Duo - Cisco ACS & ISE Guide

Cisco Access Control System (ACS) is a policy-based security server that provides standards-compliant Authentication, Authorization, and Accounting (AAA) services to your network. ACS facilitates the administrative management of Cisco and non-Cisco devices and applications.

Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure access to network resources. Cisco ISE functions as a policy decision point and enables enterprises to ensure compliance, enhance infrastructure security, and streamline service operations. Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices.

Authentication Protocol and Identity Store Compatibility

To authenticate and authorize a user or host, ACS and ISE uses the user definitions in identity stores. There are two types of identity stores:

- Internal—Identity stores that ACS and ISE maintains locally (also called local stores) are called internal identity stores. For internal identity stores, ACS and ISE provides interfaces for you to configure and maintain user records.
- External—Identity stores that reside outside of ACS and ISE are called external identity stores. ACS and ISE requires configuration information to connect to these external identity stores to perform authentication and obtain user information. Cisco ACS and ISE supports the following external identity stores: LDAP, External MAB Database (ACS Only), Microsoft AD, RSA SecureID Server, RADIUS Identity Stores.

When it comes to Duo and ACS/ISE the two can be integrated via a RADIUS Identity Store or LDAP. RADIUS Identity Store is the recommended way and what this document will cover. Regardless, of which method you use for integrating, there are limitations around which authentication protocols can be used against them. The tables listed below contains the compatibility for all of the supported identity stores for ACS and ISE.

Non-EAP Authentication Protocol and User Database Compatibility

Identity Store	ASCII/PAP	MSCHAPv1/MSCHAPv2	CHAP
Internal	Yes	Yes	Yes
Microsoft AD	Yes	Yes	No
LDAP	Yes	No	No
RSA Identity Store	Yes	No	No
RADIUS Identity Store	Yes	No	No

EAP Authentication Protocol and User Database Compatibility

Identity	EAP-	EAP-	PEAP-	PEAP	EAP-FAST	PEAP-	EAP-FAST-

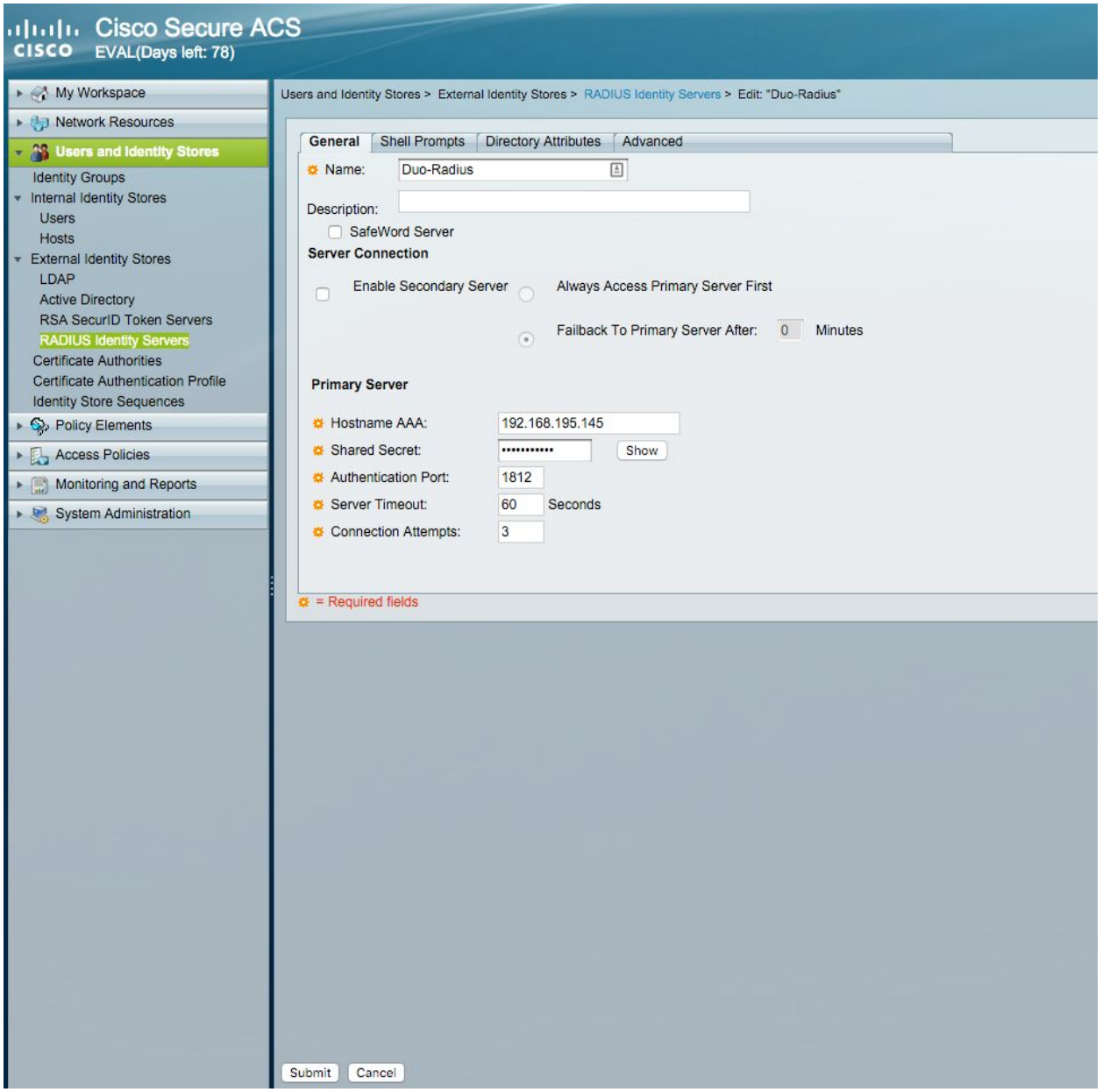
Store	MD5	TLS	TLS	EAP-MSCHAPv2	MSCHAPv2	GTC	GTC
Internal	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft AD	No	Yes	Yes	Yes	Yes	Yes	Yes
LDAP	No	Yes	Yes	No	No	Yes	Yes
RSA Identity Store	No	No	No	No	No	Yes	Yes
RADIUS Identity Store	No	No	No	No	No	Yes	Yes

ACS Duo Integration Steps

1. Sign up for a Duo account.
2. Log in to the Duo Admin Panel and navigate to **Applications**.
3. Click **Protect an Application** and locate **RADIUS** in the applications list. Click **Protect this Application** to get your **integration key**, **secret key**, and **API hostname**. See Getting Started for help.
4. Install the Duo Authentication Proxy
5. Configure the Proxy

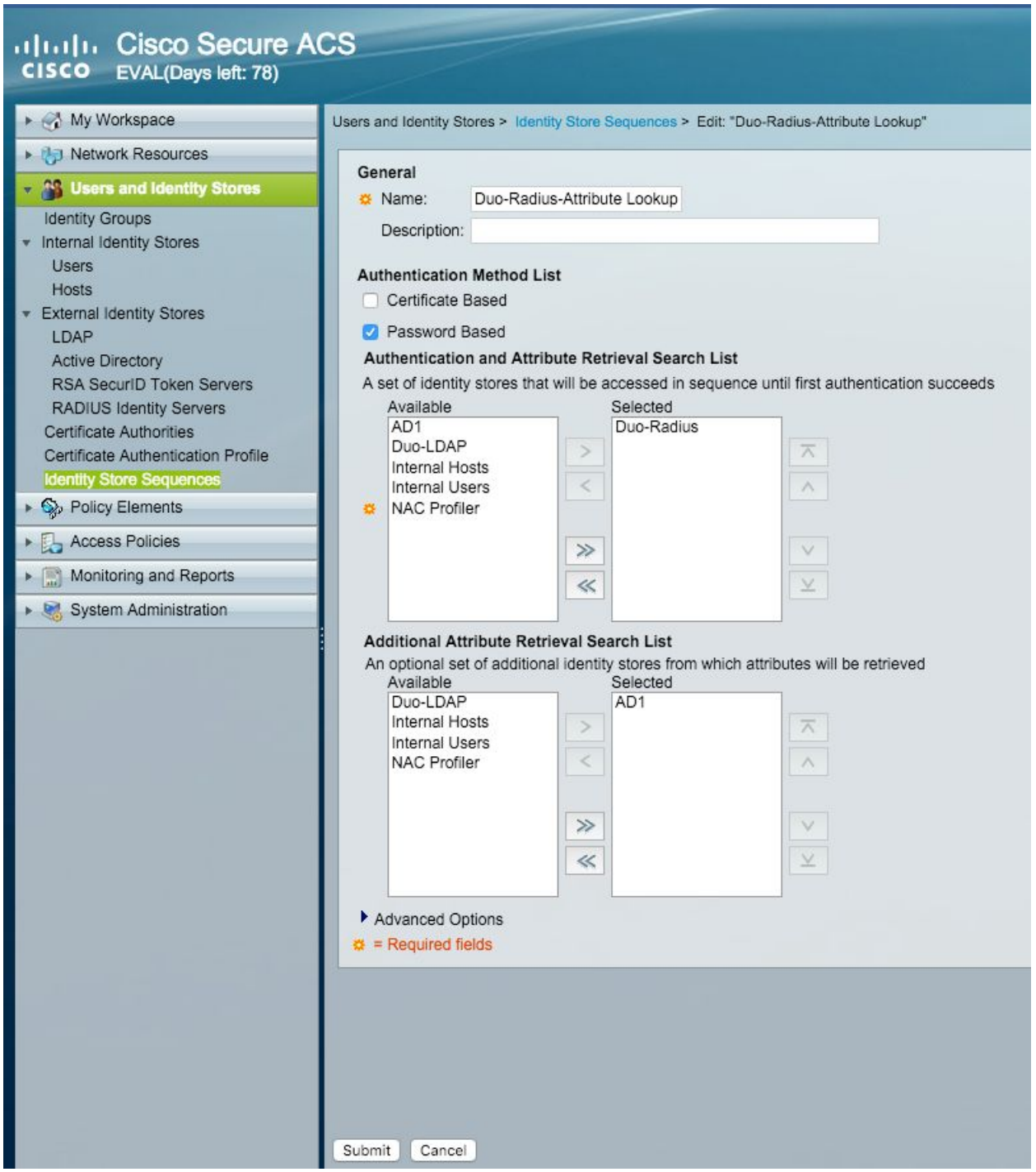
```
[ad_client]
host=1.2.3.4
service_account_username=duoservice
service_account_password=password1
search_dn=cn=Users,dc=example,dc=com

[radius_server_auto]
ikey=DIXXXXXXXXXXXXXXXXX
skey=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
api_host=api-XXXXXXXX.duosecurity.com
radius_ip_1=<IP Address of ACS Server>
radius_secret_1=thisisalsoaradiussecret
client=ad_client
port=1812
failmode=safe
```

6. Start the AuthProxy: `net start DuoAuthProxy`
7. Login to Cisco ACS
8. Go to **Users and Identity Stores > External Identity Stores > RADIUS Identity Servers** and select **Create**
9. From here enter in a Name, IP Address of the AuthProxy Server, and Shared Secret of the AuthProxy server. Change the server timeout to 60 seconds and then select **Submit**.



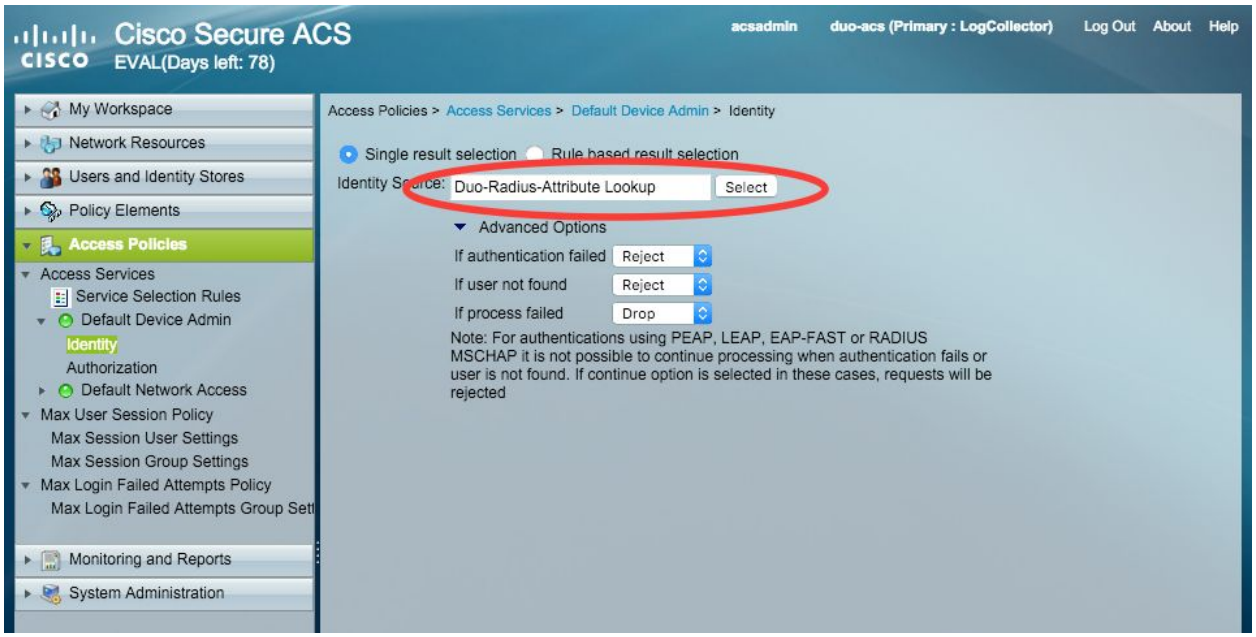
10. Now go to **Users and Identity Stores > Identity Store Sequences** and select **Create.**
11. From here enter in a Name, select Password Based, under Authentication move your

AuthProxy configuration under Selected and then move their AD server under Selected for Additional Attributes.

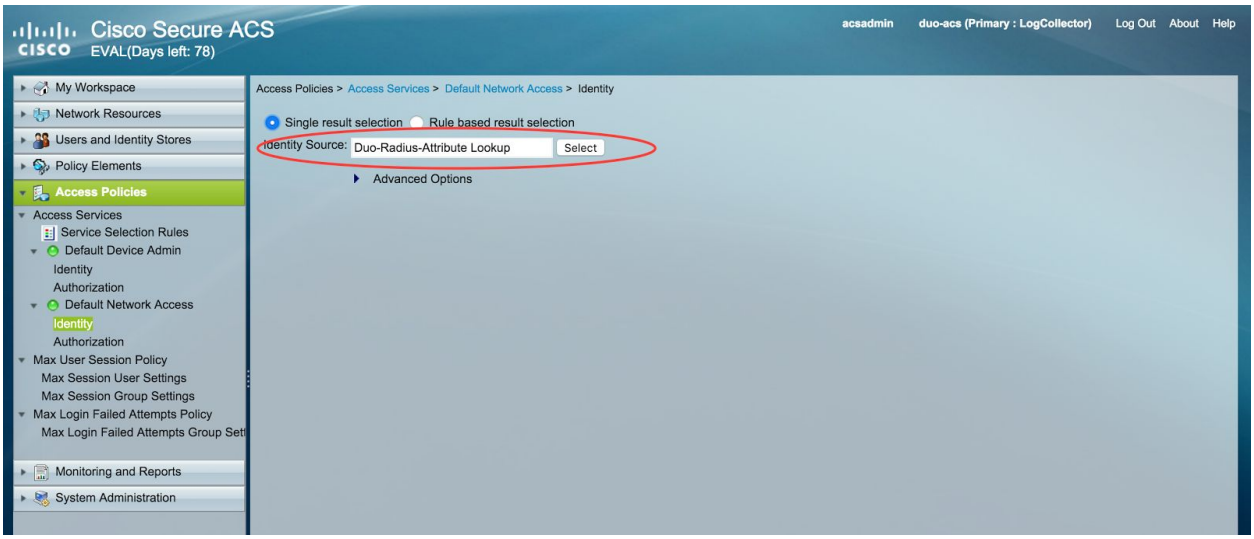


12. Now change your Access Policies to use the Identity Source you created for Duo. This is done under **Access Policies > Access Services > <Rule Name> > Identity**.

TACACS:



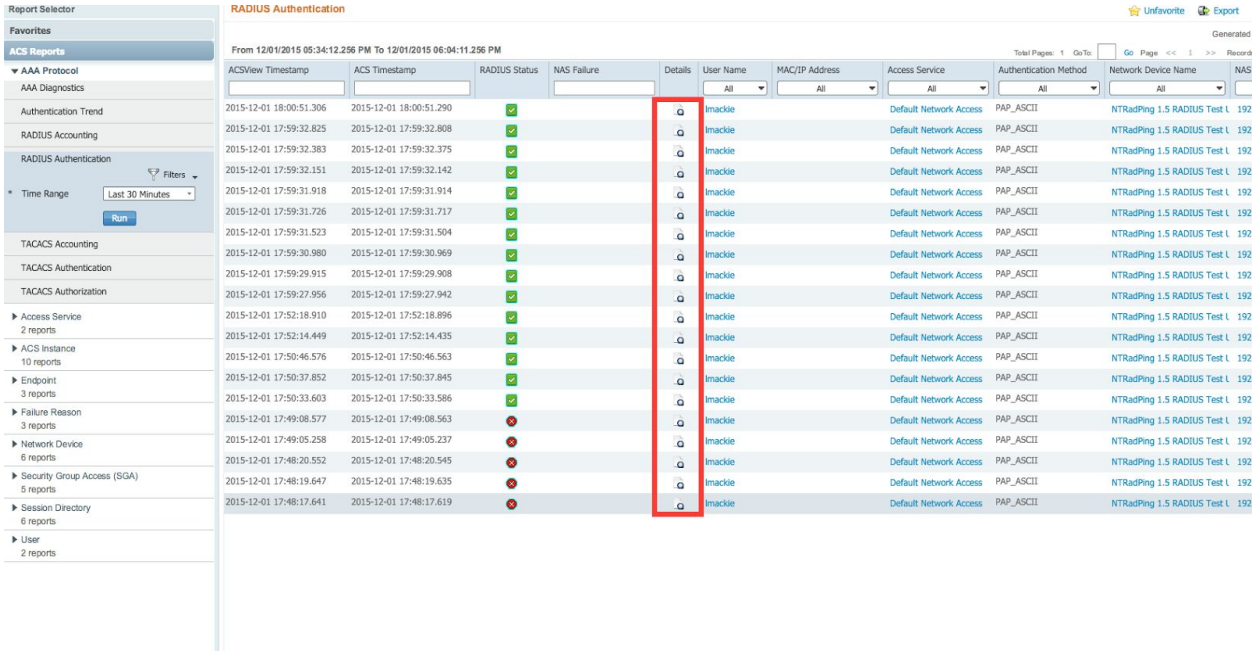
RADIUS:



ACS Troubleshooting

In the web interface, choose **Monitoring and Reports > Launch Monitoring and Report Viewer** to open the Monitoring and Reports Viewer in a secondary window. From here select Reports. This will also open

in a secondary window. Now you will want to select AAA Protocol and then RADIUS Authentication or TACACS+ Authentication. Clicking on the magnifying glass will take you to the authentication details for a request you are troubleshooting.

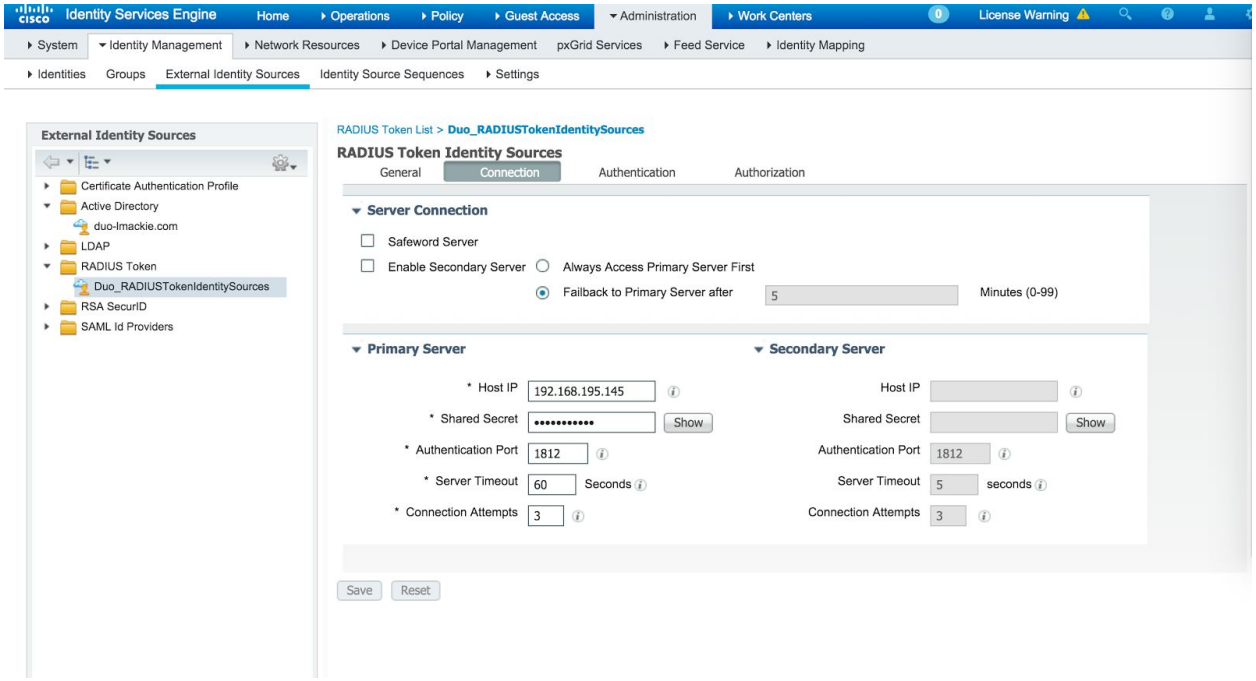


ISE Duo Integration Steps

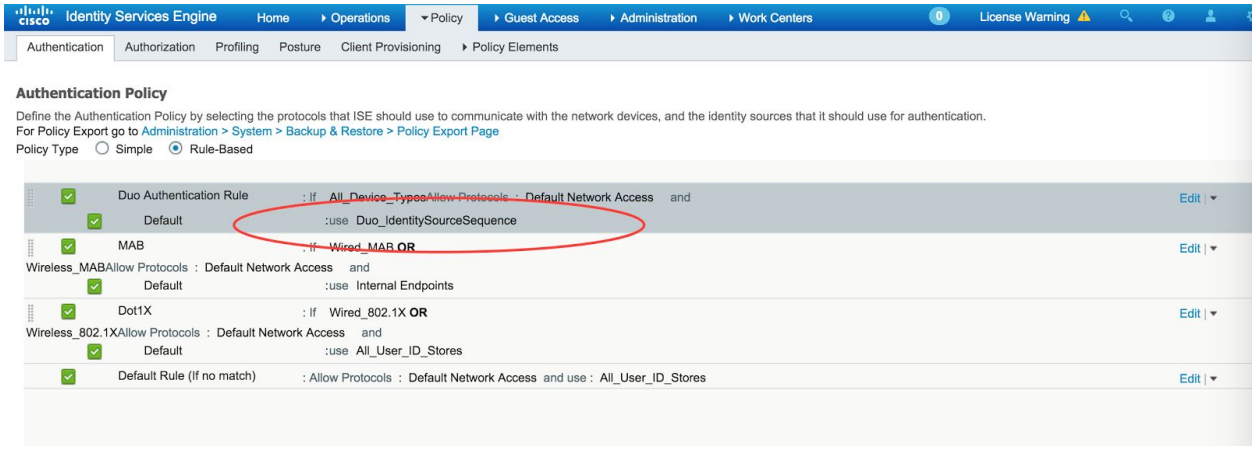
1. Sign up for a Duo account.
2. Log in to the Duo Admin Panel and navigate to **Applications**.
3. Click **Protect an Application** and locate **RADIUS** in the applications list. Click **Protect this Application** to get your **integration key**, **secret key**, and **API hostname**. See Getting Started for help.
4. Install the Duo Authentication Proxy
5. Configure the Proxy

```
[ad_client]
host=1.2.3.4
service_account_username=duoservice
service_account_password=password1
search_dn=cn=Users,dc=example,dc=com

[radius_server_auto]
ikey=DIXXXXXXXXXXXXXXXXX
skey=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
api_host=api-XXXXXXXX.duosecurity.com
radius_ip_1=<IP Address of the ISE Server>
radius_secret_1=thisisalsoaradiussecret
client=ad_client
port=1812
failmode=safe
```

6. Start the AuthProxy: `net start DuoAuthProxy`
7. Login to Cisco ISE
8. Go to **Administrators > External Identity Sources > RADIUS Token** and select **Add**
9. From here select **Connection** and then enter in IP Address of the AuthProxy Server, and Shared Secret of the AuthProxy server. Change the server timeout to 60 seconds and then select **Save**.



10. Now change your Authentication Policy to use the External Identity Source you created for Duo. This is done under **Policy > Authentication**.



ISE Troubleshooting

In the web interface, choose **Operations > RADIUS LiveLog**. This will show you all the RADIUS Authentications for the past 24 hours. Clicking on the magnifying glass will take you to the authentication details for a request you are troubleshooting.