Mode:	
		Promiscuous Mode: MAC Address Changes:	Accept
		Promiscuous Mode: MAC Address Changes: Forged Transmits:	Accept

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.

Disk Format In which format do you	want to store the virtual disks?	
Source OVF Template Details Name and Location Disk Format Network Mapping Ready to Complete	Datastore: Available space (GB):	datastore1 (7) 3234.1
	Thick Provision Lazy Ze	eroed
	C Thick Provision Eager 2	Zeroed
	C Thin Provision	

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

Name and Location Specify a name and loc	ation for the deployed template
Source OVF Template Details Name and Location Disk Format Network Mapping Ready to Complete	Name: Gisco Wireless Lan Controller The name can contain up to 80 characte

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

Disk Format In which format do you	want to store the virtual disks?	
Source OVF Template Details Name and Location Disk Format Network Mapping Ready to Complete	Datastore: Available space (GB):	datastore1 (7) 3234.1
	Thick Provision Lazy Z	eroed
	C Thick Provision Eager	Zeroed
	C Thin Provision	

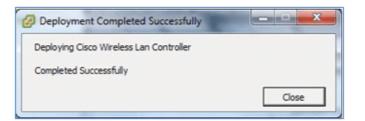
12. Accept the Network Mapping default, and click Next.

Network Mapping What networks should t	he deployed template use?	
Source OVF Template Details Name and Location	Map the networks used in this OVF t	template to networks in your inventory
Disk Format	Source Networks	DestinationNetworks
Network Mapping Ready to Complete	VM Network	VM Network

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

Ready to Complete Are these the options yo	ou want to use?	
Source OVF Template Details Name and Location	When you click Finish, the dep Deployment settings:	loyment task will be started.
Disk Format	OVF file:	C:\Users\Demo\Desktop\AS_CTVM_7_3_1_24Low
Network Mapping	Download size:	148.8 MB
Ready to Complete	Size on disk:	8.1 GB
	Name:	Cisco Wireless Lan Controller
	Host/Cluster:	localhost
	Datastore:	datastore1 (7)
	Disk provisioning:	Thick Provision Lazy Zeroed

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



Two important things to note regarding upgrading virtual controllers:

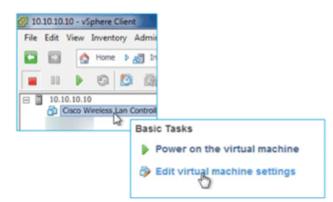
- The OVA image is needed only for first time installation.
- The .AES image can be subsequently used for upgrading/downgrading.

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).

lardware Options Resources]	Virtual Machine Versio		
Show All Devices	Add Remove	Device Status		
Hardware Summary		Connect at power on		
Memory CPUs Video card	5120 MB 1 Video card	Adapter Type Current adapter: E1000		
VMCI device SCSI controller 0 Hard disk 1	Restricted LSI Logic Parallel Virtual Disk	MAC Address		
CD/DVD drive 1	[datastore1 (7)] Cisco	@ Automatic C Manual		
Network adapter 1 Network adapter 2 Floppy drive 1	VM Network VM Network Floppy 1	DirectPath I/O Status: Not supported Network Connection Network label:		
		VM Network VM Network VMCC Data Port		

3. Map Network adapter 2 to vWLC Data Port.

-3	Network adapter 1 (edite	vWLC Service Port			
43	Network adapter 2	VM Network	DirectPath I/O		
4	Floppy drive 1	Floppy 1	Status:	Not supported 0	
			Network Connection	n	
			VM Network		-
			WH Network		
			VWLC Data Port VWLC Service Port	2	

4. Confirm the correct mapping.

0_	CD/DVD drive 1	[datastore1 (7)] Cisco .
12	Network adapter 1 (edite	vWLC Service Port
10	Network adapter 2 (edite	vWLC Data Port
녑	Floppy drive 1	Floppy 1

Virtual Controller Console Port

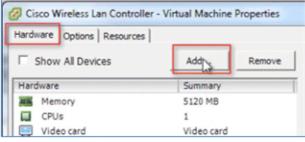
The console port gives access to the console prompt of the WLC. As a result, the VM can be provisioned with serial ports in order to connect to these. In the absence of serial ports, the vSphere Client Console is connected to the console on the vWLC.

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.



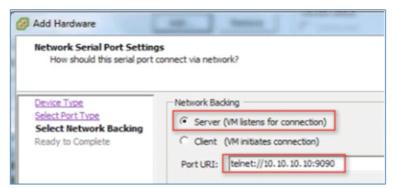
2. On the vWLC Hardware tab, click Add.

Device Type What sort of device d	o you wish to add to your virtual machine?
Device Type Select Port Type	Choose the type of device you wish to

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

Serial Port Type What media should this	virtual serial port access?
Device Type Select Port Type Select Network Backing Ready to Complete	Select the type of media you would like the virtual serial port to access Serial Port Output
	$\ensuremath{\mathbb{C}}$ Use physical serial port on the host
	C Output to file
	C Connect to named pipe
	Connect via Network

- 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.

Ready to Complete Review the selected opt	ions and click Finish to add the hardware.	
Device Type Select Port Type	Options:	
Select Network Backing	Hardware type:	Serial Port
Ready to Complete	Serial port type: Serial port direction:	Network serial port Publish
	Port URI:	telnet://10.10.10.10:9090
	Use virtual serial port concentrator:	
	Connect at power on:	Yes
	Yield CPU on poll:	Yes

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

CD/DVD drive 1 [datastore1 (7)] Network adapter 1 (edite Network adapter 2 (edite VWLC Data Por VWLC Data Por	
Floppy drive 1 Floppy 1 New Serial Port (adding) telnet://10.10	
	Use network Server (VM listens for connection) Client (VM initiates connection) Port URI: telnet://10.10.10.10:9090 Use Virtual Serial Port Concentrator

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**.

	me 🕨 🔊 🕅	Security	Profile	-	
8 8	ation (33 day	Services			
8 10.10.10.10	Line Manual	I/O Ded	lizertar (Artive Dire	arton Caniral	
Starage Networking Starage Adapters Network Adapters Advanced Settings Pount Networksenet	vpix ESI Shell Local Security Authentication NTP Deenon SSH Direct Console UI	Server (Active Directory Service)			
Software		5009	41	Refresh	Pflagentie
Licensed Featu Time Configura DNS and Rout	ation	10 (TCP) 2124-4535 (TCP) 10 (TCP) (TCP) 2 (TCP) 2 (TCP) 2 (TCP) 2 (AS (TCP) (UOP) 10.290 (TCP)(DP)	41 42 43 43 43 43 43 43 43		27
Authentication Virtual Machine	i Services e Startup/Shutdown e Swapfile Location	2.008.109	AT		

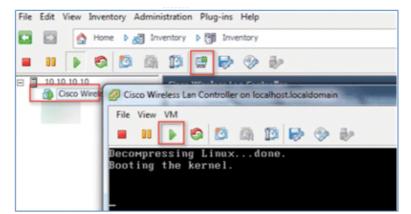
8. In the Firewall Properties window, select VM serial port connected to vSPC, and click OK.

ig services on remote check box to provide and stop when all of t abel red Services	hosts. access to a service or heir ports are closed, o	client. Daemons		when their ports		
ult, remote clients are g services on remote i check box to provide and stop when all of t abel red Services	hosts. access to a service or heir ports are closed, o	client. Daemons or as configured	will start automatically will start automatically will start automatically will be a start automatically w	when their ports		
ult, remote clients are g services on remote i check box to provide and stop when all of t abel red Services	hosts. access to a service or heir ports are closed, o	client. Daemons or as configured	will start automatically will start automatically will start automatically will be a start automatically w	when their ports		
ig services on remote check box to provide and stop when all of t abel red Services	hosts. access to a service or heir ports are closed, o	client. Daemons or as configured	will start automatically will start automatically will start automatically will be a start automatically w	when their ports		
check box to provide and stop when all of t abel red Services	access to a service or heir ports are closed, o	or as configured			are	
and stop when all of t abel red Services	heir ports are closed, o	or as configured				
ed Services	Incom	ing Ports				
ed Services	Incom	ning Ports	A Annalase Bard			
			Outgoing Ports	Protocols	Daemon	
e Shell						
SH Server	22			TCP	Stopped	
SH Client			22	TCP	N/A	
	ment Protocol					
uped						
					N/A	
	ed to vSPC					I
ault Tolerance	8100,		80,8100,8200	TCP,UDP	N/A	
					•	
Properties						
ral						
ina.	UM carial part coop	acted to uSDC				
	The sense por contra	ected to vor c				
age information:						
all Settings						
ed IP Addresses:	Al					
	BH Client Network Manager aped NS Client M serial port connects TP Client sult Tolerance Froperties ral ce: age Information: all Settings	BH Client Network Management Protocol aped NS Client S3 M serial port connected to vSPC TP Client sult Tolerance Froper ties ral ce: VM serial port conn age Information: all Settings	SH Client Network Management Protocol aped NS Client S3 M serial port connected to vSPC TP Client sult Tolerance Froperties ral ce: VM serial port connected to vSPC age Information: all Settings	SH Client 22 Network Management Protocol aped NS Client 53 53 M serial port connected to vSPC 0-65535 TP Client 123 sult Tolerance 8100,8200 m re Properties real ce: VM serial port connected to vSPC age Information: all Settings	SH Client 22 TCP Intervent Management Protocol aped 53 53 UDP,TCP NS Client 53 53 UDP,TCP M serial port connected to vSPC 0-65535 TCP TP Client 123 UDP nult Tolerance 8100,8200 TCP,UDP	SH Client 22 TCP N/A Retwork Management Protocol aped NS Client 53 53 UDP,TCP N/A M serialport connected to vSPC 0-65535 TCP N/A TP Client 123 UDP Stopped nult Tolerance 8100,8200 80,8100,8200 TCP,UDP N/A TT Properties real ce: VM serial port connected to vSPC age Information: all Settings

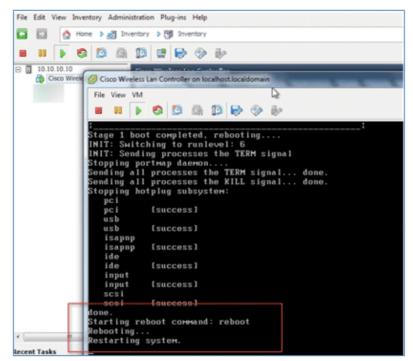
Start up the vWLC

Complete these steps:

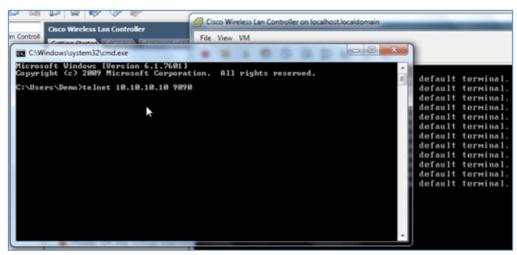
1. Start the vWLC, and select the console in order to observe the first-time installation process.



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:

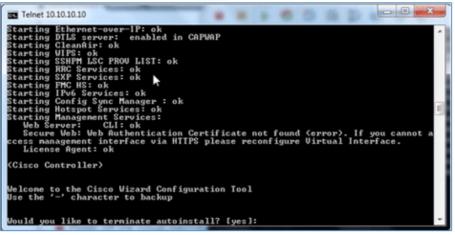


4. The Telnet session will now manage the console to the vWLC.



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.

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



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

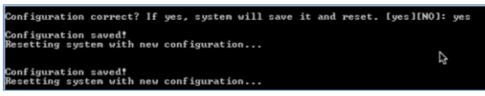
Telnet 10.10.10.10
Systen Name [Cisco_08:5b:c2] (31 characters max): AUTO-INSTALL: no interfaces registered.
AUTO-INSTALL: process terminated no configuration loaded wWLC
whic Enter Administrative User Name (24 characters max): admin Enter Administrative Password (3 to 24 characters): ******** Re-enter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

7. 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

configuration, which may result in APs not joining in the process.

Enter Country Code list (enter 'help' for a list of countries) [US]: Enable 802.11b Network [YES][no]: Enable 802.11g Network [YES][no]: Enable 802.11g Network [YES][no]: Enable Auto-RF [YES][no]: Configure a NTP server now? [YES][no]: yes Enter the NTP server's IP address: 10.10.10.1 Enter a polling interval between 3600 and 604800 secs: _

8. Complete the configuration and allow the vWLC to reset.



9. It is suggested that you ping the vWLC management interface in order to ensure that it has come online. Log in to the vWLC.

Starting RRC Services: ok Starting RRC Services: ok Starting FRC HS: ok Starting FRC HS: ok Starting IPv6 Services: ok Starting Config Sync Manager : ok
Starting Hotspot Services: ok
CAWindows/system32/cmd.exe - ping 1 Starting Management Services:
Web Server: CLI: ok
Reply from 10.10.11.224: Desti Secure Web: ok
Reply from 10.10.11.224: Desti License Agent: ok Reply from 10.10.11.224: Desti
Reply from 10.10.11.1.224 Desti (Cisco Controller)
Reply from 10.10.11.224: Desti
Reply from 10.10.11.224: Desti Enter User Name (or 'Recover-Config' this one-time only to a
Reply from 10.10.11.224: Desting factory defaults)
Reply from 10.10.11.224: Desti
Reply from 10.10.11.224: DestiUser: admin
Reply from 10.10.11.224: Desti Password: MAMMAN Reply from 10.10.11.224: Destination most unreachanie.
Reply from 10.10.11.224: Destination nost unreachable. Reply from 10.10.11.224: Destination host unreachable.
Reply from 10.10.11.224: Destination host unreachable.
Reply from 10,10,11,224: Destination host unreachable.
Reply from 10.10.11.224: Destination host unreachable. Reply from 10.10.11.20: bytes=32 time=421ms TTL=128
Reply from 10.10.11.20; bytes=32 time=121ms TiL=120 Reply from 10.10.11.20; bytes=32 time(ins TIL=128
Reply from 10.10.11.20: bytes 32 time ins TL-128
Reply from 10,10,11,20: bytes=32 time<1ms TTL=120
Replý fron 10.10.11.20: hýtes=32 tine<1ns TTL=128

10. You can issue the **show interface summary** command and ping the gateway from the vWLC.

Number of Interfaces				
Interface Name est	Port	Vlan Id 	IP Address	
 nanagement	1	11	10.10.11.20	
service-port	N/A	N/A	0.0.0.0	
virtual	N/A	N/A	1.1.1.1	

11. Connect to vWLC management using a web browser

cisco	indows Security				1 - I
cisce	The server 10.10 password.	0.11.20 at Cisco Contro	iller requires a use	mame and	i.
Wirela		admin			
		Remember my cr	edentials		Login
			ОК	Cancel	coger

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

						Saye	Comig
cisco	MONITOR WLANS C	ONTROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEC
Monitor Summary > Access Points > Cisco CleanAir	Summary 0 Access	Points Supported	o Virtual Wir	eless Controlle	er		
Statistics CDP Rogues	Controller Summary Management IP Address	10.10.11.20	Rogue Su			0	
Clients	Service Port IP Address		Active Roge	ue Clients		0	
Circino	Software Version	7.3.1.241	Adhoc Roge	ues		0	
Multicast	Emergency Image Version	7.3.1.241	Rogues on	Wired Network		0	
	System Name	VWLC	Top WLANS				
	Up Time	0 days, 0 hours, 2 minutes					
	System Time Fri Jun 8 10:43:1		TOP WEAK				
	Redundancy Mode	N/A	Profile Name	Profile Name # of Clients		f Clients	
	802.11a Network State	Enabled					
	802.11b/g Network Enabled		Most Reco	ent Traps			
	Local Mobility Group	demo					

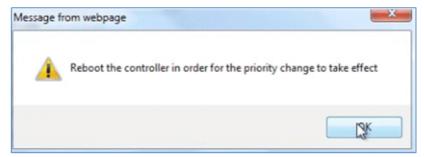
13. Go to Management > Software Activation > Licenses. Select base-ap-count, and set the Priority to High.

cisco	MONITOR WLANS	CONTROLLER WIRELESS SECURITY MANAGEMENT
Management	License Detail	
Summary > SNMP HTTP-HTTPS Telnet-SSH Serial Port	Name Type Version Comment	base-ap-count evaluation 1.0
Local Management Users User Sessions	Status Expires	EULA Not Accepted 8 weeks, 4 days
 Logs Mgmt Via Wireless Software Activation 	Built-In License Maximum Count	Yes 200
Licenses License Level Commands License Agent	Counts Used Priority	0 Low Set Priority Low High

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

Message from w	vebpage 📃 🚬	
Are	you sure you want to change the priority of this license?	
	Cancel	
	End User License Agreement (EULA)	83
	Applicable to the Limited Warranty Statement and End User License" shall survive termination of this Agreement. Customer Records. Customer grants to Cisco and its independent accountants the right to examine Customer's books, records and accounts during Customer's normal business hours to verify compliance with this Agreement. In the event such audit discloses non-compliance with this Agreement, Customer shall promptly pay to Cisco the appropriate license fees, plus the reasonable cost of conducting the audit. Export. Software and Documentation, including technical data, may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Software and Documentation used in the strict and the federal Acquisition Regulation ("FAR") (48 C.F.R.) 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in FAR 12.212. Consistent with FAR 12.212 and DOD FAR Supp. 227.7022-1 through 227.7202-4, and notwithstanding any other FAR or other contractual clause to the contrary in any agreement into which this End User Cicense Agreement may be incorporated, Customer may provide to Government end user or, if this Agreement is direct. Government end user will acquire, the Software and Documentation with only those rights set forth in this End User License Agreement. Use of either the Software or Documentation or both constitutes agreement and "commercial computer software for Concumentation or both constitutes agreement or software and Documentation are "commercial computer software" and "commercial computer software for the software or constitutes acceptance of the rights and restrictions herein. Limited	·
	Accept Decline	

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



16. Reboot the vWLC.

cisco	MONITOR WLANI CONTROLLER WIRELESS SECURITY MANAGEMENT	Sage COMMANDS HELP EEEDBACK
Commands Download File	System Reboot	Tyve and Reboot
Upload File Rebool Config Boot > Scheduled Reboot	Warning: The configuration of the controller is changed and not saved yet. Click on "Save and Reboot" to save the changes before the controller is rebooted, or click on "Reboot without Save" to reboot the controller without saving the changes. Please be aware that in either case, all the	
Reset to Factory Default Set Time	connections will be lost. To regain the connection, please log in again after the controller is rebooted.	
Login Banner		

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

MONITOR	WLANS		VIRELESS	SECURITY	MANAGEMENT	co
Summary						
	200 A	ccess Points Support	ed			
		La.	Cisco	Virtual Wir	eless Controlle	F
Controller	Summar	Y		Rogue Su	mmary	
Managemer	nt IP Addres	ss 10.10.11.20		Active Rog	APc	
Service Por	t IP Addres	s 0.0.0.0		Active Rog		
Software Ve	ersion	7.3.1.241				
Emergency	Image	791941		Adhoc Rog	ues	

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

CAPWAP-3-ERRORLOG: Did not get log server settings from DHCP.
CAPWAP-3-ERRORLOG: Could Not resolve CISCO-CAPWAP-CONTROLLER
CAPWAP-3-ERRORLOG: Go join a capwap controller
CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: 10.10.11.20 peer_port: 5246
CAPWAP-5-DTLSREQSUCC: DTLS connection created sucessfully peer_ip: 10.10.11.20 peer_port: 5246
CAPWAP-5-SENDJOIN: sending Join Request to 10.10.11.20
LINK-6-UPDOWN: Interface DotllRadio0, changed state to down
LINK-5-CHANGED: Interface Dotl1Radio0, changed state to reset
CAPWAP-5-JOINEDCONTROLLER: AP has joined controller vWLC
ac first hop mac = IP:10.10.11.20 Hop IP:10.10.11.20 IDB:BVI1

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

		LESS SECURITY
All APs		
Current Filter		None
Number of APs		1
AP Name	AP Model	
APf866.f267.f7af	AIR-CAP35	02I-A-K9

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

ONITOR	WLANS	CONTR	OLLER	WIREL	ESS	SECURITY
II APs > [Details fo	or APf8	66.f26	7.67af		
General	Crede	ntials	Inter	faces	Hig	h Availability
General						
AP Nam	e	APf	366.f267	67af		
Location	1	defa	ult locat	ion		
AP MAC	Address	f8:6	6:f2:67:	67:af		
Base Ra	dio MAC	58:1	bc:27:92	:47:d0		
Admin 5	Status	Ena	ble 🕶			
AP Mode	e	loca	l			
AP Sub	Mode	loca		-		
Operatio	onal Status	mor	Connect stor	tor		

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

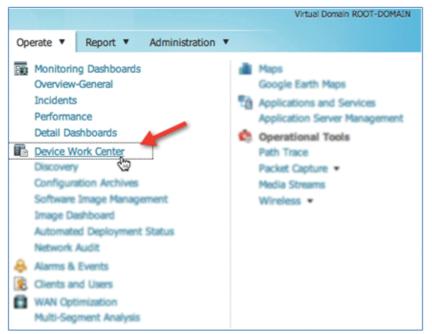
Virtual Controller Management with Cisco Prime 1.2

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.

۵	Home	Design 🔻	Deploy	•	Operate	•	Report	•
				楢	Discovery	ø	Configura	ation
Device Group > A ALL	LL					/		
/ Edit X Del	lete 🤏 Syn	Groups & S	ites +	Add	Device	D.I	k Import	
Device N	ame 🔺	Reachabil	ity	11	Addres	S	(Devi

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

 General Para 			*
[* IP Address	10.10.10.5	
SNMP Param	eters		
	Version	v2c *	
	* Retries	2	
	* Timeout	10	(secs)
	* Community	•••••	
• Telnet/SSH P	arameters		
	Protocol	Teinet *	
	Timeout	60	(secs)
	Username		
	Password		
Con	firm Password		
En	able Password		
Confirm En	able Password		

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

	ce Group > ALL				
LL					
/1	Edit 🗙 Delete 🦓 Syna	Groups & Sites 🔻 😡	Add Device Bulk I	mport	
P			-		
	Device Name	Reachability	IP Address	Device Type	Collection Status
	Device Name SiteB-vWLC	Reachability Reachable	IP Address 10.10.21.5	Device Type Cisco Virtual Wir	Collection Status

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.

/ 1	idit 💙 Dalata 🖏	Q.mc	Groups & Sites 💌 😪	Add Davice B	lk Import	
	Device Name	a l	Reachability	IP Address	Device Type	Collection Status
4	SiteA-vWLC	-	Reachable	10.10.11.5	Cisco Virtual Wireless LAN Co	Managed
						-
ב	SiteB-vWLC		Reachable	10.10.21.5	Cisco Virtual Wireless LAN Co	Managed

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

Device Work Center			Discovery 🗱 0	Configuration Archives 🚳 Software Image Management	i 📰 Image Dash	iteard 🤤 Automa	ted Deployment Status 🔝 N	ketwork.
Device Group	Device Group > Device 1 Cisco VERTUAL Se			i. Series Window LAN Controller			Delected 0 Total 3	
Sa ALL	/ fidt)(Delate 4	Sync Groups & Sites	* 👷 Add Device	Bulk Import Ratiout Download Configure		Show All		- 7
* 💄 Device Type	Device •	Reachability	IP Address	Device Type	Status	Software V	Inventory Collection	M
 Southed AP Souther Controller 	SteC-vWLC	Reachable	10.10.31.5	Cisco Virtual Wireless LAN Controller	Managed	7.3.1.57	2012-Jul-24, 03:00:03 PDT	-
Sisce VSRTUAL Series Wireless UAN Controlle	Stell-WLC	Reachable	10.10.21.5	Cisco Virtual Wireless LAN Controller	Managed	7.3.1.57	2012-Jul-24, 03:00:03 POT	-
A Site Groups A User Defined	SteA-VM.C	Reachable	10.10.11.5	Cisco Virtual Wiveless LAN Controller	Managed	7.3.1.57	2012-Jul-24, 03:00:03 PDT	-

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

adaada Gisco Prime			Virtual Domein ROOT-DOMAIN rest +
cisco Infrastructure	🕼 Home Design * Deploy	v * Operate * Report * Administration	•
Overview Incidents Performance	Detail Deshboards		
General Client Security	Hesh GeanAir Context Aware		
Filters () *Time Frame Past 1 Ho.	r • 60		
Network Device Summary			Top N CPU Utilization
Total Menaged Device Court: 3	Ap Availability: 3	Total Unvacitable Device Count: 0	Device Name Device IP Average Maximum SteB-vWLC 10.10.21.5 0% 0% SteB-vWLC 10.10.31.5 0% 0% SteB-vWLC 10.10.31.5 0% 0%
Witneless Controller	Reschuble Unified AP		
No. 1	¥≣		
Top N Memory Utilization			
Device Name Device IP Inst	ance Average • Maximum	Minimum Current	
SiteA-vWLC 10.10.11.5	21% 21%	21% 21%	
SiteC-vWLC 10.10.31.5 SiteB-vWLC 10.10.21.5	21% 21%	21% 21%	C%-50% S1%-70% 71%-90% 891%-100%
SH88-VWLC 10.10.21.5	21% 21%	21% 21%	

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**.

	Virtual Domain ROOT-DOMAIN root 👻	a
	Switch to Classic Theme	~
ninistration 🔻	Preferences	
	Change Password	
	Logout	

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.

Reports Admini	stration 🔻		₽ ⊕ 9	0
	Ľ	Add Controllers		°
Mobility Group Name	Reachability	Bulk Update Controllers Reboot Controllers		2
rfsiteb	Reachable	Download Software(TFTP)		
rfsitea	Reachable	Download Software(FTP) Download IDS Signatures Download Customized WebAuth Download Vendor Device Certificate		

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

cisco Infrastruct	ure	🏠 н	lome Mc
Add Controllers Configure > Controllers > Ad	ld Controllers		
General Parameters			
Add Format Type	Device Info	\$	
IP Addresses	10.10.31.5		(comma-s
🗆 Wism Auto Add 🕖			
SNMP Parameters ①			
Version	v2c	\$	
Retries	2		
SNMP Timeout	10		(secs)
Community	•••••		
Telnet/SSH Parameters)		
Protocol	Teinet	•	
Username	admin		
Password			
Confirm Password			
Teinet Timeout	60		(secs)
Add			

13. Cisco Prime Infrastructure will display this notification:

Add Contr Configure > (rollers Controlers > Add Controllers Result
IP Address	Status
10.10.31.5	Controller is added. It will appear in Configure->Controller page once inventory collection is completed. Otherwise, go to Configure->Unknown Device page to check the status.
General Par	amotors

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.

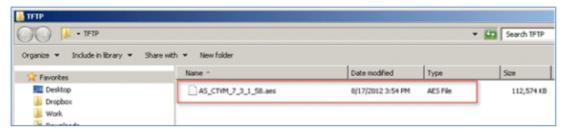
	India Osco Prime Isco Infrastructu	re	🟠 Home Ma	onitor • Configu	re • Services •	Reports Administratio	on i 🕶
	gure > Controllers						- 5
0	IP Address	Device Name	Device Type	Location	SW Version	Mobility Group Name	Reachability Status
-	P Address 10.10.31.5 d?	Device Name SiteC-vWLC	Device Type VWLC	Location	SW Version 7.3.1.57	Mobility Group Name	Reachability Status
				Location			Reachability Status Reachable Reachable

Upgrade the Virtual Controller

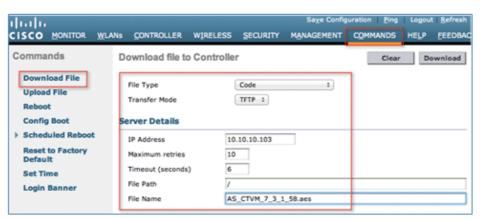
In the early steps of installation, the Cisco Virtual Controller initially required an OVA file for new virtual appliance creation. However, maintaining virtual controller features and software upgrades require a common AES file downloadable from the Cisco website.

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.

cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	Sa <u>x</u> MANAGEMENT	e Configuration	Eing HELP	Logout Refrest
Commands	Download file to	Controller					Clear	Download
Download File Upload File Reboot Config Boot	File Type Transfer Mode Server Details			Code TFTP =	1			
Scheduled Reboot Reset to Factory Default Set Time	IP Address Maximum retries Timeout (seconds)		10.1 10 6	0.10.103				
Login Banner	File Path File Name		L	CTVM_7_3_1_				
	TFTP File transf pre-download t For the new Code to ta	he image to	APs befor	e rebootir	ng to reduce	network do	wntim	

4. Click Save and Reboot.

MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	Sa <u>v</u> M <u>A</u> NAGEMENT	e Configuration	Ping HELP	Logout <u>R</u> efresh
System Reboot				Sav	e and Reboot	Reboo	t without Save
Warning: The coni changed and not s Reboot" to save the rebooted, or click reboot the control Please be aware t connections will b please log in again	aved yet. Click he changes befor on "Reboot with ler without savin hat in either cas e lost. To regain	on "Save and re the contro- nout Save" to ng the chang se, all the n the connect	d Iler is es. ion,				

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.

	isco Infrastr			🏠 Home	Monitor + (lanfigure * Services *	Reports * Administration		
	pre > Controller								✓ Select a command Add Controllers Remove Controllers
ø	IP Address A		Device Name	Device Type	Location	SW Version	Mobility Group Name	Reachability Statu	Bulk Update Controllers Reboot Controllers
	10.10.11.5	dP	SiteA-vWLC	VWLC		7.3.1.57	rfsitea	Reschable	Download Software(TFTP).
2	10.10.21.5	ø	SiteB-vWLC	VWLC		7.3.1.57	rfsibeb	Reschable	Download Software/FTP).
	10.10.31.5	0	SteC-WLC	VWLC		7.3.1.57	rfsitec	Reschable	Download IDS Signatures Download Customized WebAuth
									Download Vendor Device Certifica Download Vendor CA Certificate

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 Configure > Controllers > Down	Controller nload 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
ownload Type	
Download Type 🕖	Now O Scheduled
TFTP Servers	○ Local machine ⊛ TFTP server
Server Name	New External TFTP Server
Server IP Address	10.10.10.103
Maximum Retries	10
Timeout	6 (secs)
File Path	7
Server File Name	AS_CTVM_7_3_1_58.aes
Download Cancel	

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

🔖 Títpd32 by Ph. Jounin		_OX
Current Directory C:\Users\ \Desktop\TFT	P. E	lowse
Server interfaces 10.10.103	• S	how Dir
Tftp Server Log viewer		
🎕 \AS_CTVM_7_3_1_58.aes to 10.10.1 🗙 🖬	progress	
File size : 115275504 45		14
	13%	15
	124	1
AS_CTVM_7_3_1_58.aes to 10.10.2 X		
File size : 115275504		
15194112 Bytes sent 949632 Bytes/sec		
		- 1
N₂ \A5_CTVM_7_3_1_58.aes to 10.10.3 ×		
File size : 115275504 14968320 Bytes sent 935520 Bytes/sec		-
14306320 byves serk 333320 byves/sec		
	He	p

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	TRANSPER_SUCCESSFUL	TITP 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	TRANSPER_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.

	India Caso Provide	ructure		The Home Monitor	· Configure *	Services * Report	s * Administration *		COMPANY I MAY Do	P000
	trollers (1733) gant > Controlle								✓ Select a command Add Controllers Remove Controllers Bulk Uodate Controllers	
8	IP Address		Device Name	Device Type	Location	SW Version	Nobility Group Name	Reachability Stat	Reboot Controllers	
8	10.10.31.5	t?	ShiC-WLC	VWLC		7.3.1.57	rfatec	Reachable	Download Software(TFTP)	Stands at 1
a.	10.10.21.5	ø	Stell-wild	VWLC		7.3.1.57	rbibib	Reachable	Download Software(TPTP).	
×	10.10.11.5	ø	Stek-vWLC	VWLC		7.3.1.57	risitee	Reachable	Download IDS Signatures Download Customized WebAuth	
-									Download Vendor Device Certificate	

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

Reboot Controllers Configure > Controllers > Reboot Controllers					
Reboot Controllers	_				
Save Config to Flash	2				
Reboot APs					
Swap AP Image	⊖Yes ⊛No				
OK Cancel					

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

Reboot Controllers
Configure > Controllers > Reboot Controllers
Please wait
Flease wait
NCS is rebooting controllers with selected configurations. This operation may take a long time.

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

Reboot Controller Configure > Controllers >	s Result 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
HasbdRbb60436202e830802be1e8931d539b67b2537
```

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
     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 <u>http://myh66.com</u> <u>http://usermanuals.us</u> <u>http://www.somanuals.com</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.com</u> <u>http://www.404manual.com</u> <u>http://www.luxmanual.com</u> <u>http://aubethermostatmanual.com</u> 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