



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=DIXXXXXXXXXXXXXXXXXXXXXX
skey=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
api_host=api-XXXXXXXXX.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**.

The screenshot shows the Cisco Secure ACS web interface. The breadcrumb navigation is "Users and Identity Stores > External Identity Stores > RADIUS Identity Servers > Edit: 'Duo-Radius'". The left sidebar shows the navigation tree with "RADIUS Identity Servers" selected. The main content area has tabs for "General", "Shell Prompts", "Directory Attributes", and "Advanced". The "General" tab is active and contains the following fields:

- Name: Duo-Radius
- Description: (empty)
- SafeWord Server:
- Server Connection:
 - Enable Secondary Server:
 - Always Access Primary Server First:
 - Fallback To Primary Server After: 0 Minutes
- Primary Server:
 - Hostname AAA: 192.168.195.145
 - Shared Secret: (masked with dots) [Show]
 - Authentication Port: 1812
 - Server Timeout: 60 Seconds
 - Connection Attempts: 3

A legend at the bottom indicates that a gear icon represents required fields. At the bottom of the form are "Submit" and "Cancel" buttons.

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



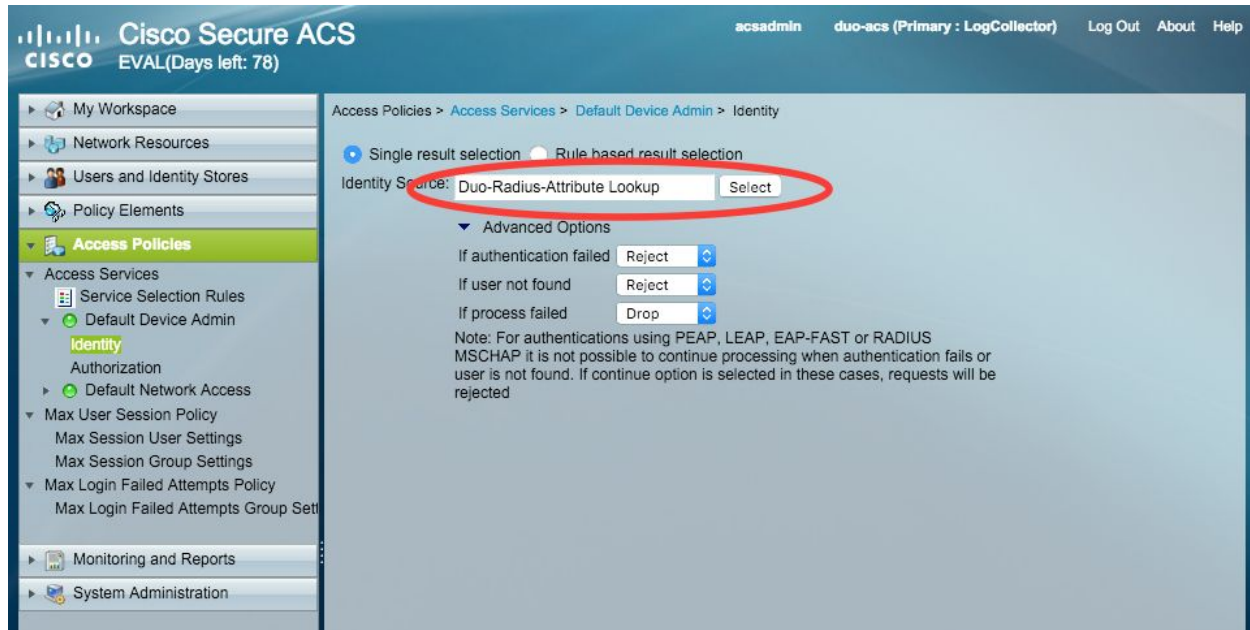
AuthProxy configuration under Selected and then move their AD server under Selected for Additional Attributes.

The screenshot shows the Cisco Secure ACS web interface. The left sidebar contains a navigation menu with categories like 'My Workspace', 'Network Resources', 'Users and Identity Stores', 'Policy Elements', 'Access Policies', 'Monitoring and Reports', and 'System Administration'. The 'Users and Identity Stores' section is expanded, showing 'Identity Groups', 'Internal Identity Stores', 'External Identity Stores', and 'Identity Store Sequences'. The main content area is titled 'Users and Identity Stores > Identity Store Sequences > Edit: "Duo-Radius-Attribute Lookup"'. It features several sections: 'General' with fields for 'Name' (Duo-Radius-Attribute Lookup) and 'Description'; 'Authentication Method List' with 'Certificate Based' unchecked and 'Password Based' checked; 'Authentication and Attribute Retrieval Search List' with 'Available' stores (AD1, Duo-LDAP, Internal Hosts, Internal Users, NAC Profiler) and 'Selected' stores (Duo-Radius); and 'Additional Attribute Retrieval Search List' with 'Available' stores (Duo-LDAP, Internal Hosts, Internal Users, NAC Profiler) and 'Selected' stores (AD1). A legend indicates that a gear icon represents required fields. At the bottom, there are 'Submit' and 'Cancel' buttons.

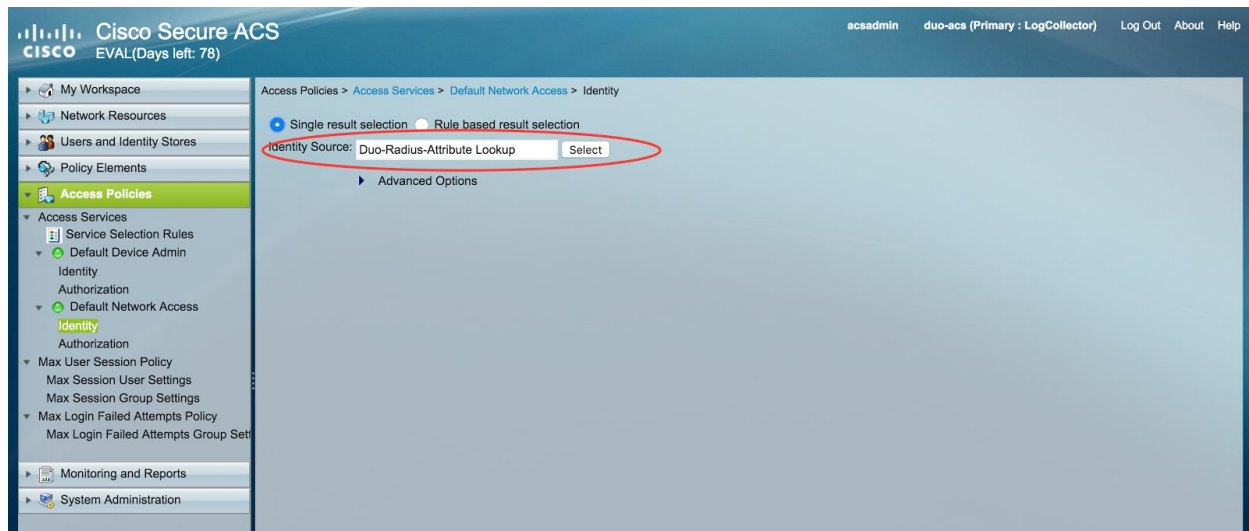
12. Now change your Access Policies to use the Identity Source you created for Duo. This is done under **Access Policies > Access Services > <Rule Name> > Identity**.



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.

Report Selector

FAVORITES

- ACS Reports
- AAA Protocol
- AAA Diagnostics
- Authentication Trend
- RADIUS Accounting
- RADIUS Authentication
- TACACS Accounting
- TACACS Authentication
- TACACS Authorization
- Access Service (2 reports)
- ACS Instance (10 reports)
- Endpoint (3 reports)
- Failure Reason (3 reports)
- Network Device (6 reports)
- Security Group Access (SGA) (5 reports)
- Session Directory (6 reports)
- User (2 reports)

RADIUS Authentication

From 12/01/2015 05:34:12.256 PM To 12/01/2015 06:04:11.256 PM

Unfavorite Export

Generated

Total Pages: 1 Go To: Go Page << >> Records

ACSView Timestamp	ACS Timestamp	RADIUS Status	NAS Failure	Details	User Name	MAC/IP Address	Access Service	Authentication Method	Network Device Name	NAS
2015-12-01 18:00:51.306	2015-12-01 18:00:51.290	✓		🔍	Imackie		Default Network Access	PAP_ASCII	NTRadPing 1.5 RADIUS Test L	192
2015-12-01 17:59:32.825	2015-12-01 17:59:32.808	✓		🔍	Imackie		Default Network Access	PAP_ASCII	NTRadPing 1.5 RADIUS Test L	192
2015-12-01 17:59:32.383	2015-12-01 17:59:32.375	✓		🔍	Imackie		Default Network Access	PAP_ASCII	NTRadPing 1.5 RADIUS Test L	192
2015-12-01 17:59:32.151	2015-12-01 17:59:32.142	✓		🔍	Imackie		Default Network Access	PAP_ASCII	NTRadPing 1.5 RADIUS Test L	192
2015-12-01 17:59:31.918	2015-12-01 17:59:31.914	✓		🔍	Imackie		Default Network Access	PAP_ASCII	NTRadPing 1.5 RADIUS Test L	192
2015-12-01 17:59:31.726	2015-12-01 17:59:31.717	✓		🔍	Imackie		Default Network Access	PAP_ASCII	NTRadPing 1.5 RADIUS Test L	192
2015-12-01 17:59:31.523	2015-12-01 17:59:31.504	✓		🔍	Imackie		Default Network Access	PAP_ASCII	NTRadPing 1.5 RADIUS Test L	192
2015-12-01 17:59:30.980	2015-12-01 17:59:30.969	✓		🔍	Imackie		Default Network Access	PAP_ASCII	NTRadPing 1.5 RADIUS Test L	192
2015-12-01 17:59:29.915	2015-12-01 17:59:29.908	✓		🔍	Imackie		Default Network Access	PAP_ASCII	NTRadPing 1.5 RADIUS Test L	192
2015-12-01 17:59:27.956	2015-12-01 17:59:27.942	✓		🔍	Imackie		Default Network Access	PAP_ASCII	NTRadPing 1.5 RADIUS Test L	192
2015-12-01 17:52:18.910	2015-12-01 17:52:18.896	✓		🔍	Imackie		Default Network Access	PAP_ASCII	NTRadPing 1.5 RADIUS Test L	192
2015-12-01 17:52:14.449	2015-12-01 17:52:14.435	✓		🔍	Imackie		Default Network Access	PAP_ASCII	NTRadPing 1.5 RADIUS Test L	192
2015-12-01 17:50:46.576	2015-12-01 17:50:46.563	✓		🔍	Imackie		Default Network Access	PAP_ASCII	NTRadPing 1.5 RADIUS Test L	192
2015-12-01 17:50:37.852	2015-12-01 17:50:37.845	✓		🔍	Imackie		Default Network Access	PAP_ASCII	NTRadPing 1.5 RADIUS Test L	192
2015-12-01 17:50:33.603	2015-12-01 17:50:33.586	✓		🔍	Imackie		Default Network Access	PAP_ASCII	NTRadPing 1.5 RADIUS Test L	192
2015-12-01 17:49:08.577	2015-12-01 17:49:08.563	✗		🔍	Imackie		Default Network Access	PAP_ASCII	NTRadPing 1.5 RADIUS Test L	192
2015-12-01 17:49:05.258	2015-12-01 17:49:05.237	✗		🔍	Imackie		Default Network Access	PAP_ASCII	NTRadPing 1.5 RADIUS Test L	192
2015-12-01 17:48:20.552	2015-12-01 17:48:20.545	✗		🔍	Imackie		Default Network Access	PAP_ASCII	NTRadPing 1.5 RADIUS Test L	192
2015-12-01 17:48:19.647	2015-12-01 17:48:19.635	✗		🔍	Imackie		Default Network Access	PAP_ASCII	NTRadPing 1.5 RADIUS Test L	192
2015-12-01 17:48:17.641	2015-12-01 17:48:17.619	✗		🔍	Imackie		Default Network Access	PAP_ASCII	NTRadPing 1.5 RADIUS Test L	192



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=DIXXXXXXXXXXXXXXXXXXXXX
skey=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
api_host=api-XXXXXXX.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**.



External Identity Sources

- Certificate Authentication Profile
- Active Directory
 - duo-lmackie.com
- LDAP
- RADIUS Token
 - Duo_RADIUSTokenIdentitySources
- RSA SecurID
- SAML Id Providers

RADIUS Token List > Duo_RADIUSTokenIdentitySources

RADIUS Token Identity Sources

General | **Connection** | Authentication | Authorization

Server Connection

- Safeword Server
- Enable Secondary Server
- Always Access Primary Server First
- Failback to Primary Server after 5 Minutes (0-99)

Primary Server

- Host IP: 192.168.195.145
- Shared Secret: [masked]
- Authentication Port: 1812
- Server Timeout: 60 Seconds
- Connection Attempts: 3

Secondary Server

- Host IP: []
- Shared Secret: [masked]
- Authentication Port: 1812
- Server Timeout: 5 seconds
- Connection Attempts: 3

Save Reset

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

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Policy Type Simple Rule-Based

Rule	Condition	Action
Duo Authentication Rule	:if All_Device_Types Allow-Protocols Default Network Access and	:use Duo_IdentitySourceSequence
MAB	:if Wired_MAB OR	
Dot1X	:if Wired_802.1X OR	
Default Rule (if no match)	: Allow Protocols : Default Network Access and use : All_User_ID_Stores	



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.

Time	Status	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device
2015-12-09 20:51:36.392	Success		Imackie			Default >> Duo Authen...	Default >> Duo Domai...	Duo_Access_Accept	NTRADPing
2015-12-09 20:51:32.936	Success		Imackie			Default >> Duo Authen...	Default >> Duo Domai...	Duo_Access_Accept	NTRADPing
2015-12-09 20:48:49.967	Failure		Imackie			Default >> Duo Authen...			NTRADPing