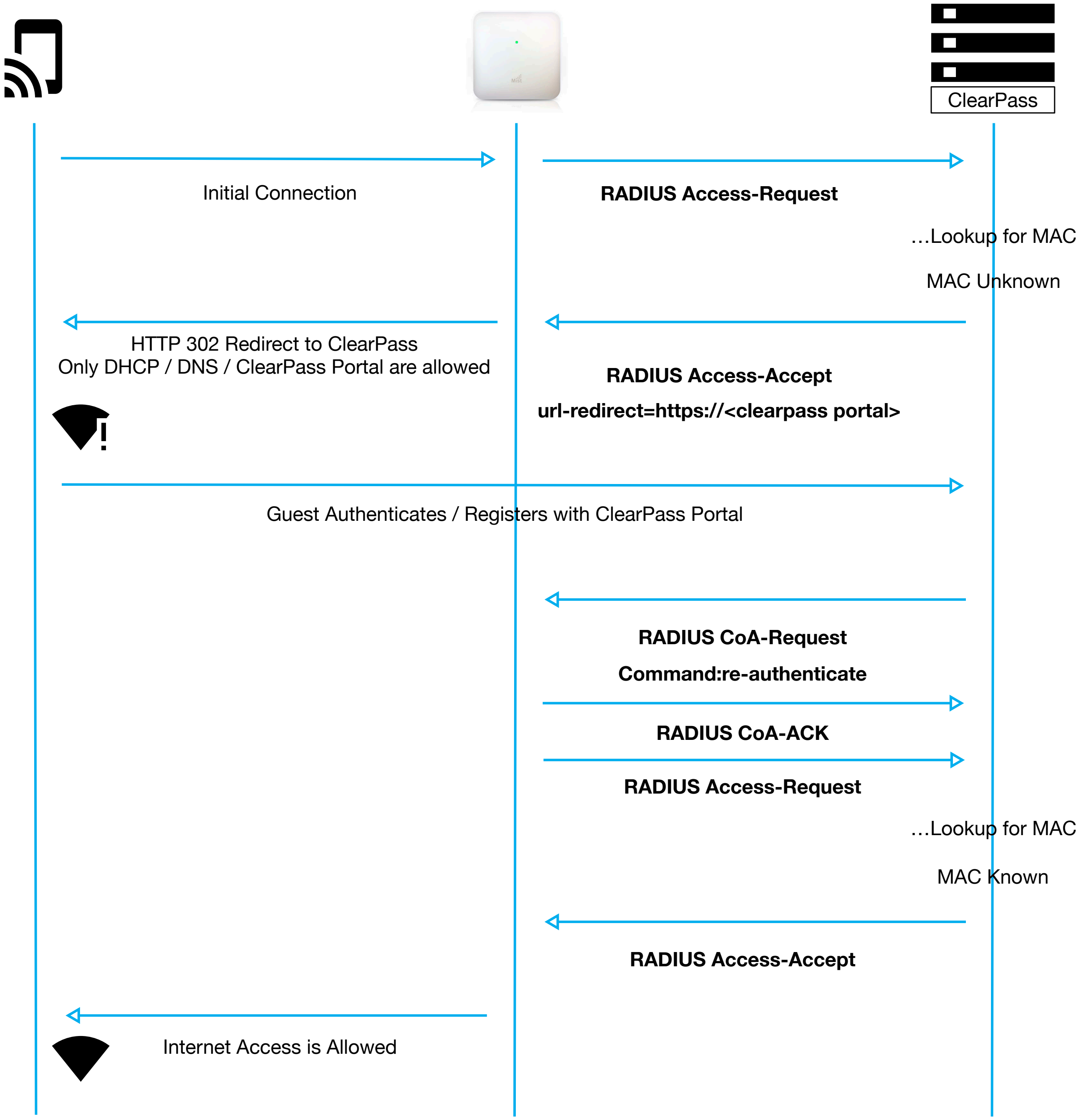
Mist - Clearpass Guest

Table of Contents

Overview

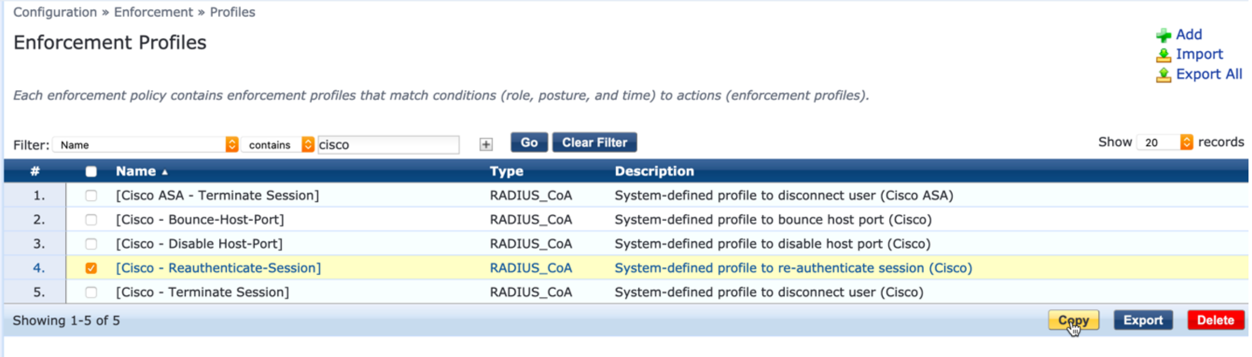
Mist seamlessly integrated with any external NAC/RADIUS solutions supporting both secure 802.1X, as well as various Guest Access workflows. This document covers integration of Mist Access Points with Aruba Clearpass Guest workflows leveraging MAC Authentication Bypass mechanisms.
The following diagram outlines the general guest onboarding flow with Mist and Clearpass:



Section 1: Clearpass Configuration

Step 1: Create CoA Profiles for Mist APs

Navigate to **Configuration → Enforcement → Profiles** and search for ‘cisco’. Select default *[Cisco – Reauthenticate-Session]* profile and **Copy** it:



Configuration » Enforcement » Profiles

Enforcement Profiles

Each enforcement policy contains enforcement profiles that match conditions (role, posture, and time) to actions (enforcement profiles).

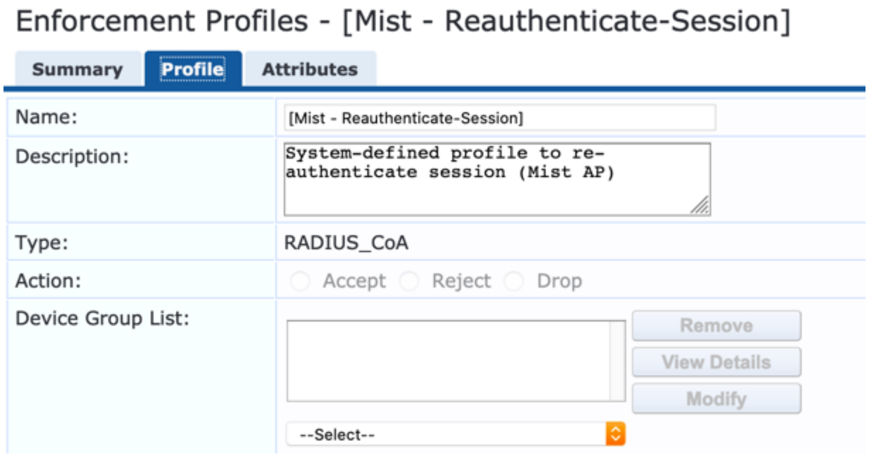
Filter: Name contains cisco

Show 20 records

#	□	Name ▴	Type	Description
1.	□	[Cisco ASA - Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Cisco ASA)
2.	□	[Cisco - Bounce-Host-Port]	RADIUS_CoA	System-defined profile to bounce host port (Cisco)
3.	□	[Cisco - Disable Host-Port]	RADIUS_CoA	System-defined profile to disable host port (Cisco)
4.	☑	[Cisco - Reauthenticate-Session]	RADIUS_CoA	System-defined profile to re-authenticate session (Cisco)
5.	□	[Cisco - Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Cisco)

Showing 1-5 of 5

Edit the new copy of that profile. Rename it as [Mist - Reauthenticate-Session] or similar:



Enforcement Profiles - [Mist - Reauthenticate-Session]

Name: [Mist - Reauthenticate-Session]

Description: System-defined profile to re-authenticate session (Mist AP)

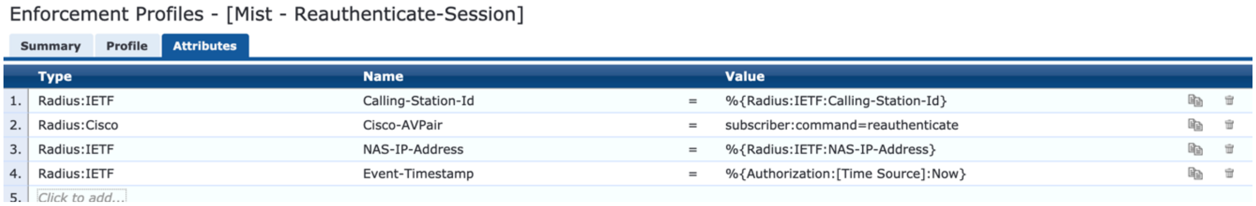
Type: RADIUS_CoA

Action: ○ Accept ○ Reject ○ Drop

Device Group List:

--Select--

Make sure to add two new attributes, *NAS-IP-Address* and *Event-Timestamp*:



Enforcement Profiles - [Mist - Reauthenticate-Session]

	Type	Name		Value
1.	Radius:IETF	Calling-Station-Id	=	%{Radius:IETF:Calling-Station-Id}
2.	Radius:Cisco	Cisco-AVPair	=	subscriber:command=reauthenticate
3.	Radius:IETF	NAS-IP-Address	=	%{Radius:IETF:NAS-IP-Address}
4.	Radius:IETF	Event-Timestamp	=	%{Authorization:[Time Source]:Now}
5.	*Click to add...*			

Overall, below are the attributes that need to be configured on the Clearpass for the Mist CoA profile:

Type	Name	Value
Radius:IETF	Calling-Station-Id	%{Radius:IETF:Calling-Station:Id}
Radius:Cisco	Cisco-AVPair	subscriber:command=reauthenticate
Radius:IETF	NAS-IP-Address	%{Radius:IETF:NAS-IP-Address}

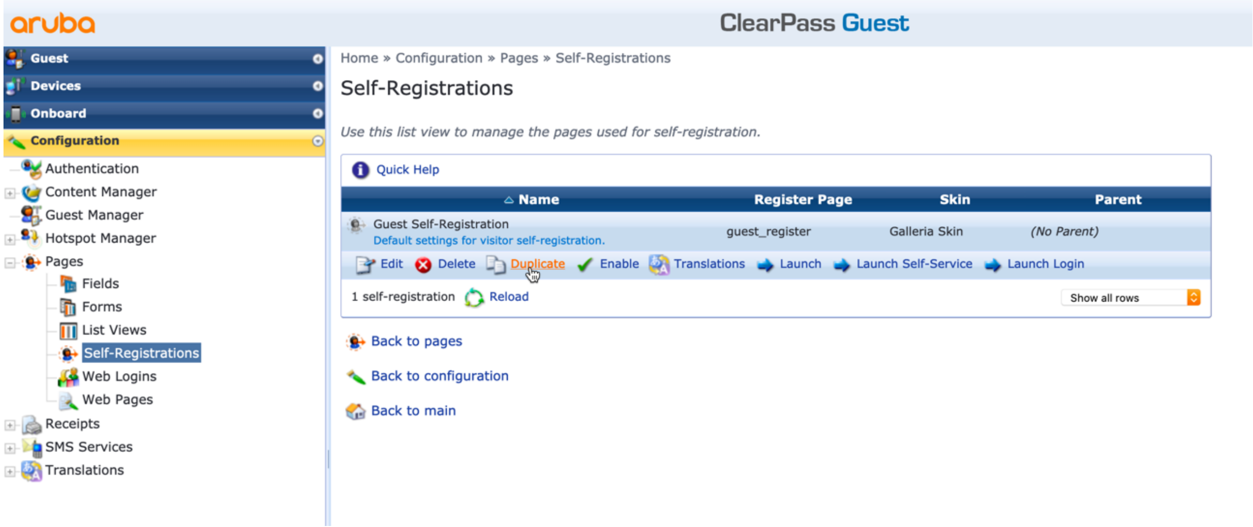
Radius:IETF	Event-Timestamp	%{Authorization:[Time Source]:Now}

Step 2: Create Guest Registration Page on the Guest Manager

Navigate to Clearpass Guest Manager:
https://<clearpass_address>/guest/

In this case we will be using Sponsored Guest Workflow with self-guest registration, but any other guest workflow will work in exactly the same manner.

First, duplicate default self-registration web page template:



Home » Configuration » Pages » Self-Registrations

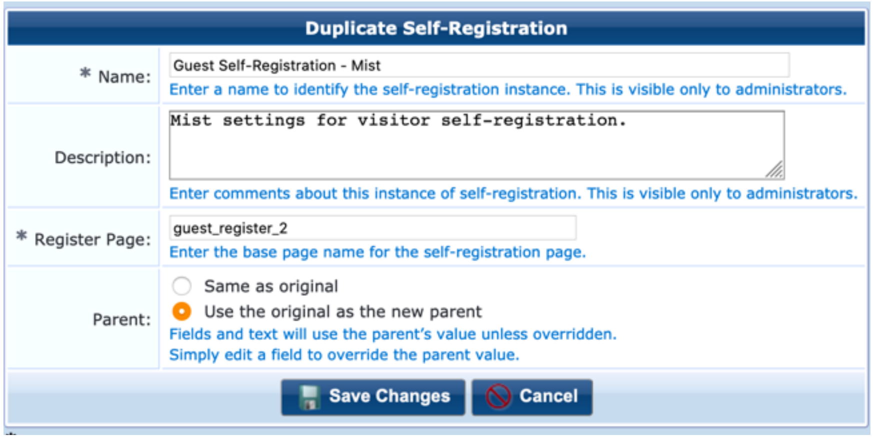
Self-Registrations

Use this list view to manage the pages used for self-registration.

Quick Help

Name	Register Page	Skin	Parent
Guest Self-Registration Default settings for visitor self-registration.	guest_register	Galleria Skin	*(No Parent)*

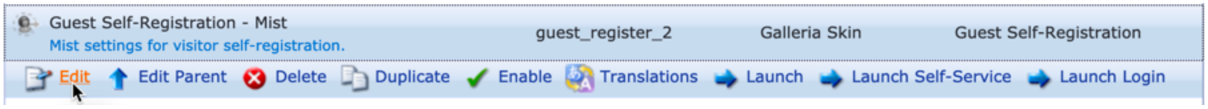
1 self-registration Reload



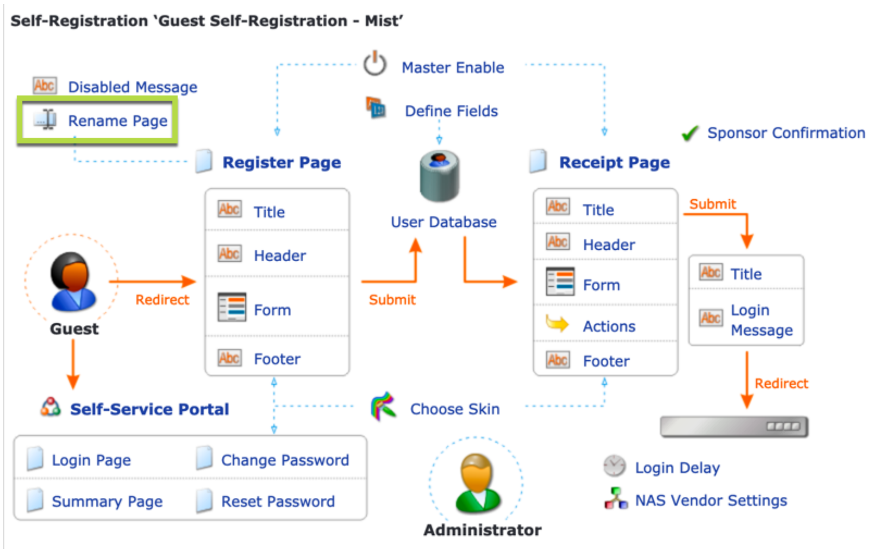
Duplicate Self-Registration

* Name:	Guest Self-Registration - Mist Enter a name to identify the self-registration instance. This is visible only to administrators.
Description:	Mist settings for visitor self-registration. Enter comments about this instance of self-registration. This is visible only to administrators.
* Register Page:	guest_register_2 Enter the base page name for the self-registration page.
Parent:	○ Same as original ● Use the original as the new parent Fields and text will use the parent's value unless overridden. Simply edit a field to override the parent value.

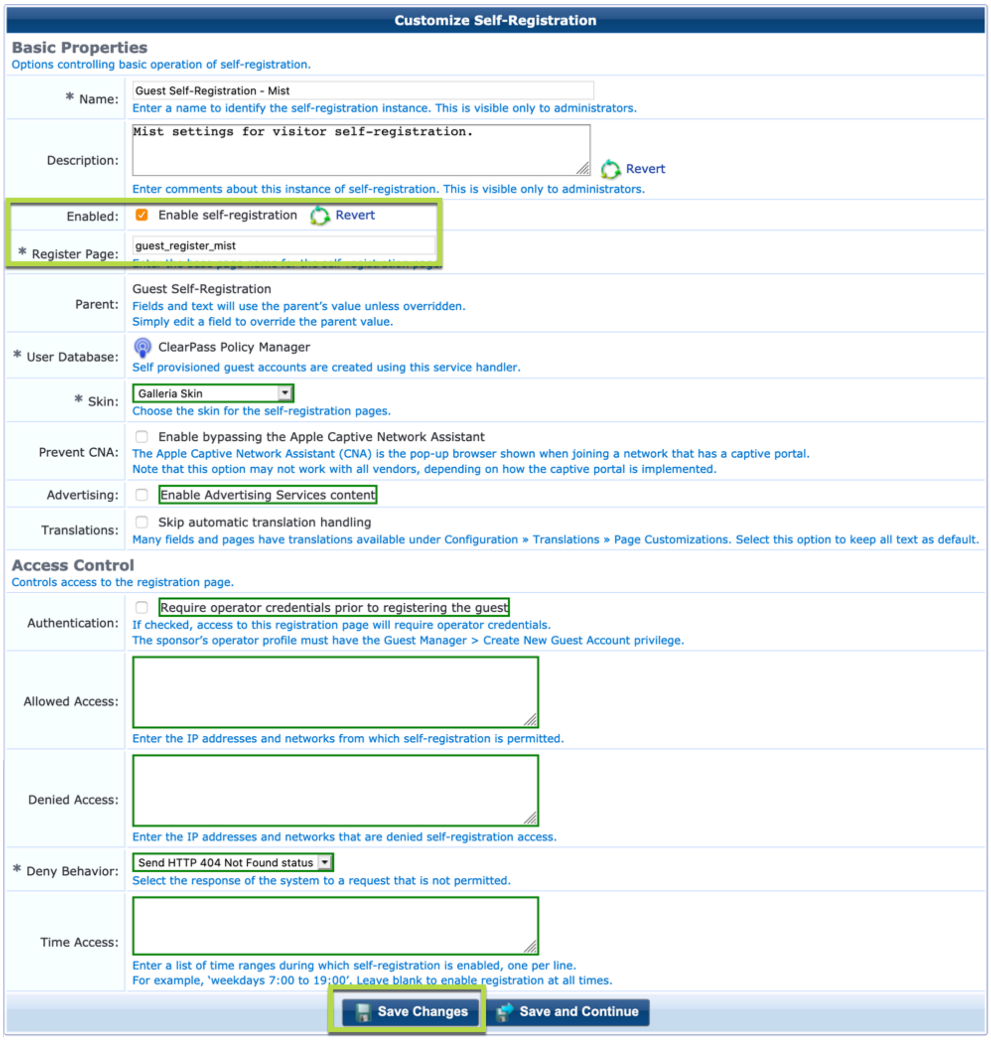
Now edit the duplicate page:



Guest Self-Registration - Mist Mist settings for visitor self-registration.	guest_register_2	Galleria Skin	Guest Self-Registration



Rename the guest registration page name and write it down. We will need it at the later step. In the example below the page name is ***guest_register_mist.php***



Customize Self-Registration

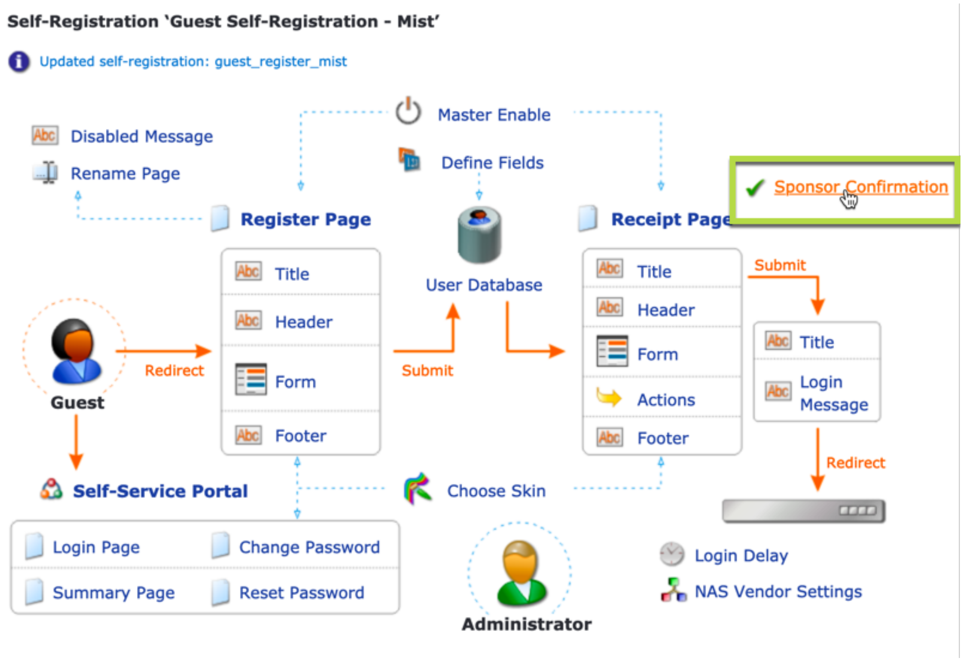
Basic Properties
Options controlling basic operation of self-registration.

* Name:	Guest Self-Registration - Mist Enter a name to identify the self-registration instance. This is visible only to administrators.
Description:	Mist settings for visitor self-registration. Revert Enter comments about this instance of self-registration. This is visible only to administrators.
Enabled:	☑ Enable self-registration Revert
* Register Page:	guest_register_mist Enter the base page name for the self-registration page.
Parent:	Guest Self-Registration Fields and text will use the parent's value unless overridden. Simply edit a field to override the parent value.
* User Database:	ClearPass Policy Manager Self provisioned guest accounts are created using this service handler.
* Skin:	Galleria Skin Choose the skin for the self-registration pages.
Prevent CNA:	□ Enable bypassing the Apple Captive Network Assistant The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not work with all vendors, depending on how the captive portal is implemented.
Advertising:	□ Enable Advertising Services content
Translations:	□ Skip automatic translation handling Many fields and pages have translations available under Configuration » Translations » Page Customizations. Select this option to keep all text as default.

Access Control
Controls access to the registration page.

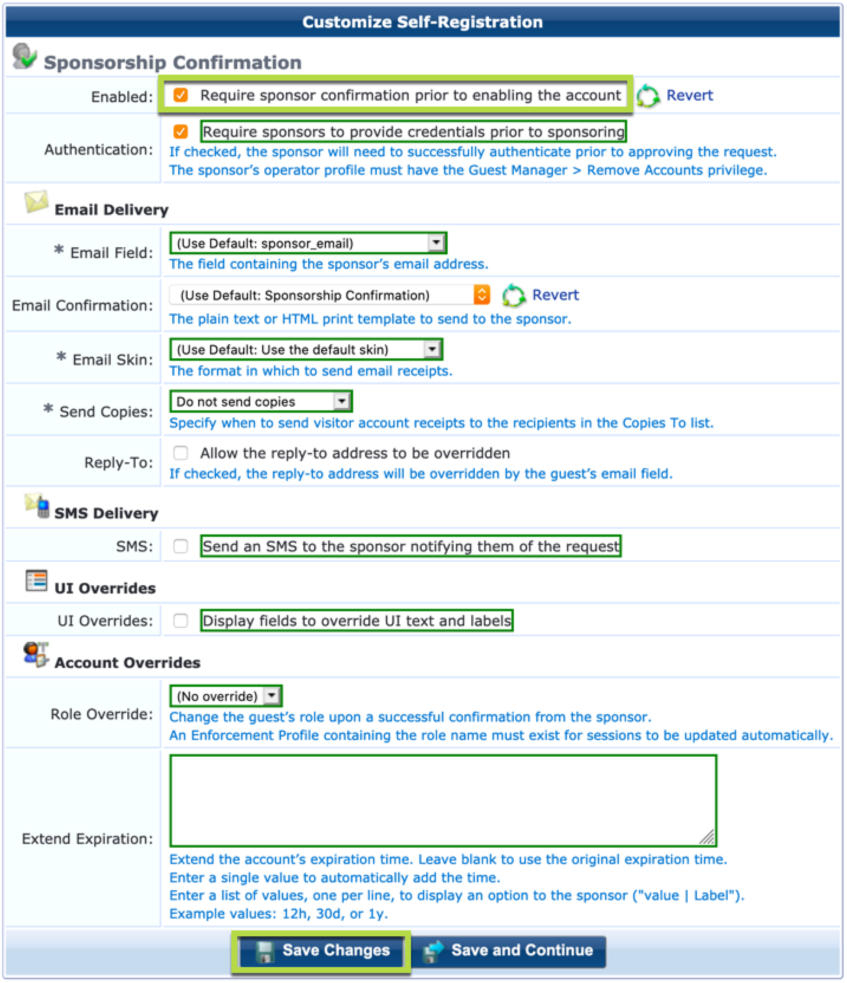
Authentication:	□ Require operator credentials prior to registering the guest If checked, access to this registration page will require operator credentials. The sponsor's operator profile must have the Guest Manager > Create New Guest Account privilege.
Allowed Access:	Enter the IP addresses and networks from which self-registration is permitted.
Denied Access:	Enter the IP addresses and networks that are denied self-registration access.
* Deny Behavior:	Send HTTP 404 Not Found status Select the response of the system to a request that is not permitted.
Time Access:	Enter a list of time ranges during which self-registration is enabled, one per line. For example, 'weekdays 7:00 to 19:00'. Leave blank to enable registration at all times.

Enable Sponsor Confirmation, since we are configuring a sponsored guest workflow:



Self-Registration 'Guest Self-Registration - Mist'

Updated self-registration: guest_register_mist



Customize Self-Registration

Sponsorship Confirmation

Enabled:	☑ Require sponsor confirmation prior to enabling the account Revert
Authentication:	☑ Require sponsors to provide credentials prior to sponsoring If checked, the sponsor will need to successfully authenticate prior to approving the request. The sponsor's operator profile must have the Guest Manager > Remove Accounts privilege.

Email Delivery

* Email Field:	(Use Default: sponsor_email) The field containing the sponsor's email address.
Email Confirmation:	(Use Default: Sponsorship Confirmation) Revert The plain text or HTML print template to send to the sponsor.
* Email Skin:	(Use Default: Use the default skin) The format in which to send email receipts.
* Send Copies:	Do not send copies Specify when to send visitor account receipts to the recipients in the Copies To list.
Reply-To:	□ Allow the reply-to address to be overridden If checked, the reply-to address will be overridden by the guest's email field.

SMS Delivery

SMS:	□ Send an SMS to the sponsor notifying them of the request

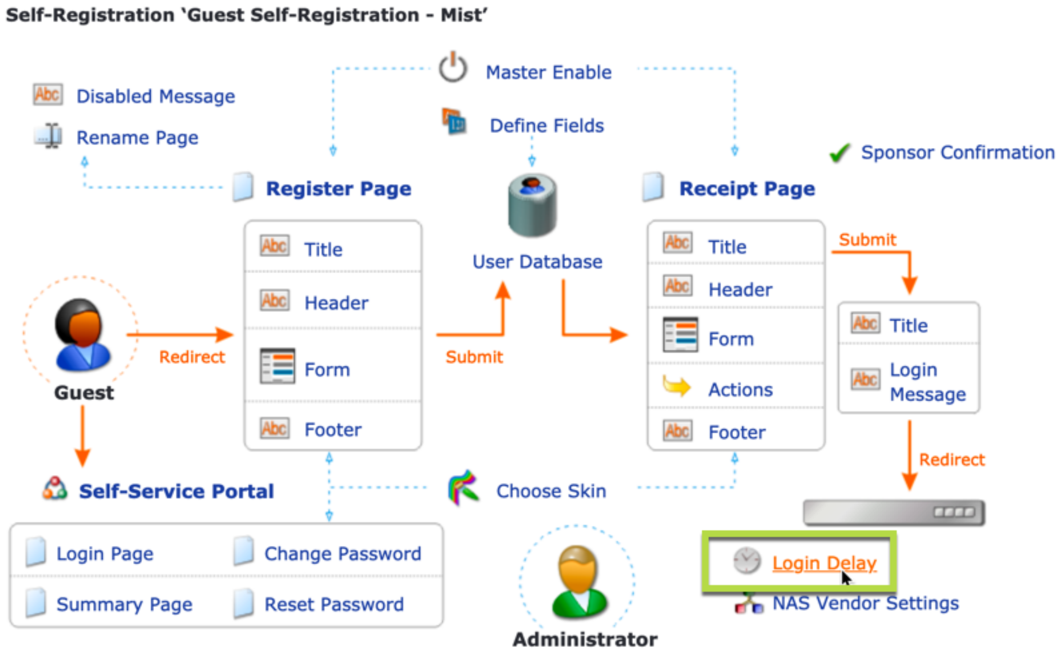
UI Overrides

UI Overrides:	□ Display fields to override UI text and labels

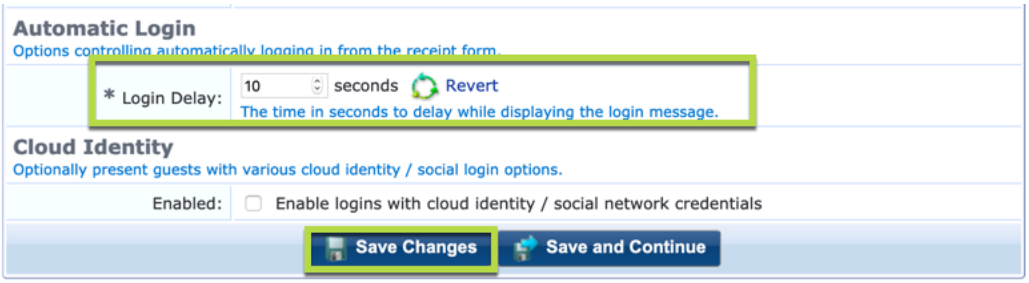
Account Overrides

Role Override:	(No override) Change the guest's role upon a successful confirmation from the sponsor. An Enforcement Profile containing the role name must exist for sessions to be updated automatically.
Extend Expiration:	 Extend the account's expiration time. Leave blank to use the original expiration time. Enter a single value to automatically add the time. Enter a list of values, one per line, to display an option to the sponsor ("value | Label"). Example values: 12h, 30d, or 1y.

As a next step configure a login delay, which will give clearpass time to send the CoA back to Mist AP and reauthorize a newly registered guest client. Login delay of 10 seconds will work for most cases, lower login delay times might cause inconsistent behavior with Clearpass:



Self-Registration ‘Guest Self-Registration - Mist’



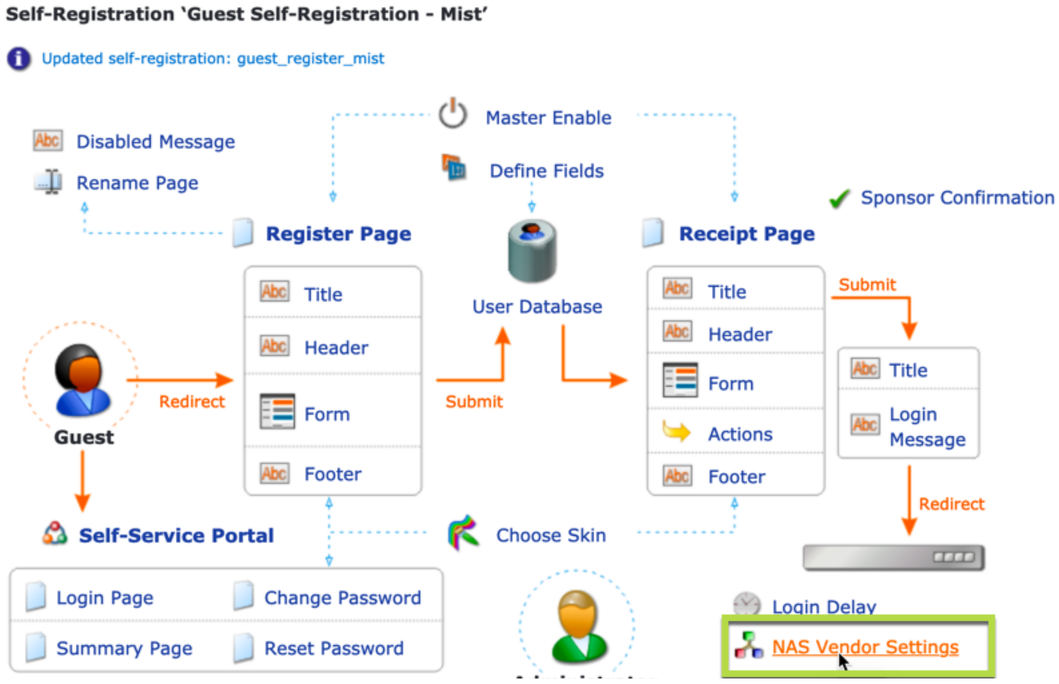
Automatic Login
Options controlling automatically logging in from the receipt form.

* Login Delay: 10 seconds Revert
The time in seconds to delay while displaying the login message.

Cloud Identity
Optionally present guests with various cloud identity / social login options.

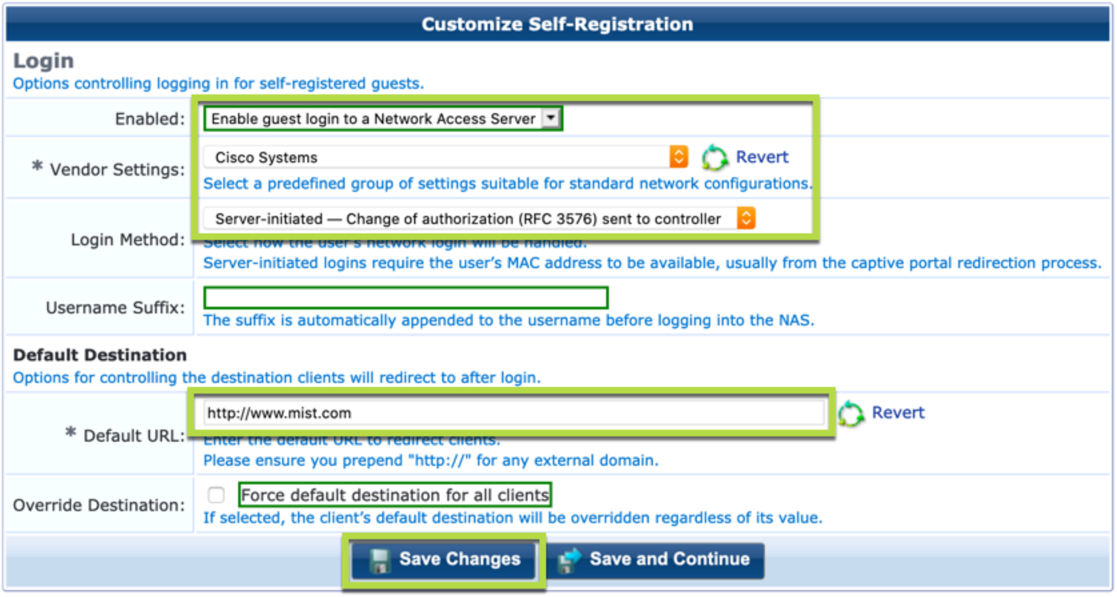
Enabled: □ Enable logins with cloud identity / social network credentials

Next, configure **NAS Vendor Settings** as follows:



Self-Registration 'Guest Self-Registration - Mist'

Updated self-registration: guest_register_mist



Customize Self-Registration

Login

Options controlling logging in for self-registered guests.

Enabled:	Enable guest login to a Network Access Server
* Vendor Settings:	Cisco Systems Revert Select a predefined group of settings suitable for standard network configurations.
Login Method:	Server-initiated — Change of authorization (RFC 3576) sent to controller Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.
Username Suffix:	The suffix is automatically appended to the username before logging into the NAS.

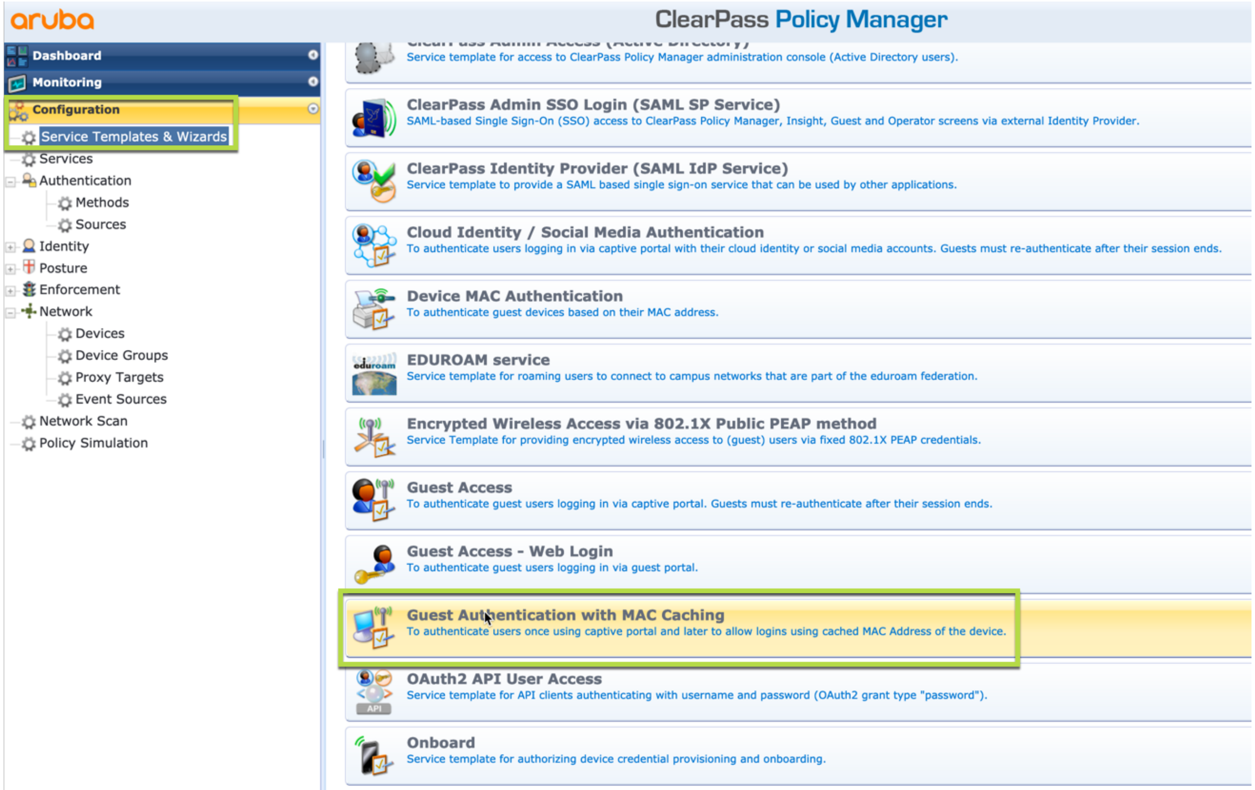
Default Destination

Options for controlling the destination clients will redirect to after login.

* Default URL:	http://www.mist.com Revert Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.
Override Destination:	□ Force default destination for all clients If selected, the client's default destination will be overridden regardless of its value.

Step 3: Use Wizard to create Guest Access config with MAC Caching

Navigate to **Configuration → Service Templates & Wizards** and use “Guest Authentication with MAC Caching”:



ClearPass Admin Access (Active Directory)
Service template for access to ClearPass Policy Manager administration console (Active Directory users).

ClearPass Admin SSO Login (SAML SP Service)
SAML-based Single Sign-On (SSO) access to ClearPass Policy Manager, Insight, Guest and Operator screens via external Identity Provider.

ClearPass Identity Provider (SAML IdP Service)
Service template to provide a SAML based single sign-on service that can be used by other applications.

Cloud Identity / Social Media Authentication
To authenticate users logging in via captive portal with their cloud identity or social media accounts. Guests must re-authenticate after their session ends.

Device MAC Authentication
To authenticate guest devices based on their MAC address.

EDUROAM service
Service template for roaming users to connect to campus networks that are part of the eduroam federation.

Encrypted Wireless Access via 802.1X Public PEAP method
Service Template for providing encrypted wireless access to (guest) users via fixed 802.1X PEAP credentials.

Guest Access
To authenticate guest users logging in via captive portal. Guests must re-authenticate after their session ends.

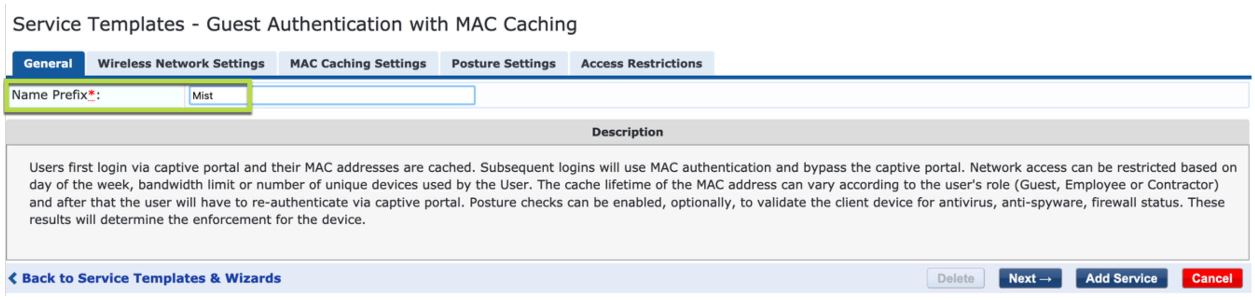
Guest Access - Web Login
To authenticate guest users logging in via guest portal.

Guest Authentication with MAC Caching
To authenticate users once using captive portal and later to allow logins using cached MAC Address of the device.

OAuth2 API User Access
Service template for API clients authenticating with username and password (OAuth2 grant type "password").

Onboard
Service template for authorizing device credential provisioning and onboarding.

Use “Mist” as the name prefix for any policies and profiles this wizard will create, it will be very useful in later steps. Then click Next:

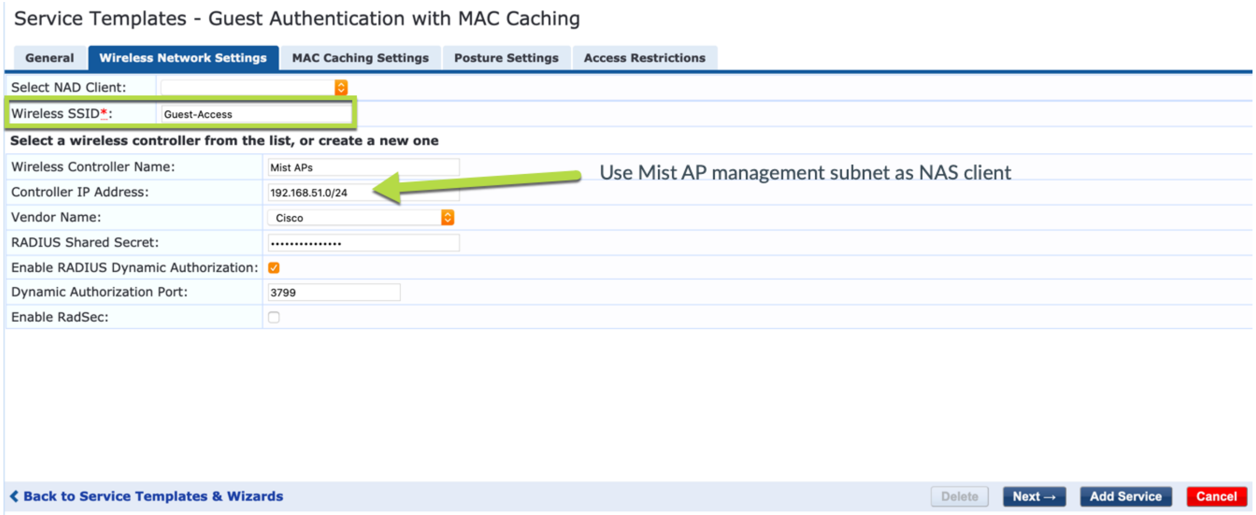

Service Templates - Guest Authentication with MAC Caching

Name Prefix*: Mist

Description

Users first login via captive portal and their MAC addresses are cached. Subsequent logins will use MAC authentication and bypass the captive portal. Network access can be restricted based on day of the week, bandwidth limit or number of unique devices used by the User. The cache lifetime of the MAC address can vary according to the user's role (Guest, Employee or Contractor) and after that the user will have to re-authenticate via captive portal. Posture checks can be enabled, optionally, to validate the client device for antivirus, anti-spyware, firewall status. These results will determine the enforcement for the device.

In the step below make sure you will use an actual Guest SSID name in the wizard, add management IP subnet of the Mist APs to allow them to talk to the Clearpass via RADIUS:



Service Templates - Guest Authentication with MAC Caching

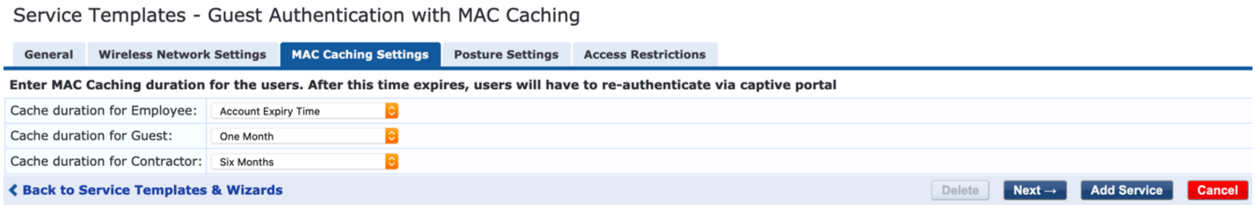
Select NAD Client:	
Wireless SSID*:	Guest-Access

Select a wireless controller from the list, or create a new one

Wireless Controller Name:	Mist APs
Controller IP Address:	192.168.51.0/24
Vendor Name:	Cisco
RADIUS Shared Secret:	················
Enable RADIUS Dynamic Authorization:	☑
Dynamic Authorization Port:	3799
Enable RadSec:	□

Use Mist AP management subnet as NAS client

Set default expiration times for each type of guest as required:

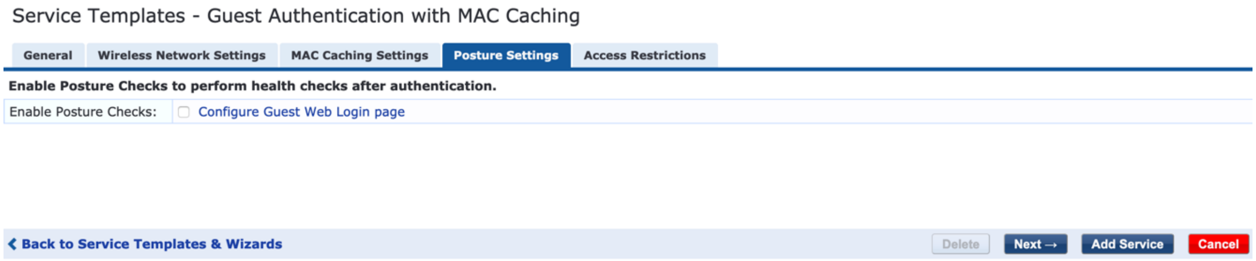


Service Templates - Guest Authentication with MAC Caching

Enter MAC Caching duration for the users. After this time expires, users will have to re-authenticate via captive portal

Cache duration for Employee:	Account Expiry Time
Cache duration for Guest:	One Month
Cache duration for Contractor:	Six Months

Skip posture checks:

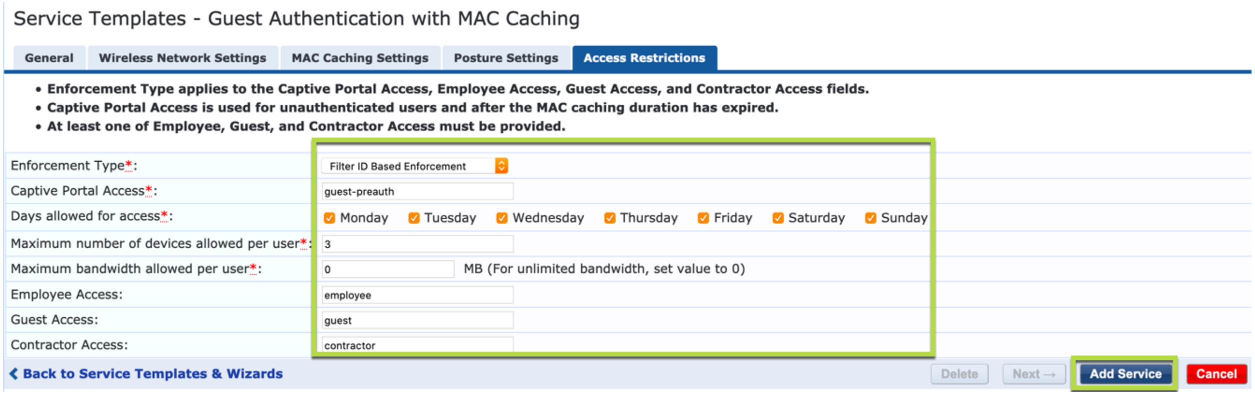


Service Templates - Guest Authentication with MAC Caching

Enable Posture Checks to perform health checks after authentication.

Enable Posture Checks: □ Configure Guest Web Login page

Select *Filter ID based enforcement* and provide guest role names. At this point it will only pre-create some Enforcement profiles that we will need to edit later on:



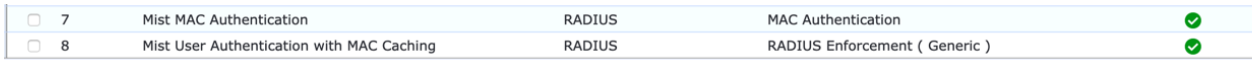
Service Templates - Guest Authentication with MAC Caching

- Enforcement Type applies to the Captive Portal Access, Employee Access, Guest Access, and Contractor Access fields.
- Captive Portal Access is used for unauthenticated users and after the MAC caching duration has expired.
- At least one of Employee, Guest, and Contractor Access must be provided.

Enforcement Type*:	Filter ID Based Enforcement
Captive Portal Access*:	guest-preauth
Days allowed for access*:	☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday
Maximum number of devices allowed per user*:	3
Maximum bandwidth allowed per user*:	0 MB (For unlimited bandwidth, set value to 0)
Employee Access:	employee
Guest Access:	guest
Contractor Access:	contractor

‹ Back to Service Templates & Wizards

As a final result, the above wizard will create two new Services on the Clearpass:



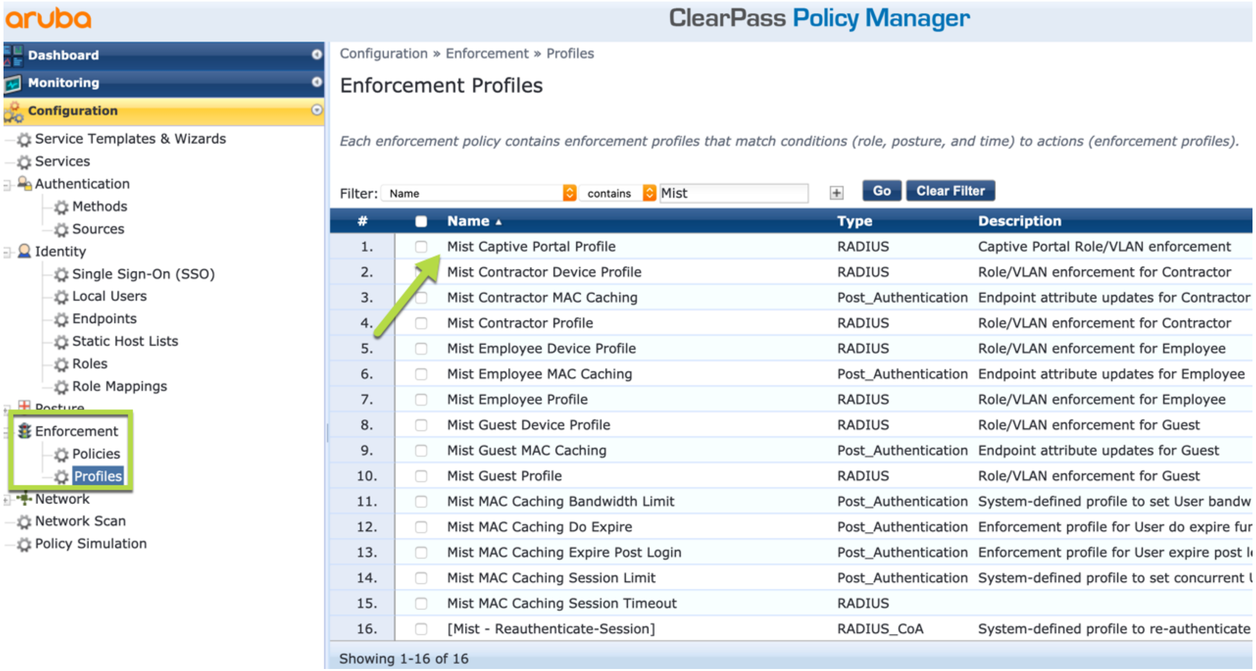
□	7	Mist MAC Authentication	RADIUS	MAC Authentication	✓
□	8	Mist User Authentication with MAC Caching	RADIUS	RADIUS Enforcement (Generic)	✓

Step 4: Edit Enforcement Profiles and Services to Integrate with Mist APs

In this section we will need to edit a few profiles and create one more service to finalize the integration.

First step is to edit the default Captive Portal profile and send url-redirect attribute back to the AP for unknown client connections.

Navigate to **Configuration → Enforcement → Enforcement Profiles → Edit** "Mist Captive Portal Profile":



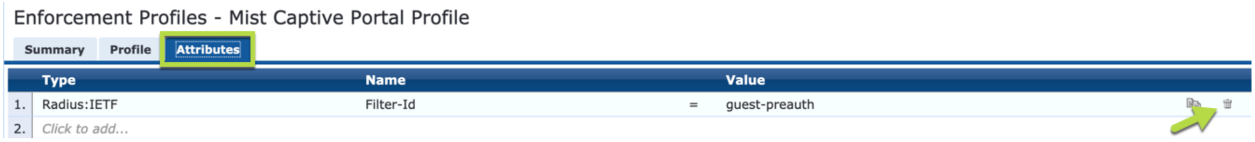
Enforcement Profiles

Each enforcement policy contains enforcement profiles that match conditions (role, posture, and time) to actions (enforcement profiles).

#	☐	Name ▲	Type	Description
1.	☐	Mist Captive Portal Profile	RADIUS	Captive Portal Role/VLAN enforcement
2.	☐	Mist Contractor Device Profile	RADIUS	Role/VLAN enforcement for Contractor
3.	☐	Mist Contractor MAC Caching	Post_Authentication	Endpoint attribute updates for Contractor
4.	☐	Mist Contractor Profile	RADIUS	Role/VLAN enforcement for Contractor
5.	☐	Mist Employee Device Profile	RADIUS	Role/VLAN enforcement for Employee
6.	☐	Mist Employee MAC Caching	Post_Authentication	Endpoint attribute updates for Employee
7.	☐	Mist Employee Profile	RADIUS	Role/VLAN enforcement for Employee
8.	☐	Mist Guest Device Profile	RADIUS	Role/VLAN enforcement for Guest
9.	☐	Mist Guest MAC Caching	Post_Authentication	Endpoint attribute updates for Guest
10.	☐	Mist Guest Profile	RADIUS	Role/VLAN enforcement for Guest
11.	☐	Mist MAC Caching Bandwidth Limit	Post_Authentication	System-defined profile to set User bandw
12.	☐	Mist MAC Caching Do Expire	Post_Authentication	Enforcement profile for User do expire fur
13.	☐	Mist MAC Caching Expire Post Login	Post_Authentication	Enforcement profile for User expire post l
14.	☐	Mist MAC Caching Session Limit	Post_Authentication	System-defined profile to set concurrent l
15.	☐	Mist MAC Caching Session Timeout	RADIUS	
16.	☐	[Mist - Reauthenticate-Session]	RADIUS_CoA	System-defined profile to re-authenticate

Showing 1-16 of 16

Delete existing filter-id attribute, we will not need it:



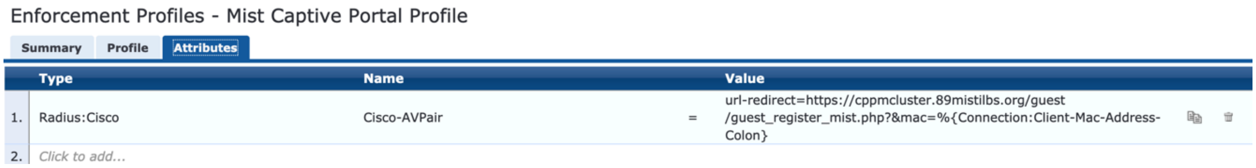
Enforcement Profiles - Mist Captive Portal Profile

	Type	Name		Value
1.	Radius:IETF	Filter-Id	=	guest-preauth
2.	*Click to add...*			

Add a new url-redirect attribute to let the AP know where a client needs to be redirected.

Follow this syntax when configuring Cisco-AVPair value:

```
url-redirect=https://<clearpass FQDN or IP>/guest/<guest-page-name>.php?&mac=%{Connection:Client-Mac-Address-Colon}
```

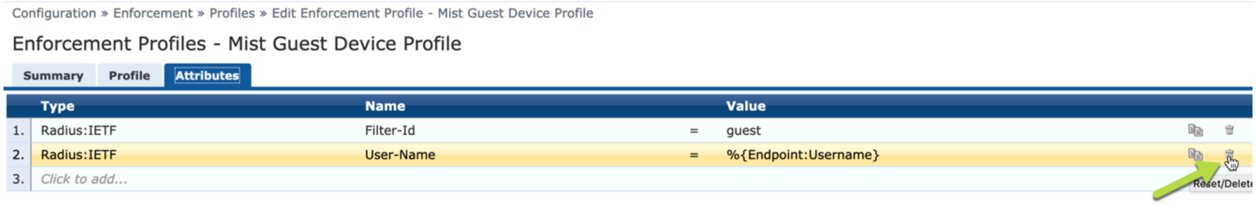


Enforcement Profiles - Mist Captive Portal Profile

	Type	Name		Value
1.	Radius:Cisco	Cisco-AVPair	=	url-redirect=https://cppmcluster.89mistilbs.org/guest /guest_register_mist.php?&mac=%{Connection:Client-Mac-Address-Colon}
2.	*Click to add...*			

Once the attribute is configured save changes.

Also, edit *Mist Guest Device Profile* and remove the last attribute that was pre-created during the wizard:

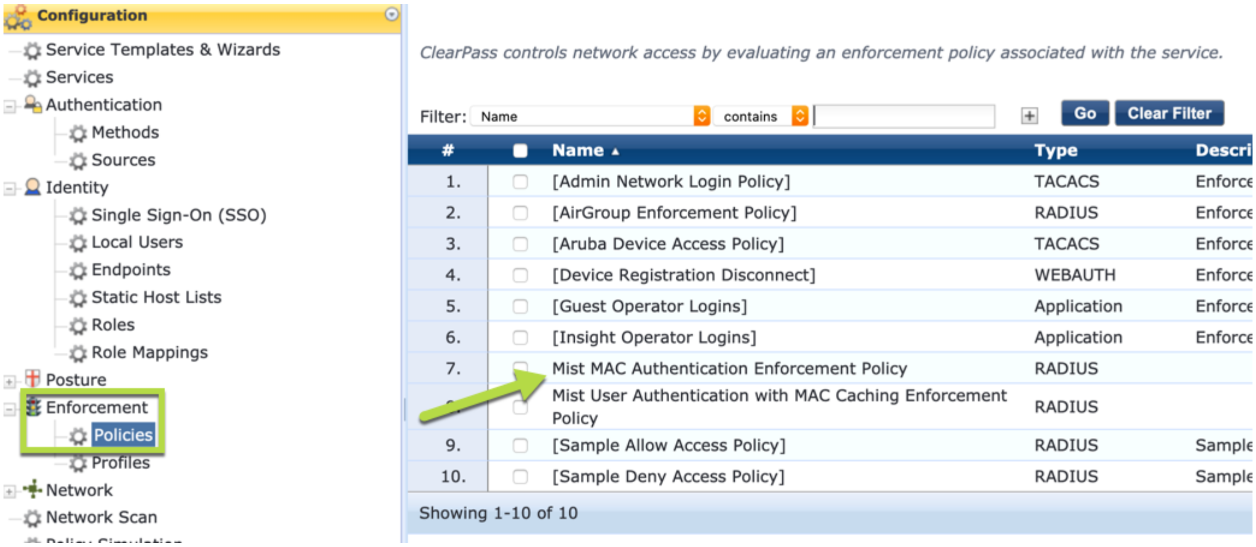


Configuration » Enforcement » Profiles » Edit Enforcement Profile - Mist Guest Device Profile

Enforcement Profiles - Mist Guest Device Profile

	Type	Name		Value
1.	Radius:IETF	Filter-Id	=	guest
2.	Radius:IETF	User-Name	=	%{Endpoint:Username}
3.	*Click to add...*			

Now navigate to **Configuration → Enforcement → Enforcement Policies → Edit** “Mist MAC Authentication Enforcement Policy”:



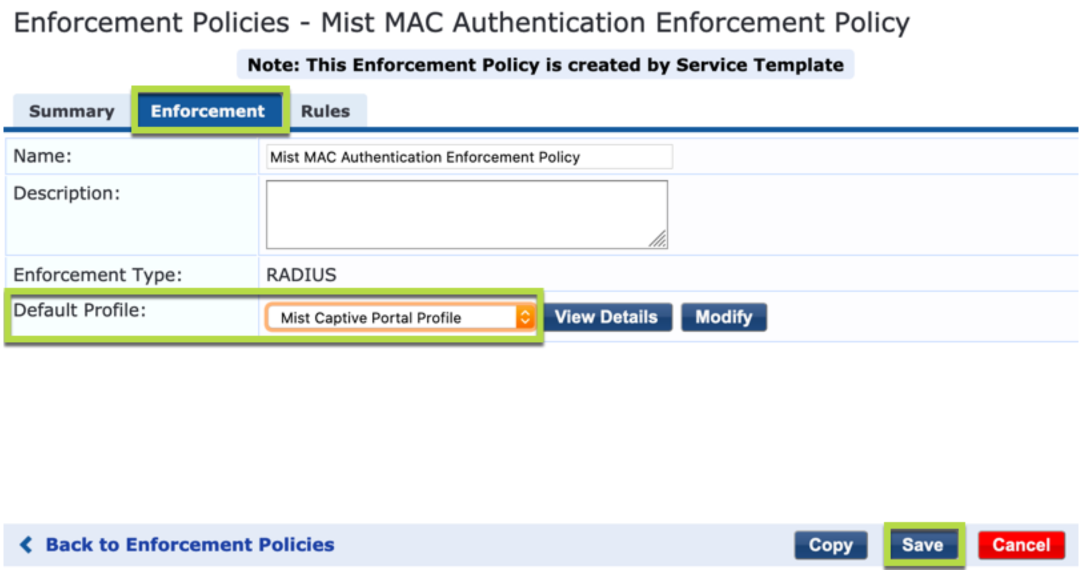
ClearPass controls network access by evaluating an enforcement policy associated with the service.

Filter: Name contains

#	☐	Name ▲	Type	Descri
1.	☐	[Admin Network Login Policy]	TACACS	Enforce
2.	☐	[AirGroup Enforcement Policy]	RADIUS	Enforce
3.	☐	[Aruba Device Access Policy]	TACACS	Enforce
4.	☐	[Device Registration Disconnect]	WEBAUTH	Enforce
5.	☐	[Guest Operator Logins]	Application	Enforce
6.	☐	[Insight Operator Logins]	Application	Enforce
7.	☐	Mist MAC Authentication Enforcement Policy	RADIUS	
8.	☐	Mist User Authentication with MAC Caching Enforcement Policy	RADIUS	
9.	☐	[Sample Allow Access Policy]	RADIUS	Sample
10.	☐	[Sample Deny Access Policy]	RADIUS	Sample

Showing 1-10 of 10

Go to Enforcement tab and change Default profile to use “Mist Captive Portal Profile” to send a redirect url for any unknown/unregistered client:



Enforcement Policies - Mist MAC Authentication Enforcement Policy

Note: This Enforcement Policy is created by Service Template

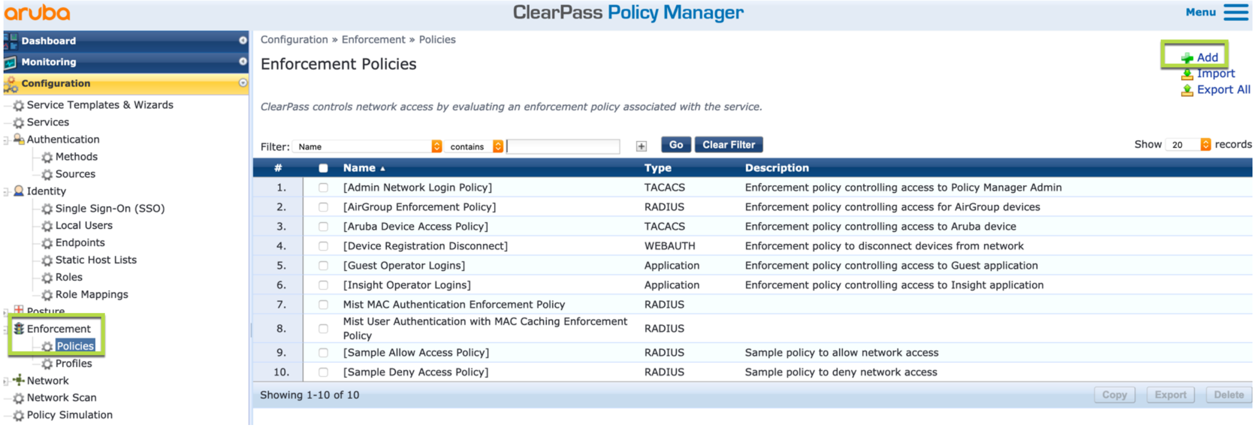
Name: Mist MAC Authentication Enforcement Policy

Description:

Enforcement Type: RADIUS

Default Profile: Mist Captive Portal Profile

At this stage, we need to create a new Enforcement Policy to handle guest user authentication via the captive portal hosted by the Clearpass. Navigate to **Configuration → Enforcement → Enforcement Policies → Add** new:



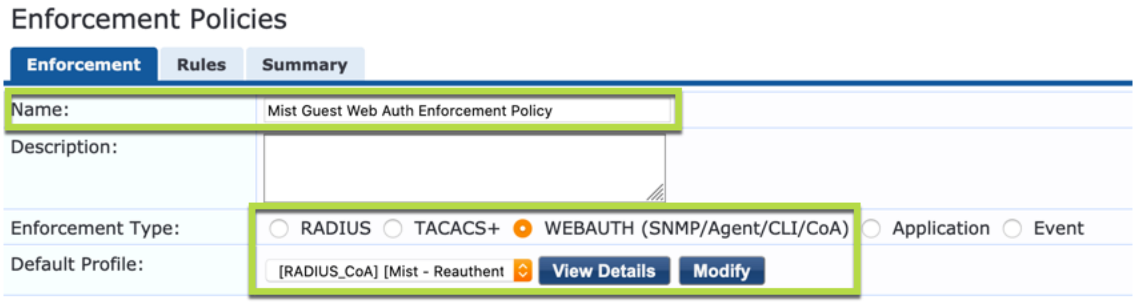
Enforcement Policies

ClearPass controls network access by evaluating an enforcement policy associated with the service.

#	Name ▲	Type	Description
1.	[Admin Network Login Policy]	TACACS	Enforcement policy controlling access to Policy Manager Admin
2.	[AirGroup Enforcement Policy]	RADIUS	Enforcement policy controlling access for AirGroup devices
3.	[Aruba Device Access Policy]	TACACS	Enforcement policy controlling access to Aruba device
4.	[Device Registration Disconnect]	WEBAUTH	Enforcement policy to disconnect devices from network
5.	[Guest Operator Logins]	Application	Enforcement policy controlling access to Guest application
6.	[Insight Operator Logins]	Application	Enforcement policy controlling access to Insight application
7.	Mist MAC Authentication Enforcement Policy	RADIUS	
8.	Mist User Authentication with MAC Caching Enforcement Policy	RADIUS	
9.	[Sample Allow Access Policy]	RADIUS	Sample policy to allow network access
10.	[Sample Deny Access Policy]	RADIUS	Sample policy to deny network access

Showing 1-10 of 10

Set type as "WEBAUTH", set default profile as [RADIUS_CoA] [Mist – Reauthenticate Session] and click next:



Enforcement Policies

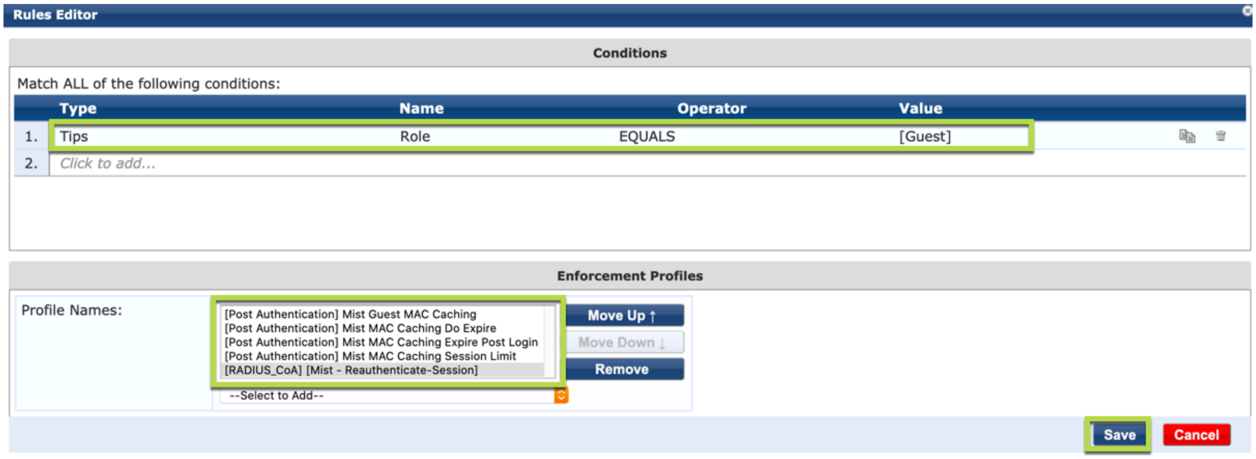
Name: Mist Guest Web Auth Enforcement Policy

Description:

Enforcement Type: ○ RADIUS ○ TACACS+ ● WEBAUTH (SNMP/Agent/CLI/CoA) ○ Application ○ Event

Default Profile: [RADIUS_CoA] [Mist - Reauthent

Create a rule to cache a client MAC once a user is authenticated as Guest for the duration specified on the guest manager settings:



Rules Editor

Conditions

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Tips	Role	EQUALS	[Guest]
2.	Click to add...			

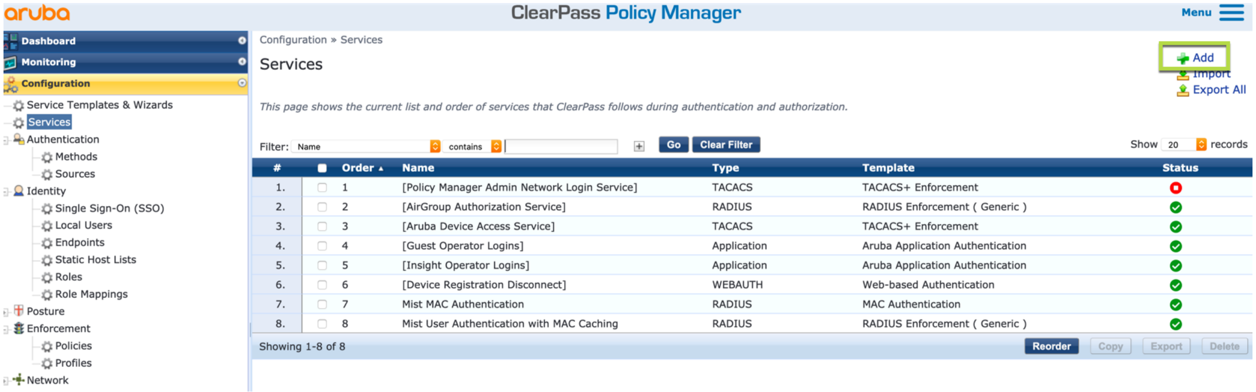
Enforcement Profiles

Profile Names:

[Post Authentication] Mist Guest MAC Caching
[Post Authentication] Mist MAC Caching Do Expire
[Post Authentication] Mist MAC Caching Expire Post Login
[Post Authentication] Mist MAC Caching Session Limit
[RADIUS_CoA] [Mist - Reauthenticate-Session]

--Select to Add--

Now navigate to **Configuration → Services** and create a new WebAuth Service:



Configuration » Services

Services

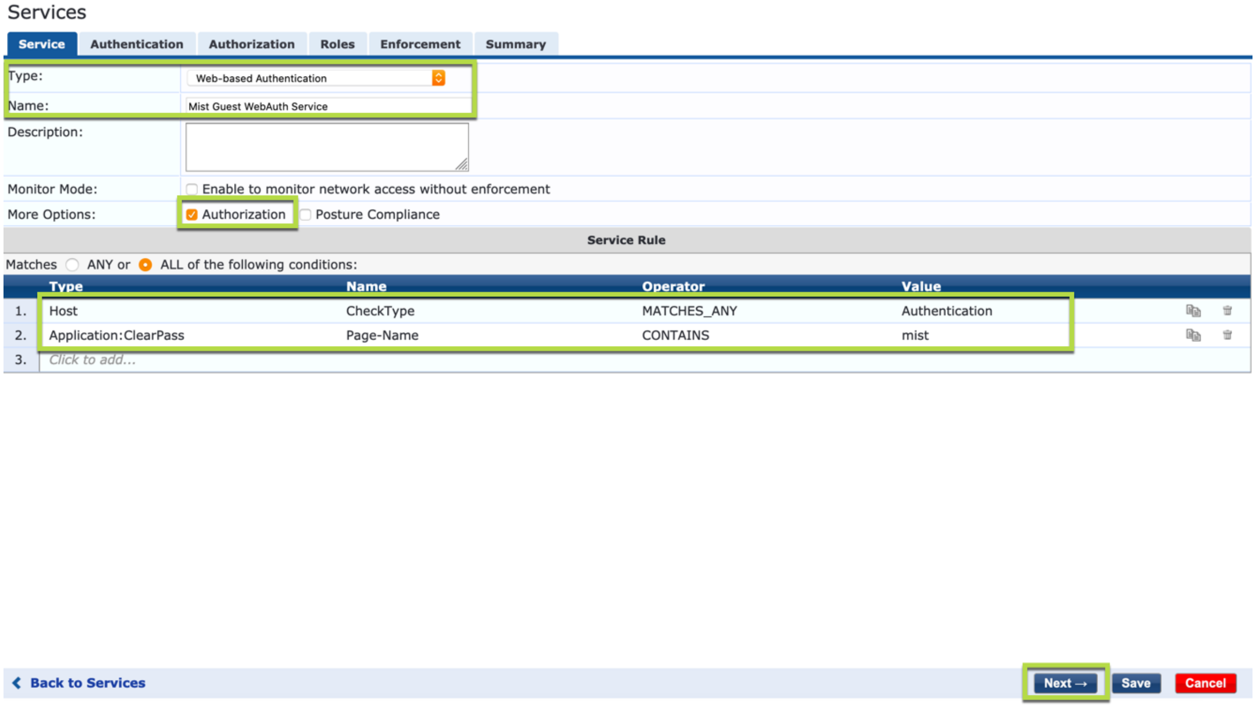
This page shows the current list and order of services that ClearPass follows during authentication and authorization.

Filter: Name contains Go Clear Filter Show 20 records

#		Order ▲	Name	Type	Template	Status
1.	□	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	●
2.	□	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	✓
3.	□	3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	✓
4.	□	4	[Guest Operator Logins]	Application	Aruba Application Authentication	✓
5.	□	5	[Insight Operator Logins]	Application	Aruba Application Authentication	✓
6.	□	6	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	✓
7.	□	7	Mist MAC Authentication	RADIUS	MAC Authentication	✓
8.	□	8	Mist User Authentication with MAC Caching	RADIUS	RADIUS Enforcement (Generic)	✓

Showing 1-8 of 8

Select **Web-Authentication** service type, enable **Authorization** checks, and add another condition to match on the guest page name that contains "mist" in its name. The last condition is optional, but it will help differentiate between different services in a large production deployment:



Type: Web-based Authentication

Name: Mist Guest WebAuth Service

Description:

Monitor Mode: □ Enable to monitor network access without enforcement

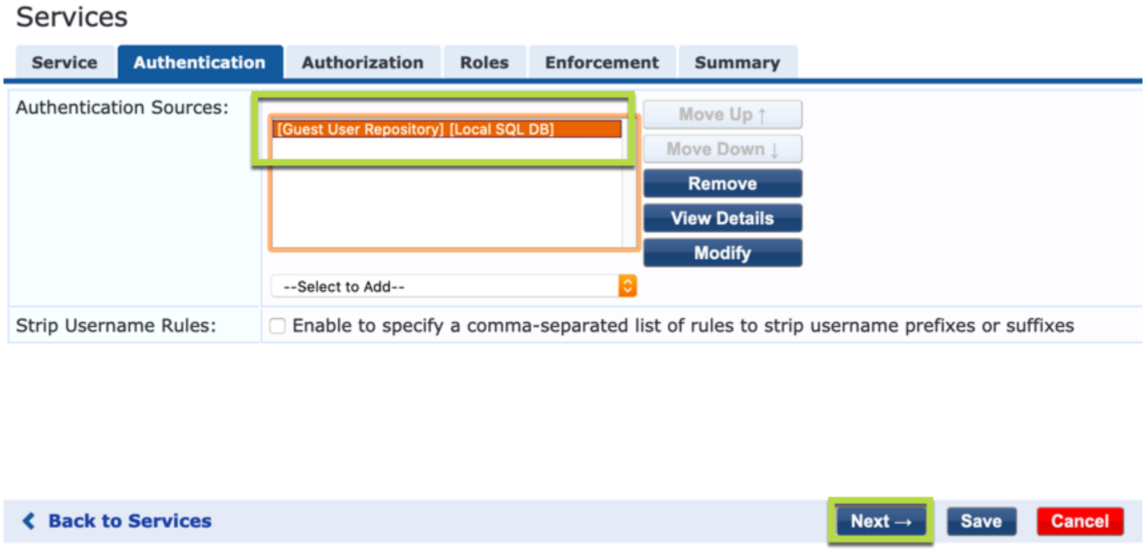
More Options: ☑ Authorization □ Posture Compliance

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Host	CheckType	MATCHES_ANY	Authentication
2.	Application:ClearPass	Page-Name	CONTAINS	mist
3.	*Click to add...*			

Select [Guest User Repository] as your authentication source and click next:

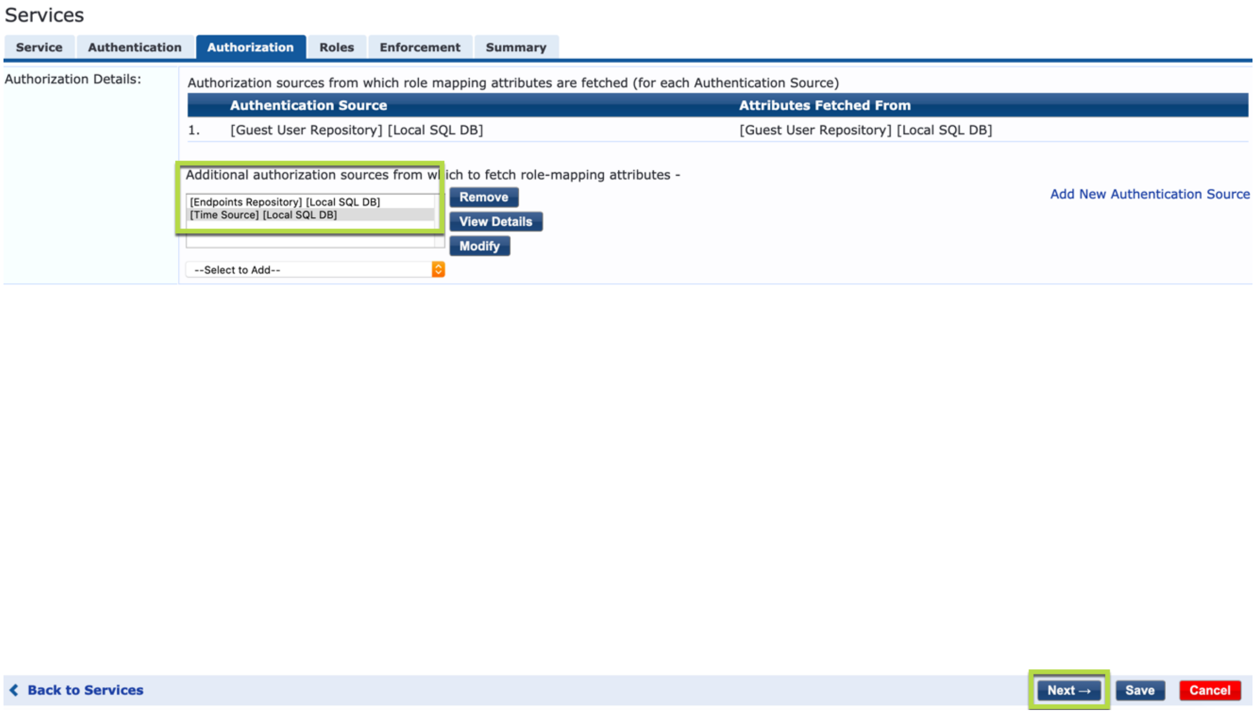


Authentication Sources: [Guest User Repository] [Local SQL DB]

--Select to Add--

Strip Username Rules: □ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

Under Authorization tab, add [Endpoints Repository] and [Time Source] as additional authorization sources and click next:



Services

Authorization Details:

Authorization sources from which role mapping attributes are fetched (for each Authentication Source)

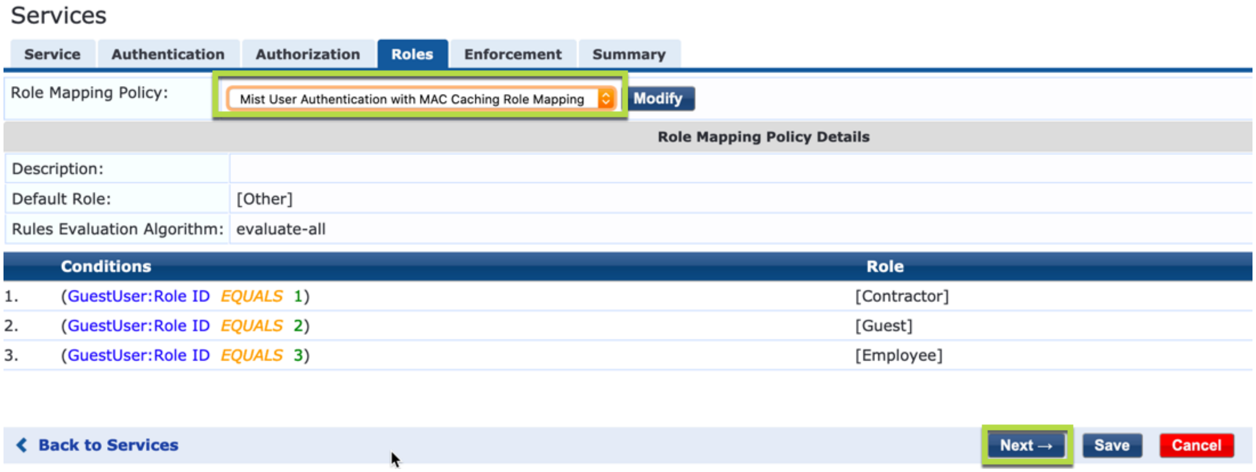
	Authentication Source	Attributes Fetched From
1.	[Guest User Repository] [Local SQL DB]	[Guest User Repository] [Local SQL DB]

Additional authorization sources from which to fetch role-mapping attributes -

[Endpoints Repository] [Local SQL DB]
[Time Source] [Local SQL DB]

--Select to Add--

Under Roles tab, select pre-created “Mist User Authentication with MAC Caching Role Mapping” policy and click next:



Services

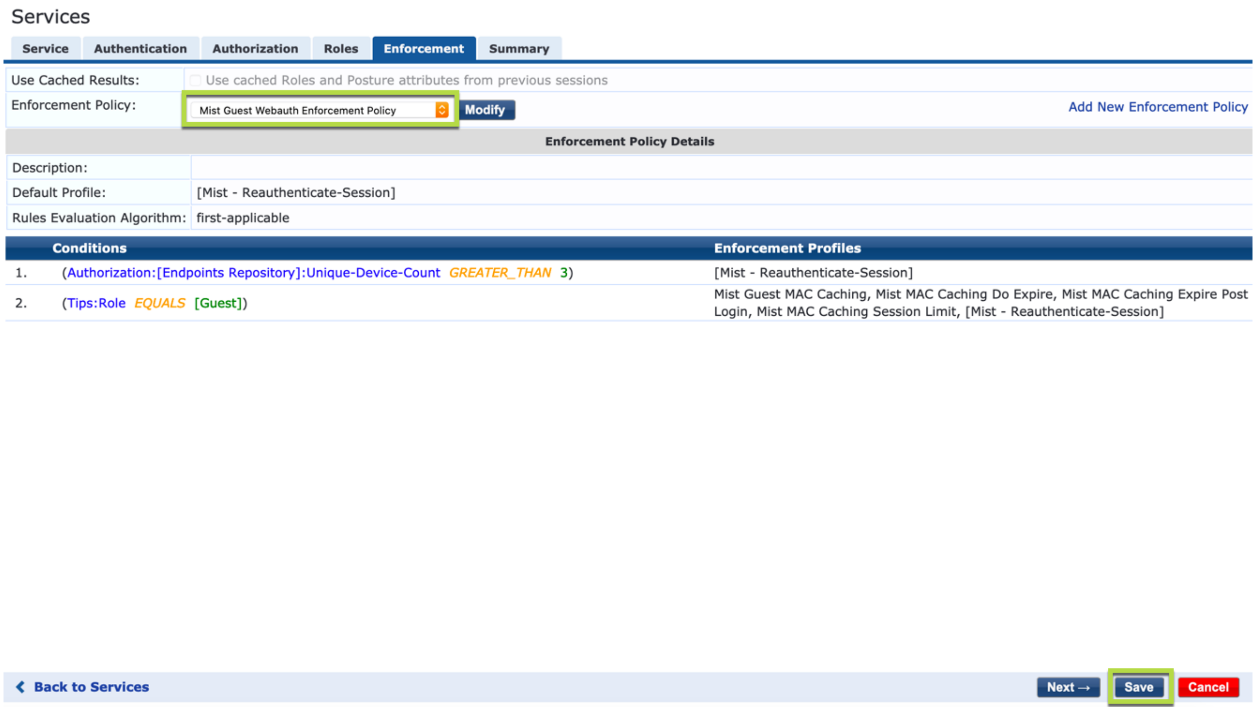
Role Mapping Policy: Mist User Authentication with MAC Caching Role Mapping

Role Mapping Policy Details

Description:	
Default Role:	[Other]
Rules Evaluation Algorithm:	evaluate-all

	Conditions	Role
1.	(GuestUser:Role ID EQUALS 1)	[Contractor]
2.	(GuestUser:Role ID EQUALS 2)	[Guest]
3.	(GuestUser:Role ID EQUALS 3)	[Employee]

Now select the enforcement policy that we created in the previous step and click save:



Use Cached Results: □ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Mist Guest Webauth Enforcement Policy

Enforcement Policy Details

Description:

Default Profile: [Mist - Reauthenticate-Session]

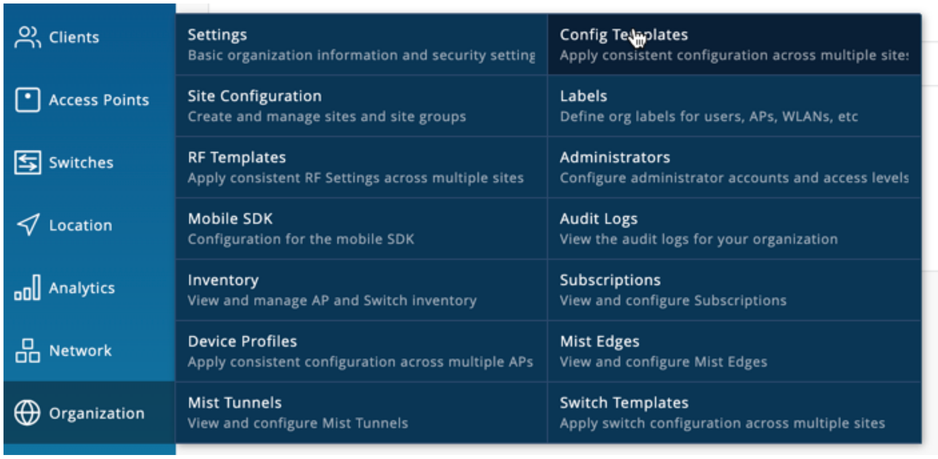
Rules Evaluation Algorithm: first-applicable

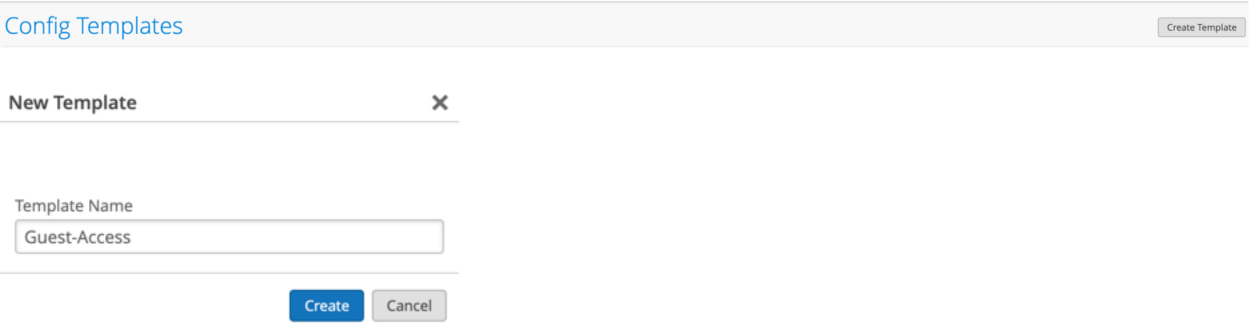
	Conditions	Enforcement Profiles
1.	(Authorization:[Endpoints Repository]:Unique-Device-Count *GREATER_THAN* 3)	[Mist - Reauthenticate-Session]
2.	(Tips:Role *EQUALS* [Guest])	Mist Guest MAC Caching, Mist MAC Caching Do Expire, Mist MAC Caching Expire Post Login, Mist MAC Caching Session Limit, [Mist - Reauthenticate-Session]

Section 2: Mist Configuration

Create a Config Template

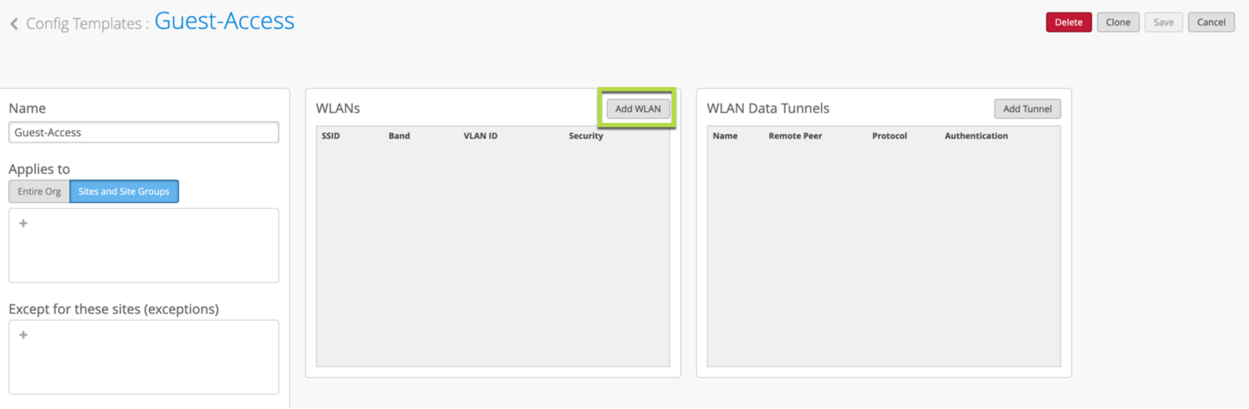
Navigate to Organization → Config Templates → Create New


Clients
Access Points
Switches
Location
Analytics
Network
Organization
Settings
Basic organization information and security setting
Config Templates
Apply consistent configuration across multiple sites
Site Configuration
Create and manage sites and site groups
Labels
Define org labels for users, APs, WLANs, etc
RF Templates
Apply consistent RF Settings across multiple sites
Administrators
Configure administrator accounts and access levels
Mobile SDK
Configuration for the mobile SDK
Audit Logs
View the audit logs for your organization
Inventory
View and manage AP and Switch inventory
Subscriptions
View and configure Subscriptions
Device Profiles
Apply consistent configuration across multiple APs
Mist Edges
View and configure Mist Edges
Mist Tunnels
View and configure Mist Tunnels
Switch Templates
Apply switch configuration across multiple sites



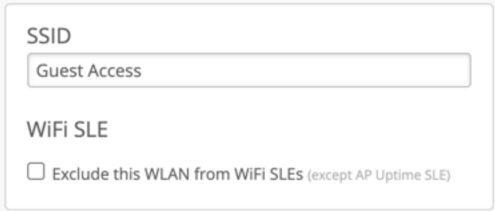
Template Name: Guest-Access

Add a WLAN within a template and assign the same SSID name you configured in the first Step on the Clearpass:



Name: Guest-Access

Applies to: Entire Org | [✓ Sites and Site Groups]



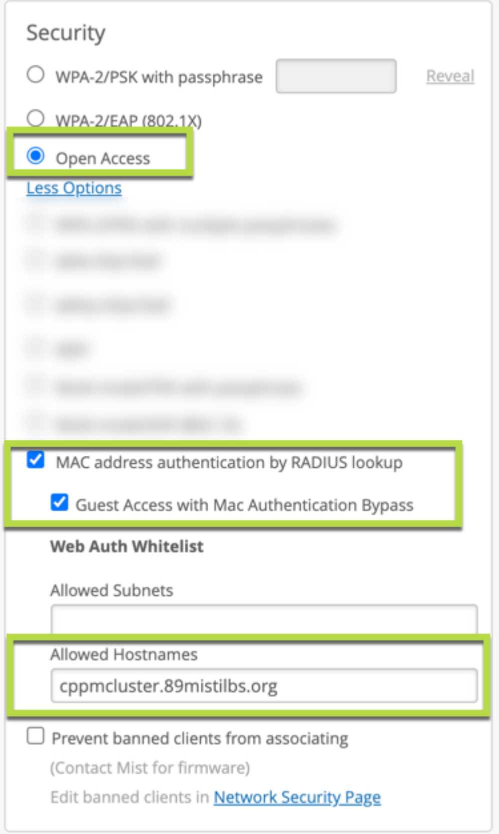
SSID

Guest Access

WiFi SLE

☐ Exclude this WLAN from WiFi SLEs (except AP Uptime SLE)

Under Allowed Hostnames field add the FQDN of the clearpass server where a guest user will be redirected to, and any additional FQDNs that need to be allowed before the user is authenticated:



Security

○ WPA-2/PSK with passphrase

○ WPA-2/EAP (802.1X)

● Open Access

☑ MAC address authentication by RADIUS lookup

☑ Guest Access with Mac Authentication Bypass

Web Auth Whitelist

Allowed Subnets

Allowed Hostnames

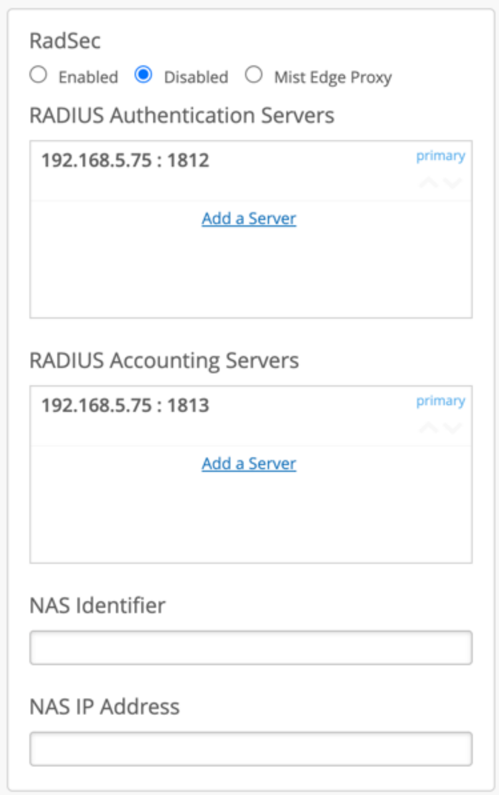
cppmcluster.89mistilbs.org

☐ Prevent banned clients from associating

(Contact Mist for firmware)

Edit banned clients in Network Security Page

Provide the IP address and Secret of the Clearpass server(s):



RadSec

○ Enabled ● Disabled ○ Mist Edge Proxy

RADIUS Authentication Servers

192.168.5.75 : 1812 primary

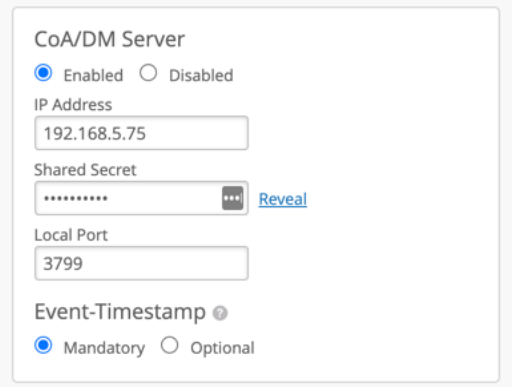
RADIUS Accounting Servers

192.168.5.75 : 1813 primary

NAS Identifier

NAS IP Address

Configure Clearpass server as allowed CoA server:



CoA/DM Server

● Enabled ○ Disabled

IP Address: 192.168.5.75

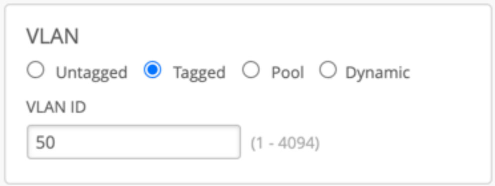
Shared Secret: ••••••••••

Local Port: 3799

Event-Timestamp

● Mandatory ○ Optional

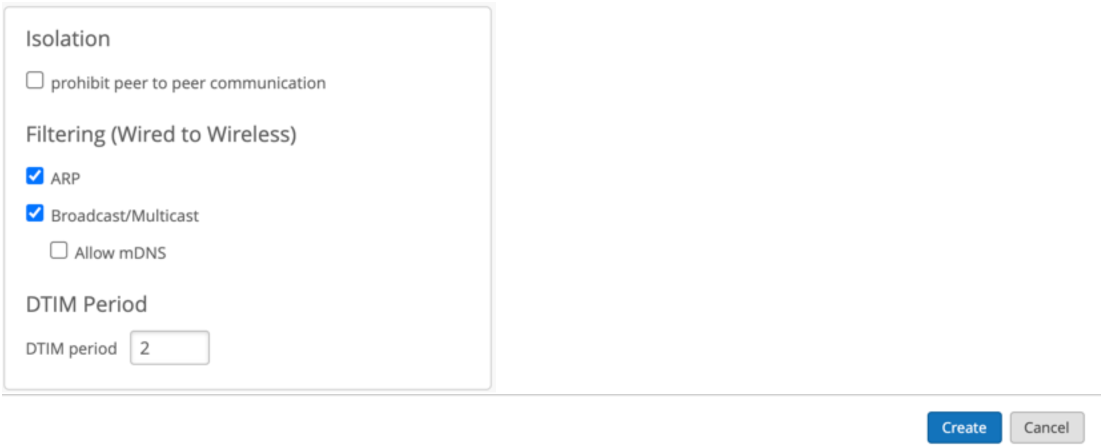
Optionally configure guest VLAN, filters etc.



VLAN

○ Untagged ● Tagged ○ Pool ○ Dynamic

VLAN ID: 50 (1 - 4094)



Isolation

□ prohibit peer to peer communication

Filtering (Wired to Wireless)

☑ ARP

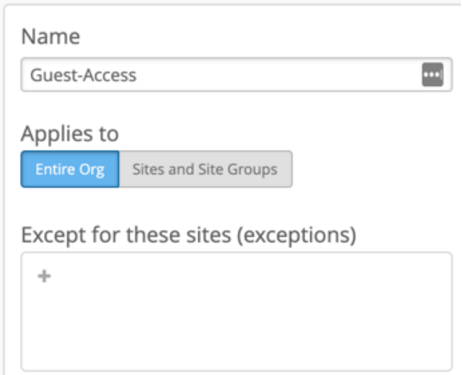
☑ Broadcast/Multicast

□ Allow mDNS

DTIM Period

DTIM period: 2

Next, assign your template to a specific Site or entire Org:

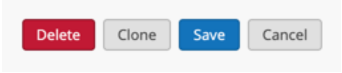


Name: Guest-Access

Applies to: [✓ Entire Org] Sites and Site Groups

Except for these sites (exceptions)

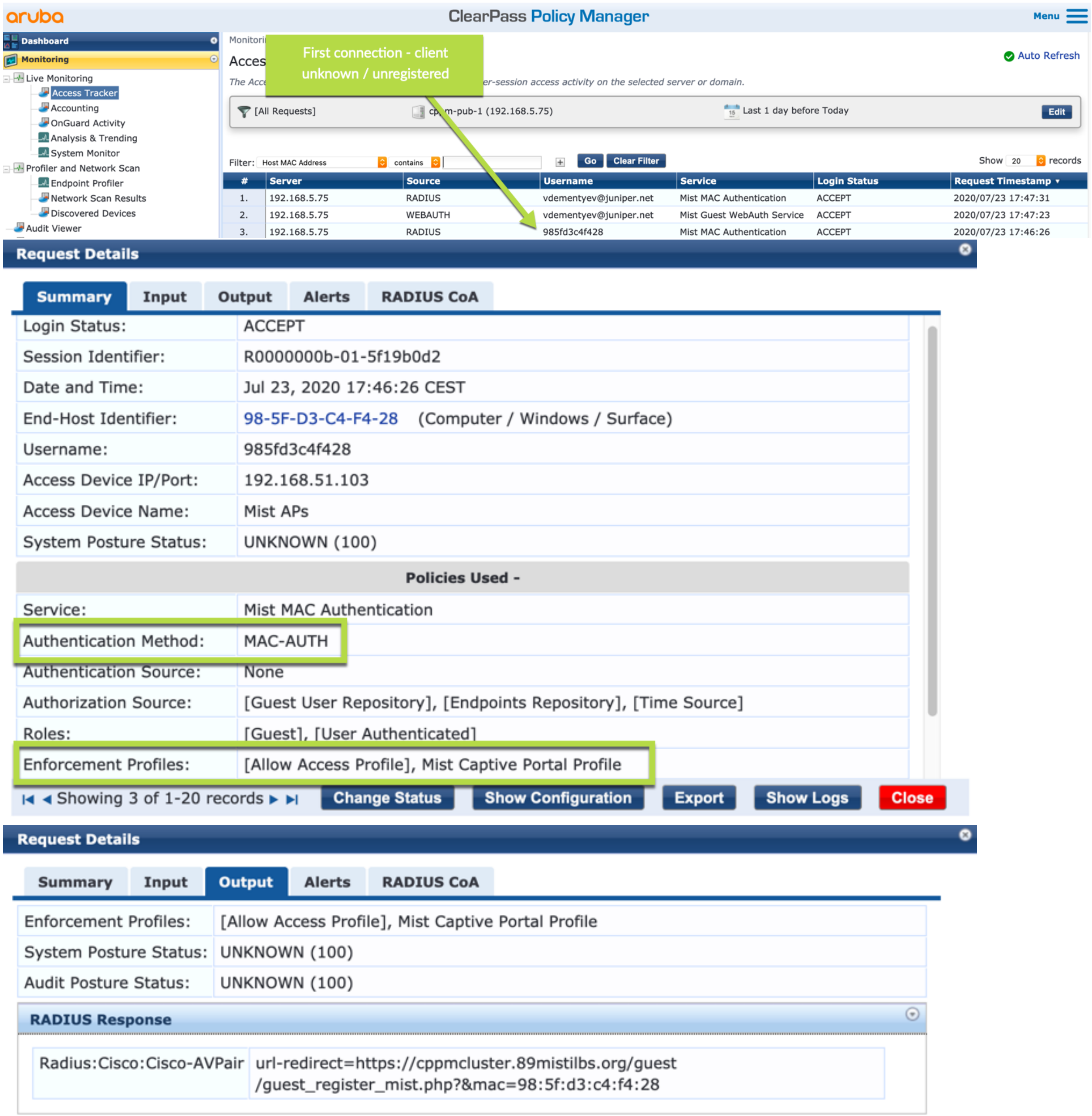
And hit Save:



Section 3: Verification

To verify navigate to the **Monitoring → Live Monitoring → Access Tracking**:

For a working flow you will see three records.
First, is a MAC Auth with a Username = Client MAC, where the client is unknown:



First connection - client unknown / unregistered

#	Server	Source	Username	Service	Login Status	Request Timestamp ▾
1.	192.168.5.75	RADIUS	vdementyev@juniper.net	Mist MAC Authentication	ACCEPT	2020/07/23 17:47:31
2.	192.168.5.75	WEBAUTH	vdementyev@juniper.net	Mist Guest WebAuth Service	ACCEPT	2020/07/23 17:47:23
3.	192.168.5.75	RADIUS	985fd3c4f428	Mist MAC Authentication	ACCEPT	2020/07/23 17:46:26

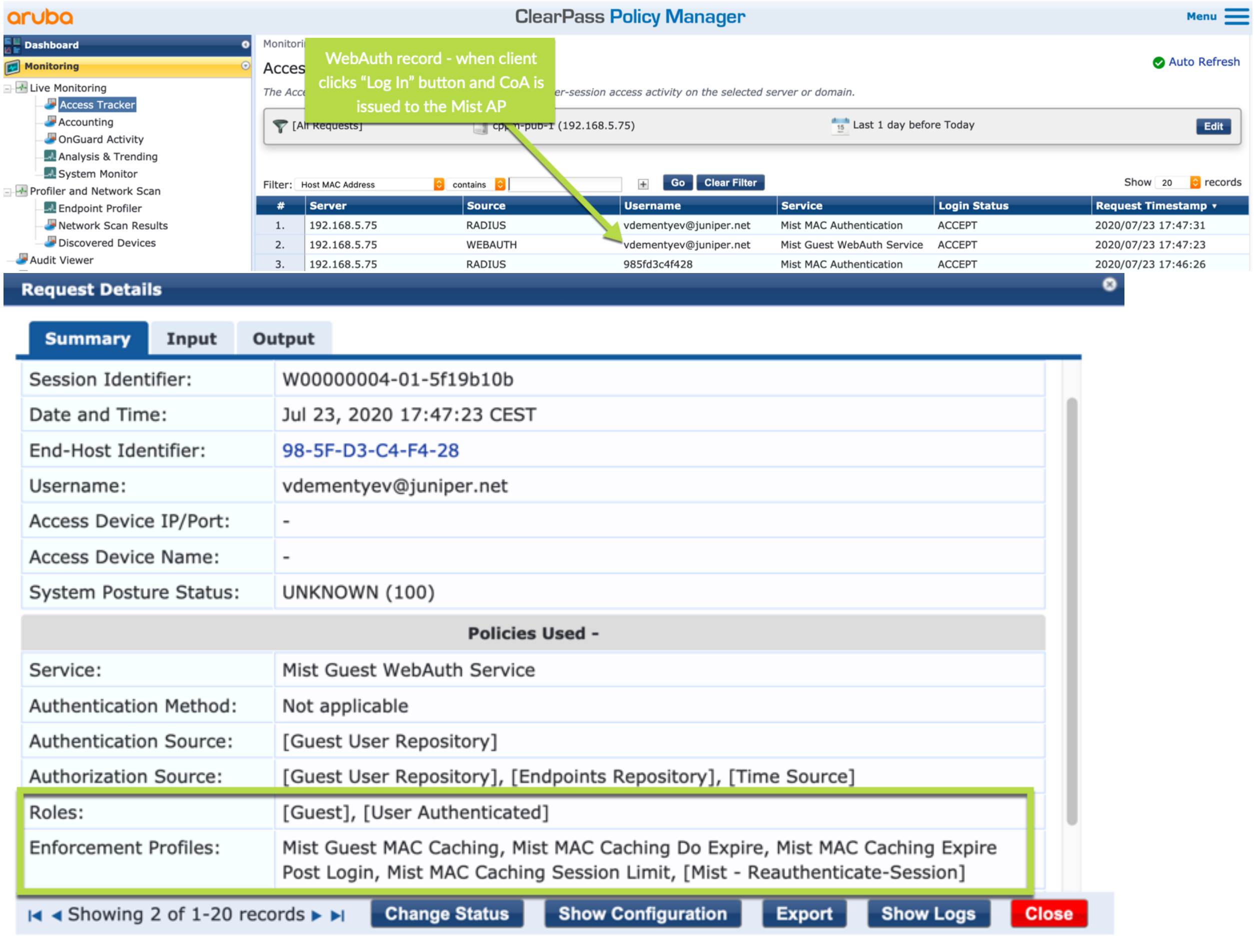
Login Status:	ACCEPT
Session Identifier:	R0000000b-01-5f19b0d2
Date and Time:	Jul 23, 2020 17:46:26 CEST
End-Host Identifier:	98-5F-D3-C4-F4-28 (Computer / Windows / Surface)
Username:	985fd3c4f428
Access Device IP/Port:	192.168.51.103
Access Device Name:	Mist APs
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	Mist MAC Authentication
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Guest User Repository], [Endpoints Repository], [Time Source]
Roles:	[Guest], [User Authenticated]
Enforcement Profiles:	[Allow Access Profile], Mist Captive Portal Profile

Enforcement Profiles:	[Allow Access Profile], Mist Captive Portal Profile
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Cisco:Cisco-AVPair	url-redirect=https://cppmcluster.89mistilbs.org/guest/guest_register_mist.php?&mac=98:5f:d3:c4:f4:28

After client has completed guest login/registration, WebAuth service will trigger that will update client record on the Clearpass and issue a CoA to the Mist AP to reauthenticate the client:



WebAuth record - when client clicks "Log In" button and CoA is issued to the Mist AP

The Acc er-session access activity on the selected server or domain.

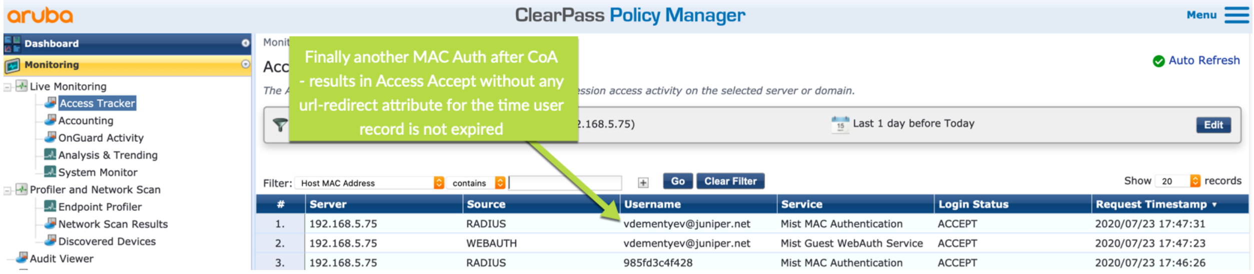
[All Requests] cp -pub-1 (192.168.5.75) Last 1 day before Today

#	Server	Source	Username	Service	Login Status	Request Timestamp ▾
1.	192.168.5.75	RADIUS	vdementyev@juniper.net	Mist MAC Authentication	ACCEPT	2020/07/23 17:47:31
2.	192.168.5.75	WEBAUTH	vdementyev@juniper.net	Mist Guest WebAuth Service	ACCEPT	2020/07/23 17:47:23
3.	192.168.5.75	RADIUS	985fd3c4f428	Mist MAC Authentication	ACCEPT	2020/07/23 17:46:26

Request Details

Session Identifier:	W00000004-01-5f19b10b
Date and Time:	Jul 23, 2020 17:47:23 CEST
End-Host Identifier:	98-5F-D3-C4-F4-28
Username:	vdementyev@juniper.net
Access Device IP/Port:	-
Access Device Name:	-
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	Mist Guest WebAuth Service
Authentication Method:	Not applicable
Authentication Source:	[Guest User Repository]
Authorization Source:	[Guest User Repository], [Endpoints Repository], [Time Source]
Roles:	[Guest], [User Authenticated]
Enforcement Profiles:	Mist Guest MAC Caching, Mist MAC Caching Do Expire, Mist MAC Caching Expire Post Login, Mist MAC Caching Session Limit, [Mist - Reauthenticate-Session]

After WebAuth is triggered and CoA is sent to the AP, there is a new MAC-Auth request that results in a simple access accept without any url-redirect inside:

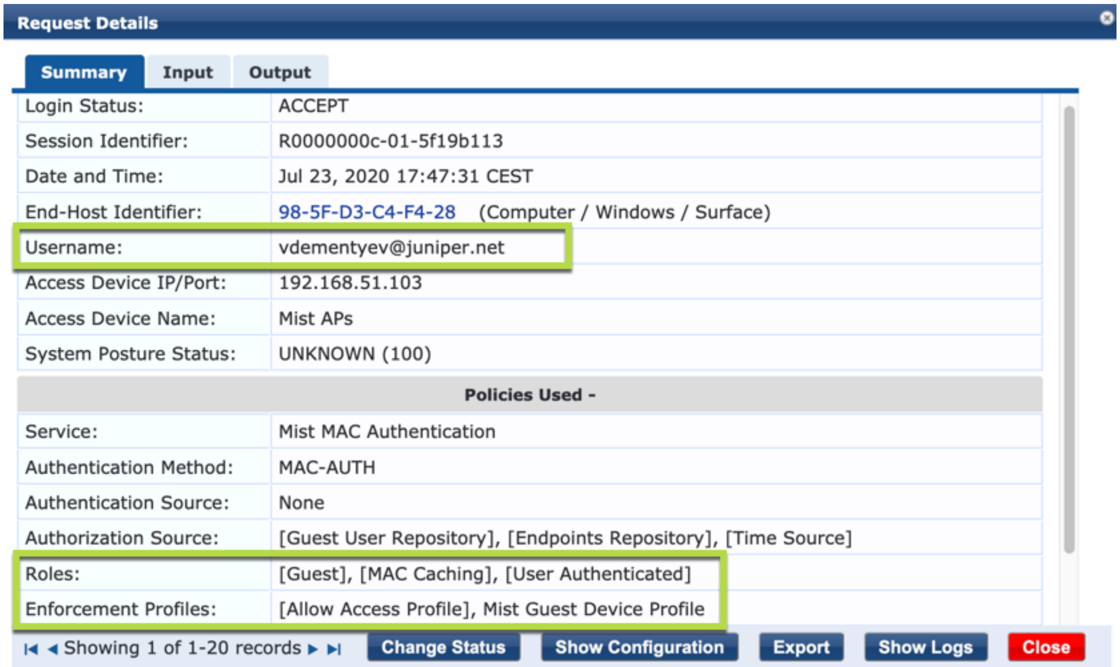


Finally another MAC Auth after CoA - results in Access Accept without any url-redirect attribute for the time user record is not expired

The A ession access activity on the selected server or domain.

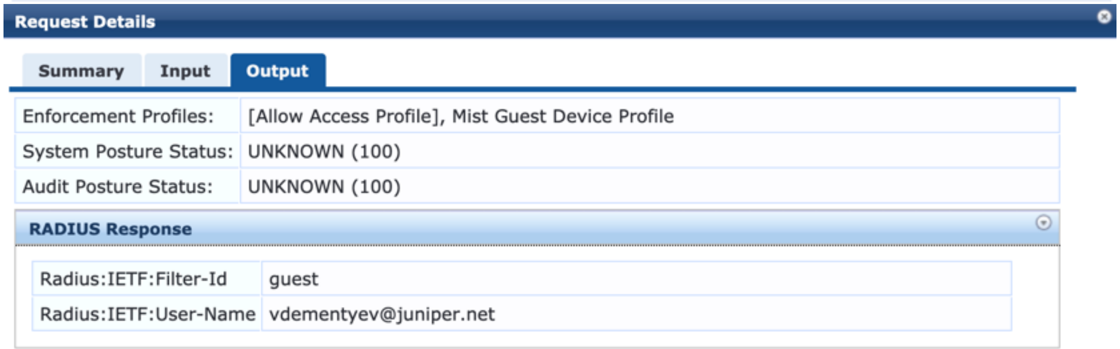
.168.5.75) Last 1 day before Today

#	Server	Source	Username	Service	Login Status	Request Timestamp ▾
1.	192.168.5.75	RADIUS	vdementyev@juniper.net	Mist MAC Authentication	ACCEPT	2020/07/23 17:47:31
2.	192.168.5.75	WEBAUTH	vdementyev@juniper.net	Mist Guest WebAuth Service	ACCEPT	2020/07/23 17:47:23
3.	192.168.5.75	RADIUS	985fd3c4f428	Mist MAC Authentication	ACCEPT	2020/07/23 17:46:26



Request Details

Login Status:	ACCEPT
Session Identifier:	R0000000c-01-5f19b113
Date and Time:	Jul 23, 2020 17:47:31 CEST
End-Host Identifier:	98-5F-D3-C4-F4-28 (Computer / Windows / Surface)
Username:	vdementyev@juniper.net
Access Device IP/Port:	192.168.51.103
Access Device Name:	Mist APs
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	Mist MAC Authentication
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Guest User Repository], [Endpoints Repository], [Time Source]
Roles:	[Guest], [MAC Caching], [User Authenticated]
Enforcement Profiles:	[Allow Access Profile], Mist Guest Device Profile



Request Details

Enforcement Profiles:	[Allow Access Profile], Mist Guest Device Profile
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:IETF:Filter-Id	guest
Radius:IETF:User-Name	vdementyev@juniper.net