**[ISE BYOD Flow Using Entra ID](https://community.cisco.com/t5/security-knowledge-base/ise-byod-flow-using-entra-id/ta-p/4400675)**

edited ‎09-08-2024 03:50 PM

[Greg Gibbs](https://community.cisco.com/t5/user/viewprofilepage/user-id/388087)

* [Introduction](https://community.cisco.com/t5/security-knowledge-base/ise-byod-flow-using-entra-id/ta-p/4400675#toc-hId-1331938100)
* [Prerequisites](https://community.cisco.com/t5/security-knowledge-base/ise-byod-flow-using-entra-id/ta-p/4400675#toc-hId--475516363)
* [Requirements](https://community.cisco.com/t5/security-knowledge-base/ise-byod-flow-using-entra-id/ta-p/4400675#toc-hId-215045111)
* [Components Used](https://community.cisco.com/t5/security-knowledge-base/ise-byod-flow-using-entra-id/ta-p/4400675#toc-hId--1592409352)
* [Assumptions](https://community.cisco.com/t5/security-knowledge-base/ise-byod-flow-using-entra-id/ta-p/4400675#toc-hId-895103481)
* [Configuration](https://community.cisco.com/t5/security-knowledge-base/ise-byod-flow-using-entra-id/ta-p/4400675#toc-hId-884600377)
* [SAML IdP Configuration](https://community.cisco.com/t5/security-knowledge-base/ise-byod-flow-using-entra-id/ta-p/4400675#toc-hId-1575161851)
* [ISE Policy Elements and BYOD Portal](https://community.cisco.com/t5/security-knowledge-base/ise-byod-flow-using-entra-id/ta-p/4400675#toc-hId--2039747075)
* [Entra ID SAML SSO Configuration](https://community.cisco.com/t5/security-knowledge-base/ise-byod-flow-using-entra-id/ta-p/4400675#toc-hId-1112719019)
* [Complete the SAML Configuration in ISE](https://community.cisco.com/t5/security-knowledge-base/ise-byod-flow-using-entra-id/ta-p/4400675#toc-hId--1822131537)
* [Complete the ISE Policy Configuration](https://community.cisco.com/t5/security-knowledge-base/ise-byod-flow-using-entra-id/ta-p/4400675#toc-hId--1142073167)
* [Configure the Wireless LAN Controller](https://community.cisco.com/t5/security-knowledge-base/ise-byod-flow-using-entra-id/ta-p/4400675#toc-hId--1571307319)
* [Verify the configuration](https://community.cisco.com/t5/security-knowledge-base/ise-byod-flow-using-entra-id/ta-p/4400675#toc-hId--89449080)

**Introduction**

***\*\*\* NOTE: Microsoft has now renamed Azure AD to Entra ID. For all references to Azure AD in this document, the same concepts apply to Entra ID.***

With the enhancements in ISE 3.0 for integrating with Entra ID via SAML IdP, it is now possible to create a BYOD Flow to provide Wireless network access using an employee’s Entra ID credentials.

The use of Entra ID credentials is an alternative to using a certificate-based method such as EAP-TLS (which requires certificate provisioning) or PEAP-MSCHAPv2. It can mitigate concerns with using other password-based authentication methods (like PEAP-MSCHAPv2) as it uses the employee’s email address as the username rather than exposing their on-premise Active Directory attributes such as sAMAccountName.

**Prerequisites**

**Requirements**

Cisco recommends that you have knowledge of these topics:

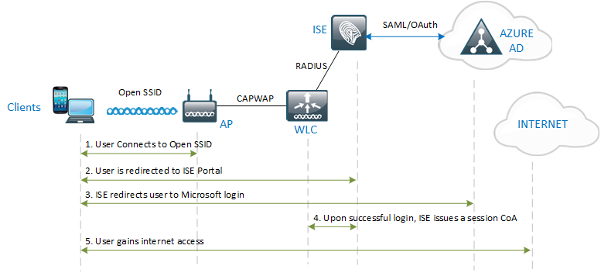
* Cisco ISE 3.0
* Basic knowledge about SAML SSO deployments
* Entra ID

**Components Used**

This configuration example is based on the following environment:

* ISE 3.0 patch 2
* AireOS-based Wireless LAN Controller (2500, 5500, etc) with software version 8.5 or higher
* A separate Wireless SSID using Open authentication
* Basic open internet access for employees
* Entra ID user accounts associated with a BYOD Security Group

The following diagram illustrates the logical flow for the solution.



The lab used to validate the solution uses a single WLC, but the same solution will also work with a Foreign & Guest Anchor architecture.

**Assumptions**

The configuration herein assumes that an SSID has been created on the WLC for the BYOD network and the WLC has already been configured as a Network Device in ISE.

See the [**AireOS WLC configuration**](https://community.cisco.com/t5/security-documents/aireos-wlc-configuration-for-ise/ta-p/3918970#toc-hId--985988915)for ISE document for Open SSID WLAN configuration and best practices.

**Configuration**

**SAML IdP Configuration**

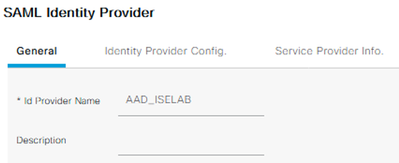
Step 1 – Create a new SAML Identity Provider for Entra ID

Navigate to ***Administration > Identity Management > External Identity Sources > SAML Id Providers***and click **Add.**

A screenshot of a computer

AI-generated content may be incorrect.

Input the Provider Id Name and optional Description values and click **Submit**.



\*\*\* NOTE: At the time of this writing, ISE cannot create more than one SAML Id Provider with the same Azure tenant ID.

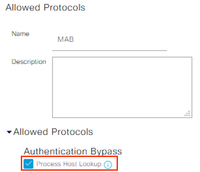
**ISE Policy Elements and BYOD Portal**

Step 2 – Create an Allowed Protocols list for MAB (if one is not already created)

Navigate to ***Policy > Policy Elements > Results > Authentication > Allowed Protocols***and click **Add**

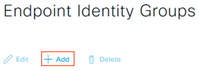


Input the Name and optional Description, select only the Process Host Lookup option, and click **Submit**.

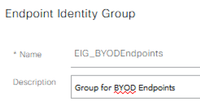


Step 3 – Create an Endpoint Identity Group for the BYOD endpoints

Navigate to ***Administration > Identity Management > Groups > Endpoint Identity Groups*** and click **Add.**



Input the Name and optional Description and click **Submit**.



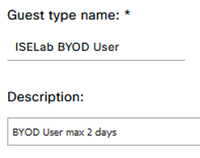
Step 4 – Configure a Guest Type for the BYOD users

Navigate to ***Work Centers > Guest Access > Portals & Components > Guest Types*** and click **Create.**

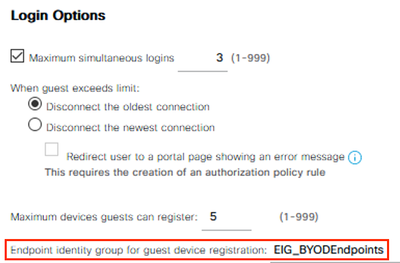
A screenshot of a computer

AI-generated content may be incorrect.

Input the Guest Type Name and optional Description



Under the Login Options section, select the Endpoint Identity Group previously created.



Configure all other preferred settings and click **Save**.

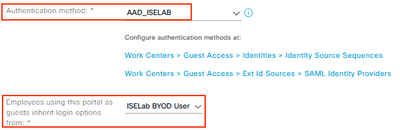
Step 5 – Configure the BYOD Portal

Navigate to ***Work Centers > Guest Access > Portals & Components > Guest Portals.***Create a new Sponsored Guest Portal or select an existing one.

Input the Portal Name and optional Description.



In the Portal Settings section, select the SAML IdP from the ‘Authentication method’ drop-down list and the Guest Type from the ‘Employees using this portal as guests…’ drop-down list.



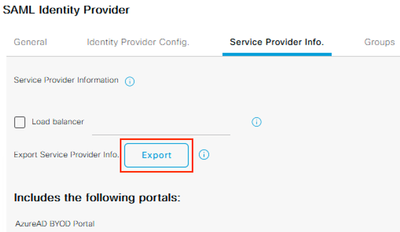
Configure all other preferred settings and click **Save**.

**Entra ID SAML SSO Configuration**

Step 6 – Export the SAML IdP info from ISE

Navigate to ***Administration > Identity Management > External Identity Sources > SAML Id Providers***and Edit the IdP.

Select the Service Provider Info tab and click **Export.**



Save and extract the zip file and open the XML file in a text editor. Record the following attribute values:

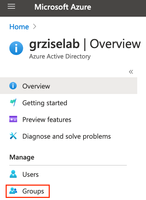
* **entityID**
* **AssertionConsumerService Locations**

Example:

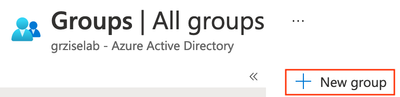
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://CiscoISE/655019f2-fa19-4517-a5f6-b59d3110830b"><md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"><md:KeyDescriptor use="signing"><ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:X509Data><ds:X509Certificate>MIIF6jCCA9KgAwIBAgIQYH/EmAAAAACOrCYAdmBsQDANBgkqhkiG9w0BAQsFADB5MSUwIwYDVQQD  
...  
snip  
...  
</ds:X509Data></ds:KeyInfo></md:KeyDescriptor><md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat><md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat><md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat><md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat><md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName</md:NameIDFormat><md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos</md:NameIDFormat><md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</md:NameIDFormat><md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://192.168.120.180:8443/portal/SSOLoginResponse.action" index="0"/><md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://ise30-sa.ise.xxx.local:8443/portal/SSOLoginResponse.action" index="1"/></md:SPSSODescriptor></md:EntityDescriptor>

Step 7 – Create a BYOD Security Group in Entra ID

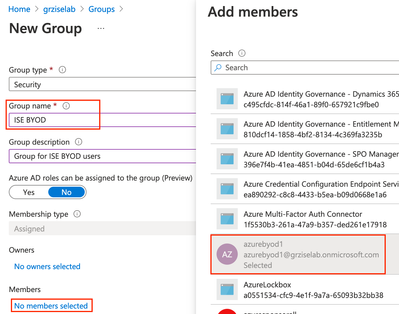
Login to the Entra ID Portal and navigate to ***Azure Active Directory > Manage > Groups***



Click **New Group**



Configure the desired Group name, click the **No members selected**link and select the associated BYOD user accounts. Click **Create.**

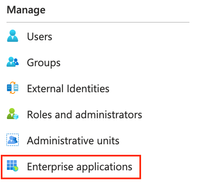


Record the **Object ID** for the new group.



Step 8 – Register the Enterprise Application

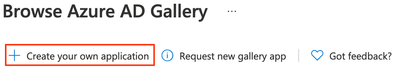
Navigate to ***Azure Active Directory > Manage > Enterprise applications***



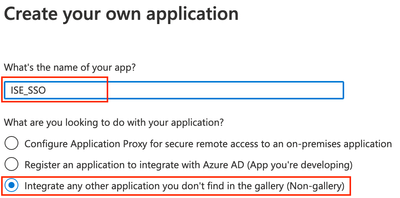
Click on **New Application**



Click on **Create your own application**

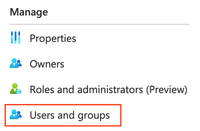


Name the application and ensure the **Non-gallery** option is selected. Click **Create**.

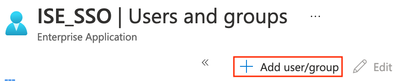


\*\*\* Note: A generic name was used as this application may also be used for other non-BYOD use cases in ISE.

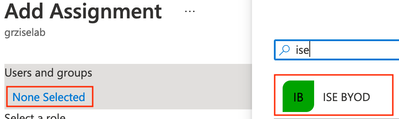
Navigate to **Manage > Users and groups**



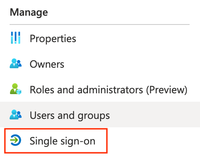
Click on **Add user/group**



Under Users and groups, click on the link for **None selected**. Click the BYOD group created earlier and click **Select**.



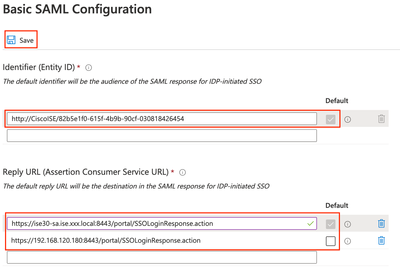
Navigate to **Manage > Single sign-on**



In the Basic SAML Configuration section, click **Edit.**



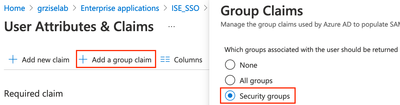
Paste the **entityID** and **Location** values recorded from XML file earlier in Step 6 and click **Save**.



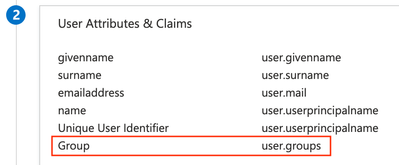
In the User Attributes & Claims section, click **Edit**.



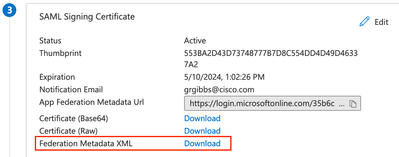
Click on **Add a group claim**. Select the **Security groups** radio button and click **Save**.



You should now see the Group claim added with a value of **user.groups**.



In the SAML Signing Certificate section, click the **Download** link for the Federation Metadata XML and save the file.



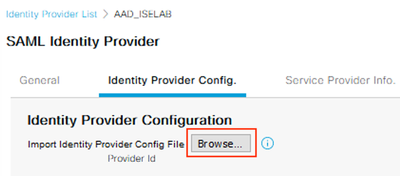
**Complete the SAML Configuration in ISE**

Step 9 – Configure the SAML IdP settings

Navigate to ***Administration > Identity Management > External Identity Sources > SAML Id Providers***.

Select the SAML IdP and click on the **Identity Provider Config** tab.

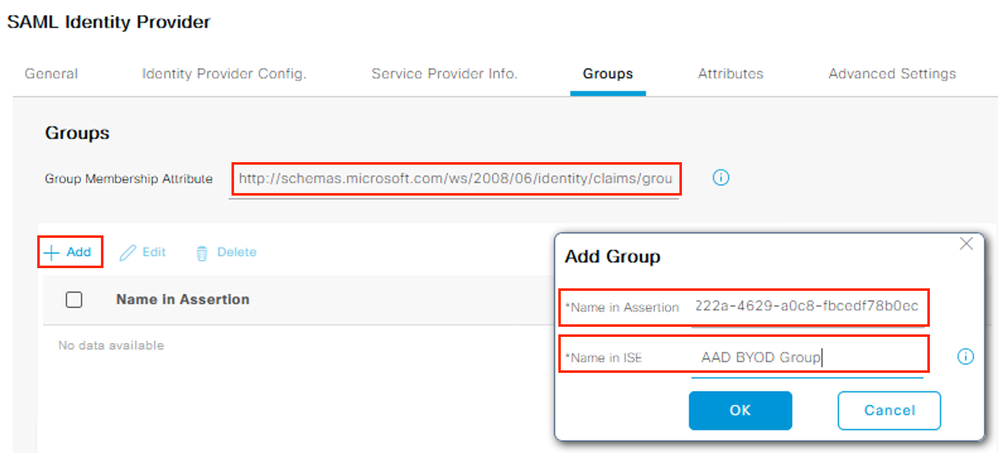
Click the **Browse** button and select the Federation Metadata XML file downloaded from Azure in the previous step.



Select the **Groups** tab and input the following URL for the Group Membership Attribute.

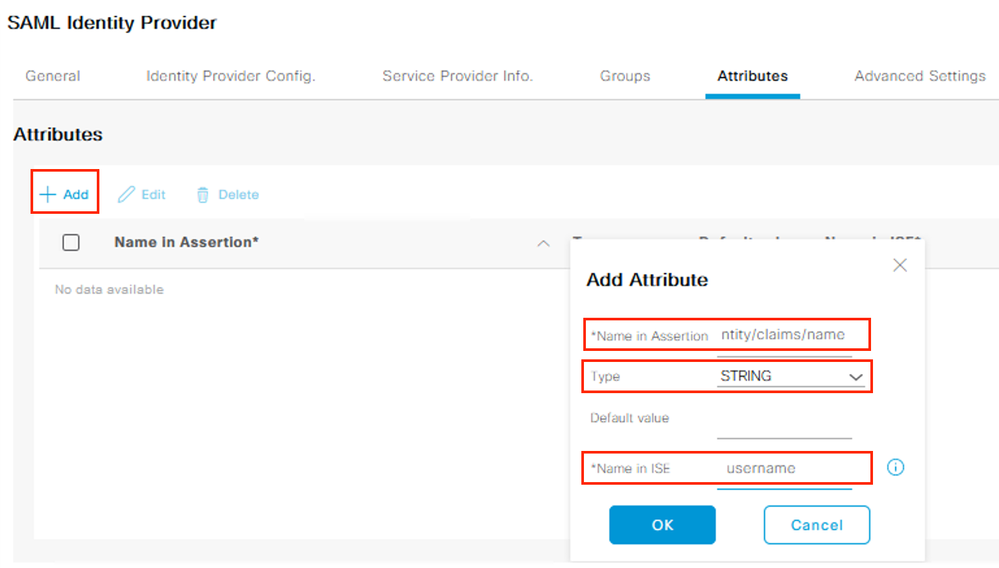
* <http://schemas.microsoft.com/ws/2008/06/identity/claims/groups>

Click the **Add** button. For the ‘Name in Assertion’ field, paste the **Object ID**copied from Azure in Step 7 and input a unique value for the ‘Name in ISE’ field. Click **OK**.



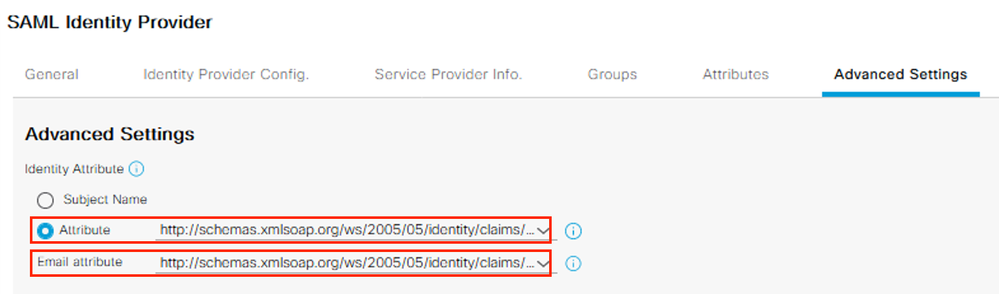
Select the **Attributes** tab and click **Add**. Input the following values and click **OK**.

|  |  |
| --- | --- |
| **Name in Assertion** | <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name> |
| **Type** | STRING |
| **Name in ISE** | username |



Select the **Advanced Settings** tab.

Under the Identity Attribute, select the **Attribute**radio button and select the available claims schema from the drop-down.

Select the same schema from the **Email attribute** drop-down. Click **Save**.  


**Complete the ISE Policy Configuration**

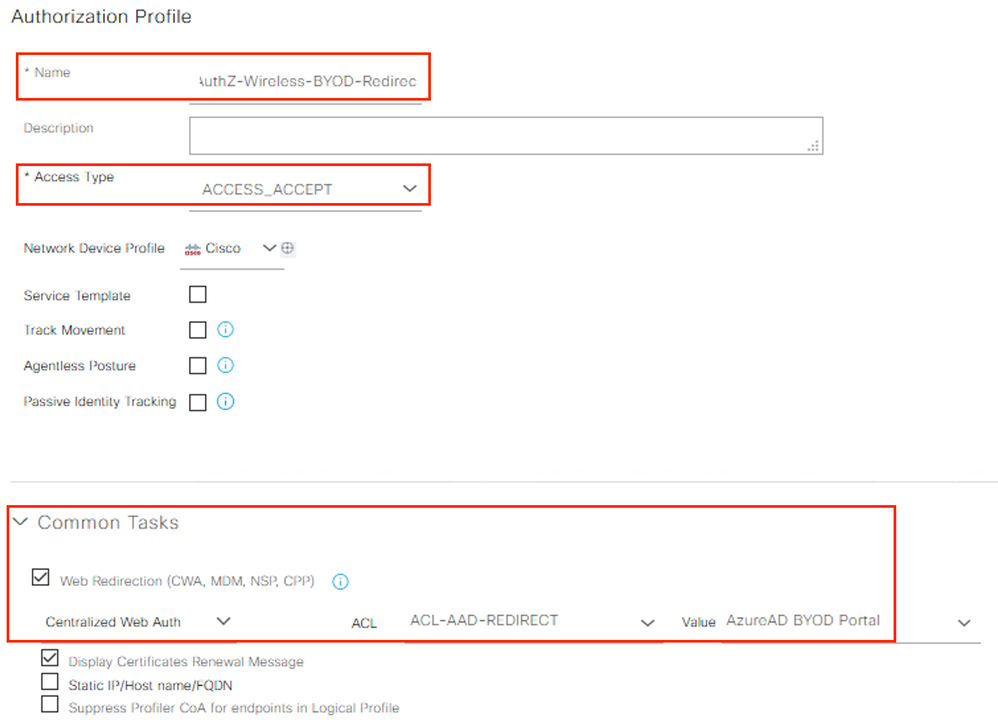
Step 10 – Create the Authorization Profiles

Navigate to ***Policy > Policy Elements > Results > Authorization > Authorization Profiles*** and click **Add**.

Create a new redirect Authorization Profile with the following values and click **Submit**.

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Value** | **Example Value** |
| Name | <profile name> | AuthZ-Wireless-BYOD-Redirect |
| Description | <optional description> |  |
| Access Type | ACCESS\_ACCEPT |  |
| **Common Tasks** | |  |
| Web Redirection (CWA, MDM, NSP, CPP) | |  |
| ACL | <WLC ACL Name> | ACL-AAD-REDIRECT |
| Value | <BYOD Portal Name> | Azure BYOD Portal |

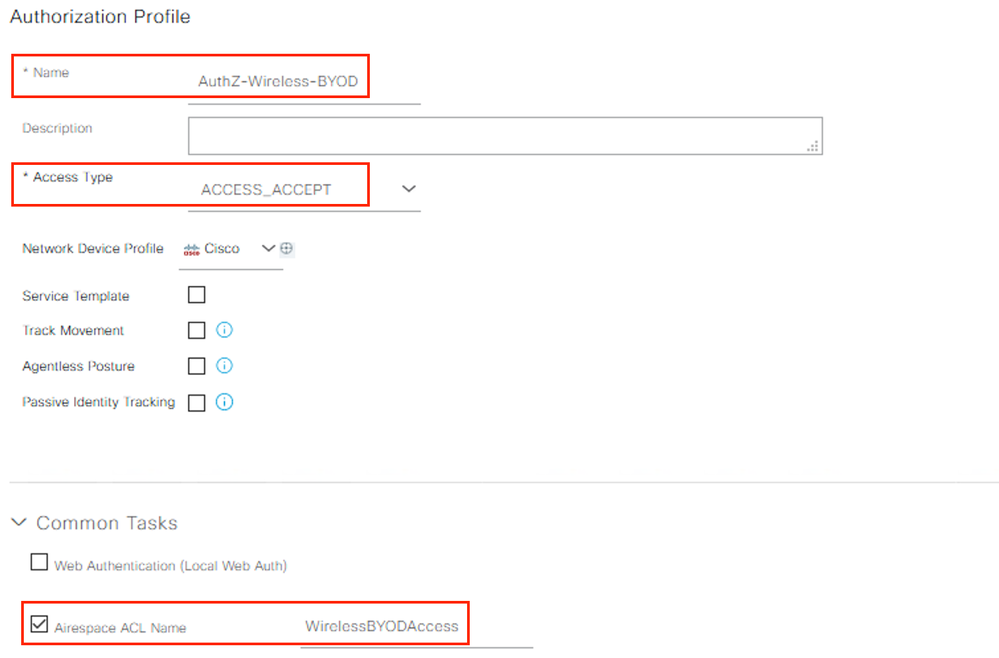
Example:



Create a new Authorization Profile to permit BYOD user access with the following values and click **Submit**.

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Value** | **Example Value** |
| Name | <profile name> | AuthZ-Wireless-BYOD |
| Description | <optional description> |  |
| Access Type | ACCESS\_ACCEPT |  |
| **Common Tasks** | |  |
| Airespace ACL Name | <WLC ACL Name> | WirelessBYODAccess |

Example:

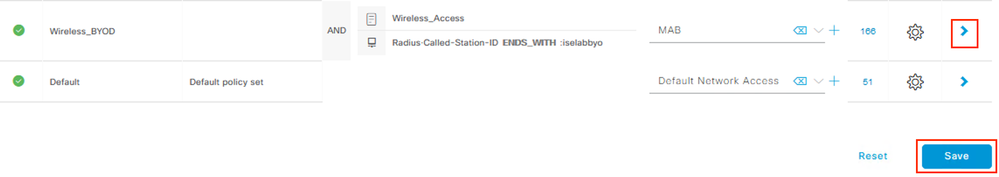


Step 11 – Create the Policy Set

Navigate to **Policy > Policy Sets** and create a new Policy Set matching the BYOD SSID. Select the Allowed Protocols list of **MAB** created earlier.

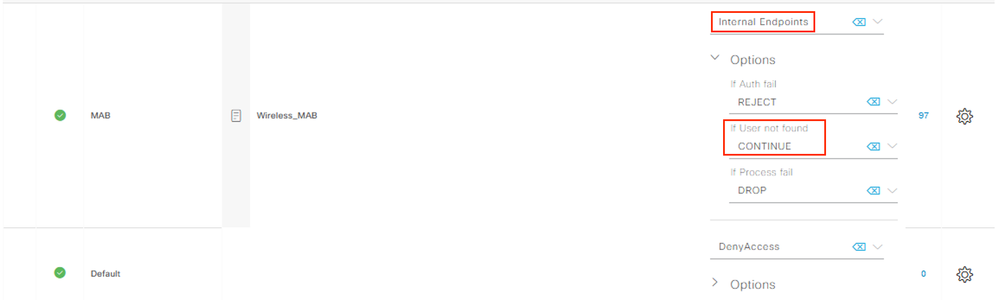
Click **Save** and then click the **>** symbol next to the new Policy Set.

Example:



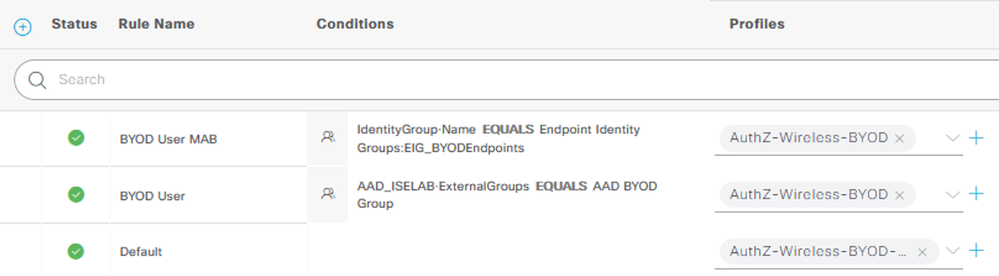
Create a new Authentication Policy with a ‘Use’ value of **Internal Endpoints**. Click the dropdown for Options and set the ‘If User not found’ option to **CONTINUE**.

Example:



Create the Authorization Policies for the redirection and successful authorizations. Select the access AuthZ Profile created in Step 10 (e.g. **AuthZ-Wireless-BYOD**) for the access policies and the redirect AuthZ Profile (e.g. **AuthZ-Wireless-BYOD-Redirect**) for the Default policy. Click **Save**.

Example:



\*\*\* Note: The ‘BYOD User MAB’ policy shown above is to take advantage of the ‘Remember Me’ Guest feature. This policy can be skipped if this feature is not desired. See the [ISE Guest Access Prescriptive Deployment Guide](https://community.cisco.com/t5/security-documents/ise-guest-access-prescriptive-deployment-guide/ta-p/3640475#toc-hId--916002297)  following link for more information on this feature.

**Configure the Wireless LAN Controller**

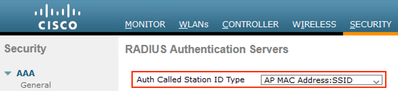
The following configuration settings are required on the Wireless LAN Controller. The sections below provide examples for both an AireOS based WLC (ex. 2504) and an IOS-XE based WLC (ex. 9800-CL).

AireOS WLC Configuration

**Configure the Wireless LAN Controller Called Station ID**

On the WLC, navigate to ***Security > AAA > RADIUS > Authentication***.

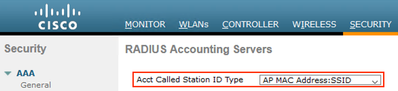
Ensure that the drop-down setting for ‘Auth Called Station ID Type’ includes the **:SSID**value.



\*\*\* Note: The above configuration is necessary to allow using the Policy Set matching condition for Called-Station-ID in Step 11.

Navigate to ***Security > AAA > RADIUS > Accounting***.

Ensure that the drop-down setting for ‘Acct Called Station ID Type’ includes the **:SSID**value.



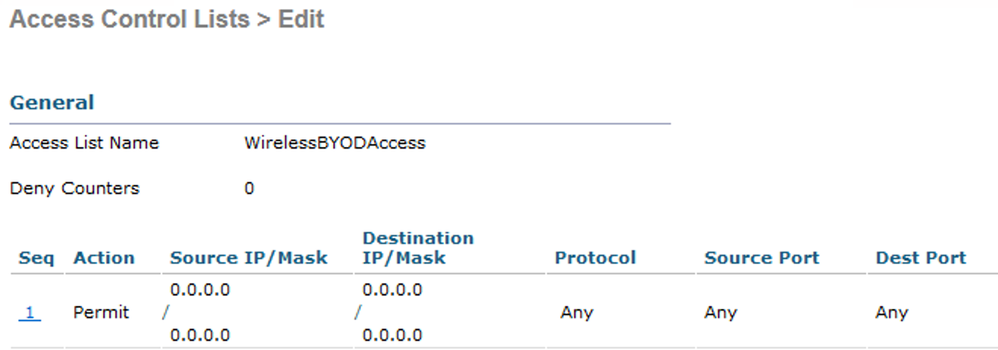
**Configure the Airespace ACLs used in the ISE Policies**

Navigate to ***Security > AAA > RADIUS > Access Control Lists > Access Control Lists***.

Click **New** and create an Airespace ACL to permit the desired access for the BYOD users.

In this example, a simple ‘permit ip any any’ ACL is used.

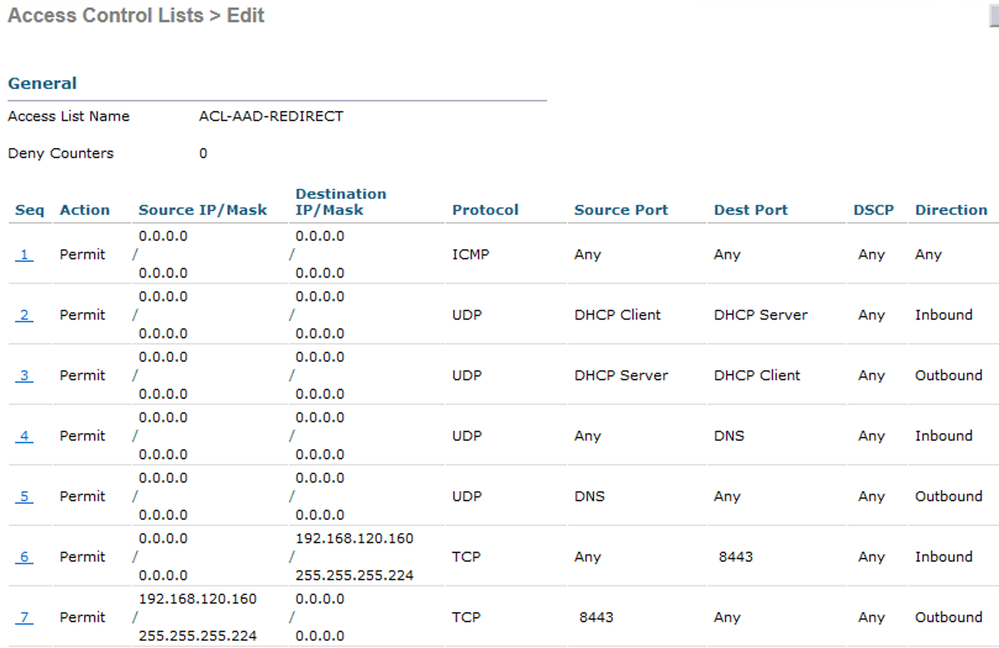
Example:



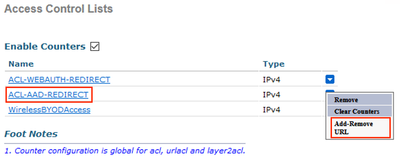
Click **New** and create an Airespace ACL for the URL redirection. At a minimum, the ACL should Permit (bypass redirection) for Inbound/Outbound traffic related to the following.

* DNS
* DHCP
* TCP/8443 traffic for the ISE BYOD Portal (unless a custom port was configured)

Example:



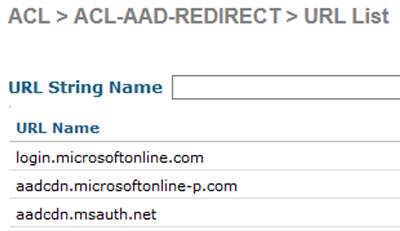
Return to the ***Access Control Lists*** page, click on the down-arrow next to the new redirect ACL and select **Add-Remove URL.**



Add the following **URL String Name** values to exempt the traffic from redirection.

* login.microsoftonline.com
* aadcdn.microsoftonline-p.com
* aadcdn.msauth.net

Example:

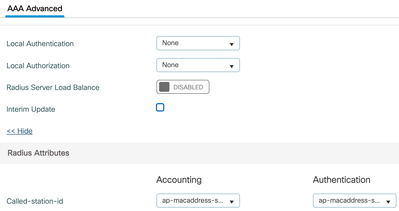


IOS-XE WLC Configuration

**Ensure the Called Station ID is configured to include the SSID name**

This step is necessary if the ISE policy is using a matching condition that includes the SSID name.   
In the WLC Admin UI, navigate to ***Configuration > Security > AAA*** and select the **AAA Advanced** tab. Click the **Show Advanced Settings** link, and select one of the options that includes 'ssid'  for both the Accounting and Authentication options in the Called Station ID setting.

Example:



**Configure the ACLs used in the ISE policies**

Navigate to ***Configuration > Security > ACL*** and create the URL Redirect ACL be used. The 'deny' statements indicate that the traffic will be exempted from redirection and should include exemptions for DNS traffic as well as the relevant ISE portals.

Example:



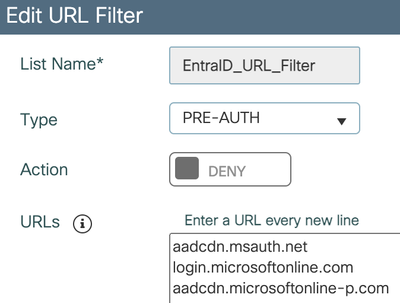
**Create a URL Filter to exempt the Microsoft FQDNs used in the SSO flow from redirection**

Navigate to ***Configuration > Security > URL Filters***, click **Add** and define the following settings:

* List Name = <name>
* Type = PRE-AUTH
* Action = DENY
* URLs = the below list of Microsoft URLs

aadcdn.msauth.net  
login.microsoftonline.com  
aadcdn.microsoftonline-p.com

Example:

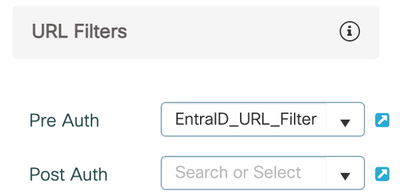


**Add the URL Filter to the Policy associated with the WLAN**

Navigate to ***Configuration > Tags & Profiles > Policy****.* Select the relevant Policy, at select the **Access Policies** tab.

In the URL Filters section, select the filter name created in the previous step for the **Pre Auth** setting (leave the Post Auth blank) and and click ***Update & Apply to Device***.

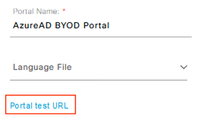
 Example:



**Verify the configuration**

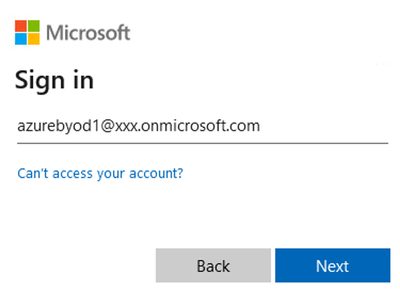
In ISE, navigate to ***Work Centers > Guest Access > Portals & Components > Guest Portals***.

Select the BYOD Portal and click the **Test portal URL** link.



The browser will be redirected to the Microsoft login. Sign in with an Entra ID user account that is a member of the BYOD group created in Step 7.

Example:



Depending on the settings configured for the BYOD Portal, you should see an AUP or Success page that includes the Entra ID login username.

