ıılıılıı cısco



Cisco TrustSec[®] How-To Guide: AnyConnect Network Access Manager Enterprise Connection Enforcement

For further information, questions and comments please contact ccbu-pricing@cisco.com

Guide

Contents

Introduction	
Executive Summary About this Document Scenario Overview Architecture Software and Hardware Requirements	
Technology Primer	5
Design Parameters	5
EAP Methods Identity Source and Database Encryption	
Configuring the Wireless LAN Controller	6
Configuring the Cisco Identity Services Engine	
Defining Authentication Policies and Authorization Profiles	17
Configuring the AnyConnect Network Access Manager	
Testing Procedure	
Appendices	

Introduction

Executive Summary

Employees connect to non-corporate WiFi access points while sitting at their desks or in a conference room, even though the corporate WiFi network is in range and working fine. Some employees connect to a third-party WiFi hotspot to check their personal email or shop on the Internet during normal business hours. Others try to gain access to a competitor's network one floor above, or to a nearby apartment complex. Still others access the guest network because it might have somewhat better performance. Employees should be connecting their corporate laptops to the corporate network, not to these other networks.

Blacklisting is the first thought we think as far as keeping employees from wandering onto other peoples' networks or their own guest networks. While this is a great idea for preventing employees from accessing the guest network, it can have some unintended consequences.

Employees need to access their home networks and WiFi hotspots so they can use the VPN to access the corporate network when they are traveling or working from home. So, while we would like to blacklist Linksys[®] to prevent employees from accessing a network at the apartment complex across the street during the day, we need to let them access their own Linksys home network at night.

Blacklisting also ends up being site specific. Blacklisting one competitor that is in the same office tower in New York does not apply in Paris or Tokyo, where there might be different competitors. Blacklisting is easy to deploy if your business has one location. It is nearly impossible to manage if you are a multinational corporation with hundreds or thousands of sites around the world.

Cisco[®] approached the problem focusing on the corporate WiFi network rather than eliminating non-corporate networks. When the corporate network is in range, there is no need to connect to any other network. When the corporate network is not in range, employees are free to connect to other networks.

Enterprise Connection Enforcement gives IT administrators the ability to select one or more WiFi networks as corporate networks. When any or all of those networks are in range, employees can connect to any of the specified corporate WiFi networks, but employees are prevented from connecting to any third party networks.

Cisco Identity Services Engine (ISE) will provide the back-end RADIUS functions and provide policy control for 802.1X authentication. In this document, EAP-FAST will be used as the authentication method.

About this Document

This document illustrates Cisco AnyConnect[®] Network Access Manager's Enterprise Connection Enforcement feature. It automatically connects to the corporate network designated by the administrator- defined corporate service set identifiers (SSIDs) in the AnyConnect Network Access Manager profile. If any end users connect to non-corporate access points, they will be denied.

When a user connects to a wired corporate network and obtains an internal IP address, the wireless connection will be dropped. EAP-FAST (MSCHAPv2) will be used as the authentication method for wireless and configured within the AnyConnect Network Access Manager profile by the administrator. Both machine and user connection types will also be defined. The ISE server will be configured to use Microsoft AD for machine and user validation, EAP-FAST (MSCHAPv2) for 802.1X authentication, and for creating the Authentication and Authorization policies. Wireless controller configuration information is also included.

In this document, the wired connection will be configured for open authentication to simulate a wired corporate connection.

Scenario Overview

The AnyConnect Network Access Manager profile will contain the EAP-FAST authentication method, and the corporate wireless network designated SSID, which will be lab005. The user will automatically to connect to the corporate wireless network. When the user tries to connect to non-corporate access points, he or she will be denied.

When the user connects to the wired network, he or she will be automatically disconnected from the wireless network.

ISE will be used as the back-end RADIUS server, and the successful authentication logs will be reviewed.



Architecture

Software and Hardware Requirements **Client:**

- Laptop or desktop computer with an Ethernet NIC or WiFi NIC and one of the following operating systems:
 - · Windows 7 SP1 x 86 (32-bit) and x64 (64-bit)
 - Windows Vista SP2 x86 and x64
 - Windows XP SP3 x86
- Windows Server 2003 SP2 x86
- Cisco AnyConnect 3.1 or greater with the Network Access Manager installed
- Cisco AnyConnect 3.1 or greater Profile Editor

Authentication Server:

Cisco ISE System 1.1.1 or greater

Network Infrastructure:

• Ethernet switch or WiFi access point configured for 802.1X

Technology Primer

The Enterprise Connection Enforcement feature will only work with WiFi networks, as well as with administratively defined networks. User-created network configurations will be ignored.

The AnyConnect Network Access Manager will initiate scan requests periodically and retrieve the scan-list to see if any corporate networks are in range and probe for hidden SSIDs on Windows 7 hosts. On Windows XP hosts, probing for hidden SSIDs is not possible and will be non-hidden.

In the event that no wired connections are available, a connection to wireless corporate networks will be allowed, and a connection to non-corporate networks will be denied.

Each corporate network shall be tagged by AnyConnect Network Access Manager and all in-range corporate networks are added to a list of available networks for matching, alternatively non-corporate networks are removed from the list of available networks for matching.

The AnyConnect Network Access Manager will start matching one corporate network to one of the adapters:

- The connection mode is automatic, the connection attempt will be made to corporate networks in the list of available networks for matching one by one until one network is successfully connected.
- If all networks in the list of available networks for matching are tried, but no successful connection is made, the AnyConnect Network Access Manager will start over again from the beginning of the list, this is not admin configurable. The AnyConnect Network Access Manager will not fall back to non-corporate networks.

There are no limitations imposed on the number of network profiles which are designated as corporate networks, and whose SSIDs are configured as non-broadcasting (for example, hidden). However, due to technical limitations in this release of the AnyConnect Network Access Manager, only one hidden SSID can be probed at a time.

Therefore, after reading the profiles sequentially from the configuration, the AnyConnect Network Access Manager will choose the first corporate and hidden network and use its SSID for probing purposes. The remaining corporate networks will be treated as broadcasting Wi-Fi networks for detection of hidden SSIDs, even though they are configured as hidden.

Design Parameters

EAP Methods

The 802.1x authentication framework has been incorporated as part of the 802.3 (Wired Security) and 802.11 (Wireless Security) standard to enable layer-2 based authentication, authorization, and accounting functions in an 802.3 wired network. Today, there are several EAP protocols available for deployment in both wired and wireless networks. The most common EAP protocols are LEAP, PEAP, EAP-FAST, and EAP-TLS. In this document EAP-FAST will be used for 802.1X authentication.

EAP-FAST: EAP-FAST (Flexible Authentication using Secure Tunneling) is defined in RFC 4851 and was developed by Cisco. The protocol was designed to address the weaknesses of LEAP while preserving the lightweight implementation. Instead of using a certificate, mutual authentication is achieved by means of a Protected Access Credential (PAC). PAC files details are covered in the Encryption section below.

EAP-FAST has three phases:

- Phase 0: An optional phase in which the PAC, can be provisioned manually or dynamically (used in this case, with ISE server)
- Phase 1: In this phase, the client and the authentication server uses the PAC to establish TLS tunnel.
- **Phase 2:** In this phase, the client credentials are exchanged inside the encrypted tunnel, using an inner method for authentication.

Identity Source and Database

When deploying in a wired/wireless network and seeking an authentication protocol, it is common to use an existing database of user and machine authentication credentials. Typical databases are Windows Active Directory (AD), LDAP, or a one-time password (OTP) database (for example, RSA SecureID). All of these databases are compatible with the EAP-FAST protocol.

When planning for deployment, there are compatibility requirements, such as EAP Chaining, which requires AD for machine and user validation. For the purpose of this document, AD will be used as the database. EAP Chaining will be enabled in the EAP-FAST protocol selection on the ISE node.

Encryption

EAP-TLS is a strong authentication method, requiring server and client-based X.509 certificates that also need PKI for certificate deployment. Another strong authentication method, EAP-FAST, does not require client side certificates for mutual authentication. Instead, Protected Access Credential (PAC) files are used, which can be provisioned either manually or automatically.

In this document, the PAC files are automatically provisioned from the ISE server to the client if the client does not contain as existing PAC file. Anonymous PAC provisioning uses EAP-TLS with an anonymous key agreement protocol to establish a highly secure TLS tunnel. In addition, MSCHAPv2 is used to authenticate the client and prevent early MITM attack detection.

Authenticated In-Band PAC provisioning uses TLS server-side authentication, requiring server certificates for establishing the highly secure tunnel. Since unauthenticated PAC provisioning does not require server side validation, it has some security risks, such as allowing rogue authentications to mount a dictionary attack. In this document, the AnyConnect Network Access Manager configuration profile will be configured for unauthenticated PAC provisioning for testing purposes only.

A PAC file is a security credential generated by the ISE server that holds information specific to the client. These PAC files, machine tunnel (also known as machine authentication) are used to establish the highly secure TLS tunnel, and user authorization for validation of user credentials during inner method authentication exchanges. They also prove that the client and machine were authenticated and the current authentication process can be optimized and bypassed. PAC type 4 has been added to support EAP Chaining.

Configuring the Wireless LAN Controller

This configuration requires the following steps:

Configure the Wireless LAN Controller (WLC) with the details of the Authentication Server

Configure WLAN parameters

Configure the dynamic interfaces (VLANs)

Configuring the WLC with the Details of the Authentication Server

The WLC needs to be configured to forward the machine and user credentials to the ISE server. The ISE server then validates these credentials (using the configured Windows database) and provides access to the wireless clients. Based on the initial WLC script install, RADIUS was configured and the values will be prefilled.

Step 1. From the controller GUI, click Security->Radius ->Authentication->New.

- Step 2. Enter the **IP address of the RADIUS server** and the **Shared Secret** key used between the RADIUS server and the WLC.
- Note: Values will be prefilled if RADIUS is configured as part of WLC installation script

The **Network User** and **Management** check boxes determine if the RADIUS-based authentication applies for users (for example, WLAN clients) and management (for example, administrative users).

In this example, the ISE is used as the RADIUS server with the IP address of 192.168.1.20 and the communication port as 1645.



ahaha							Sa <u>v</u> e Co	ntiguration Fing	Logout Refresh
CISCO	MONITOR V	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBA	CK
Security	RADIUS Au	thentic	ation Servers	s > Edit				< Back	Apply
AAA General General ALDIUS Authentication Accounting Fallback TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	Server Inde Server Addr Shared Secr Shared Secr Confirm Sha Key Wrap Port Number Server Stati	ex ress ret Format ret ared Secre	a E	1 192.168.1.20 ASCII 💌 ••• (Designed f 1645 Frahled 💌	or FIPS custor	mers and requires	a key wrap com;	pliant RADIUS serve	n
▶ Local EAP	Support for	RFC 3576		Disabled -					
Priority Order	Server Time	eout		2 seconds					
▶ Certificate	Network Use	er		Enable					
Access Control Lists	Managemen	nt		Enable					
Wireless Protection	10540			E Enable					

Configure WLAN Parameters

Configure the WLAN (the WLAN specifies a SSID and associated security parameters) which the clients use to connect to the wireless network. When you configured the basic parameters for the WLC using the configuration wizard, you also configured the initial SSID for the WLAN Controller. You can use the SSID for the WLAN or create a new SSID.

Step 1. From the GUI, **select ->WLANS**, to display the WLANs page. This page lists the WLANs that are created by the initial script controller.

Figure 2. WLAN Parameters

cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT	Save Contiguration Fing Logout Betresh
WLANs	WLANs		Entries 1 - 3 of 3
WLANS	Current Filter: None [Change	Filter) (Clear Filter)	reate New 💌 Go
Advanced	UKAN ID Type Profile Nam	e WLAN SSID	Admin Status Security Policies
	L WLAN Iaboos	lab005	Enabled [WPA2][Auth(802.1X)]
	2 WLAN vlan32	vlan32	Enabled [WPA2][Auth(802.1X)]
	3 WLAN vlan12	vlan12	Enabled [WPA2][Auth(802.1X)]
		vien12	Endoled [WF#2][Auth(du2:1A)]

Step 2. From the GUI, select->WLANS->WLAN ID 1. In this page, you can define various parameters specific to this WLAN, including General Policies, RADIUS Servers, Security Policies, and 802.1X parameters. Notice that Broadcast SSID and Status are enabled.

Note that although non-broadcast of SSID is not considered a broadcast mechanism, it is recommended to disable SSID broadcast to discourage casual WLAN observers and inadvertent client association attempts. You can also elect to create new WLANs by selecting **Create New-Go**

Figure 3. WLAN Screen

😭 🔗 🏾 🏀 Cisco_63:75:80				🙆 • 🖾 • 🖶	• 🔂 Bage • 🌀 Tgols • »
abab				Save Configuration	Ping Logout Befresh
CISCO	MONITOR WLANS CONTROL	LER WIRELESS SEC	CURITY MANAGEMENT	COMMANDS HELP FE	EDBACK
WLANs	WLANs > Edit 'lab005'			< Back	C Apply
WLANS WLANS	General Security Qo	5 Advanced			
Advanced	Profile Name	lab005			
	Туре	WLAN			
	SSID	lab005			
	Status	F Enabled			
	Security Policies	[WPA2][Auth(802.1X] (Modifications done under)] er security tab will appear a	fter applying the changes.)	
	Radio Policy	All			
	Interface/Interface Group(G)	vlan12			
	Multicast Vlan Feature	Enabled			
	Broadcast SSID	V Fachlad			

- Step 3. From the GUI, select->WLANs->WLAN ID 1->Security->AAA Servers to select the configured ISE server.
- Figure 4. RADIUS Server Selection

 cısco	MONITOR WLANS CONTROLLER	WIRELESS <u>S</u> ECURITY M	Say ANAGEMENT C <u>O</u> MMAI	re Configuration Ping Logo	ut <u>R</u> efresh
WLANs	WLANs > Edit 'lab005'			< Back A	pply
WLANs WLANs Advanced	General Security QoS A Layer 2 Layer 3 AAA Serv	vers			
	Select AAA servers below to overr Radius Servers Radius Server Overwrite interface	ide use of default servers o	on this WLAN	LDAP Servers	
	Sumi	Authentication Servers	Accounting Servers	Server None	
	Server 1 Server 2 Server 3		3 None		
	Local EAP Authentication	led		_	

Step 4. Under Security Policies, configure L2 Security for WPA+WPA2. Also select the appropriate encryption types under WPA+WPA2 Parameters. Although network access manager supports all of these encryption types, the settings chosen here depend on the client NIC card capabilities.

In this example, WPA2 Encryption AES was used.

Note: Enabling WPA encryption permits the flexibility to support older WPA clients, as well as newer WPA2-capable clients.

Step 5. Click Apply

Figure 5. L2 Security

cisco	Saye Configuration _ping _ logout _ Betres MonitorLansController wireless _ecurity managementManagementManagement
WLANs	WLANs > Edit 'lab005' <back apply<="" td=""></back>
WLANS WLANS Advanced	General Security QoS Advanced Layer 2 Layer 3 AAA Servers Layer 2 Security 4 WPA+WPA2 Image: Comparison of the security of the securety of the security of the security of
	WPA Policy Image: Constraint of the second

Configure Dynamic Interfaces (VLANS)

In this document, the wireless client will be placed in VLAN 12 after authentication. Note the VLAN ID specified under the Tunnel-Private-Group ID attribute of the RADIUS server must also exist in the WLC.

The end user is specified with the Tunnel-Private-Group ID of 12 VLAN=12) on the RADIUS server. You can see the same dynamic interface (VLAN=12) configured in the WLC.

Step 1. From the controller GUI, click **Controller->Interfaces**.

Step 2. Enter vlan12 for both the Interface Name and 12 the VLAN id.

Figure 6. VLAN Interface Configuration

ONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP FEEDBACK
Interfaces Interface I VLAN Id	> New	vlan12 12					< Back Apply
	DNITOR terfaces Interface I VLAN Id	DNITOR <u>W</u> LANS terfaces > New Interface Name VLAN Id	ONITOR WLANS CONTROLLER terfaces > New Interface Name VIan12 VLAN Id 12	DNITOR WLANS CONTROLLER WIRELESS terfaces > New Interface Name Vian12 VLAN Id 12	DNITOR WLANS CONTROLLER WIRELESS SECURITY terfaces > New Interface Name Vian12 VLAN Id 12	DNITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT terfaces > New Interface Name Vian12 VLAN Id 12	DNITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS terfaces > New Interface Name Vian12 VLAN Id 12

Step 3. Click Apply on this window.

Step 4. Enter the IP Address and default Gateway of this Network Access Manager interface.

Figure 7. Enter IP and Gateway address

						Save Co	infiguratio	in Ping Lo	gout Ketresh
cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK	
Controller General Inventory Interfaces Interface Groups Multicast > Internal DHCP Server > Mobility Management Ports > NTP > CDP > Advanced	General Informat Interface Name MAC Address Configuration Quarantine Quarantine Vian Id Physical Informat Port Number Interface Address VLAN Identifier IP Address Netmask Gateway	ControlL2x vian12 e0:5f;b1 0 ion 1 : 255:255:25 10:3:1.1	9:63:75:80		MEMAGENENT	Community	HELP	FEEDBACK	2
	Primary DHCP Sen Secondary DHCP S Access Control Li ACL Name	ver [1 erver [1 st	92.168.1.1 92.168.1.10						

Step 5. Click Apply.

Configure WLANs (SSID)

This procedure explains how to configure the WLANs in the WLC.

Step 1. From the controller GUI, select->WLANs->New to create a new WLAN.

Step 2. Enter the WLAN ID and WLAN SSID information.

In this example, VLAN12 was used for both.

Figure 8. WLAN Configuration

111111							Save Co	ntiguratio	on Ping Logout Betresh
cisco	MONITOR	WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
WLANs	WLANs >	New						<	Back Apply
 ▼ WLANS WLANS ▶ Advanced 	Type Profile N SSID ID	ame	VlA1 Vlan1 4	2 2					

Step 3. Click Apply.

Figure 9. VLAN Information

cisco		ler wireless secur	NTY MANAGEMENT	Saye Configur COMMANDS HEL	ation <u>P</u> ing Logout <u>R</u> efres P <u>F</u> EEDBACK
WLANs	WLANs > Edit 'vlan12'				< Back Apply
WLANS	General Security Qo	5 Advanced			
Advanced	Profile Name	vlan12			
	Туре	WLAN			
	SSID	vlan12			
	Status	F Enabled			
	Security Policies	[WPA2][Auth(802.1X)] (Modifications done under se	curity tab will appear a	fter applying the chang	jes.)
	Radio Policy	All			
	Interface/Interface Group(G)	vlan12			
	Multicast Vlan Feature	Enabled			

Figure 10. VLAN Information

111111	Saye Configuration Ping Logout Berresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
WLANs	WLANs > Edit 'vlan12'
VLANS WLANS	General Security QoS Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 2 Security £ WPA+WPA2
	Intering WPA+WPA2 Parameters
	WPA Policy
	WPA2 Policy 🔽
	WPA2 Encryption R AES T TKIP
	Auth Key Mgmt 802.1X

Normally, in a wireless LAN controller, each WLAN is mapped to a specific VLAN (SSID) so that a particular user that belongs to that WLAN is put into the specific VLAN mapped. This mapping is normally done under the Interface Name field of the WLAN SSID window.

Step 4. From the GUI, select->WLANS->WLAN ID->and change the interface name from Management to VLAN 12->Apply.

Figure 11. Interface Name

ululu cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY	MANAGEMENT	Sa <u>v</u> e Co C <u>O</u> MMANDS	nfiguration Ping HELP EEEDBAC	Logout <u>R</u> efresh CK
WLANs	WLANs > Edit 'vlan12'				< Back	Apply
WLANS WLANS WLANS WLANS ▶ Advanced	General Security QoS A Profile Name vlan12 Type WLAN SSID vlan12 Status IV	dvanced				
	Security Policies [WPA] (Modifie Radio Policy All Interface/Interface Group(G) [vian13 Multicast Vian Peature En Broadcast SSID F En	2][Auth(802.1X)] iations done under security 2 2 2 abled abled	y tab will appear af	ter applying the	changes.)	

Figure 12. RADIUS server configuration for VLAN 12

սիսիս				Save Con	figuration Ping	Logout Befresh
cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURIT	Y MANAGEMENT	C <u>o</u> mmands		ж
WLANs	WLANs > Edit 'vlan12'				< Back	Apply
WLANS	General Security QoS	Advanced				
Advanced	Layer 2 Layer 3 AAA S	ervers				
	Radius Servers Radius Server Overwrite interfa	ce	rs Accounting S	ervers	erver None	
		Enabled	F Enabled	2	None 💌	
	Server 1	IP:192.168.1.20, Port:	1645 Vone V	5	erver None 💌	
	Server 3	None	V None V			
	Local EAP Authentication	Incom				
	Local EAP Authentication E	nabled				

In the example provided, the RADIUS server assigns a wireless client to a specific VLAN upon successful authentication. The WLANs need not be mapped to a specific dynamic interface on the WLC. Even though the WLAN to dynamic interface mapping is done on the WLC, the RADIUS server overrides this mapping and assigns the user that comes through that WLAN to the VLAN specified under the user **Tunnel-Group-Private-ID** field in the RADIUS server.

Step 5. Check the Allow AAA Override check box to override the WLC configurations by the RADIUS server.

Step 6. Enable the Allow AAA Override in the controller for each WLAN (SSID) configured.

Step 7. From the GUI, select ->WLANS->WLAN ID->Advanced.

n

սիսիս	Sa <u>v</u> e Configurati	on Ping Logout Refresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	FEEDBACK
WLANs	WLANs > Edit 'vlan12'	Back Apply
WLANS	General Security QoS Advanced	
Advanced	Allow AAA Override 🔽 Enabled DHCP	Î
	Coverage Hole Detection DECP Server Coverride	1
	Enable Session Timeout	1
	Aironet IE 🛛 🕅 Enabled Management Frame Protection (MFP)	
	Diagnostic Channel Enabled	
	IPv6 Enable Z	
	Override Interface ACL None	_
	P2P Blocking Action Disabled 💌 802.11a/n (1 - 255) 1	_
	Client Exclusion 2 P Enabled 60 802.11b/g/n (1 - 255) 1 Timeout Value (secs)	
	Maximum Allowed O NAC State None	_
	Static IP Tunneling 12 Enabled Load Balancing and Band Select	
	Off Channel Scanning Defer Client Load Balancing	
	Scan Defer 0 1 2 3 4 5 6 7 Client Band Select #	-
	Priority	. <u>.</u>

When AAA Override is enabled, and a client has AAA and controller WLAN authentication parameters that conflict, client authentication is performed by the AAA (RADIUS) server. As part of this authentication, the operating system moves clients to a VLAN returned by the AAA server. This is predefined in the controller interface configuration

Step 8. Select->Save Configuration.

Configuring the Cisco Identity Services Engine

This section describes how to configure the Cisco Identity Services Engine (ISE), starting with adding the WLC as a network device. Active Directory will be added as en external Identity Source, and an Authentication and Authorization Policy will be created.

Add Networking Devices to ISE

Add WLC controller to ISE and provide a shared secret under Authentication Settings.

- Step 1. Select->Network Resources-Network Devices->Administration->Add.
- Step 2. Enter the name of the WLC

In this example, WLC was used.

Step 3. Enter the IPAddress.

In this example, 192.168.1.5 was used.

Step 4. Click on Authentication Settings and enter the shared secret.



🔆 System 🖉 Identity Management	Network Resources 🛃 Web Portal Management
Network Device Groups	External RADIUS Servers RADIUS Server Sequences SGA AAA Servers NAC Managers
Vetwork Devices	* Name w/c Description
Network Devices	• IP Address: 192.168.1.5 / 32
	Model Name Software Version
	Network Device Group Location Al Locations Set. To Default Device Type Al Device Types Set. To Default

Figure 15. Authentication Settings

•	٩		Authentication Settings		
\$ -	@+				
Network Devices	۲		Enable Authentication Settings		
Default Device			Protocol	RADIUS	
			* Shared Secret	•••••	Show
			Enable KeyWrap		
		•	* Key Encryption Key		Show
			* Message Authenticator Code Key	1	Show
		-	Key Input Format	ASCII O HEXAD	ECIMAL

Step 5. Click on Submit.

Add Microsoft Active Directory as the External Identity Store

Machine and user credentials will be validated against the AD domain and identified as an external identity store.

- Step 1. Select->Administration->Identity Management->External Identity Sources->Active Directory.
- Step 2. Enter Domain Name.

In this example, cfacres007.com was used.

Step 3. Enter the Identity Store Name.

In this example, the default "AD1" was used.

Figure 16. Active Directory Configuration)



Step 4. Click on Save Configuration.

Step 5. Select the ISE node, ISE, and Join Domain.

Figure 17. Joining the Domain

CISCO Identity Services Engin	e 🗸 Adminis	tration 👻		
🔆 System 🖉 Identity Manage	ment 📷	Network Resources 🛛 🛃 Web Portal	Management	
Identities Groups External Ide	ntity Sources	Identity Source Sequences Settings		
External Identity Sources	0 0 0 0	Active Directory > ADI Connectoor Advanced Settings * Ider One or more nodes may be selected Test Connection. ♥ Low ♥ Test Connect ♥ Ise	Groups Attributes	× ad then a leave operation is required before

Step 6. Click on OK. You should see a message that the node was joined successfully.

Figure 18. Join Operation Successful

nt Sources	Network Re Identity St	Join Operation Status The list below shows the sta Status: Successful	itus of the requeste	d operation for each node.	
	Active Direct	ISE Node		Status	
	Conne	ise		Completed.	
- 100 v					
۲	One or				
	Test Co				
۲	92 30				
۲	115				

You should now see that ISE is successfully connected to the domain in Figure 5.

Figure 19. ISE successfully connected to domain



Configure Active Directory Groups

- Step 1. Select->Administrative->Identity Management->External Identity-Sources-Active Directory.
- Step 2. Select->Groups->Add.
- Step 3. Select any active directory groups that you will use for your deployment.
- Note: If you leave the "*" by default, this will display all the AD groups (up to 100).

Figure 20. Retrieved Groups from Active Directory

CISCO Identity Services E A Home Operations System A Identity U Identities Groups Ettern	Select Dire This dialo Use * for v Domain Filter:	ectory Groups g is used to select groups fro wildcard search (i.e. admin*) cfacres007.com	om the Directory. Click Retrieve Groups to read directory. . Search filter applies to group name and not the fully qualified path	
External Identity Sources	 Nam cfacr 	e te 9007 com/Builtn/Accourt 0 e 9007 com/Builtn/Administs e 9007 com/Builtn/Distribute e 9007 com/Builtn/Distribute e 9007 com/Builtn/Incoming e 9007 com/Builtn/Retwork re 9007 com/Builtn/Performa e 9007 com/Builtn/Performa	Deperators Tabris Deperators Tabris Deperators Torest Trust Builders Configuration Operators Ince Log Users Ince Monitor Users	0roup Type LOCAL LOCAL LOCAL LOCAL LOCAL LOCAL LOCAL LOCAL LOCAL LOCAL

Step 4. Click OK, and then Save Configuration.

Define Identity Store Source

Identity Source Sequences define the order in which the Cisco ISE will look for the validation of user and machine credentials in the different databases, and will be configured to search in Active Directory.

- Step 1. Select->Administration->Identity Management->Identity Source Sequence->Add.
- Step 2. Enter name of Identity Source.

In this case, CorpUsers was used

Step 3. Under Authentication Search List, select AD1 and click on >. This will show up under Selected.

ISE - RADIUS Servers - 192.168.1.20		🗿 • 🖸 • 🖾 👼	• Page • Safety • Tools • 🕡
alfielte CISCO Identity Services Engine			ise admin Logout Feedb
🛕 Home Operations 🗸 Policy 🗸 Administration 🗸		and the second	👓 Task Navigator 👻 👩
🔆 System 🙀 Identity Management 🕋 Network Resources 👩 Web Portal Management			
dentities Groups External Identity Sources Identity Source Sequences Settings			
r Identity Source Sequence			
*Name CorpUsers	٦		
Certificate Based Authentication			
Select Certificate Authentication Profile			
▼ Authentication Search List			
A set of identity sources that will be accessed in sequence until first authentication succeeds			
Available Selected			
Internal Endpoints Internal Users AD1			
9 нер		Alarms 📀	807 A 1 0 0 Notifications (0)

Figure 21. Identity Source Sequence

Step 4. Click on Submit.

Defining Authentication Policies and Authorization Profiles

Authentication Policies

Authentication policies define the conditions between the client and ISE node when 802.1X occurs. They define the RADIUS attribute conditions and authentication protocols that are required for successful authentication, as well as for the external or internal database used for validation of machine and user credentials.

The Authentication policy consists of the following elements:

Results: Define authentication protocols

Configure the authentication method between ISE server and client.

In this example, EAP-FAST is defined as the authentication protocol.

Note: We could have chosen to use the default authentication protocol. In this document, we have elected to add the EAP-FAST protocol to provide the reader with experience for creating authentication protocols.

Conditions: Set the RADIUS attributes to match on 802.1X-based RADIUS authentication requests.

ISE ships with pre-defined 802.1X conditions that will be used when configuring policies.

In this example, predefined wireless 802.1X condition rule will be used.

Defining Identity Source Sequence: Authentication policy will use the identity source to validate the end user and machine credentials.

In this example, CorpUsers will be defined as the identity source.

Defining the Authentication Policies

In this document, we will define a Wireless Authentication policy, use EAP-FAST for the authentication protocol, and select CorpUsers as the identity source for credential validation.

Adding EAP-FAST as the Authentication Protocol

The following illustrates adding the EAP-FAST protocol.

- Step 1. Select Policy->Authentication->Policy Elements->Results->Authentication->Allowed Protocols->Add.
- Step 2. Enter the name of the allowed protocol.

In this example, EAP-FAST was entered.

- Step 3. Enable Allow Anonymous In-band PAC provisioning.
- Step 4. Enable Allow Authenticated In-band PAC provisioning, then enable the following:
 - Server Returns Access Accept After Authenticated Provisioning
- Step 5. Enable Allow Machine Authentication.

Step 6. Enable Stateless Session Resume.

Figure 22. Adding EAP-FAST Authentication Protocol)



Step 7. Click on Submit

Define Authentication Policy

A wireless authentication policy will be created, EAP-FAST selected as the allowed protocol, and CorpUsers selected as the Identity Store.

Step 1. Select Policy->Authentication->by the gear, select Actions, then insert new row above.

Figure 23. Adding Authentication Policy rule

🛕 Home Operations 👻 Policy 🔹	• Administration •	👓 Task Navigator = 🌔
Authentication S Authorizat	ton 🔀 Profing 🖉 Posture 🙀 Clent Provisioning 😭 Security Group Access 🚓 Polcy Elements	
hentication Policy		
e the Authentication Policy by selecting	the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.	
V TVDP () SITTOR (•) KUR-Kased		
MAB	: If Wired_MAB 🔿 allow protocols Allowed Protocol : Default Networ	🖗 Actions 🔹
MAB Dat1X	: If Wired_MAB islow protocols Allowed Protocol : Default Network : If Wired_802 tX islow protocols Allowed Protocol : EMPFact_EAPCICAL	Actions •
	: # Wired_MAB allow protocols Allowed Protocol : Default Network : # Wired_802 IX allow protocols Allowed Protocol : DEFault_DEFACE and ,	Actons •
	: # Wired_MAB islow protocols Adowed Protocol : Default Network : # Wired_B02 IX islow protocols Adowed Protocol : EAPFait_EAPCink and • : allow protocols Adowed Protocol : Default Network islow protocols CopUser	Actions •
MAB Default Rule (If no match)	If Weed_MAB	Actions *
	If Wired_MAB Jalow protocols Allowed Protocol : Defbut Network If Wired_S02 tX Jalow protocols (Allowed Protocol : LEPFat_EAPOCh) and , alow protocols (Allowed Protocol : Defbut Network) and use identity source : Corputer	Actons •

Step 2. Replace standard rule 1 name with wireless.

- Step 3. Click on + next to Condition(s)
- Step 4. Select Existing Condition from the library from the drop-down menu, then select ->Compound Condition->Wireless 802.1X
- Step 5. Click on >, click on the + next to Internal Users, then select CorpUsers for the Identity Source

Figure 24. Authentication Policy



Step 6. Click on Save.

Define the Authorization Profiles

Authorization occurs once the end user has successfully authenticated. Authorization policies provide the rules that must be met before the end user is provided with full or restricted network access as determined by the associated authorization profile.

The authorization profile contains common data such as VLAN information and other RADIUS attributes, and consists of the following elements:

Authorization Profile: Defines full or restricted network access.

In this example, we will define one profile to match the authorization condition for wireless, and provide full network access.

Conditions: Contain the authorization rules that determine the required network permissions or level of access

In this example, the default wireless condition rule will be used.

Create Authorization Profile

In this document, we will define, a Wireless Authorization Policy, based on the default wireless 802.1X condition. Then, we will provide the appropriate level of access as defined by the corresponding authorization profile, WIRELESSACCESS

- Step 1. Select->Policy->Authorization->Policy Elements->Results->Authorization->Authorization Profiles->Add
- Step 2. Enter name of profile.

In this example, WIRELESSACCESS was used

Step 3. Select VLAN, and enter VLAN ID.

In this example, VLAN ID 12 was used

Figure 25. Wireless Authorization Profile

Authorization	* Access ACCEPT	
Authorization Profiles	Type	
Downloadable ACLs	▼ Common Tasks	
Inline Posture Node Profiles		~
Profiling	DACL Name	
Posture	Tag ID 1 Ed	dit Tag ID/Name
Client Provisioning	12	
County Count Assas	Vision Demain Developing	

Step 4. Click on Submit.

Defining Authorization Condition Rules and Authorization Policies

Once the authorization profile has been created, define the authorization policy rule and the condition rule.

Define Authorization Policy

Step 1. Select->Policy->Authorization->, click on the down arrow, and Insert New Rule above.

Figure 26. Adding Authorization Policy Rule

Home Operations v Policy v	Administration +		🗝 Task Navigator = 👩
Authentication 💽 Authorization	Profing 🔗 Posture 🔍 Clent Provisioning 🔛 Security	Group Access 🤱 Policy Elements	
horization Policy			
ne the Authorization Policy by configuring n	les based on identity groups and/or other conditions. Drag and drop rules to change the	order.	
: Matched Rule Apples			
ventions (0)			
exceptions (0)			
ixceptions (0)			
ixceptions (0) itandard Status Rule Name	Conditions (dentity groups and other conditions)	Permissions	
ixceptions (0) itanderd Status Rule Name Personal Asset	Conditions (dentity groups and other conditions) EAPChaining_MachineFal_UserPass	Permissions them MachineFal_UserPass	Insert New Rule Above
ixceptions (0) itandard Status Rule Name Personal Asset Versional Asset	Conditions (dentity groups and other conditions) EAPCharing_MitchineFaLUserPass Any Any Any Any Any Any Any Any Any A	Permissions thim MachineFal_UsePass then FULLACCESS	Insert New Rule Above Insert New Rule Below
Itandard Status Rule Name Personal Asset Status Autores Personal Asset	Conditions (dentity groups and other conditions) CAPChaning_MachineFal_UsePass (Any) and Network Access Explutientication E	Permissions them MachineFall/WerPass 2 them FULLACED Queene Hindow	Insert New Rule Above Insert New Rule Below Duplicate Above
Interplanes (a) Status Rule Hame Personal Asset Versions No_EAPChaining	Conditions (identity groups and other conditions) EAPChaning_MachineFal_UserPass	Permissions then RachierPal_UsePass bten FULACCESS then Ro_EAP_Chaning_UsePass	Insert New Rule Above Insert New Rule Below Ouplicate Below Ouplicate Below

- Step 2. Replace standard rule 1 name with wireless, click on + next to select condition, and select wireless 802.1X for the condition name.
- Step 3. Click on the '+' sign next to Authz profile, then select ->Standard->Wireless Access.

Figure 27. Authorization Policy for Wireless

Authorization Policy Define the Authorization Policy by configuring rule [First Matched Rule Apples •]	s based on identity groups and/or other conditions. Drag and drop rules to chang	pe the order.	
Exceptions (0) Standard			
Status Rule Name	Conditions (identity groups and other conditions)	Permissions	2
🖋 🛃 🔹 🛛 Wireless	Any 🔷 Mreless_802.1X	♦ thin WrelessAcc.	Done
Personal Asset	f EAPChaining_MachineFal_UserPass	then MachineFall_UserPass	Edt •
No_EAPChaining	/ NO_EAPChaining	then No_EAP_Chaining_UserPass	Edt •

Step 4. Click on Save.

Configuring the AnyConnect Network Access Manager

Network Access Manager Installation and Configuration

Installing AnyConnect Network Access Manager Step 1. Extract the contents of the **AnyConnect ISO image** to a folder

Run setup

Note: Please note that you will require local admin rights during the installation.

Step 2. Enable AnyConnect Diagnostics and Reporting Tool.

Step 3. Enable AnyConnect Network Access Manager

Figure 28. Installation Selector)

Authorization Poiky			
efne the Authorization Policy by configuring n	ies based on identity groups and/or other conditions. Drag and drop rules to chang	e the order.	
st Matched Rule Apples			
Exceptions (0)			
Standard			
Status Rule Name	Conditions (identity groups and other conditions)	Permisions	
Status Rule Name	Conditions (identity groups and other conditions)	Permasons then WirelessAcc	Done
Status Rule Name Status Rule Name Status Parsonal Asset	Conditions (Identity groups and other conditions) (Any) (Weekess_802.1X / EAPDhaning_MachineFal_UserPass	Permissions WeekessAcc. then MachineFal_UserPass	Done Edt •

Note: You will see the message in Figure 28 after a completed install of the AnyConnect Secure Mobility Client. As part of the core install, the AnyConnect Quality Improvement feature is enabled by default. This feature provides Cisco with customer-installed AnyConnect modules, and enabled features. Crash dumps may also be included. This feature can be completely disabled by using the Profile Editor or just for disabling crash dumps. Corporate privacy is maintained by hashing the machine name; however, crash dumps may contain personal information, which is why the EULA license is displayed.

Figure 29. AnyConnect Quality Improvement Feature



Creating an AnyConnect Network Access Manager Profile with the Profile Editor

The Profile Editor will also be required to configure the AnyConnect Network Access Manager Configuration Profile for EAP-FAST authentication.

Note: Please note that the AnyConnect Network Access Manager configuration should be saved as configuration.xml, and saved to the 'NewConfigFiles' directory. Right-click on the AnyConnect GUI in the system tray, then select 'Network Repair'. This will place the configuration.xml file into the AnyConnect Network Access Manager system directory.

Open the profile editor, and access the current system configuration.

Step 1. Select **file open** from the drop-down menu, and open the **configuration.xml** file as shown in Figure 30.

Figure 30.Opening Configuration.xml file)

🕈 Cisco Ar	nyConnect Secure Mobility Client 🛛 🛛 🔀
(į)	Some AnyConnect components may be configured to collect device data and/or redirect network traffic to cloud services operated by Cisco Systems.
	All data collected is protected under the Cisco Online Privacy Statement and the AnyConnect Supplement. For more information on the data collected and these privacy policies, please click below.
	By using this product you agree to allow data to be collected and/or redirected if configured to do so at any time.
	If you do not agree, contact your AnyConnect Solution Administrator or uninstall the product.
	More Information
	✓ I have read and understand this message.

- Step 2. Keep the defaults, and select->Networks.
- Step 3. Define your networks.

```
In this example, Corporate was defined for the administrative network profile, as illustrated in Fig 31.
```

- Step 4. Enable WiFi network, then enter SSID value.
 - In this example, lab005 was used.
- Step 5. Enable the following:
 - Hidden Network
 - · Corporate Network

Figure 31. Wireless Network Profile Description



Step 6. Select ->Next.

Step 7. Select->Authenticating Network.

Authenticating Network settings contain the 802.1X settings that contain MACSec configuration settings, and also 802.1X network connectivity settings

Step 8. Under Association Mode, from the drop-down menu, select encryption to match your WLC configuration.

In this example, WPA2 enterprise (AES) was selected

Figure 32. Network Security Level

Network Groups	Name:	Corporate	Security		
	Group Membership				
	In group:	(auto-generated)			
	 In all groups (Global) 				
	Choose Your Network Media				
	Wired (802.3) Network				
	Select a wired network if the	he endstations will be connecting to the network with a traditional			
	ethernet cable.				
	WI-Fi (wireless) Network				
	Select a WFi network if the endstations will be connecting to the network via a wireless				
	radio connection to an Access Point.				
	SSID (max 32 chars):	Labcos			
		Hidden Network Corporate Network			
	Association Timeout (sec)	5			
	Common Settings				
	Script or application on each user	's machine to run when connected.			
		Browse Local Machine			
	Connection Times & (ear.)	*			
	connection (meour (sec.)	•			

Step 9. Select ->Next.

Step 10. Select Machine and User Connection.

Note: Machine and User Connection determines the network connection types

Figure 33. Network Connection Type

Networks	Security Level				Media Type
	Open Network	k			Security Leve
	Open network secure type o Shared Key N Shared Key N access points.	s have no security, f network. etwork etworks use a share . This is a medum s	and are open to anybody wind the second	thin range. This is the least en end stations and network	Connection Ty
	Authenticating Network				
	Authenticating networks provide the hightest level of security and are perfect for				
	enterprise level networks. Authentication networks require radius servers, and other network infrastructure.				
	-802. 1X Settings	30	startPeriod (sec.)	30	
	heldPeriod (sec.)	60	maxStart	3	

Step 11. Select->Next.

Step 12. Select EAP-FAST as the EAP method, then uncheck Validate Server Identity.

Note: EAP-FAST will be the method of Authentication, and EAP-MSCHAPv2 will be the inner method.

In this example, root certificate and ISE identity certificate are not installed, which is why Validate Server Identity is unchecked.

Step 13. Leave the defaults.

Figure 34. EAP-FAST Selection

Client Policy Client Policy Authentication Policy Networks	Networks Profile:ility Client\Network Access Manager\system\configuration.xml	
	Network Connection Type	Media Type
	Machine Connection	Security Leve
	This should be used if the and station should be aste the actual before the user lass is	Connection Ty
	This should be used if the end station should log onto the network before the user logs in.	Machine Aut
	This is typically used for connecting to domains, to get GPO's and other updates from the	Credentials
	network before the user has access.	User Auth
	O User Connection	Credentials
	The user connection should be used when a machine connection is not necessary. A user	
	connection will make the network available after the user has logged on.	
	Machine and User Connection	
	This type of connection will be made automatically when the machine boots. It will then be	
	brought down, and back up again with different credentials when the user logs in.	

- Step 14. Select->Next.
- Step 15. Leave PAC files set for empty, as shown in Figure 22, then select Next.

Note: PAC file will be provisioned from ISE

Figure 35. PAC Files

twork Access Manager Client Policy Authentication Policy	Networks Profile:ility Client\Network Access Manager\system\	configuration.xml
Networks	EAP Methods	Media Type
	O EAP-TLS O PEAP	Security Lev
		Connection Ty
	C EAP-TTLS O EAP-FAST	Machine Au
	C LEAP	PAC Files
		Credentials
	FAD.FAST Settions	Credentals
	(III) foldet from The th	
	Valdate Server Identity	
	Inner Methods based on Credentials Source	
	Authenticate using a Password	
	V EAP-MSCHAPv2 V EAP-GTC	
	If using PACs, allow unauthenticated PAC provisioning	
	Authenticate using a Certificate	
	O When requested send the dient certificate in the dear	
	 Only send client certificates inside the tunnel 	
	Send client certificate using EAP-TLS in the tunnel	
	Use PACs	

Step 16. Leave defaults for machine identity, then select ->next.

Note: Machine identity credentials will be sent to the ISE server for validation.

Figure 36. Machine Identity Credentials

File Help		
He Hep Network Access Manager Clent Polcy Automotason Polcy Networks	Networks Profile:ility Client\Network Access Manager\system\configuration.xml	
	PAC fies Add Password protected Remove	Media Type Security Leve Connection Ty Machine Aut PAC Files Credentals User Auth Credentals



Step 18. Leave the defaults.

Figure 37. EAP-FAST for user authentication

Network Access Manager	Networks Profile:ility Client\Network	Access Manager\system\configur	ation.xml
	Machine Identity		Media Type
Network Groups	Unprotected Identity Pattern:	host/anonymous	Security Leve
	Protected Identity Pattern:		Connection Ty
		host/[username]	Machine Aut
			PAC Files
	Machina Cradestials		Credentais
	Produce dicuctions		User Auth
	Use Machine Credentials		Credentials
	Clike Static Credentials		
	O dat state d contais		
	Password:		

Step 19. Select -> Next.

Step 20. Leave PAC files empty, then select ->Next.

Figure 38.	PAC Files
------------	-----------

File Help		
Clent Policy	Networks Profile:ility Client\Network Access Manager\system\configuration	on.xml
	EAP Methods	Media Type
	O EAP-TLS O PEAP	Security Leve
		Connection Ty
	C EAP-TTLS O EAP-FAST	Machine Aut
	O LEAD	PAC Files
	0.004	Credentials
	Extend user connection beyond log off	User Auth
	EAD EAST Settore	PAC Files
	CAPTASI Settings	Credentials
	Validate Server Identity	
	Enable Fast Reconnect	
	Disable when using a Smart Card	
	Inner Methods based on Credentials Source	_
	Authenticate using a Password	
	EAP-MSCHAPV2	
	If using PACs, allow unauthenticated PAC provisioning	

Step 21. Leave the defaults for user credentials.

Note: User credentials will be sent to the ISE server for validation

ls

Clent Policy Authentication Policy Authentication Policy	Networks Profile:ility Client\Network Access Manager\system\configuration.xml	
	DAC flag	Media Type
Network Groups	FAC IICS	Security Lev
		Connection T
		Machine Au
		PAC Files
		Credential
		User Auth
		PAC Fier
	Add Password protected Remove	Credentials

Step 22. Select->Done.

Figure 40. Completed Profile

Networks	User Identity	Media Type	
	Unprotected Identity Pattern:	anonymous	Security Leve
			Connection Ty
	Protected Identity Pattern:	[username]	Machine Aut
			PAC Files
	User Credentials	Credentials	
		User Auth	
	 Use single sign On Credentia 	PAC Files	
	Prompt for Credentials	Credentials	
	C Remember Forever		
	(ii) Remember while Use		
	O Never Remember		
	O Use Static Credentials		
	Password:		
	1		

Step 23. Click file and save as configuration.xml.

Figure 41. Saving configuration.xml

ient Policy Profile:	Networks Profile:ility Client\Network Access Manager\system\configuration.xml					
etworks Network						
Name	Media Type	Group*				
wired	Wred	Global				
Corporate	Wreless	(auto-generated)	Add			
			Edt			
			Delete			
* A petwork	in group 'Clobal' is a member of allor					
Alleuron	ingroup dooa is a mender of avg	0000.				

Step 24. Run network repair, then right-click on AC GUI, and click on Network Repair.



Network Access Manager Clent Polcy Ag Authentication Policy Network Groups	Networks Profile:ien	tNetwork Access Mar	ager/newConfigFiles/co	nfiguration.xml		
	Network					
	Name	Media Type	Group*			
	wired	Wred	Global			
	Corporate	Wreless	(auto-generated)	Add		
				Edt		
				Delete		
	-					
	* A network in gr	roup 'Global' is a member of all gr	oups.			-
	100000000000000000000000000000000000000					Open AnyConnect
						 Enable Status Popup
						VPN Connect
						VPN Connect Network Group
						VPN Connect Network Group Network Repair
						VPN Connect Network Group Network Repair Disable Wireless
						VPN Connect Network Group Network Repair Disable Wireless
					leno	VPN Connect Network Group Network Repair Disable Wireless About
					leno	VPN Connect Network Group Network Repair Sale Wireless About 6)
					leno	VPN Connect Network Group Disable Wireless About 0 Disable Wireless About 0 Disable Wireless
					leno	VPN Connect Network Group O C Network Group Disable Writes About O C 2 C 2 About
					lene	VPN Connect Network Group Disable Werkers Babert Disable Werkers About Disable Werkers A
	4				leno	VPN Connect Network Group Disable Wreters About 0 C 2 2 2 About 0 C 2 2 2 Customize-

Testing Procedure

• Click on the AC GUI, and then connect to Corporate.

Figure 43. Connect to Corporate



• Click on any other non-corporate APs. You should see the following error message:

Figure 44. Non-Corporate Connection

isco Anyl	Connect
4	Your system administrator does not allow connecting to non-corporate networks when corporate networks are in range.
	ОК

• View the **ISE Authentication Live Logs**. You will see separate transactions for successful machine and user credentials.

Figure 45. Live Authentication Logs

A Home Operations	• Po	icy v	Administration	,				🕶 Task Navigator 🔹 👩
Authentications	ità Er	dpoint P	rotection Service	💆 Alarms	👖 Reports 💊	Troubleshoot		
Live Authentications								
🙀 Add or Remove Columns 🕶	😵 Ref	tesh				Refresh	Every 1 minute Show Latest 20 records	within Last 5 minutes *
îme	Status	Details	Identity	Network Device	Authorization Profiles	Event Falure Reason	Session ID]
Jun 26,12 03:09:41.169 PM		ò	Jeppich	wic	WirelessAccess	Authentication	0501a8c000000096fe0e94f	
Jun 26,12 03:09:40.759 PM		0	jeppich	wic	WrelessAccess	Authentication	0501a8c0000000845e0e94f	
Jun 26,12 03:08:58.736 PM		ò	host/labstation	wic	WirelessAccess	Authentication	0501a8c0000000845e0e94f	
Jun 26,12 03:08:57.824 PM		.0	host/labstation	wic	WirelessAccess	Authentication	0501a8c000000076cdfe94f	
Jun 26,12 03:05:21.751 PM		ò	jeppich	wic	PermitAccess	Authentication	0501a8c000000076cdfe94f	
Jun 26,12 03:05:21.293 PM		ò	jeppich	wic	PermitAccess	Authentication	0501a8c0000000650dfe94f	
Jun 26,12 03:04:54.068 PM		à	host/labstation	wic	PermitAccess	Authentication	0501a8c0000000650dfe94f	
him 26 12 02-04-52 650 PM		12	hast/hhstation	wir	PermitAccess	Authentication	0501a8c00000005f64ce94f	

Appendices

Configuring the Switch for Multiple VLANs

In order to allow multiple VLANs through the switch, the following commands were configured on the switch port connecting to the controller:

interface GigabitEthernet1/0/6

description Trunk Port to WLC

switchport trunk encapsulation dot1q

switchport mode trunk

Interface VLAN Configuration is listed below:

Interface VLAN12

Description of AP VLAN

ip address 10.3.1.2 255.255.255.0

Gigabit Switch Port Configuration is listed below:

Interface Gigabit Ethernet 1/0/10

Description of access port connection to Cisco AP

switchport access vlan 12

switchport mode access

Configure the WLC for Basic Operation and Register the Lightweight APs to the Controller Use the startup configuration wizard on the command-line interface (CLI) to configure the WLC for basic operation. Alternatively, you can also use the GUI to configure the CLI. This document explains the configuration on the WLC with the startup configuration wizard on the CLI.

After the WLC boots the first time, it enters into the startup configuration wizard. Use the configuration wizard to configure basic settings. You can access the wizard using the CLI or the GUI. The output shows an example of the startup configuration on the GUI:

Welcome to the Cisco Wizard Configuration Tool

Use the '-' character to backup

System Name: Cisco_63:75:80

Enter Administrative User Name (24 characters max): jeppich

Enter Administrative Password (24 characters max): *******

Management Interface IP Address: 192.168.1.5

Management Interface Netmask: 255.255.255.0

Management Interface Default Router: 192.168.1.1

Management Interface VLAN Identifier (0=tagged):

Management Interface DHCP Server IP Address: 192.168.1.1

AP Manager Interface IP Address: 192.168.1.6

AP Manager is on Management subnet, using same values

AP Manager Interface DHCP Server 192.168.1.1

Virtual Gateway IP Address: 1.1.1.1

Mobility/RF Group Name: lab005

Network Name (SSID): lab005

Allow Static IP Addresses [YES][no] yes

Configure a Radius Server now [YES][no] yes

Enter Country Code (enter 'help' for a list of countries) (US):

Enable 802.11b Network [YES][no] yes

Enable 802.11a Network [YES][no] yes

Enable 802.11g Network [YES][no] yes

Enable Auto-Rf [YES][no] yes

Configuration saved!

Resetting system with new configuration

These parameters set up the WLC for basic operation. In this example configuration the WLC uses 192.168.1.5 as the management interface IP address and 192.168.1.6 as the AP-manager interface IP address.

Before any other features can be configured on the WLC, the Lightweight APs have to register with the WLC. This document assumes that the Lightweight AP is registered to the WLC.

Refer to the "Register the Lightweight AP to the WLC section of WLAN Controller Failover for Lightweight Access Points Configuration Example" for information on how the Lightweight APs register with the WLC. For reference with this configuration example, the AP 1130 is deployed on the same subnet.



Americas Headquarters Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA