

# WLC 2FA using TACACS and Duo

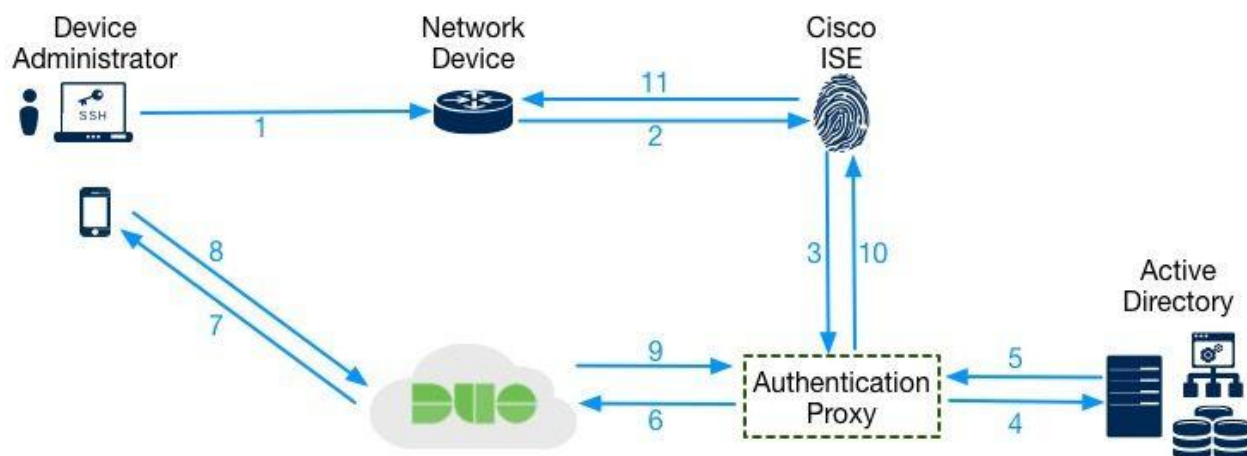
Detailed steps and Architecture diagram are referred from Cisco Community.

<https://community.cisco.com/t5/security-documents/duo-mfa-integration-with-ise-for-tacacs-device-administration/tac-p/3951156#M6538>

Configuration steps and testing are done in my home lab.

## Authentication and Authorization Flow

1. Admin user initiates a shell connection to a network device where he/she uses Active Directory based credentials
2. Network device forwards the request to the TACACS+ server (ISE)
3. ISE sends the authentication request to Duo's Authentication Proxy
4. The proxy forwards the request to Active Directory for the 1st factor authentication
5. Active Directory informs the Authentication Proxy if the authentication was successful
6. Upon successful AD authentication, the Authentication Proxy sends an authentication request to Duo cloud for 2nd factor authentication
7. Duo cloud sends a "push" to the admin user
8. Admin user "approves" the "push"
9. Duo informs the Authentication Proxy of the successful push
10. Authentication proxy informs ISE of a successful Authentication
11. ISE Authorizes the admin user



## Devices Used

- Cisco ISE version 2.6
- WLC 2504 8.5.135.0
- Windows Server 2008 R2
- Duo iOS App version 3.30.0.11

## WLC configuration

This is the simplest part, just point your WLC to ISE for TACACS authentication.

The screenshot shows the Cisco WLC configuration interface for TACACS+ Authentication Servers. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted), MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows the Security menu with AAA expanded to TACACS+ Authentication. The main content area displays a table with the following data:

Server Index	Server Address(Ipv4/Ipv6)	Port	Admin Status
1	192.168.129.10	49	Enabled

The screenshot shows the Cisco WLC configuration interface for TACACS+ Accounting Servers. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted), MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows the Security menu with AAA expanded to TACACS+ Accounting. The main content area displays a table with the following data:

Server Index	Server Address(Ipv4/Ipv6)	Port	Admin Status
1	192.168.129.10	49	Enabled

The screenshot shows the Cisco WLC configuration interface for TACACS+ Authorization Servers. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted), MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows the Security menu with AAA expanded to TACACS+ Authorization. The main content area displays a table with the following data:

Server Index	Server Address(Ipv4/Ipv6)	Port	Admin Status
1	192.168.129.10	49	Enabled

### Security

- ▼ AAA
  - General
  - ▼ RADIUS
    - Authentication
    - Accounting
    - Fallback
    - DNS
    - Downloaded AVP
  - ▼ TACACS+
    - Authentication
    - Accounting
    - Authorization
    - Fallback
    - DNS
  - LDAP
  - Local Net Users
  - MAC Filtering
  - ▼ Disabled Clients
  - User Login Policies
  - AP Policies
  - Password Policies
- ▶ Local EAP
- Advanced EAP
- ▼ Priority Order
  - Management User

### Priority Order > Management User

#### Authentication

Not Used		Order Used for Authentication	
RADIUS	>	TACACS+ LOCAL	Up
	<		Down

*If LOCAL is selected as second priority then user will be authenticated against LOCAL only if first priority is unreachable.*

## ISE configuration

Add WLC to ISE as network device and optionally assign it to a device group.

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC > Network Devices > Network Device Groups > Network Device Profiles > External RADIUS Servers > RADIUS Server Sequences > NAC Managers > External MDM > Location Services. The main page title is "Network Devices List > WLC". The left sidebar contains "Network Devices", "Default Device", and "Device Security Settings". The main content area is titled "Network Devices" and contains the following fields:

- \* Name: WLC
- Description: (empty)
- IP Address: \* IP: 192.168.129.50 / 32
- \* Device Profile: Cisco
- Model Name: (empty)
- Software Version: (empty)
- \* Network Device Group: (empty)
- Location: All Locations (Set To Default)
- IPSEC: No (Set To Default)
- Device Type: WLC (Set To Default)
- RADIUS Authentication Settings
- TACACS Authentication Settings
  - Shared Secret: (masked) (Show) (Retire) (i)
  - Enable Single Connect Mode:
  - Legacy Cisco Device
  - TACACS Draft Compliance Single Connect Support

Built TACACS policy starting with Result, again this can be any way you want to configure, for simplicity, I have configured full WLC access.

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID > Overview > Identities > User Identity Groups > Ext Id Sources > Network Resources > Policy Elements > Device Admin Policy Sets > Reports > Settings. The main page title is "TACACS Profiles > WLC FULL ACCESS". The left sidebar contains "Conditions", "Network Conditions", "Results", "Allowed Protocols", "TACACS Command Sets", and "TACACS Profiles". The main content area is titled "TACACS Profile" and contains the following fields:

- Name: WLC FULL ACCESS
- Description: (empty)
- Task Attribute View / Raw View (Task Attribute View selected)
- Common Tasks
  - Common Task Type: WLC
  - All
  - Monitor
  - Lobby
  - Selected
  - WLAN
  - Controller
  - Wireless
  - Security
  - Management
  - Commands
  - The configured options give a mgmtRole Debug value of 0xfffffff8 (i)
- Custom Attributes

## Configure external radius token (adding DUO proxy server on ISE)

Identity Services Engine Administration > External Identity Sources > RADIUS Token Identity Sources

**External Identity Sources**

- Certificate Authentication Profile
- Active Directory
  - pod1ad
  - LDAP
  - ODBC
- RADIUS Token
  - DUO**
  - RSA SecurID
  - SAML Id Providers
  - Social Login

**RADIUS Token List > DUO**

**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  Minutes (0-99)

**Primary Server**

- \* Host IP:  *i*
- \* Shared Secret:
- \* Authentication Port:  *i* ↔ custom port, can be anyport till the time its same on both ISE and DUO proxy
- \* Server Timeout:  Seconds *i* ↔ default is 30 sec, recommend it to increase it to 60
- \* Connection Attempts:  *i*

**Secondary Server**

- I don't have any secondary DUO proxy, but if you have you can configure secondary as well
- Host IP:  *i*
- Shared Secret:
- Authentication Port:  *i*
- Server Timeout:  seconds *i*
- Connection Attempts:  *i*

## Make sure your AD is integrated and active

Identity Services Engine Administration > External Identity Sources > pod1ad

**External Identity Sources**

- Certificate Authentication Profile
- Active Directory
  - pod1ad**
  - LDAP
  - ODBC
- RADIUS Token
  - RSA SecurID
  - SAML Id Providers

**Connection** | Whitelisted Domains | PassiveID | Groups | Attributes | Advanced Settings

- \* Join Point Name:  *i*
- \* Active Directory Domain:  *i*

Join | Leave | Test User | Diagnostic Tool | Refresh Table

<input type="checkbox"/>	ISE Node	ISE Node Role	Status	Domain Controller	Site
<input type="checkbox"/>	ise.pod1.com	STANDALONE	<input checked="" type="checkbox"/> Operational	winsrv.pod1.com	Default-First-Site-Name

## Create Identity Source sequence

Cisco Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Identity Source Sequences List > DUO\_AD

### Identity Source Sequence

#### Identity Source Sequence

\* Name

Description

#### Certificate Based Authentication

Select Certificate Authentication Profile

#### Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available

Internal Endpoints  
Internal Users  
Guest Users  
All\_AD\_Join\_Points

Selected

DUO  
pod1ad

#### Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

- Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"
- Treat as if the user was not found and proceed to the next store in the sequence

Built authentication and authorization policy, again there are multiple ways to go about it, I have just done in a simple way.

Policy Sets → Default

Reset All Hitcounts Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	Default	Tacacs Default policy set		Default Device Admin	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✔	Default		DUO_AD	0	<input type="text" value="REJECT"/> <input type="text" value="REJECT"/> <input type="text" value="DROP"/>

Authorization Policy (2)

+	Status	Rule Name	Conditions	Results	
				Command Sets	Shell Profiles
Search					
+	✔	WLC_TACACS_AUTZ	AND	DEVICE Device Type EQUALS All Device Types#WLC Network Access Protocol EQUALS TACACS+ pod1a3 ExternalGroups EQUALS pod1.com/Users/Domain Admins	Select from list + WLC FULL ACCESS x - +
+	✔	Default			DenyAllCommands + Deny All Shell Profile x - +

## Configure DUO

Login to duo portal and choose the application you want to protect, in our case Cisco ISE, click protect this application. If you don't have duo account, you can create a free one for 30 days.

DUO

Dashboard

Device Insight

Policies

**Applications**

Protect an Application

Users

Groups

Endpoints

2FA Devices

Administrators

Reports

Phishing

Search for users, groups, applications, or devices

Dashboard > Applications > Protect an Application

## Protect an Application

Add an application that you'd like to protect with Duo two-factor authentication. You can start with a small "proof-of-concept" installation — it takes just a few minutes, and you're the only one that w

Documentation: [Getting Started](#)

**Choose an application below to get started.**

RADIUS

**Cisco ISE RADIUS** [Protect this Application](#) | [Read the documentation](#)

Note down integration key, Secret Key and API hostname, you will need when configuring DUO proxy.

Dashboard > Applications > Cisco ISE RADIUS

## Cisco ISE RADIUS

Follow the [Cisco ISE RADIUS instructions](#).

### Details

**Integration key**  [select](#)

**Secret key**  [select](#)

Don't write down your secret key or share it with anyone.

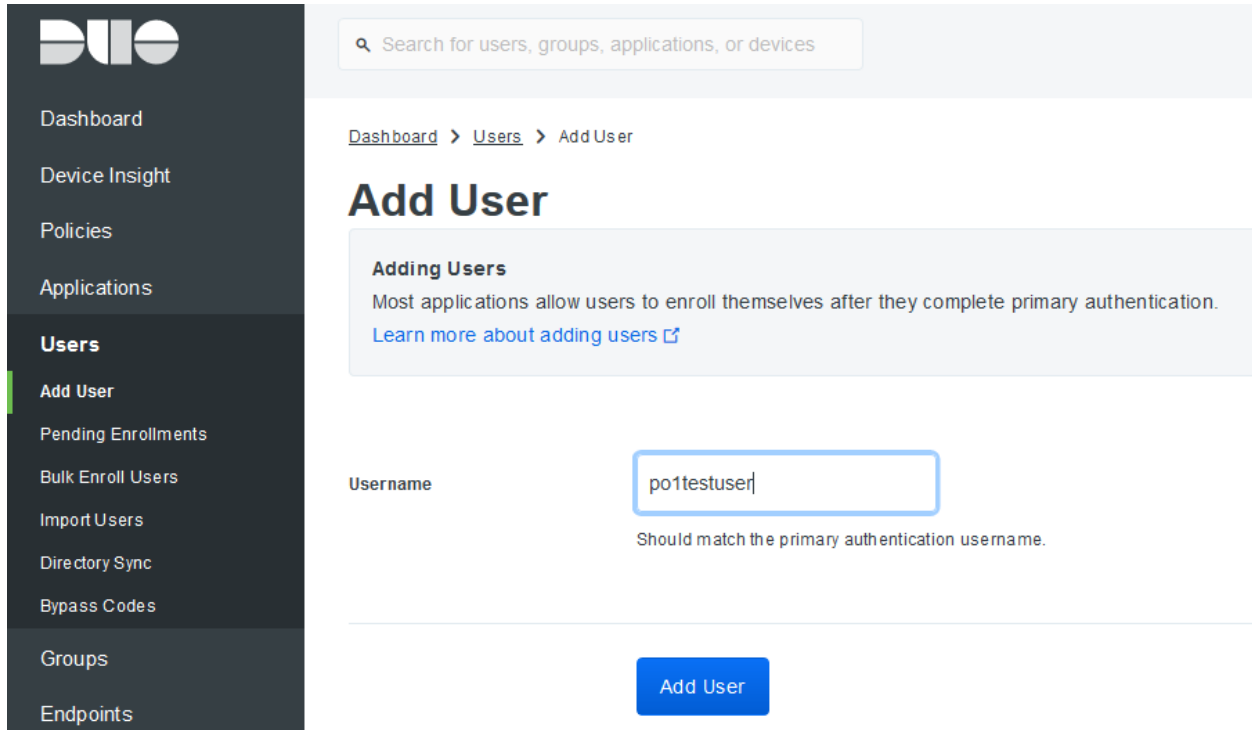
**API hostname**  [select](#)



You will need users enrolled through DUO to authenticate, you can integrate AD group or add users manually, for convenience of this configuration, I have added myself manually. Look through DUO documentation for full user integration and bulk enrollment.

<https://duo.com/docs/enrolling-users>

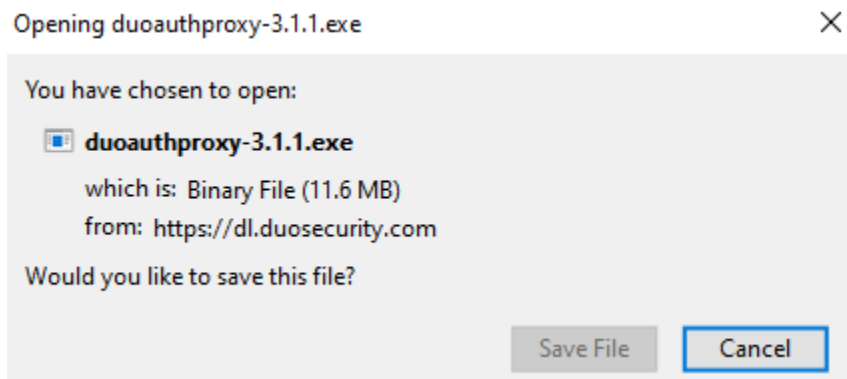
If you have only few admins, you need access to network devices then just adding users manually should work fine. This username should match AD username or whatever name to be defined In your ISE policy to authenticate users. In my case as you will see, the user has to be part of domain admin to access device.



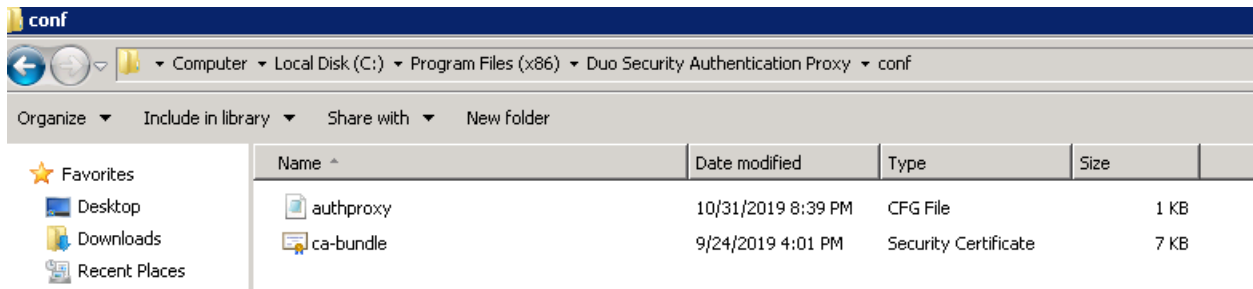
Download authentication proxy setup file from

<https://duo.com/docs/authproxy-reference>

I am using Windows Server 2008 R2 or later (Server 2016 or 2019 recommended) as authentication proxy.



Once installation is complete, configure the DUO proxy settings by editing authproxy file.



### ad\_client

Add an `[ad_client]` section if you'd like to use an Active Directory domain controller to perform primary authentication. This section accepts the following options:

#### REQUIRED

<code>host</code>	The hostname or IP address of your domain controller.
<code>service_account_username</code>	The username of an account that has permission to read from your Active Directory database. We recommend creating a service account that has read-only access.
<code>service_account_password</code>	The password corresponding to <code>service_account_username</code> . If you're on Windows and would like to encrypt this password, see <a href="#">Encrypting Passwords</a> and use <code>service_account_password_protected</code> instead.
<code>search_dn</code>	The LDAP distinguished name (DN) of an Active Directory container or organizational unit (OU) containing all of the users you wish to permit to log in. For example: <pre>search_dn=DC=example,DC=com</pre>

To use RADIUS Auto, add a [radius\_server\_auto] section, which accepts the following options:

**REQUIRED**

<code>ikey</code>	Your Duo integration key, obtained from the details page for the application in the Duo Admin Panel.						
<code>skey</code>	Your Duo secret key, obtained from the details page for the application in the Duo Admin Panel.  If you're on Windows and would like to encrypt this password, see <a href="#">Encrypting Passwords</a> and use <code>skey_protected</code> instead.						
<code>api_host</code>	Your Duo API hostname (e.g. <code>api-XXXXXXXXX.duosecurity.com</code> ), obtained from the details page for the application in the Duo Admin Panel.						
<code>radius_ip_1</code>	IP address or IP address range for RADIUS clients. Only clients with configured addresses and shared secrets will be allowed to send requests to the Authentication Proxy. If two server configurations have the same or overlapping IP ranges, the request will go to whichever comes first in the file.  This can be a single IP address (e.g. <code>1.2.3.4</code> ), a specification in CIDR notation (e.g. <code>1.2.3.0/24</code> ), or an IP address range (e.g. <code>3.3.3.3 - 3.3.3.6</code> for the IPs 3.3.3.3, 3.3.3.4, 3.3.3.5, and 3.3.3.6).						
<code>radius_secret_1</code>	The secret shared with RADIUS clients matching <code>radius_ip_1</code> .  If you're on Windows and would like to encrypt this password, see <a href="#">Encrypting Passwords</a> and use <code>radius_secret_protected_1</code> instead.						
<code>client</code>	The mechanism that the Authentication Proxy should use to perform primary authentication. This should correspond with a "client" section elsewhere in the config file. <table border="1" data-bbox="444 1100 1208 1346"> <tr> <td><code>ad_client</code></td> <td>Use Active Directory for primary authentication. Make sure you have an <code>[ad_client]</code> section configured.</td> </tr> <tr> <td><code>radius_client</code></td> <td>Use RADIUS for primary authentication. Make sure you have a <code>[radius_client]</code> section configured.</td> </tr> <tr> <td><code>duo_only_client</code></td> <td>Do not perform primary authentication. Make sure you have a <code>[duo_only_client]</code> section configured.</td> </tr> </table> <p>This parameter is optional if you only have one "client" section. If you have multiple, each "server" section should specify which "client" to use.</p>	<code>ad_client</code>	Use Active Directory for primary authentication. Make sure you have an <code>[ad_client]</code> section configured.	<code>radius_client</code>	Use RADIUS for primary authentication. Make sure you have a <code>[radius_client]</code> section configured.	<code>duo_only_client</code>	Do not perform primary authentication. Make sure you have a <code>[duo_only_client]</code> section configured.
<code>ad_client</code>	Use Active Directory for primary authentication. Make sure you have an <code>[ad_client]</code> section configured.						
<code>radius_client</code>	Use RADIUS for primary authentication. Make sure you have a <code>[radius_client]</code> section configured.						
<code>duo_only_client</code>	Do not perform primary authentication. Make sure you have a <code>[duo_only_client]</code> section configured.						

Example, the key, secret and api\_hostname are the ones discussed above. Note how the port number defined is same as radius token defined on ISE.

```

authproxy - Notepad
File Edit Format View Help
[ad_client]
host=192.168.129.13
service_account_username=duoservice
service_account_password=
search_dn=DC=pod1,DC=com

[radius_server_auto]
ikey=
skey=
api_host=
radius_ip_1=192.168.129.10
radius_secret_1=
client=ad_client
port=18120
failmode=safe

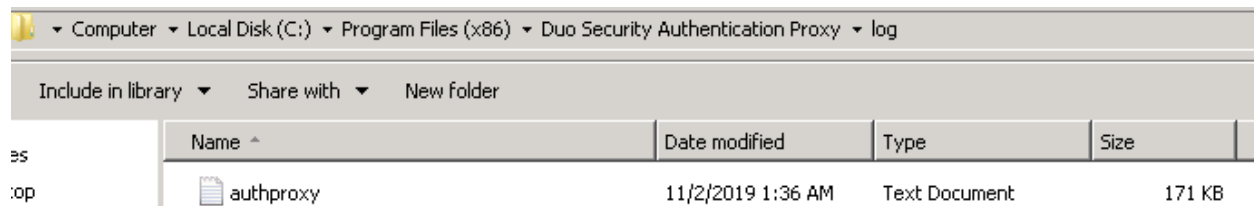
```

Once setup start the Proxy service for DUO, access as administrator.



At this point the DUO proxy should be listening for connections.

You can open the log file and see the logs to verify



```
2019-10-31T20:39:57+0000 [-] DuoForwardServer starting on 18120
2019-10-31T20:39:57+0000 [-] Starting protocol <duoauthproxy.lib.forward_serv.DuoForwardServer object at 0x02D97CF0>
2019-10-31T20:39:57+0000 [-] FIPS mode is not enabled
2019-10-31T20:39:57+0000 [-] AD Client Module Configuration:
2019-10-31T20:39:57+0000 [-] {'host': '192.168.129.13',
  'search_dn': 'DC=pod1,DC=com',
  'service_account_password': '*****',
  'service_account_username': 'duoservice'}
2019-10-31T20:39:57+0000 [-] RADIUS Automatic Factor Server Module Configuration:
2019-10-31T20:39:57+0000 [-] {'api_host': '...',
  'client': 'ad_client',
  'failmode': 'safe',
  'ikey': '...',
  'port': '18120',
  'radius_ip_1': '192.168.129.10',
  'radius_secret_1': '*****',
  'skey': '*****[40]'}
2019-10-31T20:39:57+0000 [-] Duo Security Authentication Proxy 3.1.1 - Init Complete
```

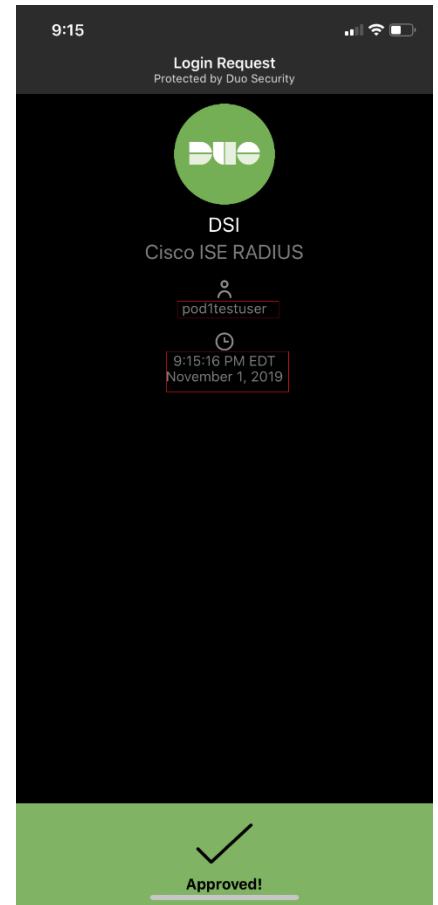
You can also confirm that the Proxy is able to communicate with AD and Radius

```
2019-10-31T20:39:57+0000 [duoauthproxy.lib.log#info] Testing section 'ad_client' with configuration:
2019-10-31T20:39:57+0000 [duoauthproxy.lib.log#info] {'host': '192.168.129.13',
  'search_dn': 'DC=pod1,DC=com',
  'service_account_password': '*****',
  'service_account_username': 'duoservice'}
2019-10-31T20:39:57+0000 [duoauthproxy.lib.log#info] There are no configuration problems
2019-10-31T20:39:57+0000 [duoauthproxy.lib.log#info] -----
2019-10-31T20:39:57+0000 [duoauthproxy.lib.log#info] Testing section 'radius_server_auto' with configuration:
2019-10-31T20:39:57+0000 [duoauthproxy.lib.log#info] {'api_host': '...',
  'client': 'ad_client',
  'failmode': 'safe',
  'ikey': '...',
  'port': '18120',
  'radius_ip_1': '192.168.129.10',
  'radius_secret_1': '*****',
  'skey': '*****[40]'}
2019-10-31T20:39:57+0000 [duoauthproxy.lib.log#info] There are no configuration problems
2019-10-31T20:39:57+0000 [duoauthproxy.lib.log#info] -----
2019-10-31T20:39:57+0000 [duoauthproxy.lib.log#info] SUMMARY
2019-10-31T20:39:57+0000 [duoauthproxy.lib.log#info] No issues detected
```

## Testing

### Login to WLC CLI

```
192.168.129.50:22 - Tera Term VT
File Edit Setup Control Window Help
User: podttestuser
Password: *****
(2504WLC) > show time
Time..... Fri Nov 1 09:15:29 2019
Timezone delta..... 0:0
Timezone location..... (GMT -5:00) Eastern Time (US a
nd Canada)
NTP Servers
NTP Version..... 3
NTP Polling Interval..... 600
Index      NTP Key Index      NTP Server      Status
NTP Msg Auth Status
-----
(2504WLC) >
```



## ISE Logs

Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device N...	Network Device IP	Device Type
✓	🔒	podttestuser	Authorization	Authentication Policy	Default >> WLC_TACACS_AUTZ	ise	WLC	192.168.129.50	Device Type#All Dev...
✓	🔒	podttestuser	Authentication	Default >> Default		ise	WLC	192.168.129.50	Device Type#All Dev...

## Auth Proxy Log

```
[DuoForwardServer (UDP)] Received new request id 11 from ('192.168.129.10', 36360)
[DuoForwardServer (UDP)] (('192.168.129.10', 36360), podttestuser, 11): login attempt for username 'podttestuser'
[DuoForwardServer (UDP)] Sending AD authentication request for 'podttestuser' to '192.168.129.13'
[duoauthproxy.modules.ad_client._ADAuthClientFactory#info] Starting factory <duoauthproxy.modules.ad_client._ADAuthClientFactory object at 0x02FEBE30>
[duoauthproxy.modules.ad_client._ADAuthClientFactory#info] http POST to https://[redacted].duosecurity.com:443/rest/v1/preauth
[duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <duoauthproxy.lib.http._DuoHTTPClientFactory: https://[redacted].duosecurity.com:443/rest/v1/preauth>
[duoauthproxy.modules.ad_client._ADAuthClientFactory#info] Stopping factory <duoauthproxy.modules.ad_client._ADAuthClientFactory object at 0x02FEBE30>
[HTTPPageGetter (TLSMemoryBIOProtocol),client] (('192.168.129.10', 36360), podttestuser, 11): Got preauth result for: 'auth'
[HTTPPageGetter (TLSMemoryBIOProtocol),client] Invalid ip, ip was None
[HTTPPageGetter (TLSMemoryBIOProtocol),client] http POST to https://[redacted].duosecurity.com:443/rest/v1/auth
[duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <duoauthproxy.lib.http._DuoHTTPClientFactory: https://api-7d069152.duosecurity.com:443/rest/v1/auth>
[duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <duoauthproxy.lib.http._DuoHTTPClientFactory: https://api-7d069152.duosecurity.com:443/rest/v1/preauth>
[HTTPPageGetter (TLSMemoryBIOProtocol),client] (('192.168.129.10', 36360), podttestuser, 11): Duo authentication returned 'allow': success. Logging in in...
[HTTPPageGetter (TLSMemoryBIOProtocol),client] (('192.168.129.10', 36360), podttestuser, 11): Returning response code 2: AccessAccept
[HTTPPageGetter (TLSMemoryBIOProtocol),client] (('192.168.129.10', 36360), podttestuser, 11): Sending response
[duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <duoauthproxy.lib.http._DuoHTTPClientFactory: https://[redacted].duosecurity.com:443/rest/v1/auth>
```