# Symantec VIP Integration with ISE

# Table of Contents

# Overview

Symantec Validation and ID Protection (VIP) with Intelligent Authentication (IA) is a cloud-based strong authentication service. It is designed to protect networks and applications against unauthorized access. It integrates Cisco's Central Web Authentication (CWA) with Cisco Identity Services Engine (ISE) and Cisco Wireless LAN Controller (WLC). It provides an easy, scalable, and cost-effective method of implementing an additional security layer, without additional investment in hardware or software. This whitepaper provides details of how VIP integrates with Cisco CWA, ISE, and WLC.

# Symantec VIP

Symantec VIP enables enterprises to secure networks and applications and prevent malicious access by unauthorized attackers. VIP is a unified solution, providing two-factor and risk-based credential-less authentication. It relies on open standards that integrate into enterprise applications. Furthermore, VIP uses device and behavior profiling to deliver multi-factor authentication to users, without requiring any hardware or software-based authentication credentials.

Key VIP features are:

- Cloud-based authentication deployment, without hardware or software installation
- Options for hardware and software credential generation, including free options for mobile devices
- Device and behavior profiling to deliver strong authentication without requiring hardware or software credentials
- Integration with enterprise infrastructure, such as RADIUS in either standard or custom configuration with plug-ins
- Self-service application for end users, including credential activation and synchronization

# Cisco Identity Services Engine (ISE)

The Cisco Identity Services Engine (ISE) is a policy platform that combines multiple services: authentication, authorization, and accounting (AAA), posture, profiling, device on-boarding, and guest management. It allows enterprises to gather contextual information from networks, users, and devices. Administrators can then use the collected data to apply governance decisions across any network infrastructure.

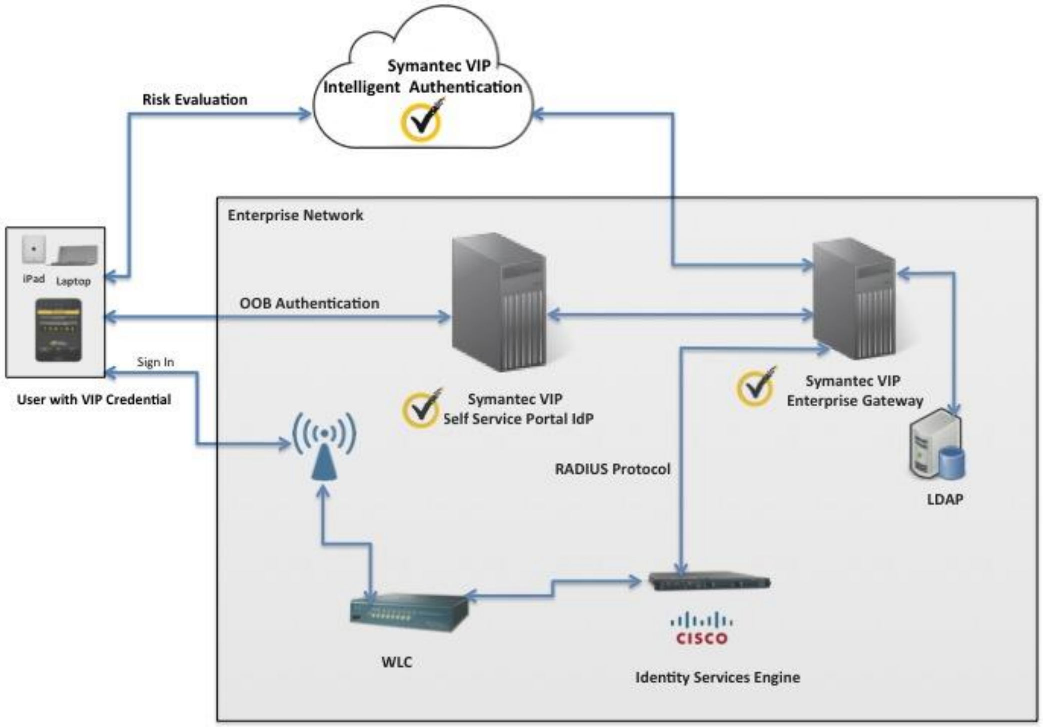
# Cisco Centralized Web Authentication

Web Authentication allows users to submit their credentials through a web portal and authenticate to the network. Central Web Authentication (CWA) is a process whereby a policy server, such as Cisco ISE, is used to centrally authenticate users. ISE supports the RADIUS protocol and also adds cascading layers of profiling and access controls.[i]

# VIP in Action

Your user requires access to internal resources using a personal device over the corporate wireless network. The user connects to an open SSID and is authenticated using only his or her user name and password. The wireless network is configured with the appropriate policies and access controls, although this configuration is transparent to users. The user sees a VIP-configured web portal with ISE. Among other benefits, this scenario provides the benefits of ISE, strong device ID, and multi-factor authentication with out-of-band verification.

***Figure 1 VIP Enterprise Gateway Architecture***



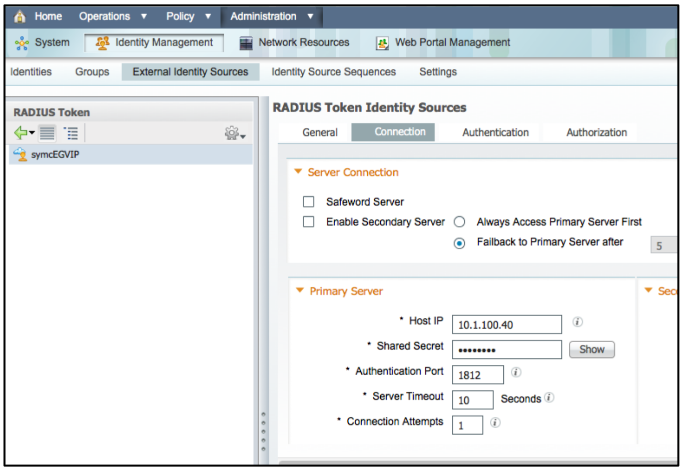
After the VIP Enterprise Gateway is installed and configured, it connects to ISE over RADIUS to authenticate user name and password. It also connects to the VIP user service to perform additional verification. Additionally, the ISE Guest Portal can be configured with javascript-embedded web pages that are made available from Symantec.

# ISE Configuration

The two sub-sections in this section provide high-level overviews of administrator configuration and end-user login.

## Administrator Configuration of VIP with ISE

1) Configure ISE with Enterprise Gateway
   a) In the ISE Admin Portal, navigate to **Administration → Identity Management → External Identity Sources → RADIUS Token** to create a new radius token identity source.  (In this example it is **symcEGVIP**.)



Server Connection

□ Safeword Server

□ Enable Secondary Server ○ Always Access Primary Server First

● Failback to Primary Server after 5

Primary Server

* Host IP 10.1.100.40

* Shared Secret •••••••• Show

* Authentication Port 1812

* Server Timeout 10 Seconds

* Connection Attempts 1

   b) Navigate to **Administration → Identity Management → Identity Source Sequence** to create a new identity source sequence (e.g. issEGVIP); in the authentication search list select the identity name you created.
   c) Define the authentication and authorization policies on ISE. Sample policies are shown here.

Authentication Policy

| Enabled | Name | | Condition | | Protocols | | Identity Source | Options |
|---|---|---|---|---|---|---|---|---|
| ✓ | MAB | IF | Wired_MAB<br>**OR**<br>Wireless_MAB | allow protocols | HostLookup | and use | Internal Endpoints | Reject<br>Continue<br>Drop |
| ✓ | Dot1X | IF | Wired_802.1X<br>**OR**<br>Wireless_802.1X | allow protocols | PEAPoTLS | and use | DOT1X_Sequence | Reject<br>Reject<br>Drop |
| ✓ | Default Rule (if no match) | | | allow protocols | Default Network Access | and use | DenyAccess | Reject<br>Reject<br>Drop |

Authorization Policy

| Status | Rule Name | Identity Groups | Other Conditions | Permissions |
|---|---|---|---|---|
| ✓ | Wireless Black List Default | **Blacklist** | Wireless_Access | Blackhole_Wireless _Access |
| ✓ | Profiled Cisco IP Phones ISE | **Cisco-IP-Phone** | - | Cisco_ IP_Phones |
| ✓ | Guest Flow | **Any** | Wireless_MAB<br>AND<br>Network Access:Use Case EQUALS Guest Flow | WLC-FullAccess |
| ✓ | Wireless MAB | **Any** | Wireless_MAB | WLC-cwaEgVIP |
| ✓ | Default | *no matches* | | DenyAccess |

d) Set up the authorization profiles in WLC as shown in these examples.

| Authorization Profiles |
|---|
| WLC-FullAccess<br>Access Type = ACCESS_ACCEPT<br>Airespace-ACL-Name = WLC-ACL_PERMIT-ALL-TRAFFIC |

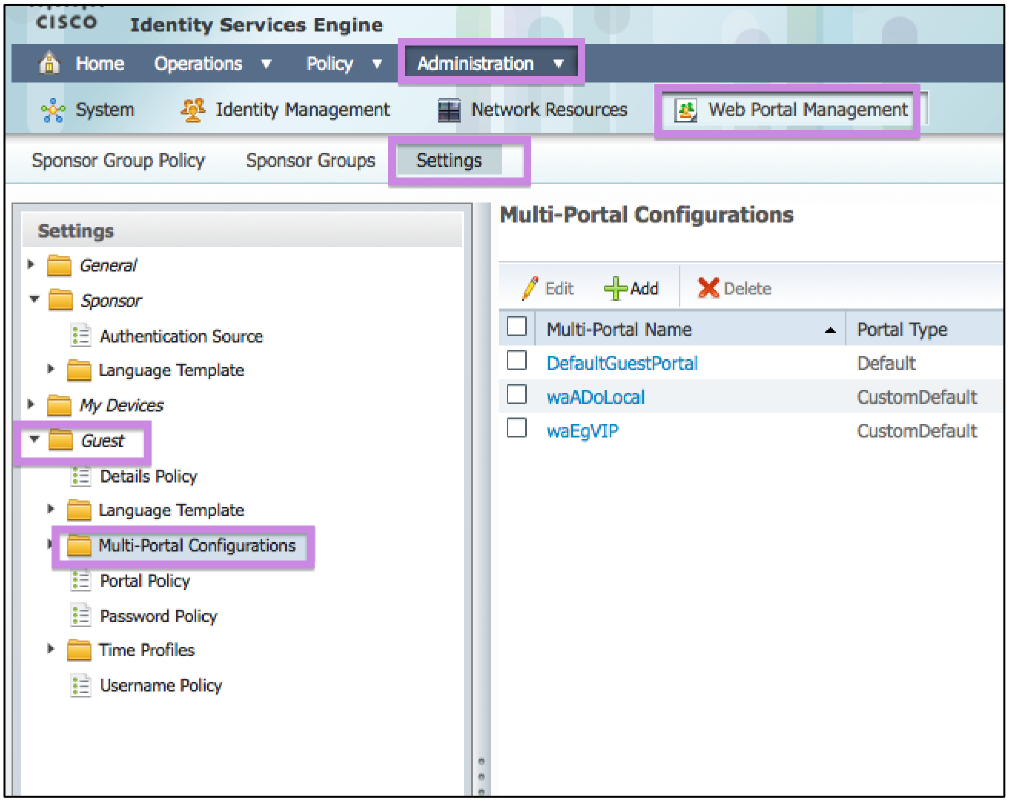
WLC-cwaEgVIP

Access Type = ACCESS_ACCEPT

Web Authentication | Centralized | ACL WLC-ACL_ISE-RESTRICTED | Redirect | Manual | waEGVIP

2) Upload Custom Web Portal to ISE.

Upload the Symantec pages with javascript to Cisco ISE. **Navigate to Administration → Web Portal Management → Settings → Guest → Multi-Portal Configurations** to create a custom default portal, as shown in the example.

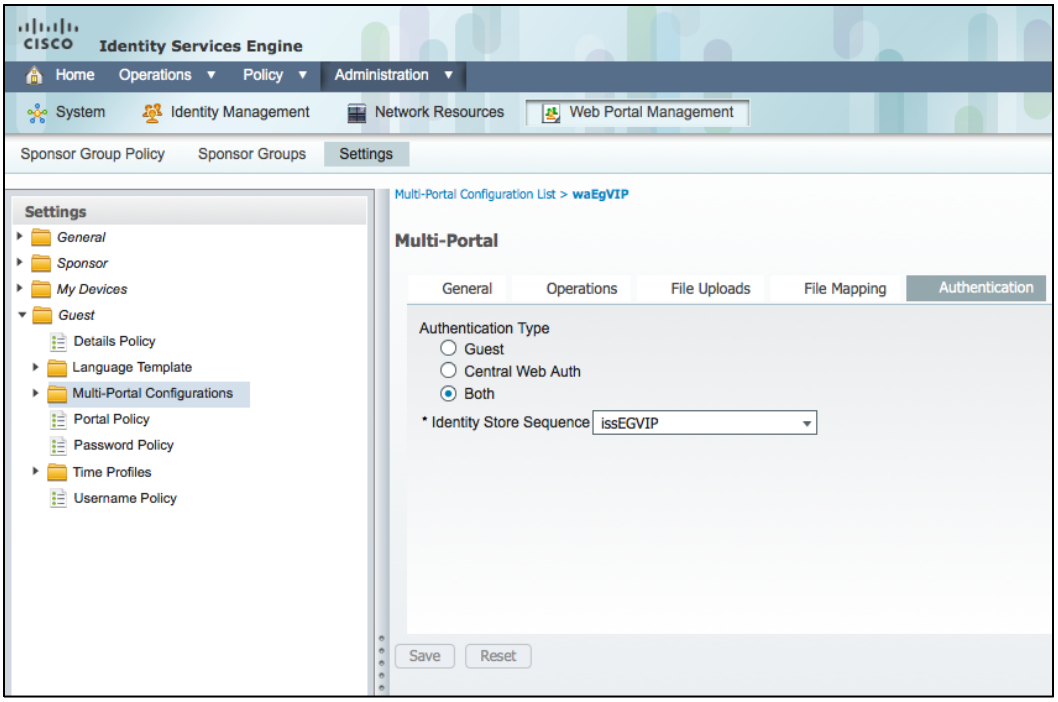


| □ | Multi-Portal Name ▲ | Portal Type |
|---|---|---|
| □ | DefaultGuestPortal | Default |
| □ | waADoLocal | CustomDefault |
| □ | waEgVIP | CustomDefault |

| |
|---|
| **Name**: waEgVIP |
| **Portal Type**: Custom Default Portal (Upload files) |
| **Operations**: AUP not used and un-check all the check boxes |
| **File Uploads**<br>• style.css<br>• login-symc-egvip.html |

| |
|---|
| • logo.png<br>• error.html<br>• success-google.refresh.html<br>• pageBg.jpg |
| **File Mapping**<br>• Login file → Login-symc-egvip.html<br>• AUP file → aup.html<br>• Guest Success File → success-google-refresh.html<br>• Error page file → error.html |

For authentication, select check box both and also identity store sequence to be issEGVIP.

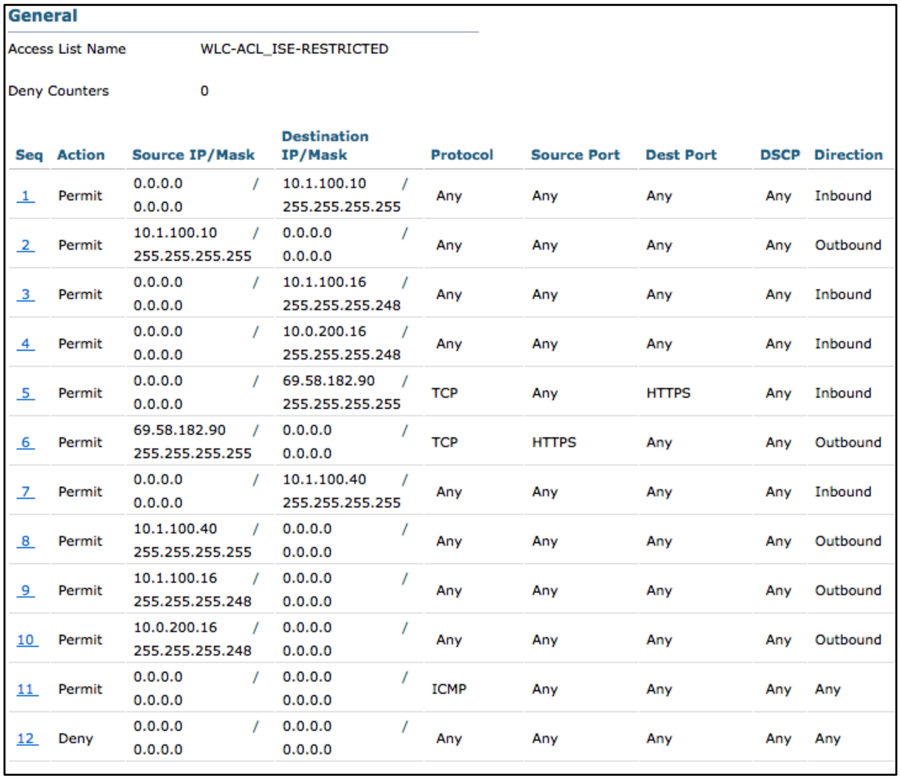


Authentication Type
○ Guest
○ Central Web Auth
● Both

* Identity Store Sequence: issEGVIP

3) Configure ISE in WLC.

a) Define the Access Control List in WLC to connect to the VIP User Service and the DMZ listener of the IDP proxy, as shown in this example.



General

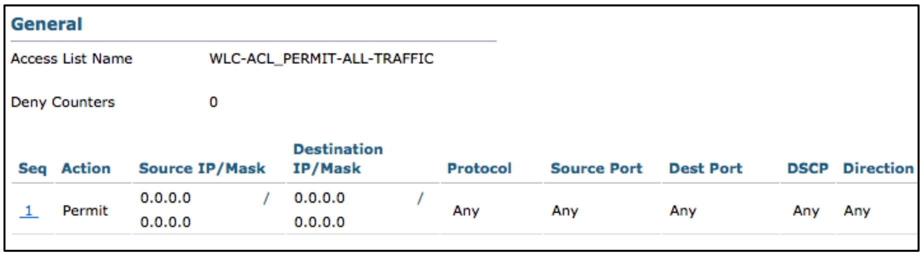
Access List Name WLC-ACL_ISE-RESTRICTED

Deny Counters 0

| Seq | Action | Source IP/Mask | Destination IP/Mask | Protocol | Source Port | Dest Port | DSCP | Direction |
|---|---|---|---|---|---|---|---|---|
| 1 | Permit | 0.0.0.0 / 0.0.0.0 | 10.1.100.10 / 255.255.255.255 | Any | Any | Any | Any | Inbound |
| 2 | Permit | 10.1.100.10 / 255.255.255.255 | 0.0.0.0 / 0.0.0.0 | Any | Any | Any | Any | Outbound |
| 3 | Permit | 0.0.0.0 / 0.0.0.0 | 10.1.100.16 / 255.255.255.248 | Any | Any | Any | Any | Inbound |
| 4 | Permit | 0.0.0.0 / 0.0.0.0 | 10.0.200.16 / 255.255.255.248 | Any | Any | Any | Any | Inbound |
| 5 | Permit | 0.0.0.0 / 0.0.0.0 | 69.58.182.90 / 255.255.255.255 | TCP | Any | HTTPS | Any | Inbound |
| 6 | Permit | 69.58.182.90 / 255.255.255.255 | 0.0.0.0 / 0.0.0.0 | TCP | HTTPS | Any | Any | Outbound |
| 7 | Permit | 0.0.0.0 / 0.0.0.0 | 10.1.100.40 / 255.255.255.255 | Any | Any | Any | Any | Inbound |
| 8 | Permit | 10.1.100.40 / 255.255.255.255 | 0.0.0.0 / 0.0.0.0 | Any | Any | Any | Any | Outbound |
| 9 | Permit | 10.1.100.16 / 255.255.255.248 | 0.0.0.0 / 0.0.0.0 | Any | Any | Any | Any | Outbound |
| 10 | Permit | 10.0.200.16 / 255.255.255.248 | 0.0.0.0 / 0.0.0.0 | Any | Any | Any | Any | Outbound |
| 11 | Permit | 0.0.0.0 / 0.0.0.0 | 0.0.0.0 / 0.0.0.0 | ICMP | Any | Any | Any | Any |
| 12 | Deny | 0.0.0.0 / 0.0.0.0 | 0.0.0.0 / 0.0.0.0 | Any | Any | Any | Any | Any |

Note: Actions in Sequential Lines 5 and 6 allow endpoints to reach the VIP cloud service and Actions in Sequential Lines 7 and 8 are for the DMZ listener of the IDP proxy.

b) Define general access to permit all traffic, as shown in this example.



General

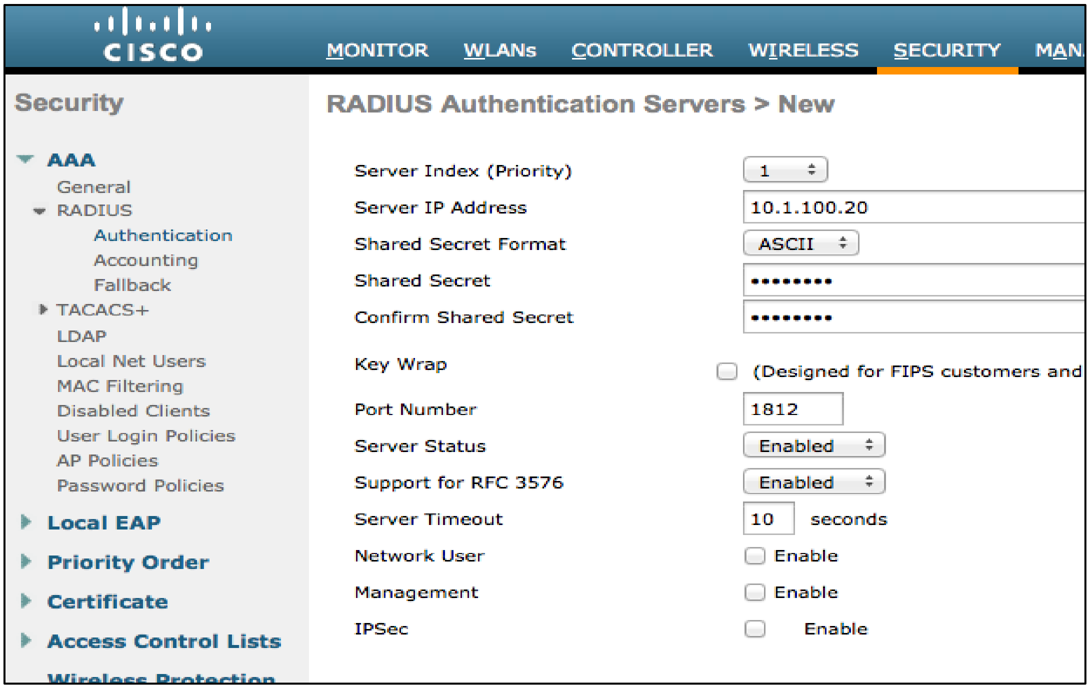
Access List Name WLC-ACL_PERMIT-ALL-TRAFFIC

Deny Counters 0

| Seq | Action | Source IP/Mask | Destination IP/Mask | Protocol | Source Port | Dest Port | DSCP | Direction |
|---|---|---|---|---|---|---|---|---|
| 1 | Permit | 0.0.0.0 / 0.0.0.0 | 0.0.0.0 / 0.0.0.0 | Any | Any | Any | Any | Any |

c) Implement security by enabling radius authentication for authentication and accounting for ISE.

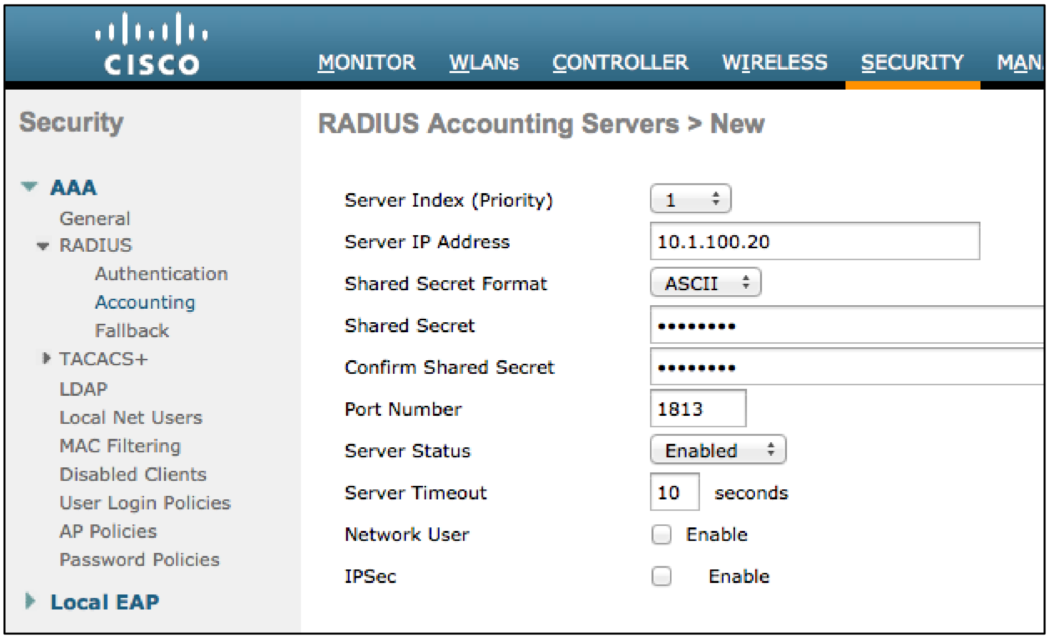
**AAA -> RADIUS -> Authentication: Add ISE and enable RFC 3576**



RADIUS Authentication Servers > New

| | |
|---|---|
| Server Index (Priority) | 1 |
| Server IP Address | 10.1.100.20 |
| Shared Secret Format | ASCII |
| Shared Secret | •••••••• |
| Confirm Shared Secret | •••••••• |
| Key Wrap | □ (Designed for FIPS customers and |
| Port Number | 1812 |
| Server Status | Enabled |
| Support for RFC 3576 | Enabled |
| Server Timeout | 10 seconds |
| Network User | □ Enable |
| Management | □ Enable |
| IPSec | □ Enable |

**AAA -> RADIUS -> Accounting: Add ISE**



RADIUS Accounting Servers > New

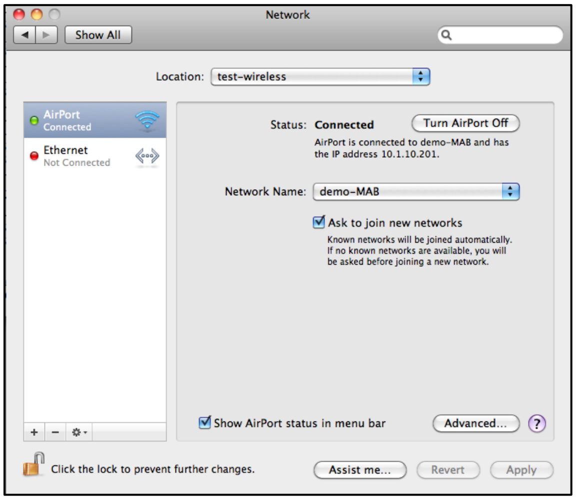
| | |
|---|---|
| Server Index (Priority) | 1 |
| Server IP Address | 10.1.100.20 |
| Shared Secret Format | ASCII |
| Shared Secret | •••••••• |
| Confirm Shared Secret | •••••••• |
| Port Number | 1813 |
| Server Status | Enabled |
| Server Timeout | 10 seconds |
| Network User | □ Enable |
| IPSec | □ Enable |

d) Configure the WLAN in this manner:

| |
|---|
| Profile Name: demo-MAB |
| SSID: demo-MAB<br>• Security -> Layer 2: None with MAC Filtering checked<br>• Security -> Layer 3: None |
| AAA Servers: select ISE as both the authentication server and the accounting server |
| Advanced<br>• Allow AAA Override<br>• NAC State Radius NAC |
| Enable this WLAN |

# End-User Strong Authentication Login

1) The end user connects to the SSID.



Location: test-wireless

Status: Connected

AirPort is connected to demo-MAB and has the IP address 10.1.10.201.

Network Name: demo-MAB

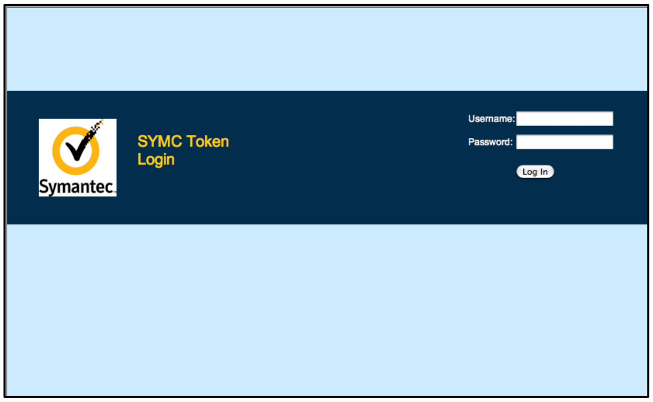
☑ Ask to join new networks

Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.

☑ Show AirPort status in menu bar

Click the lock to prevent further changes.

2) After getting connected to the SSID, when the user tries to access a resource or web page, the VIP-enabled login page for CWA appears.

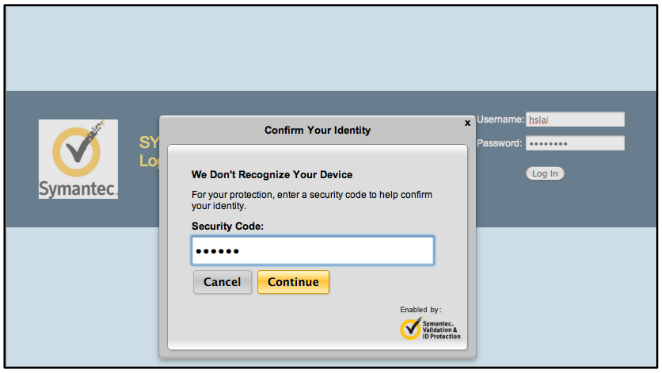


SYMC Token Login

Username:

Password:

3) If it is the first time the user logs in from a specific device, then after entering the credentials, the user must pass a challenge by entering a security code.



Confirm Your Identity

We Don't Recognize Your Device

For your protection, enter a security code to help confirm your identity.

Security Code: ••••••

Username: hslai

Password: ••••••••

4) If all credentials, including the security code, are valid, the user gains access to requested resource or web page.

For detailed information regarding VIP integration, please refer to the VIP Integration Guide on VIP Manager.

# References

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_40_webauthentication_dg.pdf

http://www.cisco.com/en/US/products/ps11640/products_configuration_example09186a0080ba6514.shtml

http://www.cisco.com/en/US/products/ps11640/products_configuration_example09186a0080bead09.shtml

# Conclusion

The integration of Symantec VIP and Identity Services Engine balances usability and security without altering the user's authentication experience.

[i] - http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_40_webauthentication_dg.pdf