Configure Guest Flow with ISE 2.0 and Aruba WLC

Contents

Introduction

This document descrbies steps to configure guest portals with Aruba Wireless LAN Controller (WLC). From Identity Services Engine (ISE) version 2.0 support for third party Network Access Devices (NAD) is introduced. ISE currently supports integration with Aruba Wireless for Guest, Posture and Bring Your Own Device (BYOD) flows.

> **Note**: Cisco is not responsible for configuration or support for devices from other vendors.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

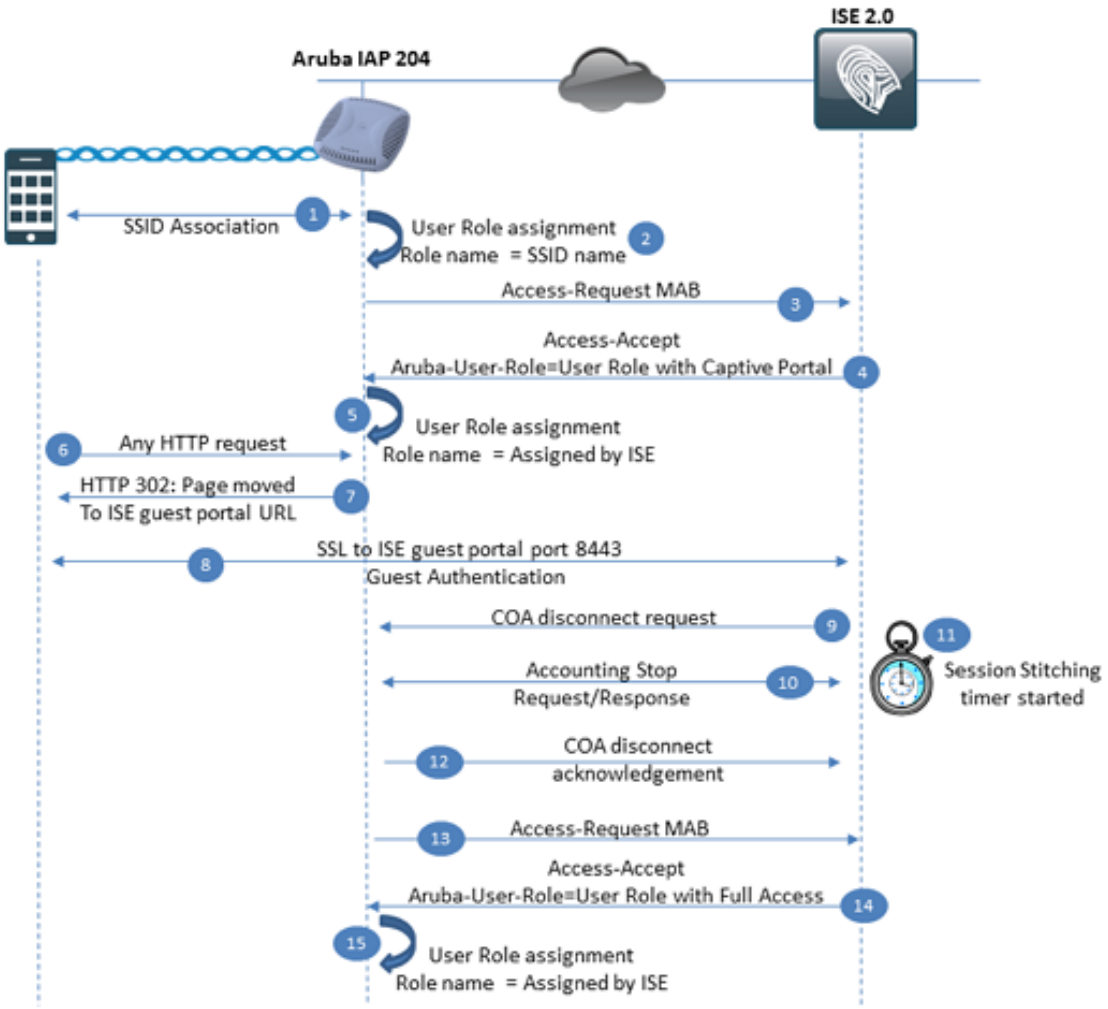
- Aruba IAP configuration
- Guest flow on ISE

Components Used

- Aruba IAP 204 software 6.4.2.3
- Cisco Identity Services Engine 2.0

Background Information

Guest Flow



Step 1. User is associated to the Service Set Identifer (SSID). SSID can be configured as open or with pre-shared key authentication.

Step 2. Aruba applies User-Role to this connection. First user-role is always SSID itself. User-role contains different settings like VLAN, Access-Control restriction, Captive-Portal setting and more. In current example default user-role assigned to SSID has only Permit-All statement.

Step 3. SSID is configured to provide MAC filtering over external radius server. Radius MAB (MAC Authentication Bypass) access-request is sent to ISE.

Step 4. At policy evaluation time ISE selects authorization profile for Guest. This authorization profile contains Access Type equal to ACCESS_ACCEPT and Aruba-User-Role equal to User-Role name configured locally on Aruba WLC (Wireless LAN Controller). This user role is configured for Captive-Portal and traffic is redirected towards ISE.

Aruba User-Roles

Main component that is used by Aruba WLC is User-Role. User-Role defines access restriction applicable to user at the time of connection. Access restriction can include: Captive Portal redirection, Access Control List, VLAN (Virtual Local Area Network), Bandwidth limitation and others. Every SSID that exists on Aruba WLC has default User-Role where User-Role is equal to SSID name, all users connected to specific SSID initially get restrictions from default role. User-Role can be overwritten by Radius server, in this case Access-Accept should contain Aruba Vendor specific attribute Aruba-User-Role. Value from this attribute is used by WLC to find local user-role.

Step 5. With attribute Aruba-User-Role WLC checks locally for configured user roles and applies required one.

Step 6. User initiates HTTP request in the browser.

Step 7. Aruba WLC intercepts request because of user-role configured for Captive portal. As a response to this request WLC returns HTTP Code 302 Page moved with the ISE guest portal as a new location.

Step 8. User establishes SSL connection to ISE on port 8443, and provides username/password in guest portal.

Step 9. ISE sends COA disconnect request message to Aruba WLC.

Step 10. After COA disconnect message WLC drops connection with user and informs ISE that connection should be terminated using Radius Accounting-Request (Stop) message. ISE has to confirm that this message has been received with Accounting.

Step 11. ISE starts Session Stitching timer. This timer is used to bind session before and after COA together. During this time ISE remembers all session parameters like username, etc. Second authentication attempt must be done before this timer expire to select correct Authorization policy for client. In case if timer expires, new Access-Request will be interpreted as a completely new session and authorization policy with Guest Redirect will be applied again.

Step 12. Aruba WLC confirms previously received COA disconnect request with COA disconnect acknowledgement.

Step 13. Aruba WLC sends new MAB Radius Access-Request.

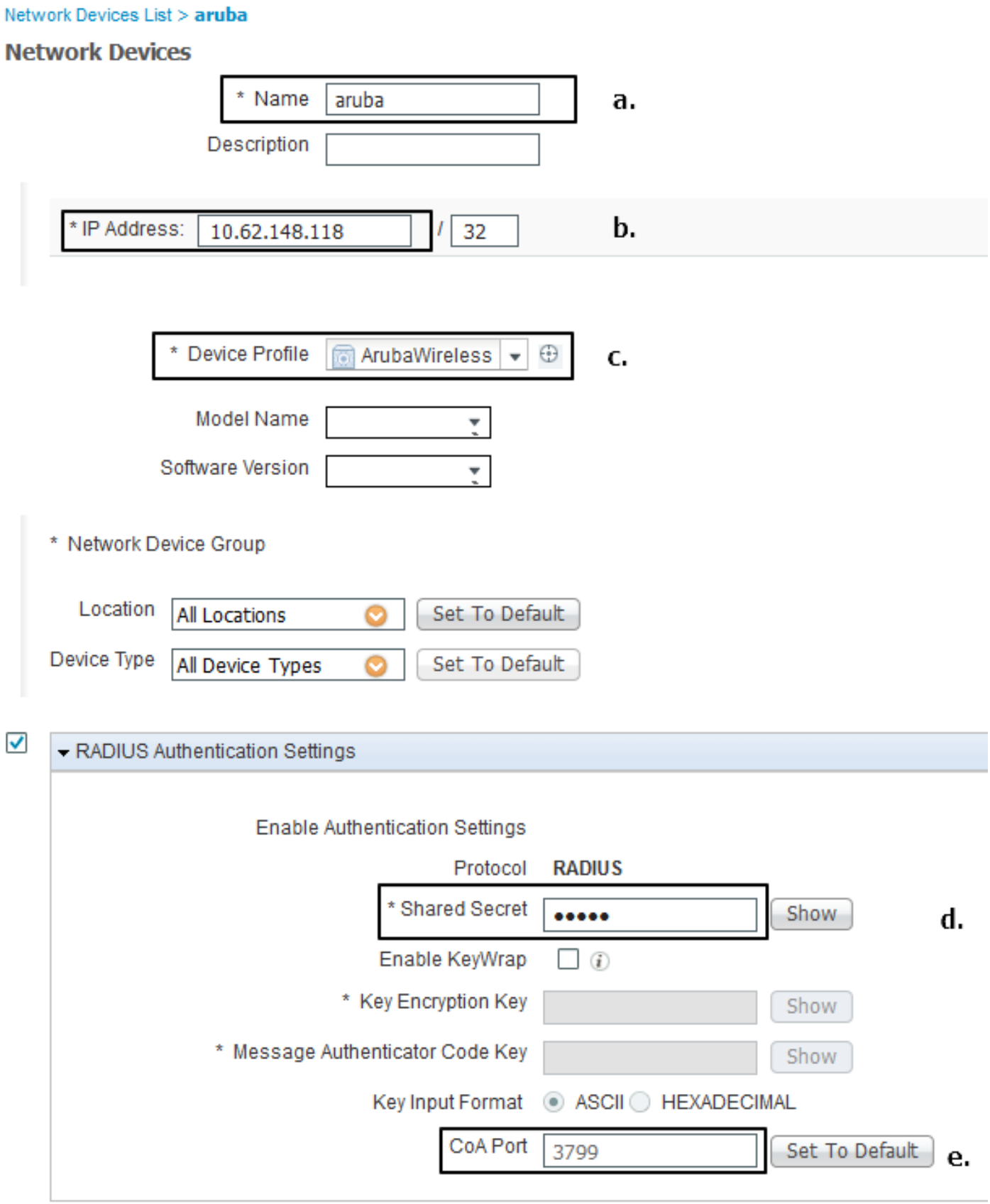
Step 14. At policy evaluation time ISE selects authorization profile for Guest after authentication. This authorization profile contains Access Type equal to ACCESS_ACCEPT and Aruba-User-Role equal to User-Role name configured locally on Aruba WLC. This user role configured to permit all traffic.

Step 15. With attribute Aruba-User-Role WLC checks locally configured user roles and applies required one.

Configure

Step 1. Add Aruba WLC as NAD in ISE.

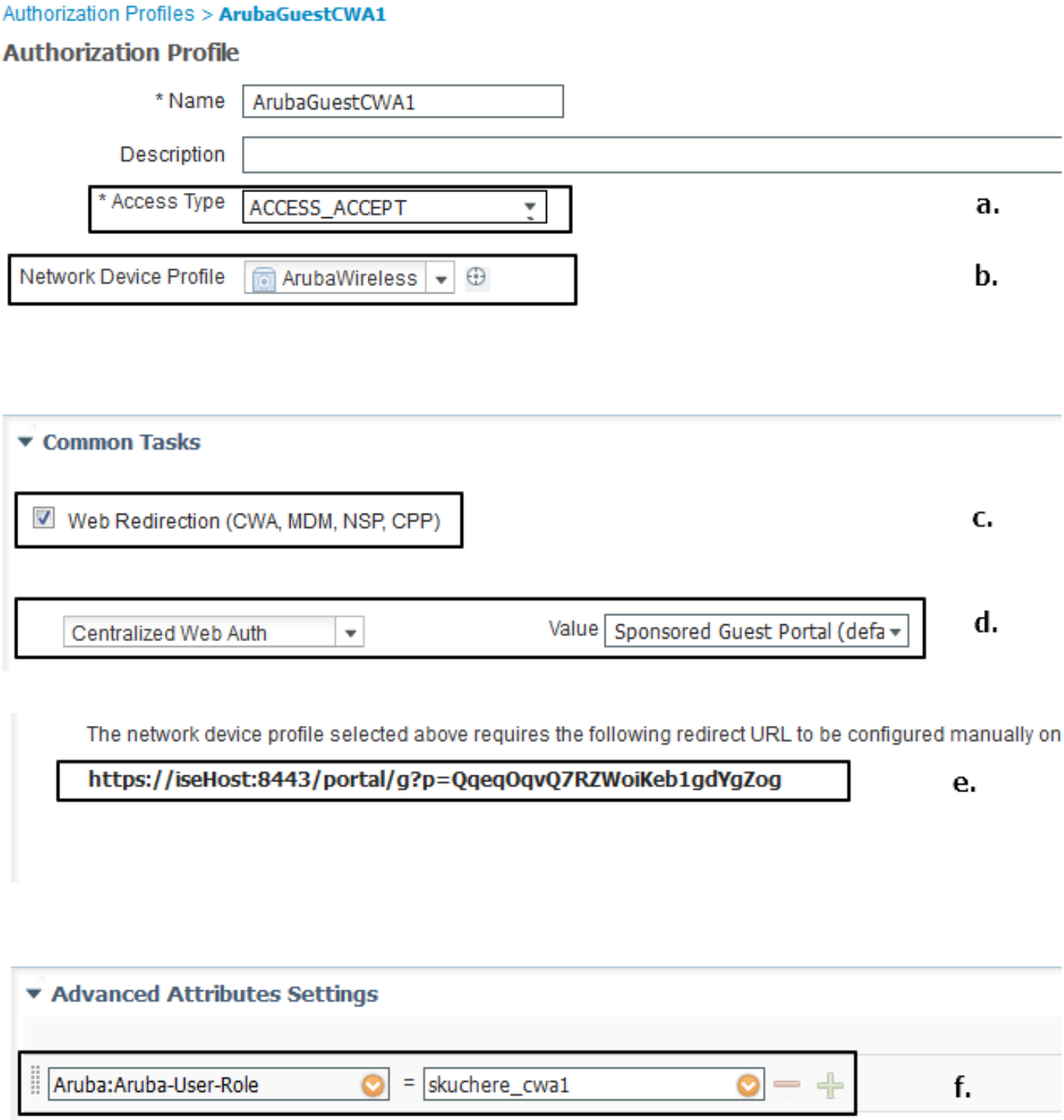
Navigate to **Administration > Network Resources > Network Devices** and click **Add**



1. Provide Network Access Device (NAD) name.
2. Specify NAD IP address.
3. Choose Network Device Profile. For Aruba WLC you may use built-in profile ArubaWireless.
4. Provide pre-shared key.
5. Define COA port, device form current example use UDP port 3799 for COA.

Step 2. Configure Authorization Profiles.

Navigate to **Policy > Policy Elements > Results > Authorization > Authorization Profile** and click **Add.** First you have to create authorization profile for Central Web Authentication (CWA) redirect, as shown in the image.

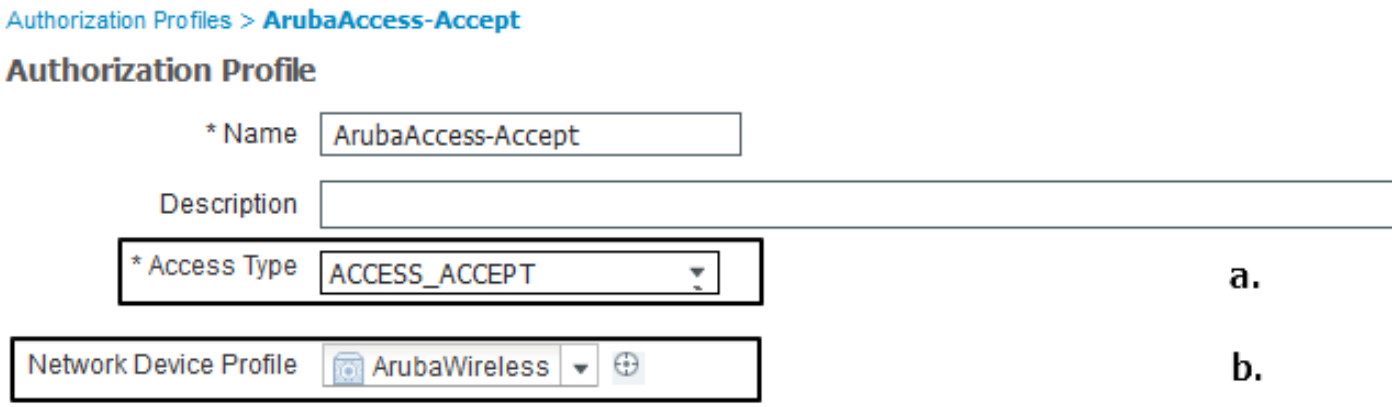


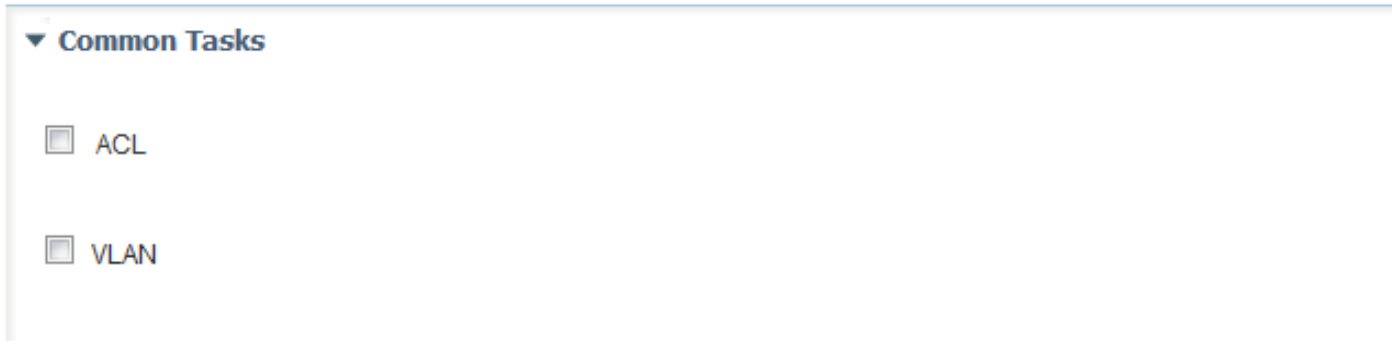
Note: By default all Authorization Profiles have network device type equal to Cisco. If NAD itself is configured as ArubaWireless and authorization profile is created for other device type, this profile is never matched for this device.

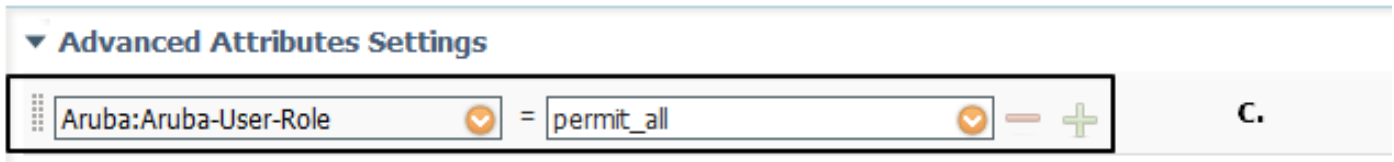
1. Define **Access-Type** as **Access-Accept**.
2. In N**etwork Device Profile** select **ArubaWireless**.

3. In common task section, enable **Web Redirection** option.
4. As a redirection type select **Centralized Web Auth** and select guest portal that you would like to use for redirection.
5. The URL that ISE presents should be defined on Aruba WLC as external Captive portal URL.
6. In **Advanced Attribute Settings** section, define Aruba User-Role attribute value.

Second authorization profile should be created to provide access for guest users after portal authentication:







1. Define **Access-Type** as **Access-Accept**.
2. In **Network Device Profile** select **ArubaWireless**.
3. In **Advanced Attribute Settings** section define Aruba User-Role attribute value. Later on you will configure local User-role on Aruba WLC with the same name.

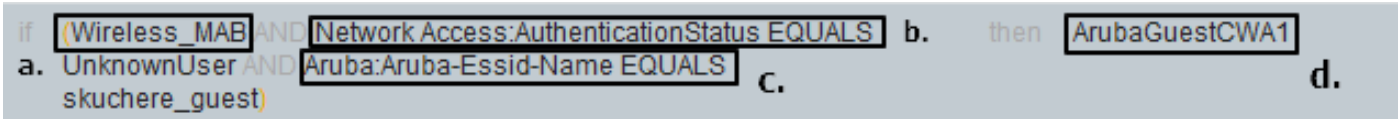
Step 3. Configure Authorization Policy.

First authorization policy is responsible for user redirection to guest portal. In simplest case, you can use built in compound condition

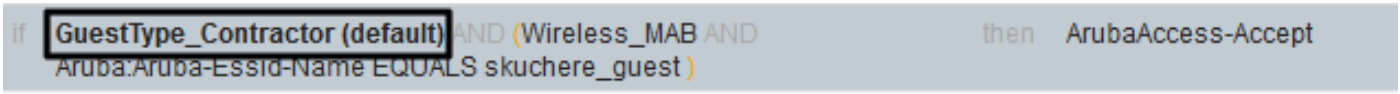
- Wireless_MAB (a.) and
- Network Access AuthenticationStatus equal to Unknown user (b.) and

- Aruba Aruba-Essid-Name equal to your guest SSID name (c.).

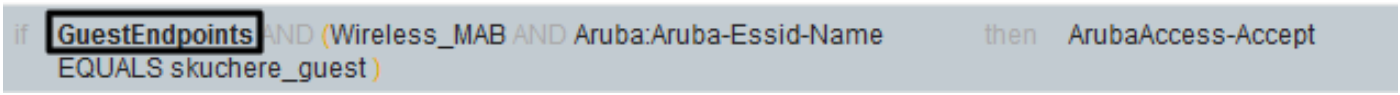
For this policy, configure authorization profile with redirect to guest portal as a result (d.)



Second authorization policy should provide access for guest user after authentication via the portal. This policy can rely on session data (User Identity Group/Use case guest flow and so on). In this scenario user should reconnect before Session Stitching timer expire:



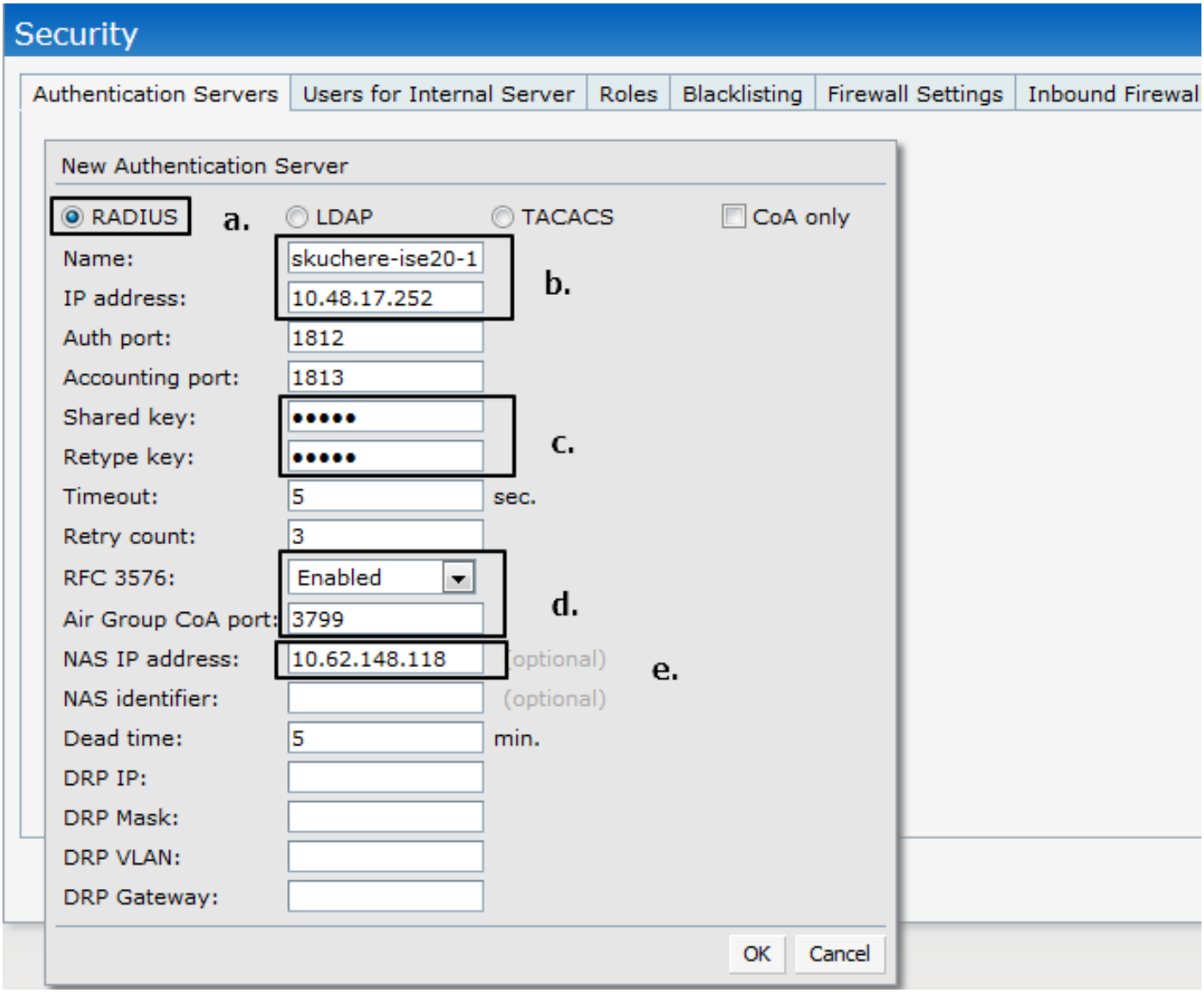
To protect yourself from Session Stitching timer expiration you can rely on endpoint data instead of session data. By default, Sponsored Guest portal on ISE 2.0 is configured for automatic guest device registration (Guest device is automatically placed in Guest_Endpoints endpoint identity group). This group can be used as a condition:



Authorization policy in correct order:

Step 4. Configure Radius Server on Aruba.

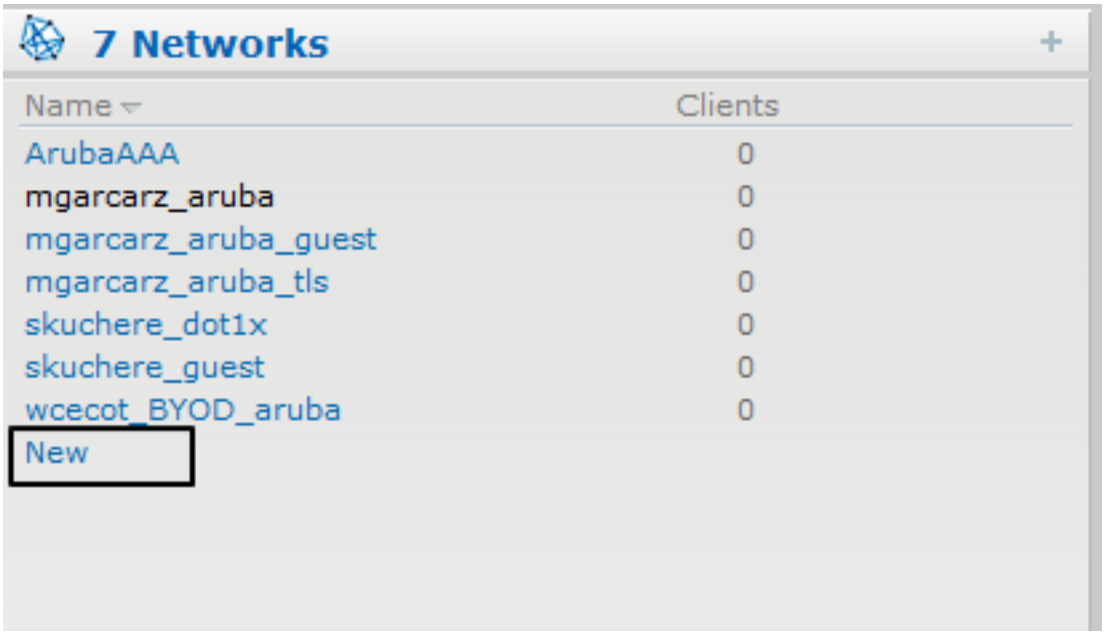
Navigate to **Security > Authentication Servers** and click **New:**



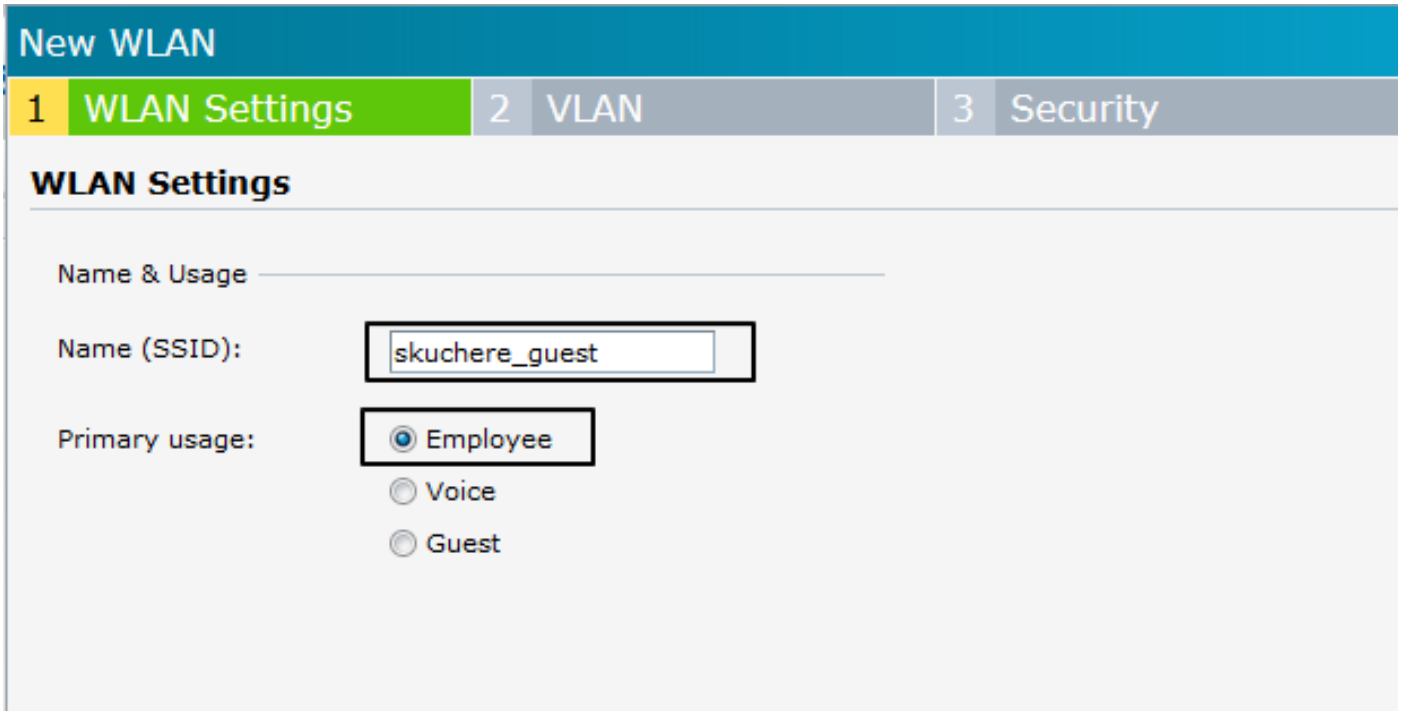
1. Choose RADIUS as AAA protocol.
2. Define AAA server name and IP address.
3. Specify pre-shared key.
4. Enable RFC 3576 support and define COA port.
5. Specify Aruba WLC management interface IP as NAS IP address.

Step 5. Create guest SSID on Aruba.

In the dashboard page select **New** at the end of network list. SSID creation wizard should start. Follow wizard steps.

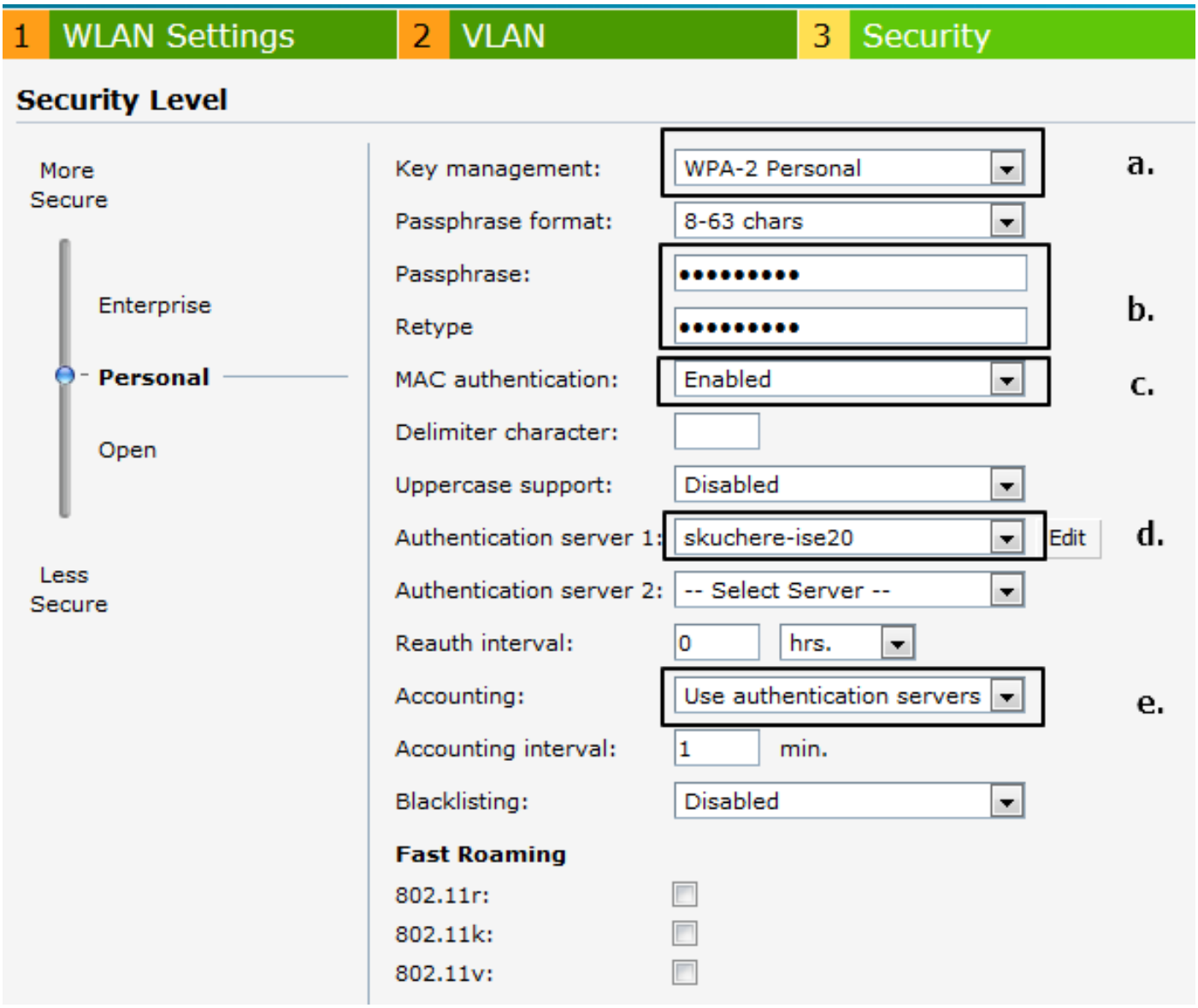


Step 1. Define SSID name and select SSID type. Here, SSID type Employee is used. This SSID type has default role with permit all and no Captive Portal Enforcement. Also, you can choose type Guest. In such scenario you should define captive portal settings during SSID configuration.



Step 2. VLAN and IP address assignment. Here, settings are left as defaults, as shown in the image.

Step 3. Security settings. For guest SSID you can select Open or Personal. Personal requires pre-shred key.



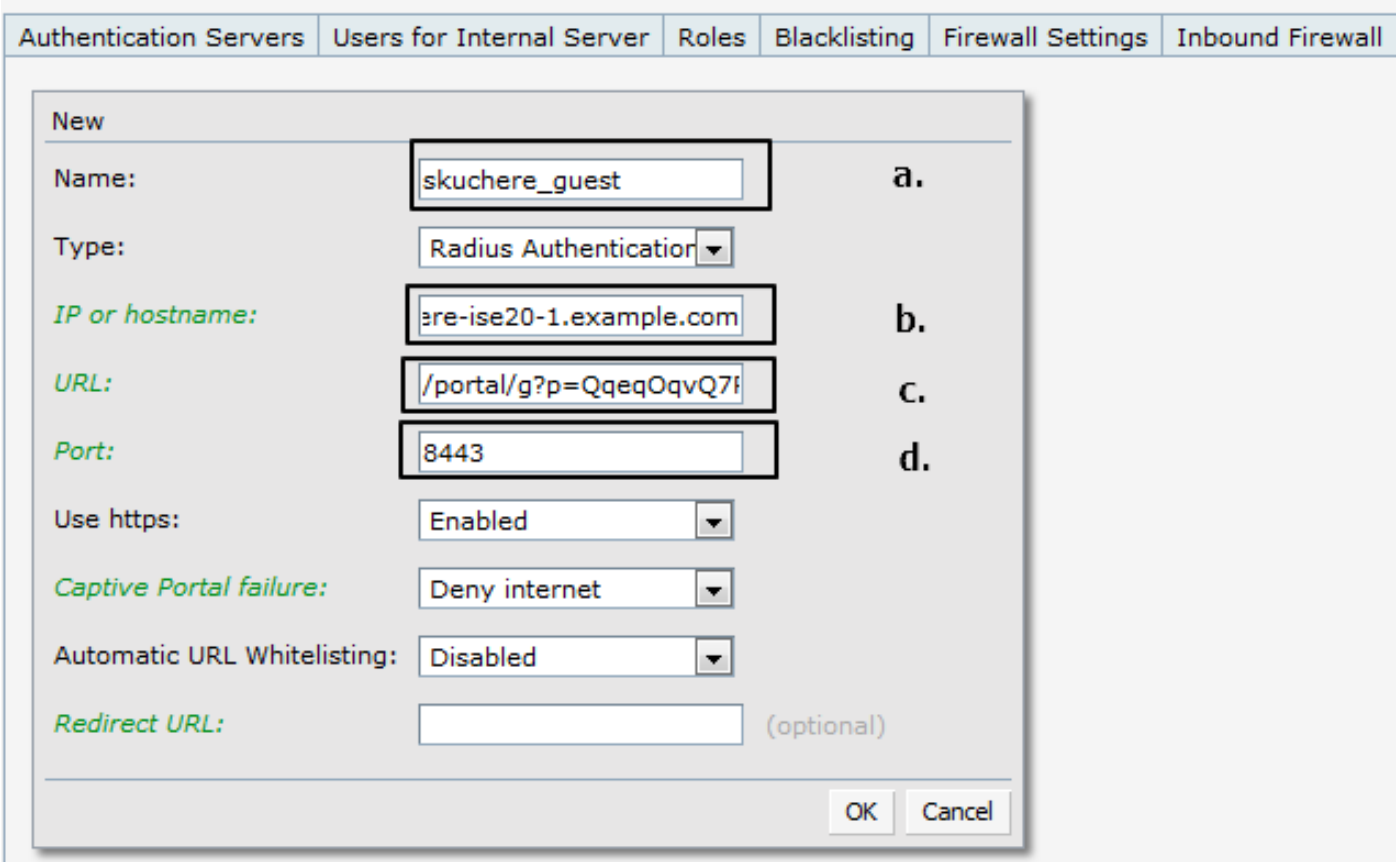
1. Choose Key Management mechanism.
2. Define pre-shared key.
3. To authenticate user against ISE using MAB MAC filtering need to be enabled.
4. In authentication server list choose your AAA server.
5. To enable accounting towards previously defined AAA server choose Use Authentication

server in drop-down list.

Note: Accounting is crucial with third-part NADs. If Policy Service Node (PSN) does not receive Accounting-Stop for user from NAD, session may get stuck in Started state.

Step 6. Configure Captive Portal.

Navigate to **Security > External Captive Portals** and create new portal, as shown in the image:



Step 1. Specify captive portal name.

Steo 2. Define your ISE FQDN or IP address. If you use IP address, ensure that this IP defined in Subject Alternative Name(SAN) field of Guest Portal Certificate.

Note: You may use any PSN server, but user should be always redirected to the server where MAB took place. Usually you have to define FQDN of the Radius server that has been configured on SSID.

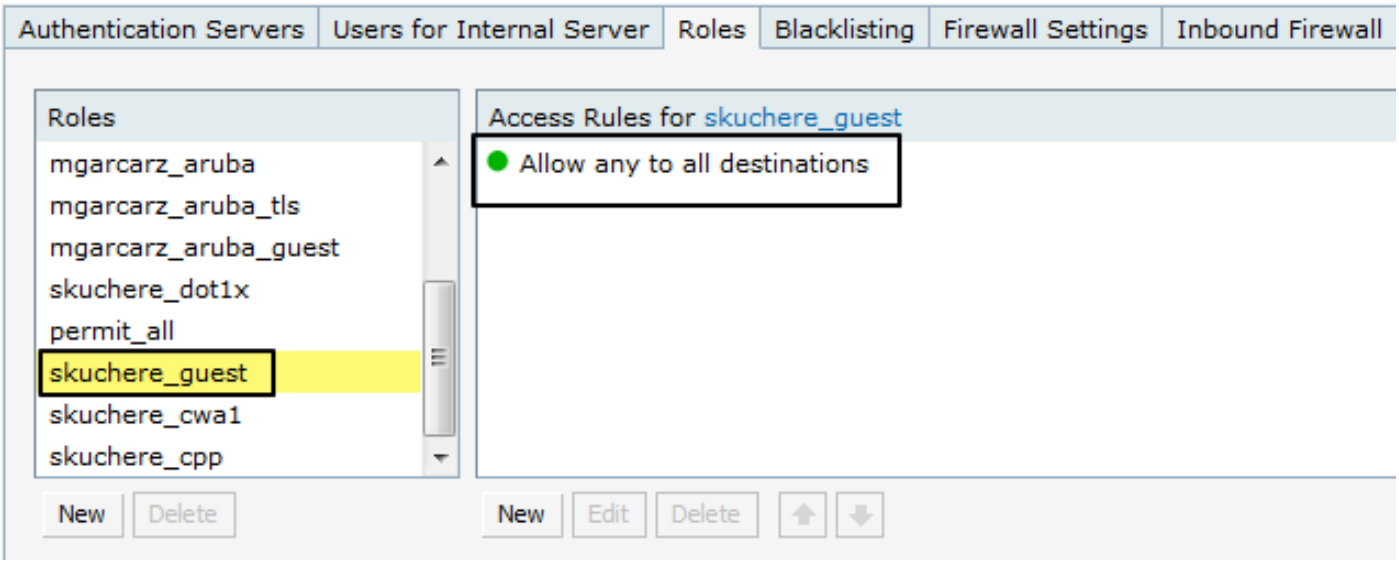
Step 3. Provide redirect from ISE authorization profile. You should put here the part after port number,

Step 4. Define ISE guest portal port.

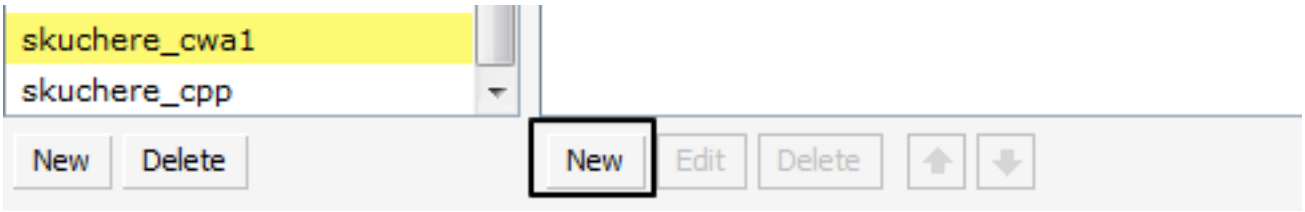
Step 7. Configure User-Roles.

Navigate to **Security > Roles.** Ensure that after SSID is created, new role with the same name is present in the list with access rule permit any to all destinations. Additionally, create two roles: one

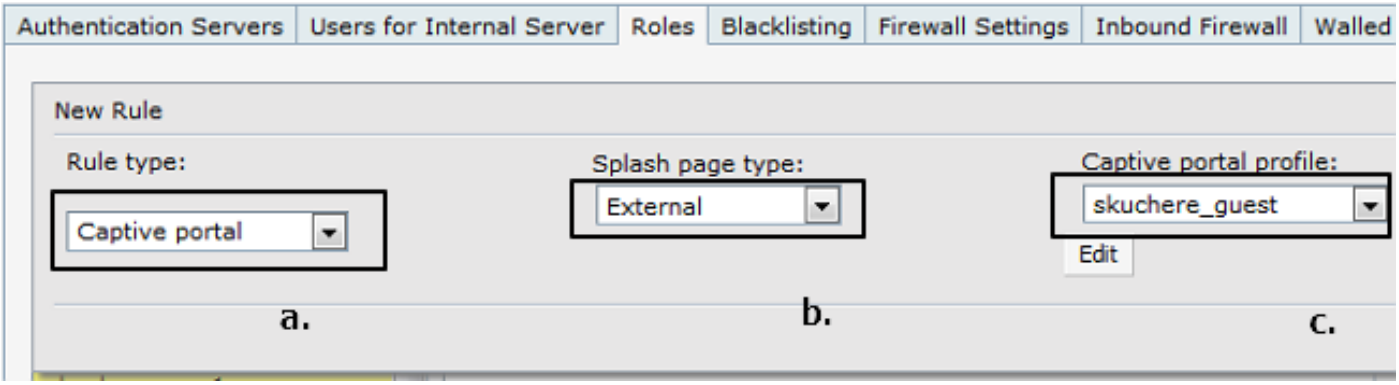
for CWA redirect and second for permit access after authentication on guest portals. Names of these roles should be identical to Aruba User-Role defined in ISE authorization profiles.



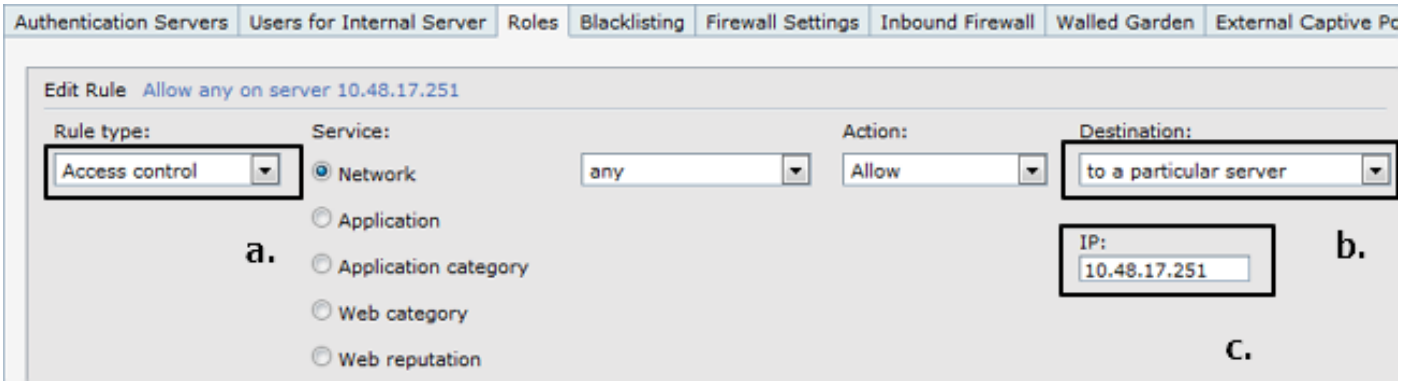
As shown in the image, create new user role for redirect and add security restriction.



For first restriction you need to define:

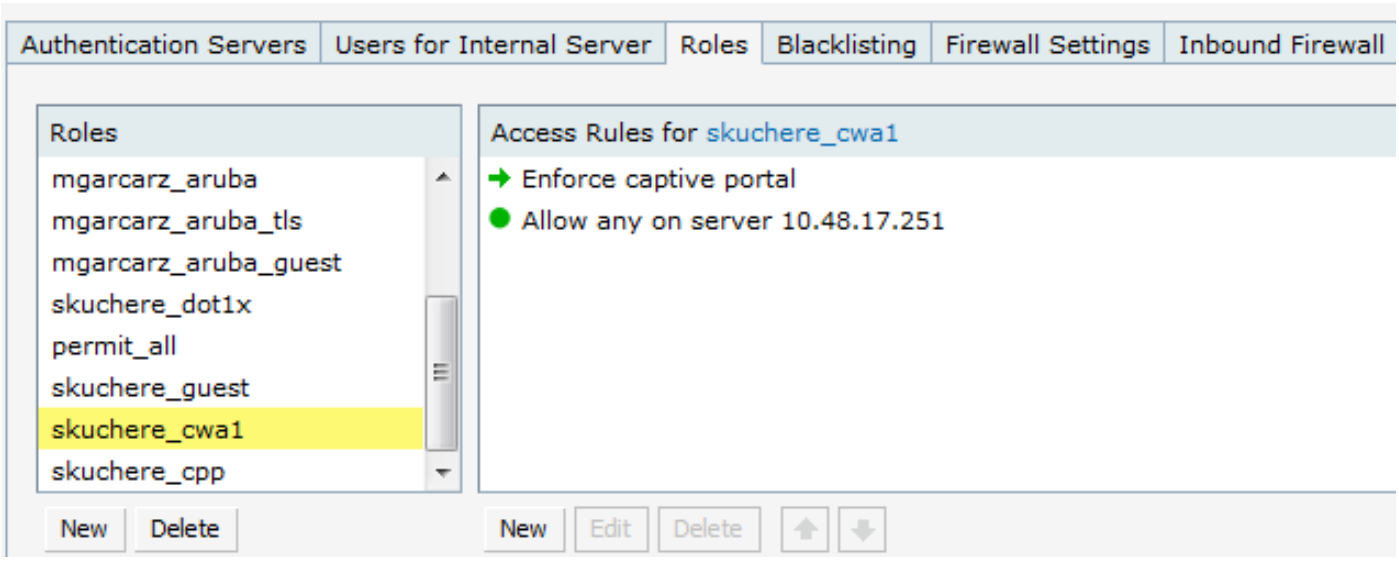


For second restriction you need to define:



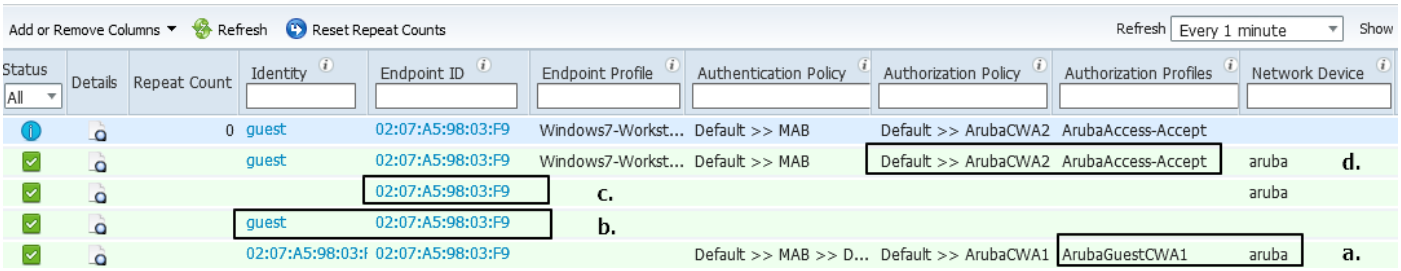
As shown in the image, default rule Allow any to all destinations can be deleted. This is a

summary result of role configuration.



Verify

Example of guest flow in ISE **Operations > Radius Livelog**.



1. First MAB and as a result, an authorization profile with CWA redirect and User-Role that have Captive portal configured on Aruba side.
2. Guest authentication.
3. Successful Change of Authorization (CoA).
4. Second MAB and as a result an authorization profile with permit access and User-Role that has permit all rule on Aruba side.

On Aruba side you can use **show clients** command to ensure that user is connected, IP address is assigned and correct user-role is assigned as a result of authentication:

```
04:bd:88:c3:88:14# show clients

Client List
-----------
Name              IP Address    MAC Address        OS     Network        Access Point       Channel  Type  Role
----              ----------    -----------        --     -------        ------------       -------  ----  ----
02-07-A5-98-03-F9  10.62.148.77  02:07:a5:98:03:f9  Win 7  skuchere_guest  04:bd:88:c3:88:14  11       GN    skuchere_cwa1
Number of Clients   :1
Info timestamp      :92552
```

Troubleshoot

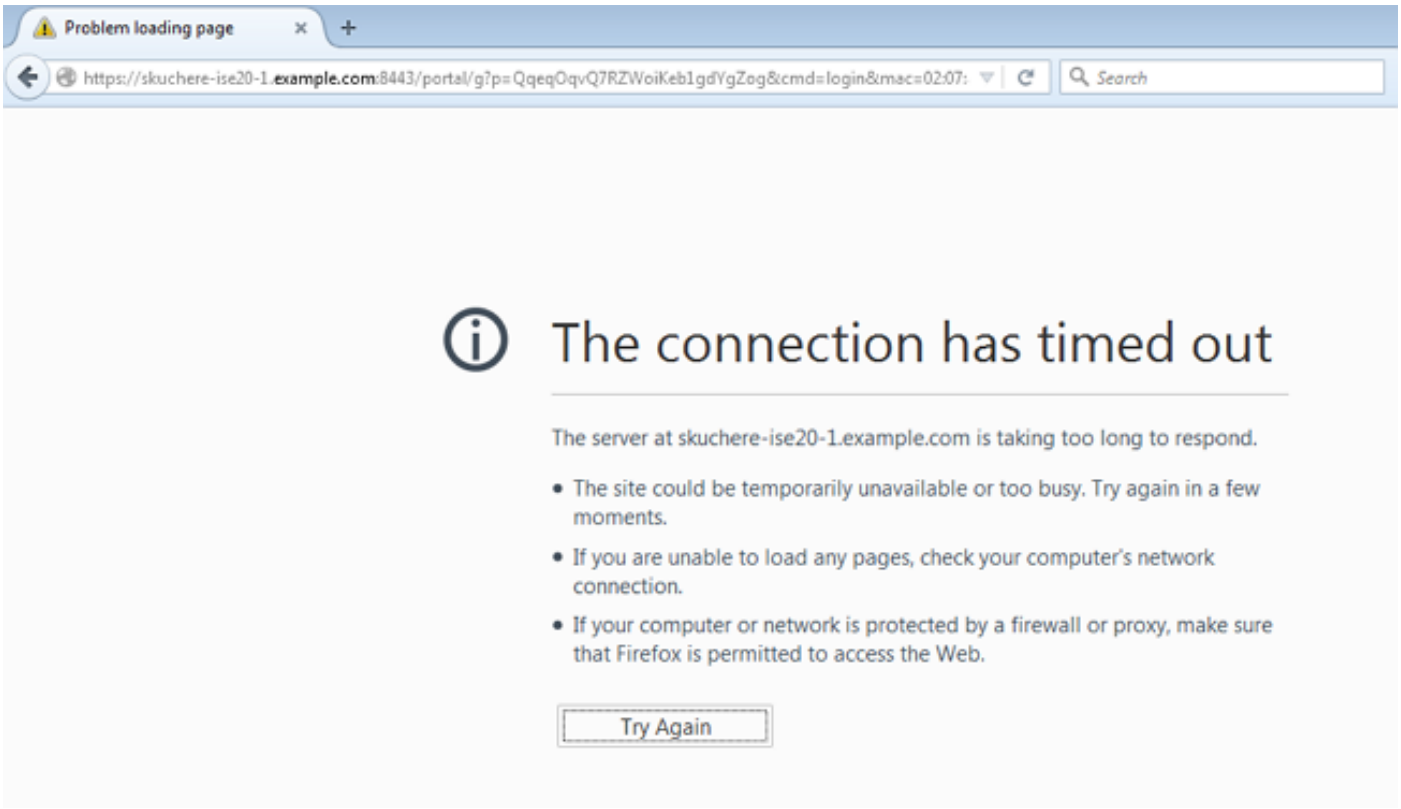
Failed COA

In ISE settings, ensure that Aruba NAD is configured with correct Network device type on ISE side and COA port is correctly defined in NAD settings. On Aruba side ensure that RFC 3576 is

enabled in Authentication Server settings and COA port is defined correctly. From network perspective check that UDP port 3799 is allowed between ISE and Aruba WLC.

Redirect issue

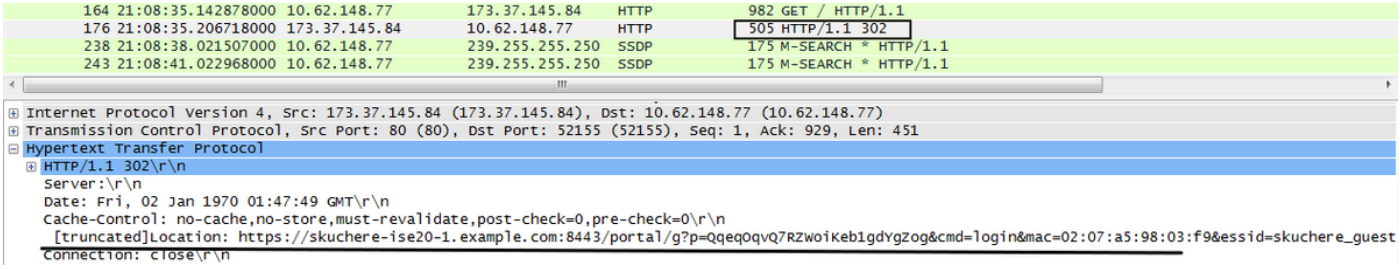
User sees ISE url in browser but ISE page is not displayed, as shown in the image:



On user side ensure that ISE FQDN can be successfully resolved to correct IP. On Aruba side check that ISE url is defined correctly in captive portal settings and traffic towards ISE allowed in User-Role access restrictions. Aslo check that Radius server on SSID and ISE PSN in captive portal settings is the same device. From network perspective check that TCP port 8443 is allowed from user segment to ISE.

No Redirection URL Present in User Browser

On user side ensure that as result of each HTTP request Aruba WLC returns HTTP code 302 page moved with ISE URL.



Session Stitching Timer Expired

Typical symptom of this problem is that user is redirected for second time to guest portal. In this case in ISE Radius Livelog you should see that after COA for second authentication Authorization

profile with CWA has been selected again. On Aruba side, check actual user role with the help of **show clients** command.

As a workaround for this issue you may use endpoint based authorization policy on ISE for connections after successful guest authentication.