

Configure Duo Two Factor Authentication for ISE Management Access

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Network Diagram](#)

[Configuration](#)

[Duo Configuration](#)

[ISE Configuration](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes the steps required to configure external two-factor authentication for Identity Services Engine (ISE) management access. In this example, the ISE administrator authenticates against the RADIUS token server and an additional authentication in the form of push notification is sent by Duo Authentication Proxy server to the administrator's mobile device.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- RADIUS Protocol
- Configuring ISE RADIUS Token server and identities

Components Used

The information in this document is based on these software and hardware versions:

- Identity Services Engine (ISE)
- Active Directory (AD)
- Duo Authentication Proxy Server
- Duo Cloud Service

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.


```
radius_ip_1=10.127.196.189
radius_secret_1=*****
failmode=secure
client=ad_client
port=1812
```

Sample IP address of the ISE server

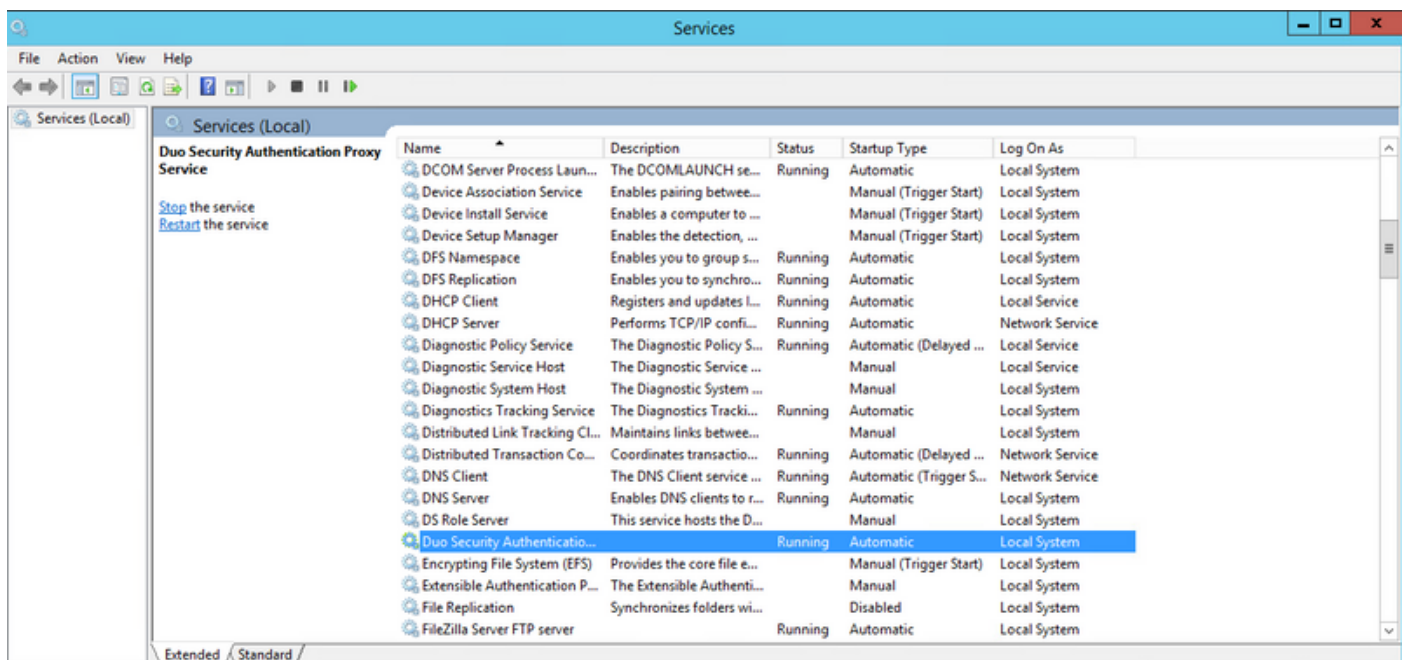
Step5. Configure ad_client with your Active Directory details. Duo Auth Proxy uses the below information to authenticate against AD for the primary authentication.

```
[ad_client]
host=10.127.196.230
service_account_username=< AD-username >
service_account_password=< AD-password >
search_dn=CN=Users,DC=gce,DC=iselab,DC=local
```

Sample IP address of the Active Directory

Note: If your network requires HTTP proxy connection for internet access, add http_proxy details in authproxy.cfg.

Step6. Restart the Duo Security Authentication Proxy Service. Save the file and **Restart** the **Duo service** on the windows machine. Open the Windows Services console (services.msc), locate **Duo Security Authentication Proxy Service** in the list of services, and click **Restart** as shown in the image:



Step7. Create a username and activate Duo Mobile on the end device:

<https://duo.com/docs/administration-users#creating-users-manually>

Add user on Duo Admin Panel. Navigate to **Users > add users**, as shown in the image:

The screenshot shows the Duo Admin console interface. On the left is a dark sidebar with navigation options: Dashboard, Policies, Applications, Users (highlighted), Add User (highlighted), Pending Enrollments, Bulk Enroll Users, Import Users, Directory Sync, Bypass Codes, 2FA Devices, Groups, Administrators, and Reports. The main content area has a search bar at the top with the text "Search for users, groups, applications, or devices". Below the search bar is a breadcrumb trail: "Dashboard > Users > Add User". The main heading is "Add User". A section titled "Adding Users" contains the text "Most applications allow users to enroll themselves after they complete primary authentication." and a link "Learn more about adding users". Below this is a form field for "Username" with the value "duoadmin" and a note "Should match the primary authentication username.". At the bottom right of the form is a blue "Add User" button.

Ensure the end user has the Duo app installed on the phone.

The screenshot shows the "Phones" section of the Duo Admin console. It features a heading "Phones" and a sub-heading "You may rearrange the phones by dragging and dropping in the table." On the right side, there is a blue "Add Phone" button. Below the text is a large empty box with the message "This user has no phones. [Add one.](#)"

The screenshot shows the Duo Admin console "Add Phone" page. The sidebar is the same as in the previous image, but "Users" is highlighted, and "Add User" is selected. The main content area has a search bar at the top with the text "Search for users, groups, applications, or devices". Below the search bar is a breadcrumb trail: "Dashboard > Users > duoadmin > Add Phone". The main heading is "Add Phone". Under the heading, there is a "Type" section with two radio buttons: "Phone" (selected) and "Tablet". Below this is a form field for "Phone number" with a dropdown menu showing the United States flag and the value "+1 201-555-5555". To the right of the phone number field is a link "Show extension field". At the bottom right of the form is a blue "Add Phone" button.

Select **Activate Duo Mobile**, as shown in the image:

Device Info



Not using Duo Mobile
[Activate Duo Mobile](#)

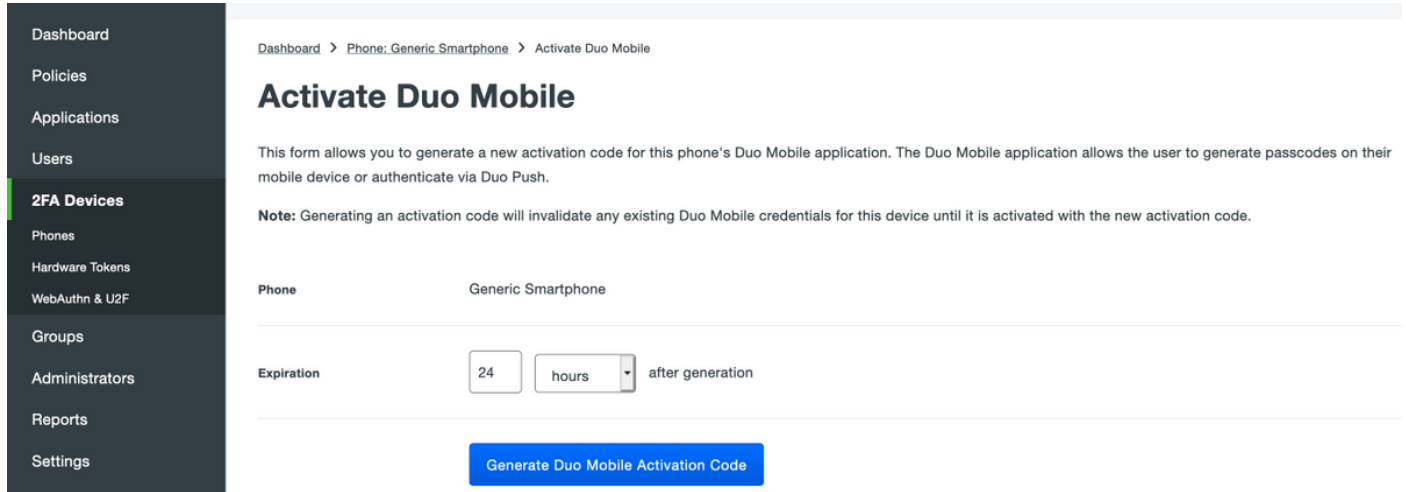


Model
Unknown



OS
Generic Smartphone

Select **Generate Duo Mobile Activation Code**, as shown in the image:



Dashboard > Phone: Generic Smartphone > Activate Duo Mobile

Activate Duo Mobile

This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to generate passcodes on their mobile device or authenticate via Duo Push.

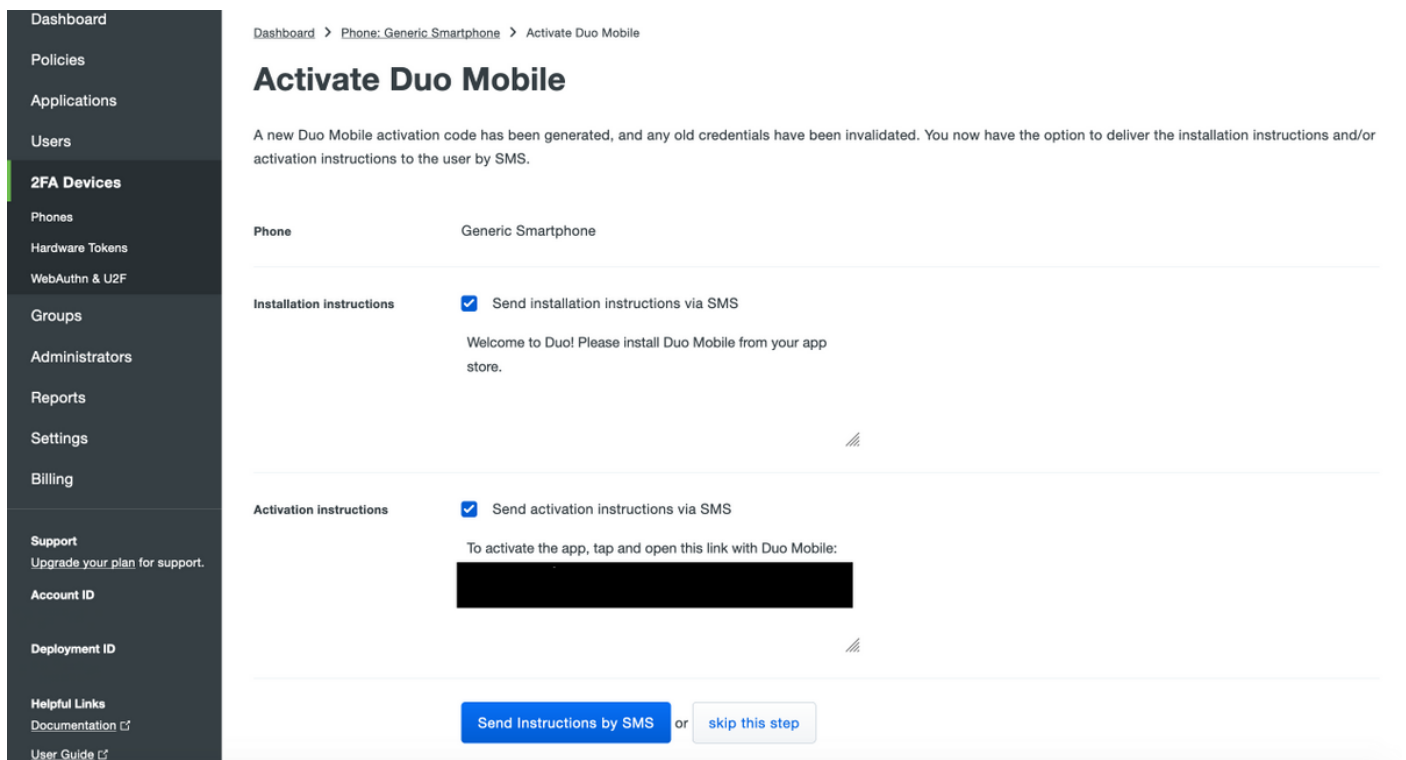
Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.

Phone: Generic Smartphone

Expiration: 24 hours after generation

[Generate Duo Mobile Activation Code](#)

Select **Send Instructions by SMS**, as shown in the image:



Dashboard > Phone: Generic Smartphone > Activate Duo Mobile

Activate Duo Mobile

A new Duo Mobile activation code has been generated, and any old credentials have been invalidated. You now have the option to deliver the installation instructions and/or activation instructions to the user by SMS.

Phone: Generic Smartphone

Installation instructions: Send installation instructions via SMS

Welcome to Duo! Please install Duo Mobile from your app store.

Activation instructions: Send activation instructions via SMS

To activate the app, tap and open this link with Duo Mobile:

[Send Instructions by SMS](#) or [skip this step](#)

Click the link in the SMS, and Duo app gets linked to the user account in the **Device Info** section, as shown in the image:

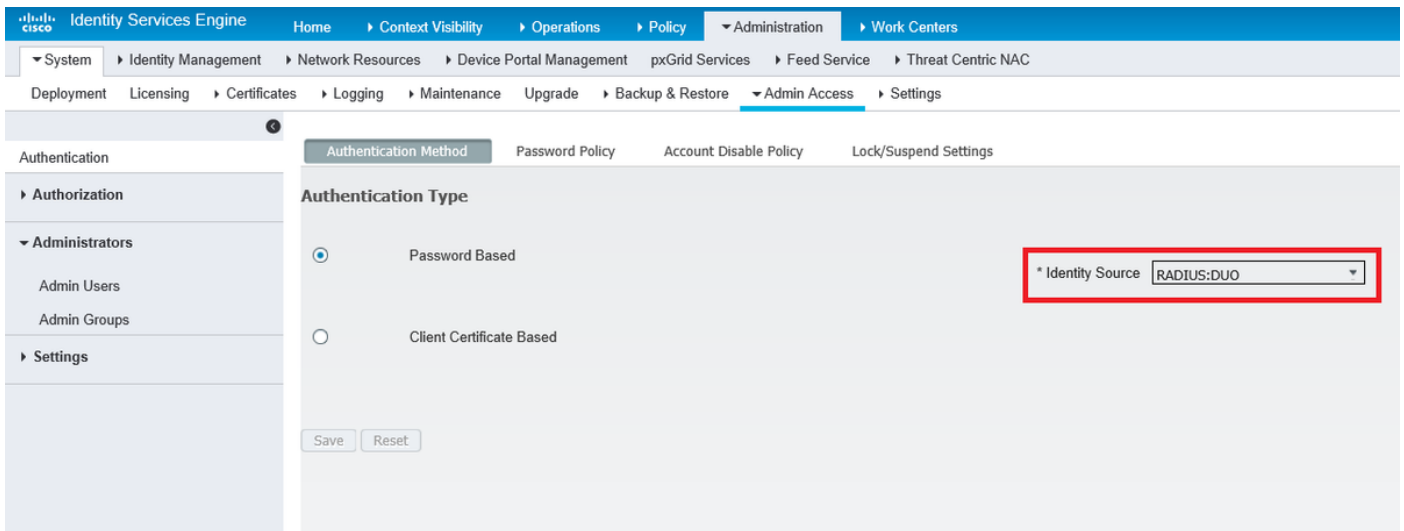
ISE Configuration

Step1. Integrate ISE with Duo Auth Proxy.

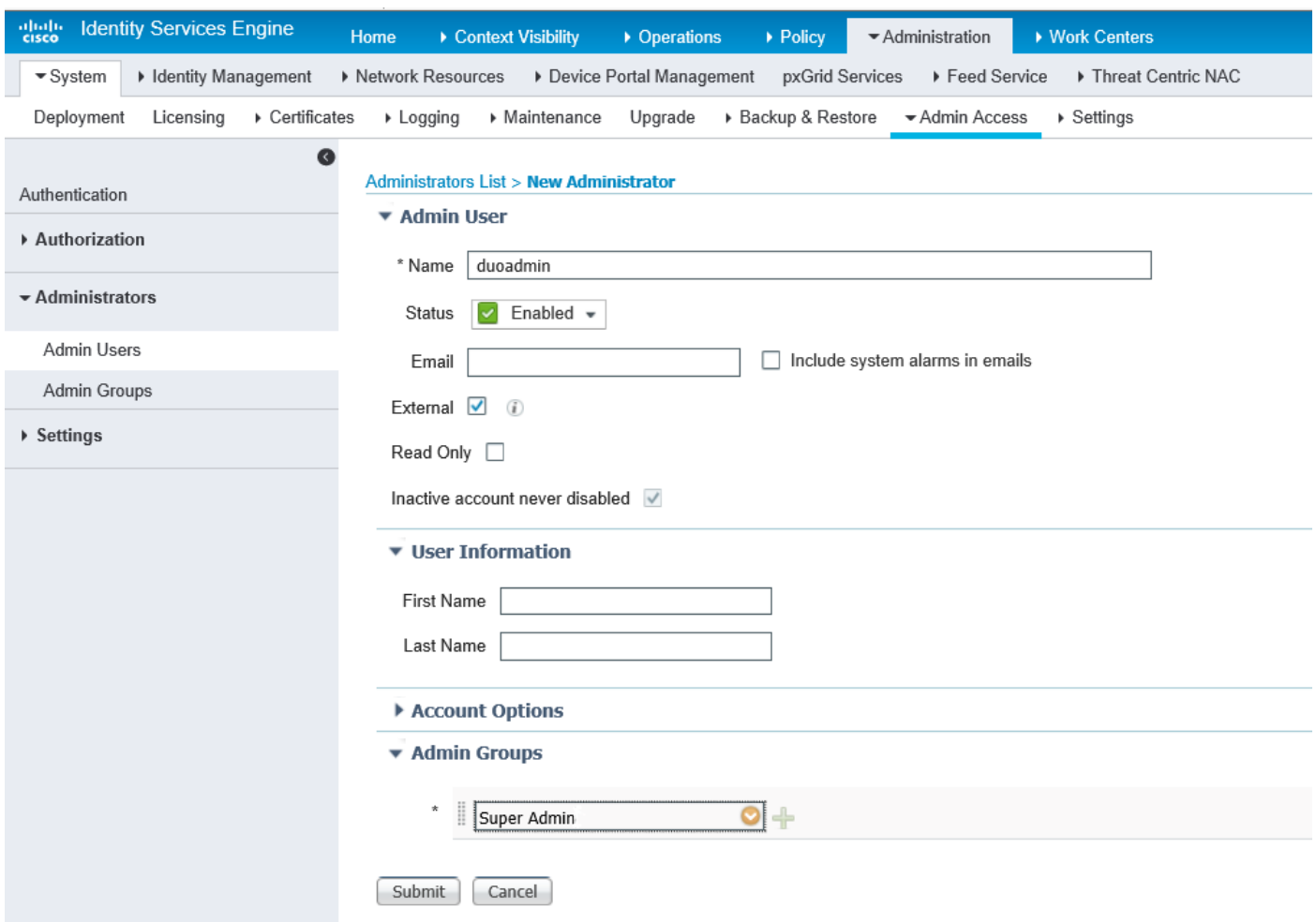
Navigate to **Administration > Identity Management > External Identity Sources > RADIUS Token**, click **Add** to add a new RADIUS Token server. Define server name in general tab, IP address and shared key in connection tab, as shown in the image:

Note: Set Server Timeout as 60 seconds so that users have enough time to act on the push

Step2. Navigate to **Administration > System > Admin Access > Authentication > Authentication Method** and **Select** previously configured RADIUS token server as the Identity Source, as shown in the image:



Step3. Navigate to **Administration > System > Admin Access > Administrators > Admin Users** and Create an admin user as External and provide super admin privilege, as shown in the image:



Verify

Use this section in order to confirm that your configuration works properly.

Open the ISE GUI, select RADIUS Token Server as Identity Source and login with admin user.



Identity Services Engine

Username

Password

Identity Source

[Problem logging in?](#)

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

To troubleshoot issues related to Duo proxy connectivity with Cloud or Active Directory, enable debug on Duo Auth Proxy by adding "debug=true" under main section of authproxy.cfg.

The logs are located under the following location:

C:\Program Files (x86)\Duo Security Authentication Proxy\log

Open the file **authproxy.log** in a text editor such as Notepad++ or WordPad.

Log snippets of Duo Auth Proxy receiving request from ISE and sending it to Duo Cloud.

```
2019-08-19T04:59:27-0700 [DuoForwardServer (UDP)] Sending request from 10.127.196.189 to radius_server_auto
2019-08-19T04:59:27-0700 [DuoForwardServer (UDP)] Received new request id 2 from ('10.127.196.189', 62001)
2019-08-19T04:59:27-0700 [DuoForwardServer (UDP)] (('10.127.196.189', 62001), duoadmin, 2): login attempt for username u'duoadmin'
2019-08-19T04:59:27-0700 [DuoForwardServer (UDP)] Sending AD authentication request for 'duoadmin' to '10.127.196.230'
2019-08-19T04:59:27-0700 [duoauthproxy.modules.ad_client._ADAuthClientFactory#info] Starting factory
```


Log snippets of Duo Auth Proxy unable to reach Duo Cloud.

```
2019-08-19T04:59:27-0700 [duoauthproxy.modules.ad_client._ADAuthClientFactory#info] Stopping
factory
2019-08-19T04:59:37-0700 [-] Duo preauth call failed
Traceback (most recent call last):
File "twisted\internet\defer.pyc", line 654, in _runCallbacks
File "twisted\internet\defer.pyc", line 1475, in getResult
File "twisted\internet\defer.pyc", line 1416, in _inlineCallbacks
File "twisted\python\failure.pyc", line 512, in throwExceptionIntoGenerator

File "duoauthproxy\lib\radius\duo_server.pyc", line 111, in preauth
File "twisted\internet\defer.pyc", line 1416, in _inlineCallbacks
File "twisted\python\failure.pyc", line 512, in throwExceptionIntoGenerator
File "duoauthproxy\lib\duo_async.pyc", line 246, in preauth
File "twisted\internet\defer.pyc", line 1416, in _inlineCallbacks
File "twisted\python\failure.pyc", line 512, in throwExceptionIntoGenerator
File "duoauthproxy\lib\duo_async.pyc", line 202, in call
File "twisted\internet\defer.pyc", line 654, in _runCallbacks
File "duoauthproxy\lib\duo_async.pyc", line 186, in err_func
duoauthproxy.lib.duo_async.DuoAPIFailOpenError: API Request Failed: DNSLookupError('api-
xxxxxxxxx.duosecurity.com',)

2019-08-19T04:59:37-0700 [-] (('10.127.196.189', 62001), duoadmin, 3): Failmode Secure - Denied
Duo login on preauth failure
2019-08-19T04:59:37-0700 [-] (('10.127.196.189', 62001), duoadmin, 3): Returning response code
3: AccessReject
2019-08-19T04:59:37-0700 [-] (('10.127.196.189', 62001), duoadmin, 3): Sending response
```

Related Information

- [RA VPN authentication using DUO](#)
- [Technical Support & Documentation - Cisco Systems](#)