

Extreme (Enterasys) Identifi

Modified on: Tue, 18 Nov, 2014 at 8:33 AM

IMPORTANT NOTICE: Your controller must be running 09.15 software or above for the integration to work correctly.

Open a web browser and log in to your Extreme Identifi controller.



Click on "VNS" on the top menu and then "New..." "START VNS WIZARD" on the left menu and follow the instructions below:

Name: Guest

Category: Captive Portal

VNS Creation Wizard

This wizard enables you to quickly configure a Virtual Network Segment of a specific type by requiring the essential settings only. Other mandatory fields will be completed according to best practice standards.

Please begin by entering the name for the new VNS and select the Category.

Name:	<input type="text" value="Guest"/>
Category:	<input type="text" value="Captive Portal"/>

Click **Next** to continue

- **Enabled:** Ticked
- **SSID:** Guest WiFi (or whatever you like)
- **Authentication Mode:** Firewall Friendly External Captive Portal
- **Mode:** Routed
- **Gateway:** 10.1.0.1
- **Mask:** 255.255.255.0
- **VLAN ID:** 50 (choose another if you already use VLAN 50) and ensure Untagged is ticked
- **Redirection URL:** *insert access_url here*
- **Enable Authentication:** Ticked
- **Enable DHCP:** Ticked

Basic Settings

Guest, Captive Portal

Enabled:

Name: Guest

Category: Captive Portal

SSID:

Authentication Mode:

Mode:

Gateway:

Mask:

VLAN ID: (1 - 4094) Untagged Tagged

Redirection URL:

Identity:

Shared Secret:

Enable Authentication:

Enable DHCP:

Click **Next** to continue

- **Radius Server:** Add New Server
- **Server Alias:** guest1
- **Hostname/IP:** *insert radius_server here*
- **Shared Secret:** *insert radius_secret here*
- **Roles:** Tick both Authentication and Accounting

Authentication

Guest, Captive Portal, Firewall Friendly External Captive Portal

Radius Server:

Server Alias:

Hostname/IP:

Shared Secret:

Roles: Authentication
 MAC-based Authentication
 Accounting

Click **Next** to continue

- **DHCP Option:** Local DHCP Server
- **Address Range:** 10.1.0.2 - 10.1.0.254
- **Lease:** default = 3600, max = 2592000
- **DNS Servers:** 8.8.8.8

DHCP

Guest, Captive Portal, Firewall Friendly External Captive Portal

DHCP Option:	Local DHCP Server ▼
Address Range:	From: 10.1.0.2
	To: 10.1.0.254
B'cast Address:	10.1.0.255
Lease (seconds):	default: 3600 max: 2592000
DNS Servers:	8.8.8.8
WINS:	

Click **Next** to continue

From the Filter ID drop down list, select **Non-Authenticated**.

Tick the **Enable** and then **Allow** box for each of the following:

- DNS (0.0.0.0/0:53, UDP)
- DHCP Server (0.0.0.0/0:67, UDP)

And tick the **Enable** and then **Deny** box for:

- (0.0.0.0/0)

Filtering

64, Captive Portal, Firewall Friendly External Captive Portal

Filter ID:

Enable	Allow	Deny	Filter Description
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	R-Login (0.0.0.0/0:513, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	R-Shell (0.0.0.0/0:514, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	LPR (0.0.0.0/0:515, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	RIP (0.0.0.0/0:520, UDP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	SOCKS (0.0.0.0/0:1080, TCP AND UDP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	CITRIX ICA (0.0.0.0/0:1494, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	RADIUS (0.0.0.0/0:1812, UDP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	RADIUS Accounting (0.0.0.0/0:1813, UDP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	NFS (0.0.0.0/0:2049, UDP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	X11 - Range Start (0.0.0.0/0:6000, TCP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	X11 - Range End (0.0.0.0/0:6063, TCP)
<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>	DHCP Server (0.0.0.0/0:67, UDP)
<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	DHCP Client (0.0.0.0/0:68, UDP)
<input type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>	(0.0.0.0/0)

Click **Next** to continue

Set the **Privacy** to **None**

Privacy

Guest, Captive Portal, Firewall Friendly External Captive Portal

WARNING: To use 11n, Privacy can only be "None" or WPA v.2 with AES only Encryption

None

Static Keys (WEP)

WPA - PSK

Click **Next** to continue

- **Select APs:** Select All radios including sites (unless you want to apply the guest access to a particular AP/site, in which case select what you need).

Radio Assignment

Guest, Captive Portal, Firewall Friendly External Captive Portal

AP Default Settings

To add this VNS to the AP Default Settings Profile, please select which radio(s) you would like to broadcast this VNS.

- Radio 1
- Radio 2

AP Selection

Use the drop down list on the left to select the groups of APs and sites that will serve the VNS (such as "All APs" or "radio 1". The list to the right will show the resulting assignment. Note that if your VNS is set to Enabled, and an AP radio or site has the maximum 8 VNSs assigned, the VNS will not be assigned to the AP or site.

Select APs:

WMM:

WARNING: To use 11n, WMM is required.

Radio 1	Radio 2	AP/Site Name
✓ a/n	✓ b/g	0000135022795600

Click **Next** to continue and then **Finish** to confirm.

Success!

Your VNS has been created. Click close to navigate to its configuration.
Click **Close** to exit the wizard.

Now, on the page you are returned to, under **Default Roles**, click the **Edit** button beside **GuestNonAuthPolicy**

Default Roles

Non-Authenticated:

Click on the **Policy Rules** tab and then click **Add** at the bottom. Leave all the boxes at their defaults but set the following:

- **Layer 3,4 IP/subnet:** User Defined = *insert walled_garden_ip here*
- **Access Control:** Allow

Filter Rule Definition
?
✕

Direction

In Filter:

Out Filter:

Classification

Layer 2

Ethertype:

Mac Address:

Priority:

Layer 3,4

IP/subnet:

Port:

Protocol:

ToS/DSCP: 0x (DSCP:) Mask:

Application

Application:

Action

Access Control:

Class of Service:

Click **OK** to Save and then click on **Add** again to add another Rule. This time, set the following:

- **Layer 3,4 IP/subnet:** User Defined = *insert walled_garden2_ip here*
- **Access Control:** Allow

Click **OK** to Save and then click on **Add** again to add another Rule. This time, set the following:

- **Layer 2 Ethertype:** Address Resolution Protocol (ARP)
- **Access Control:** Allow

Click **OK** to Save

Important: You need to select each the bottom three entries you just added and click the **Top** button to move them to the top of the list.

Next, under **Global** on the left, choose **Authentication**.

The screenshot shows a network management interface with a top navigation bar containing 'Home', 'Logs', 'Reports', 'Controller', 'AP', 'VNS', and 'Radars'. The 'VNS' tab is active. On the left, a sidebar menu has 'Global' selected, and 'Authentication' is highlighted. The main content area is titled 'RADIUS Servers' and includes a 'Strict Mode' checkbox and a table of RADIUS servers.

	Server	Default	Retries	Timeouts	Ports	Pr				
	Alias ▼	Hostname/IP	Protocol	Auth	Acct	Auth	Acct	Auth	Acct	Auth
<input type="checkbox"/>	guest1	radius...	PAP	3	3	5	5	1812	1813	1

Click on **guest1** and change the following:

- **Default Protocol:** PAP

RADIUS Server

Server Alias:	<input type="text" value="guest1"/>
Hostname/IP:	<input type="text" value="radius@radius.com"/>
Shared Secret:	<input type="password" value="*****"/> <input type="button" value="Unmask"/>
Default Protocol:	<input type="text" value="PAP"/>

Authentication

Priority:	<input type="text" value="1"/>
Total Number of Tries:	<input type="text" value="3"/>
RADIUS Request Timeout:	<input type="text" value="5"/> (seconds)
Port:	<input type="text" value="1812"/>

Accounting

Priority:	<input type="text" value="1"/>
Total Number of Tries:	<input type="text" value="3"/>
RADIUS Request Timeout:	<input type="text" value="5"/> (seconds)
Interim Accounting Interval:	<input type="text" value="30"/> (minutes)
Port:	<input type="text" value="1813"/>

Click on **Save** to continue

Next, click on **WLAN Services** on the left and then click on **GuestWLAN**

WLAN: GuestWLAN

WLAN Services	Privacy	Auth & Acct	QoS										
Authentication This type of authentication requires the user to be on a bridged at controller or routed topology.													
Mode: <input type="text" value="Firewall Friendly External"/> <input type="button" value="Configure..."/>													
<input type="checkbox"/> Enable MAC-based authentication													
RADIUS Servers													
<input type="text"/> <input type="button" value="Use"/>													
<table border="1"><thead><tr><th>Server</th><th>Auth</th><th>Acct</th><td rowspan="3"><input type="button" value="New"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/></td></tr></thead><tbody><tr><td>guest1</td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td></tr><tr><td> </td><td> </td><td> </td></tr></tbody></table>				Server	Auth	Acct	<input type="button" value="New"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/>	guest1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
Server	Auth	Acct	<input type="button" value="New"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/>										
guest1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>											

Under the **Auth & Acct** tab click on **Configure...** and then set the following:

- **EWC IP & Port:** Ticked
- **Associated BSSID:** Ticked
- **Station's MAC address:** Ticked
- **Use HTTPS for User Connections:** Unticked
- **Send Successful Login To:** custom specific URL: *insert redirect_url here*

Configure



Redirect to External Captive Portal

Identity:

Shared Secret:
Shared secret should be between 16 - 255 characters

Redirection URL:

Note: token=<integer_val>&dest=<original_target_url>
will be APPENDED to the redirection URL

EWC IP & port
Replace EWC IP with EWC FQDN:

AP name & serial number

Associated BSSID

VNS Name

Station's MAC address

Currently assigned role

Containment VLAN (if any) of assigned role

Timestamp

Signature

Redirect From External Captive Portal

Use HTTPS for User Connections:

Send Successful Login To:

*

View Sample

Close

Cancel

Click on **Close** to save

Next, click on the **guest1** under Server and choose the **Configure** button just to the right. Set the following:

- **Auth type: PAP**

RADIUS Parameters

Server: guest1

	Port	Timeout	NAS IP	NAS Identifier	Auth Type	
Auth	1812	5	VNS IP	VNS NAME	PAP	▲
Acct	1813	5	VNS IP	VNS NAME	-	▼

NAS IP Address: Use VNS IP address or use:

NAS identifier: Use VNS name or use:

Auth. type: ▼

NAS port type: *Wireless Other*

Click on **OK** to save

Finally, click on **Network** on the left and then **Topologies**. Click on the **GuestTopology** entry and then choose the **Exception Filters** tab.

Click on the **Add** button. Enter the following:

- **IP/subnet:port:** 10.1.0.1/32:80
- **Protocol** TCP
- **In Filter:** Destination (dest)

Topology: GuestTopology

Rule	In	Allow	IP : Port	Protocol
U	dest ▼	<input checked="" type="checkbox"/>	10.1.0.1/32:80 (HTTP)	TCP
I	dest ▼	<input type="checkbox"/>	192.168.2.1/32:60606	TCP
I	dest ▼	<input type="checkbox"/>	0.0.0.0/0:50200	TCP
I	dest ▼	<input checked="" type="checkbox"/>	192.168.2.1/32:32768-65535	TCP
I	dest ▼	<input checked="" type="checkbox"/>	192.168.2.1/32:32768-65535	UDP
I	dest ▼	<input checked="" type="checkbox"/>	192.168.2.1/32:67 (DHCP Server)	UDP
I	dest ▼	<input checked="" type="checkbox"/>	255.255.255.255/32:67 (DHCP Server)	UDP
I	dest ▼	<input checked="" type="checkbox"/>	192.168.2.1/32	ICMP
I	dest ▼	<input type="checkbox"/>	0.0.0.0/0	N/A

I: internal (read-only), U: user defined, D: default. Rules with Allow unchecked are denied.

Up Down

Add Delete

Add Predefined

Edit Filter

IP/subnet:port:

Protocol: ▼

In Filter: ▼

OK Cancel

New Delete Save

Click **OK** to save.