Cisco live!
What You Make Possible
Deploying Wireless Guest Access

Paul Nguyen
Abstract

This session focuses on design requirements and deployment considerations for wireless Guest access solution. It discusses the main components of an end-to-end guest access solution including how to provide network access to visitors and route guest traffic across the network that is safe and secure. Attendees will be introduced to a detailed discussion on various guest access services directly on the wireless LAN controllers (WLC), management of Guest services using Cisco Prime Infrastructure (PI), and integration with the Identity Services Engine (ISE) for various external web authentication services such as sponsored and self-service options. We will also discuss FlexConnect, Guest Anchor, and enhanced guest security with WLC and ISE. This session is especially useful for those attendees responsible for the Design Deployment Operations and Management of Enterprise Campus Wireless Networks. It is assumed that all those attending this session have a working knowledge of LAN switching and routing, fundamentals in 802.1X and Network Admission Control. Knowledge of 802.11 WLAN fundamentals and WLAN security is required.
Agenda

- Overview: Guest Access as a Supplementary User Authentication
- Guest Access Control & Path Isolation
- Secure Guest in FlexConnect
- Guest Authentication Portal
- Guest Provisioning
- Monitoring & Reporting
- Demo
Session Objectives

• Understand what wireless Guest Access Services are made of.
• Learn about the importance of isolating Guest traffic.
• See how guest access is integrated in Cisco Wireless Solution.
• Securing FlexConnect is simple to understand and configure.
• Discover how Cisco ISE enhances Guest Services overall.
Guest Access Overview
Evolution of Network Access
Age of the Borderless Network

- Mobile Workers
- Personal Devices
- Hotspot
- Internet
- VPN
- Campus Network
- Branch Network
- Employee (Sales) Managed Desktop?
- Printers (Sales)
- Wireless Employee
- IP Camera
- Guest
- Game Console
- Contractor
- Wireless Employee
- Security Systems
- Internal Resources
- Employee (Finance) Managed Desktop?
- Printer (Payroll)
Context-Based Access
Who = User Identity

- **Known/Managed Users (Long-term)**

Examples: Employees/Staff, Faculty/Students, Extended Access Partners/Contractors

Primary Auth Methods: 802.1X or Agent-based

Considerations:
- Identity Stores
- EAP types and supplicant

- **Unknown/Unmanaged Users (Temporary or Infrequent Access)**

Examples: Guests, Visitors, Short-term Partners/Contractors

Primary Auth Method: Web authentication

Considerations:
- Web Redirection and Authentication Portals
- Guest Provisioning and Identity Stores
Corporate vs Guests

- Users with Corporate Devices with their AD user id can be assigned to Employee VLAN

- Guests authenticate via Web Auth and are assigned to a GUEST-ACL on the Guest VLAN
Requirements for Secure Guest Access

Technical
- No access until authorized
- Guest traffic should be segregated from the internal network
- Web-based authentication
- Full auditing of location, MAC, IP address, username
- Overlay onto existing enterprise network
- Bandwidth and QoS management

Usability
- No laptop reconfiguration, no client software required
- Plug & Play
- Splash screens and web content can differ by location
- Easy administration by non-IT staff
- “Guest network” must be free or cost-effective and non-disruptive

Monitoring
- Mandatory acceptance of disclaimer or Acceptable Use Policy (AUP) before access is granted
- Logging and Monitoring
- Must not require guest desktop software or configuration
Guest Access Components

- Customizable Login Page
- 802.1X/MAB Compatibility
- Parity for Wired / Wireless
- Centralized Web Page Management
- Flexible
- Access Policies
- Centralized Accounting
- Sponsored Guest Credentials

Identity Services Engine

ACS 5.1

Centralized Accounting

Existing Credential Stores

Integrated Access Authentication
Guest Access Control & Path Isolation
Access Control
End-to-End Wireless Traffic Isolation

The fact
• Traffic isolation achieved via CAPWAP valid from the AP to the WLAN Controller

The challenge
• How to provide end-to-end wireless guest traffic isolation, allowing internet access but preventing any other communications?
Path Isolation
Why Do We Need It for Guest Access?

• Extend traffic logical isolation end-to-end over L3 network domain
• Separate and differentiate the guest traffic from the corporate internal traffic (security policies, QoS, bandwidth, etc.)
• Securely transport the guest traffic across the internal network infrastructure to DMZ
Guest Access Control

Cisco WLAN Controller Deployments

- CAPWAP tunnel is a Layer 2 tunnel (encapsulates original Ethernet frame)
- Same CAPWAP tunnel used for data traffic of different SSIDs
- Control and data traffic tunneled to the controller via CAPWAP: data uses UDP 5247, control uses UDP 5246
- Data traffic bridged by WLAN controller on a unique VLAN corresponding to each SSID
- Traffic isolation provided by VLANs is valid up to the switch where the controller is connected
Solution #1: Path Isolation using EoIP

WLAN Controller Deployments with EoIP Tunnel

- Use of up to 71 EoIP tunnels to logically segment and transport the guest traffic between remote and anchor controllers
- Other traffic (employee for example) still locally bridged at the remote controller on the corresponding VLAN
- No need to define the guest VLANs on the switches connected to the remote controllers
- Original guest’s Ethernet frame maintained across CAPWAP and EoIP tunnels
- Redundant EoIP tunnels to the Anchor WLC
- virtual WLC models can not terminate EoIP connections (no anchor role) or support IPSec Encrypted Tunnels on the remote WLC
- 2500 can now support up to 15 EoIP tunnels.
Guest Network Redundancy

- Using EoIP Pings (data path) functionality Anchor WLC reachability will be determined.
- Foreign WLC will send pings at configurable intervals to see if Anchor WLC is alive.
- Once an Anchor WLC failure is detected a DEAUTH is sent to the client.
- Remote WLC will keep on monitoring the Anchor WLC.
- Under normal conditions round-robin fashion is used to balance clients between Anchor WLCs.
Implementing Guest Path Isolation Using WLC

Building the EoIP Tunnel

1. Specify a mobility group for each WLC
2. Open ports for:
   • Inter-Controller Tunneled Client Data
   • Inter-Controller Control Traffic
   • EoIP tunnel protocol
   • Other ports as required
3. Create Guest VLAN on Anchor controller(s)
4. Create identical WLANs on the Remote and Anchor controllers
5. Configure the mobility groups and add the MAC-address and IP address of the remote WLC
6. Create the Mobility Anchor for the Guest WLAN
7. Modify the timers in the WLCs
8. Check the status of the Mobility Anchors for the WLAN
Guest Path Isolation

WLAN Controller Deployments with EoIP Tunnel
Remote Controller Configuration

• Anchor and Remote WLCs are configured in different Mobility Groups
Guest Path Isolation
WLAN Controller Deployments with EoIP Tunnel
Anchor and Remote Controller Configuration

- Configure Guest WLANs on the Remote and Anchor controllers
- Configure Guest VLAN on the Anchor WLC

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>VLAN Identifier</th>
<th>IP Address</th>
<th>Interface Type</th>
<th>Dynamic AP Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>employee_vlan</td>
<td>30</td>
<td>10.10.30.6</td>
<td>Dynamic</td>
<td>Disabled</td>
</tr>
<tr>
<td>guest_vlan</td>
<td>12</td>
<td>10.10.12.6</td>
<td>Dynamic</td>
<td>Disabled</td>
</tr>
<tr>
<td>management</td>
<td>20</td>
<td>10.10.20.5</td>
<td>Static</td>
<td>Enabled</td>
</tr>
<tr>
<td>service-port</td>
<td>N/A</td>
<td>0.0.0.0</td>
<td>Static</td>
<td>Not Supported</td>
</tr>
<tr>
<td>virtual</td>
<td>N/A</td>
<td>1.1.1.1</td>
<td>Static</td>
<td>Not Supported</td>
</tr>
<tr>
<td>wired_vlan 11</td>
<td>11</td>
<td>0.0.0.0</td>
<td>Dynamic</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Guest Path Isolation

WLAN Controller Deployments with EoIP Tunnel Anchor and Remote Controller Configuration

- Configure the mobility groups and add the MAC-address and IP address of the remote WLCs.
Guest Path Isolation
WLAN Controller Deployments with EoIP Tunnel
Remote Controller Configuration

- Create the mobility anchor for the guest WLAN on Remote WLCs
Guest Path Isolation

WLAN Controller Deployments with EoIP Tunnel
Anchor Controller Configuration

- Create the Mobility Anchor for the guest WLAN on Anchor WLC

On the Anchor WLC select "local" for Anchor controller
Path Isolation
WLAN Controller Deployments with EoIP Tunnel
Anchor Controller

- Modify the timers and DSCP on the Anchor WLCs

- Check the status of the mobility anchors for the WLAN
Guest Path Isolation

Firewall Ports and Protocols

• Open ports in both directions for:
  - EoIP packets: IP protocol 97
  - Mobility: UDP Port 16666

Inter-Controller Data/Control Traffic

• Optional management/operational protocols:
  - SSH/Telnet: TCP Port 22/23
  - TFTP: UDP Port 69
  - NTP: UDP Port 123
  - SNMP: UDP Ports 161 (gets and sets) and 162 (traps)
  - HTTPS/HTTP: TCP Port 443/80
  - Syslog: TCP Port 514
  - RADIUS Auth/Account: UDP Port 1812 and 1813

Must be Open!

Do NOT Open!
Solution #2: Guest Path Isolation using VRF

Campus Virtualization

- Virtual Routing / Forwarding (VRF) or VRF-lite is the L3 virtualization used in Enterprise Campus networks
- Guest isolation is done by dedicated VRF instances
Guest Path Isolation using VRF
WLC and VRF Virtualization

- CAPWAP Path Isolation at Access Layer
- L2 Path Isolation between WLC and Default Gateway
- L3 VRF Isolation from WLC to Firewall Guest DMZ interface
## Wireless Guest Access

### Deployment Options Summary

<table>
<thead>
<tr>
<th></th>
<th>No DMZ WLC</th>
<th>VRF</th>
<th>DMZ WLC</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco Unified Wireless</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provisioning Portal</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User Login Portal</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Traffic Segmentation</td>
<td>VLANs thru Network</td>
<td>VRF thru Network</td>
<td>Yes—Tunnels or VLANs</td>
</tr>
<tr>
<td>User Policy Management</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Reporting</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Overall Functionality</strong></td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td><strong>Overall Design Complexity</strong></td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
</tr>
</tbody>
</table>
Securing Guest with FlexConnect
FlexConnect and External WebAuth

- ISE for external webauth with FlexConnect central authentication with local switching.
- Guest client is provided with URL/ACL permit to ISE
- Clients does webauth with ISE
- Guest moves to local switching

```
interface GigabitEthernet1/0/4
  description AP-3600-1
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 109
  switchport trunk allowed vlan 3,109
  switchport mode trunk
```
Guest with FlexConnect

- **Identity Services Engine**
- **Active Directory Server**
- **Certificate Authority Server**

- **WLC - Virtual Controller (FlexConnect Mode)**
- **Cisco 3750 Switch**
- **EOIPTunnel**
- **ASA Firewall**
- **Branch VLAN**
- **DMZ VLAN**

**Branch Office**

**Internet**

**Corporate Intranet**

**Guests**
CWA on Wireless Controllers

Blocking non-HTTP/DHCP/DNS Traffic

Guest-SSID

WLC

MAB

Default Policy

Redirect ACL & URL Redirect

AD / CA

ISE Guest DB

ISE

© 2013 Cisco and/or its affiliates. All rights reserved.
Foreign Controller – Step-by-Step

Pre-Requisites

Default Mobility Domain Name

Layer 2 Security

None

Layer 2 Security

None

MAC Filtering

NAC

NAC State

Radius NAC

Client Profiling

DHCP Profiling

HTTP Profiling

RADIUS Authentication Servers

Call Station ID Type

System MAC Address

Use AES Key Wrap

(Designed for FIPS customers and requi

MAC Delimiter

Hyphen

Table:

<table>
<thead>
<tr>
<th>Network User</th>
<th>Management</th>
<th>Server Index</th>
<th>Server Address</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>✔</td>
<td>2</td>
<td>10.1.100.21</td>
<td>1812</td>
</tr>
</tbody>
</table>

RADIUS Accounting Servers

MAC Delimiter

Hyphen

Network User

Server Index

Server Address

Port

IPSec

☑ 2

10.1.100.21

1813

Enabled
Foreign Controller – Step-by-Step

Configure Interfaces

1. Configure Interfaces
   - `dmz-guest`
   - `employee`
   - `quest`

Static Mobility Group Members

Configure Mobility Group Members

2. Configure Mobility Group Members

<table>
<thead>
<tr>
<th>Local Mobility Group</th>
<th>DOC_Anchor</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>IP Address</td>
</tr>
<tr>
<td>00:50:56:b0:01:0e</td>
<td>10.1.100.61</td>
</tr>
<tr>
<td>d0:c2:82:dd:88:00</td>
<td>10.10.20.5</td>
</tr>
</tbody>
</table>
Foreign Controller – Step-by-Step

1. Configure Interfaces
   - dmz-guest
   - employee
   - guest

2. Configure Mobility Group Members
   - Static Mobility Group Members
     - Local Mobility Group: DOC_Anchor
     - MAC Address: 00:50:56:b0:01:0e, IP Address: 10.1.100.61, Group Name: DOC_Anchor
     - MAC Address: d0:c2:82:dd:88:00, IP Address: 10.10.20.5, Group Name: DOC_Anchor

3. Configure WLAN
   - WLAN ID: 1, Type: WLAN, Profile Name: myGuest

4. Configure Mobility Anchors
   - Mobility Anchors
     - WLAN SSID: myGuest
     - Switch IP Address (Anchor): 10.10.20.5
     - Data Path up
     - Control Path up

Anchor WLC
- IP Address: 10.10.20.5, MAC Address: D0:c2:82:dd:88:00
Anchor Controller – Step-by-Step

Pre-Requisites

Default Mobility Domain Name: DOC_Anchor

Layer 2 Security: None

Layer 2 Security: None

RADIUS Authentication Servers

- Call Station ID Type: System MAC Address
- Use AES Key Wrap: (Designed for FIPS customers and required)
- MAC Delimiter: Hyphen

RADIUS Accounting Servers

- MAC Delimiter: Hyphen
- Network User: 2
- Server Index: 10.1.100.21
- Port: 1812

Allow Access to ISE for CWA (URL-Redirect)

NAC

- NAC State: Radius NAC

Client Profiling

- DHCP Profiling
- HTTP Profiling

NOT Required
**Anchor Controller – Step-by-Step**

1. **Configure Interfaces**
   - `dmz-guest`
   - `employee`
   - `quest`

2. **Configure Mobility Group Members**

### Static Mobility Group Members

<table>
<thead>
<tr>
<th>Local Mobility Group</th>
<th>DOC_Anchor</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>IP Address</td>
</tr>
<tr>
<td>d0:c2:82:dd:00:00</td>
<td>10.10.20.5</td>
</tr>
<tr>
<td>00:50:56:b0:01:0e</td>
<td>10.1.100.61</td>
</tr>
</tbody>
</table>

- **Foreign WLC**
  - 10.1.100.61/00:50:56:80:01:0E

- **Anchor WLC**
  - 10.10.20.5/00:2:c2:82:dd:00
Anchor Controller – Step-by-Step

1. Configure Interfaces

   - `dmz-guest`
   - `employee`
   - `quest`

2. Configure Mobility Group Members

   - Static Mobility Group Members

<table>
<thead>
<tr>
<th>Local Mobility Group</th>
<th>DOC_Anchor</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>IP Address</td>
</tr>
<tr>
<td>d0:c2:82:dd:88:00</td>
<td>10.10.20.5</td>
</tr>
<tr>
<td>00:50:56:b0:01:0e</td>
<td>10.1.100.61</td>
</tr>
</tbody>
</table>

3. Configure WLAN

   - WLAN ID: 1
   - Type: WLAN
   - Profile Name: myGuest

   - Mobility Anchors
     - WLAN SSID: myGuest
       - Switch IP Address (Anchor): local
       - Mobility Anchor Create: 10.1.100.61

4. Configure Mobility Anchors

   - Anchor WLC
     - 10.10.20.5/ D0:c2:82:dd:88:00

   - Foreign WLC
     - 10.1.100.61/ 00:50:56:b0:01:0e
Review Wireless CWA Config

Matched AuthC Rule = MAB

Authorization Policy

[Table

<table>
<thead>
<tr>
<th>Status</th>
<th>Rule Name</th>
<th>Conditions</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IP Phones</td>
<td>Cisco-IP-Phone</td>
<td>Cisco_IP_Phone</td>
</tr>
<tr>
<td></td>
<td>BYOD</td>
<td>BYOD and Employee</td>
<td>Employee</td>
</tr>
<tr>
<td></td>
<td>Guest</td>
<td>Guest</td>
<td>Guest</td>
</tr>
<tr>
<td></td>
<td>Contractor</td>
<td>Contractor</td>
<td>Contractor</td>
</tr>
<tr>
<td></td>
<td>Employee</td>
<td>Employee</td>
<td>Employee</td>
</tr>
<tr>
<td></td>
<td>Default</td>
<td>If no match</td>
<td>WEBAUTH</td>
</tr>
</tbody>
</table>

CWA username matches

Matched AuthZ Rule = Guest

No Supplicant

MAB

Username = 00-10-18-88-22-24
Password = 00-10-18-88-22-24

RADIUS Access-Request
AVP: Airespace ACL = Internet_Only

RADIUS Access-Accept

Layer 2 Security: None
MAC Filtering

Layer 3 Security: None

Allow AAA Override: Enabled
NAC State: Radius-NAC
CWA – Session Flow

- **Foreign WLC**: 10.1.100.61/00:50:56:80:01:0E
- **Anchor WLC**: 10.10.20.5/D0:c2:82:dd:88:00

**Client MAC Addr**: d0:23:db:e1:b1:b9
**AP Name**: BYOD-AP3600
**WLAN SSID**: Imran3
**Mobility Role**: Export Foreign
**Mobility Peer IP Address**: 10.10.20.5
**Policy Manager State**: RUN

**Client MAC Addr**: d0:23:db:e1:b1:b9
**AP Name**: 10.1.100.61
**WLAN SSID**: Imran3
**Mobility Role**: Export Anchor
**Mobility Peer IP Address**: 10.1.100.61
**Policy Manager State**: CENTRAL_WEB_AUTH

**Radius NAC State**: RUN
**AAA Override ACL Name**: ACL-WEBAUTH-REDIRECT
**AAA Override ACL**: Yes
**AAA Override ACL Applied Status**: Available
**AAA Override Flex ACL**: none
**AAA Override Flex ACL Applied Status**: Available

**Endpoint Profile**: Apple-iDevice
**MAC Address**: D0:23:DB:E1:B1:B9

---

© 2013 Cisco and/or its affiliates. All rights reserved.
CWA – Session Flow

User Open Browser

**Foreign WLC**
- IP: 10.1.100.61
- MAC: 00:50:56:80:01:0E

**Anchor WLC**
- IP: 10.10.20.5
- MAC: D0:c2:82:dd:88:00

**EoIP Tunnel**

**ISE Server**
- IP: 10.10.20.5
- MAC: D0:c2:82:dd:88:00

**Mobility Role**
- Export Foreign: RUN
- Export Anchor: RUN

**Mobility Peer IP Address**
- Foreign WLC: 10.10.20.5
- Anchor WLC: 10.1.100.61

**Policy Manager State**
- RUN

**Radius NAC State**
- RUN

**AAA Override ACL Name**
- None

**AAA Override ACL Applied Status**
- Unavailable

**AAA Override Flex ACL Name**
- None

**AAA Override Flex ACL Applied Status**
- Unavailable

**Redirect URL**
- None

**IPv4 ACL Name**
- Permit

**CTS Security Group Tag**
- Not Applicable

**AAA Override ACL Name**
- None

**AAA Override ACL Applied Status**
- Unavailable

**AAA Override Flex ACL Name**
- None

**AAA Override Flex ACL Applied Status**
- Unavailable

**Redirect URL**
- None

**IPv4 ACL Name**
- Permit
CWA – Session Flow

User Open Browser

Foreign WLC

10.1.100.61/00:50:56:80:01:0E

Anchor WLC

10.10.20./ D0:c2:82:dd:88:00

EoIP Tunnel

ISE Server

Identity | Endpoint ID | Network Device | Authorization Profiles | Identity Group | Event
---|---|---|---|---|---
ii04 | D0:23:DB:E1:B1:89 | Foreign | Guest_Authz | | ActivatedGuestProfile

Authentication Summary

Logged At: October 11, 2012 10:56:59.570 AM
RADIUS Status: Dynamic Authorization succeeded
NAS Failure: 
Username: 
MAC/IP Address: Foreign: 10.1.100.61:
Network Device: Foreign: 10.1.100.61:
Guest Services Portal
When to Use Web-Authentication?

- **Web Auth** is a supplementary authentication method
  Most useful when users can’t perform or pass 802.1X
- **Primary Use Case**: Guest Access
  Secondary Use Case: Employee who fails 802.1X

**802.1X**
- Managed 802.1X-devices
- Known users

**MAB**
- (mac-address bypass)
- Managed devices

**Web Auth**
- Users without 802.1X devices
- Users with Bad credentials
Guest Authentication Portal

Internal (Default Web Authentication Pages)

- Wireless Guest Authentication Portal is available in 4 modes:
- Customized (Downloaded Customized Web Pages)
- External Using ISE Guest Server
- External (Re-directed to external server)
Wireless Guest Authentication Portal

Internal Web Portal

- Wireless guest user associates to the guest SSID
- Initiates a browser connection to any website
- Web login page will displayed
Wireless Guest Authentication Portal

Customizable Web Portal

- Create your own Guest Access Portal web pages
- Upload the customized web page to the WLC
- Configure the WLC to use “customizable web portal”
- Customized WebAuth bundle up to 5 Mb in size can contain
  - 22 login pages (16 WLANs, 5 Wired LANs and 1 Global)
  - 22 login failure pages
  - 22 login successful pages
Wireless Guest Authentication Portal

External Web Portal

- Set in WLC > Security > WebAuth > Login
- Or override at Guest WLAN
  - Option to use Pre-Auth ACL

External (Redirect to external server)
- www.cisco.com
- https://se-guest-server:8443/guestportal/Login.action
Wireless Guest

Centralized Login Page

1) Administrator Creates WLAN Login Page on ISE
2) Wireless Guest Opens Web browser
3) Web traffic is intercepted by Wireless LAN Controller and redirected to Guest Server.
4) Guest Server returns centralized login page

Diagram:
- AP
- WLC
- ISE
- Redirect
- Centralized Login Page

Username
Password
Login
Change Password
Guest Services Provisioning
Requirements for Guest Provisioning

• Might be performed by non-IT user
• Must deliver basic features, but might also require advanced features:
  – Duration,
  – Start/End Time,
  – Bulk provisioning, …
• Provisioning Strategies :
  – Lobby Ambassador
  – Employees
Multiple Guest Provisioning Services

- Cisco Guest Access Solution supports several provisioning tools, with different feature richness.

- Included in Cisco Wireless LAN Solution:
  - Basic Provisioning
  - Advanced Provisioning

- Dedicated Provisioning:
  - Cisco Prime Infrastructure
  - Identity Services Engine

- Additional Cisco Product:
  - Customized Provisioning

- Customer Server:
  - Customer Development
Guest Provisioning Service : WLC
Cisco Wireless LAN Controller

- Lobby Ambassador accounts can be created directly on Wireless LAN Controllers
- Lobby Ambassadors have limited guest feature and must create the user directly on WLC:
  - Create Guest User – up to 2048 entries
  - Set time limitation – up to 35 weeks
  - Set Guest SSID
  - Set QoS Profile
Guest Provisioning Service
Create the Lobby Admin in WLC

- Lobby administrator can be created in WLC directly
Local WLC Guest Management

Quickly Create Guest with Time and WLAN Profile

Password is Created

The generated password for this user is i1dzMrwd

Login

Welcome to Cisco Live 2013
Welcome to London 2013

User Name: guest1
Password: 

Submit

Guest Web Login
Guest Provisioning Service : PI
Cisco Prime Network Control System

• Cisco Prime Infrastructure offers specific Lobby Ambassador access for Guest management only
• Lobby Ambassador accounts can be created directly on PI, or be defined on external RADIUS/TACACS+ servers
• Lobby Ambassadors on PI are able to create guest accounts with advanced features like:
  • Start/End time and date, duration,
  • Bulk provisioning,
  • Set QoS Profiles,
  • Set access based on WLC, Access Points or Location
Guest Provisioning Service
Lobby Ambassador Feature in Cisco Prime

• Associate the lobby admin with Profile and Location specific information
Guest Provisioning Service

Add a Guest User with PI
Guest Provisioning Service
Print/E-Mail Details of Guest User
Guest Provisioning Service
Schedule a Guest User
Cisco TrustSec Guest Services
Cisco ISE Guest Server

Guest User Creation

1. Sponsor creates Guest Account through dedicated ISE server
2. Credentials are delivered to Guest by print, email or SMS
3. Guest Authentication on Guest portal
4. RADIUS Request from WLC to Cisco ISE Server
5. RADIUS Response with policies (session timeout, …)
6. RADIUS Accounting with session information (time, login, IP, MAC, …)
7. Traffic can go through
Wireless Considerations

• WLC 7.0 – Supports LWA; 7.2 adds CWA support

• ISE Guest Services requires account activation; Initial web auth must be against ISE guest portal (LWA or CWA). As a result...
  o Requires ISE be the web auth portal for LWA; No support for hosting guest portal on WLC
  o For anchor controller deployments, requires pinhole through DMZ firewall back to ISE PSN on tcp/8443 from guest IP address pool.
Web Auth and Guest Access

- LWA vs CWA piggybacks on MAB authentication policy rule.
  Configure:
  If User Not Found = Continue (default Reject)

If MAC address lookup fails, reject the request and send access-reject.

If MAC address lookup returns no result, continue the process and move to authorization.
URL Redirection

Central Web Auth, Client Provisioning, Posture

• **Redirect URL**: For CWA, Client Provisioning, and Posture, URL value returned as a Cisco AV-pair RADIUS attribute.
  

• **Redirect ACL**: Access devices must be locally configured with ACL that specifies traffic to be permitted (= redirected) or denied (= bypass redirection)
  
  ACL value returned as a named ACL on NAD
  
  Ex: `cisco:cisco-av-pair=url-redirect-acl=ACL-POSTURE-REDIRECT`
  
  ACL entries define traffic subject to redirection (permit) and traffic to bypass redirection (deny)

• **Port ACL**: ACL applied to the port (default ACL, dACL, named ACL) that defines traffic allowed through port prior to redirection
Common URLs for Redirection

- **URL Redirect for Central Web Auth**
  Cisco:cisco-av-pair=url-redirect=
  https://ip:8443/guestportal/gateway?sessionId=SessionIdValue&action=cwa

- **URL Redirect for Client Provisioning and Posture**
  Cisco:cisco-av-pair=url-redirect=
  https://ip:8443/guestportal/gateway?sessionId=SessionIdValue&action=cpp

- **URL Redirect ACL**
  Cisco:cisco-av-pair=url-redirect-acl=ACL-WEBAUTH-REDIRECT

- **LWA URL for Default ISE Guest Portal:**
  https://ip:8443/guestportal/portal.jsp

- **LWA URL for Custom ISE Guest Portal:**
  https://ip:8443/guestportal/portals/ClientPortalName/portal.jsp

- **CWA URL redirect for Custom ISE Guest Portal:**
  Cisco:cisco-av-pair=url-redirect=
  https://ip:8443/guestportal/gateway?portal=ClientPortalName&sessionId=SessionIdValue&action=cwa
ISE Sponsored Guests – Sponsor Portal

- Customizable Web Portal for Sponsors as well
- Authenticate Sponsors with corporate credentials
  - Local Database
  - Active Directory
  - LDAP
  - RADIUS
  - Kerberos
Guest Portal Localization

Several Languages are Supported Natively in ISE 1.1

All guest user pages are translated:
• Authentication page
• Acceptable usage policy
• Success/failure page

Guest Portal Language Templates

<table>
<thead>
<tr>
<th>Language Template Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chinese Template Name</td>
<td>Guest Portal Language Template</td>
</tr>
<tr>
<td>Chinese Simplified</td>
<td>Guest Portal Language Template</td>
</tr>
<tr>
<td>English</td>
<td>English Guest Language Template</td>
</tr>
<tr>
<td>French</td>
<td>Guest Portal Language Template</td>
</tr>
<tr>
<td>German</td>
<td>Guest Portal Language Template</td>
</tr>
<tr>
<td>Italian</td>
<td>Guest Portal Language Template</td>
</tr>
<tr>
<td>Japanese</td>
<td>Guest Portal Language Template</td>
</tr>
<tr>
<td>Korean</td>
<td>Guest Portal Language Template</td>
</tr>
<tr>
<td>Portuguese</td>
<td>Guest Portal Language Template</td>
</tr>
<tr>
<td>Russian</td>
<td>Guest Portal Language Template</td>
</tr>
<tr>
<td>Spanish</td>
<td>Guest Portal Language Template</td>
</tr>
</tbody>
</table>
ISE Sponsored Guest

1. Guest is re-directed to the ISE Guest Portal when Browser is launched.

2. Guest enters the credentials created by the Sponsor

3. Account is verified on ISE decision point against the Guest User Identity Store
ISE Self-Registration

4. Guest is re-directed again to login again with auto generated username/ password.

5. Guest is provisioned with Authorization Policy for Web Access Only

6. Account is monitored via the timed profile settings.
ISE Guest User Portal Settings

- Guest Portals define what Guests Users will be allowed to perform:
  - Guests can change password
  - Guests change password at first login
  - Guests can be allowed to download the posture client
  - Guests can do self service
  - Guests can be allowed to do device registration
Cisco ISE Guest Server
Sponsor Authentication: Local Account/AD

Integrate with Active Directory

Assign user / group to Sponsor

Order Priority Sequence to AD > Internal
Cisco ISE Guest Server

Guest Portal Customization

- **Multi-Portal Policies**
- **Username Policy**
- **Password Policy**
- **Time Profiles**
- **Localization**

**Username Policy**
- General
  - Create username from email address
  - Create username from first name and last name
- Minimum Username Length
- Random
- Username may include the alphanumeric characters

**Password Policy**
- Password may include the alphabetic characters
- Minimum number of alphabetic characters to include
- Password may include the numeric characters
- Minimum number of numeric characters
- Password may include the special characters

**Time Profiles**
- Time Profile Name
- Account Type
- DefaultFirstLogin
- DefaultOneHour
- DefaultStartEnd

**Localization**
- ChineseSimplified_简体中文
- ChineseTraditional_繁體中文
- English
- French_Française
- German_Deutsch
- Italian_Italiano
- Japanese_日本語
- Korean 한국어
- Portuguese_Português
- Russian_русский
- Spanish_Español
Cisco ISE Guest Server
Sponsor Portal

- https://<ise-server-ip>:8443/sponsorportal/
Cisco ISE Guest Server

Sponsor – Guest Account Creation

Create/View/Modify
Guest Accounts

Personal Settings

Tools to Manage
Guest Accounts

Email / Print / SMS

Create Guest Account

First Name: Mary
Last Name: Smith
Email Address: mary@cisco.com
Phone Number: 408-526-4321
Company: Cisco
Optional Data 1:
Optional Data 2:
Optional Data 3:
Optional Data 4:
Optional Data 5:
Group Role: Guest
Time Profile: DefaultOneHour
Timezone: UTC

Successfully Created Guest Account: msmith

Username: msmith
Password: ~D0
First Name: Mary
Last Name: Smith
Email Address: mary@cisco.com
Phone Number: 408-526-4321
Company: Cisco
Status: AWAITING INITIAL LOGIN
Suspended: false
Optional Data 1:
Optional Data 2:
Optional Data 3:
Optional Data 4:
Optional Data 5:
Group Role: Guest
Time Profile: DefaultOneHour
Timezone: UTC
Account Start Date:
Account Expiration Date:
Language Template for Email/SMS Notifications: English
Guest Monitoring, Reporting and Troubleshooting
Live Guest Verification - ISE

- **Monitor > Operations > Authentications** window will show all Authentications including Guests
- Identity and Authorization can be found for Guests
Guest Monitoring - PI

- **Monitor > Clients and Users** window will show all Authentications including Guests
- Identity and Authorization can be found for Guests
Guest Activity Reporting - ISE

- Guest Reports
- Drill Down Guest Detail
Guest Activity Reporting - PI

Customized Profile and Scheduling

Variable Reporting Periods
Summary
What We Have Covered…

• What Guest Access Services are made of.
• The need for a secured infrastructure to support isolated Guest traffic.
• Unified Wireless is a key component of this infrastructure.
• The Guest Service components are integrated in Cisco Wired and Wireless Solution.
• Securing FlexConnect is simple to understand and configure.
• Guest Access is one of the User Access Policy available to Control and Protect enterprise Borderless Network
• Cisco TrustSec enhances Guest Services overall.
Cisco Wireless LAN Security

Expert guidance for securing your 802.11 networks

Krishna Sankar
Sid Sundaralingam
Andrew Balinsky
Darin Miller

ciscopress.com

Cisco ASA
All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance
Second Edition

Identify, mitigate, and respond to network attacks

Jazib Frahim, CCIE® No. 5459
Omar Santos

ciscopress.com
Call to Action

• **Visit** the Cisco Campus at the World of Solutions to experience Cisco innovations in action

• **Get** hands-on experience attending one of the Walk-in Labs

• **Schedule** face to face meeting with one of Cisco’s engineers at the Meet the Engineer center

• **Discuss** your project’s challenges at the Technical Solutions Clinics
Your feedback is important to us.

Complete the session survey at: www.ciscolivelondon.com/onsite or via the Cisco Live Mobile App