



# Configure Duo Single Sign-On Authentication for Remote Workers Using Secure Firewall Management Center

---

**First Published:** 2023-12-13

**Last Modified:** 2024-01-25

## Configure Duo Single Sign-On for Remote Workers Using Secure Firewall Management Center

### About Duo Single Sign-On

Duo Single Sign-On (SSO) provides users with easy access to and a consistent login experience across all the essential applications in an organization. By enabling Duo SSO, users do not have to remember multiple passwords, reducing the risks associated with credential compromise, and taking a key step towards a password-less future.

This guide provides instructions on using the cloud-hosted Duo SSO solution to secure your remote access VPN tunnel with your user's existing credentials in a local active directory or a SAML identity provider. The sample configuration described in this guide uses Microsoft Entra ID (formerly, Azure Active Directory) as the authentication source.

### Is This Guide for You?

If you are a network administrator who wants to integrate the Duo SSO solution for the remote workers in your organization using the Secure Firewall Management Center, then this guide is for you. This use case aims to provide step-by-step instructions on configuring Duo SSO authentication using Microsoft Entra ID as the primary identity provider.

### Scenario

Kit, an IT administrator of a large-scale organization, is responsible for managing the organization's IT infrastructure and ensuring its security. Kit is aware that employees access many applications using multiple usernames and passwords, and suspects that the employees may use weak passwords or reuse their passwords. With escalating cyber threats, Kit wants to strengthen its organization's security posture and streamline their IT support operations.

#### What is at risk?

With multiple passwords to remember and gain access to various applications in your organization, employees may use weaker passwords or reuse their passwords, making it easier for malicious actors to gain unauthorized

access. Frequent authentication requests might degrade the user experience and may cause employee dissatisfaction.

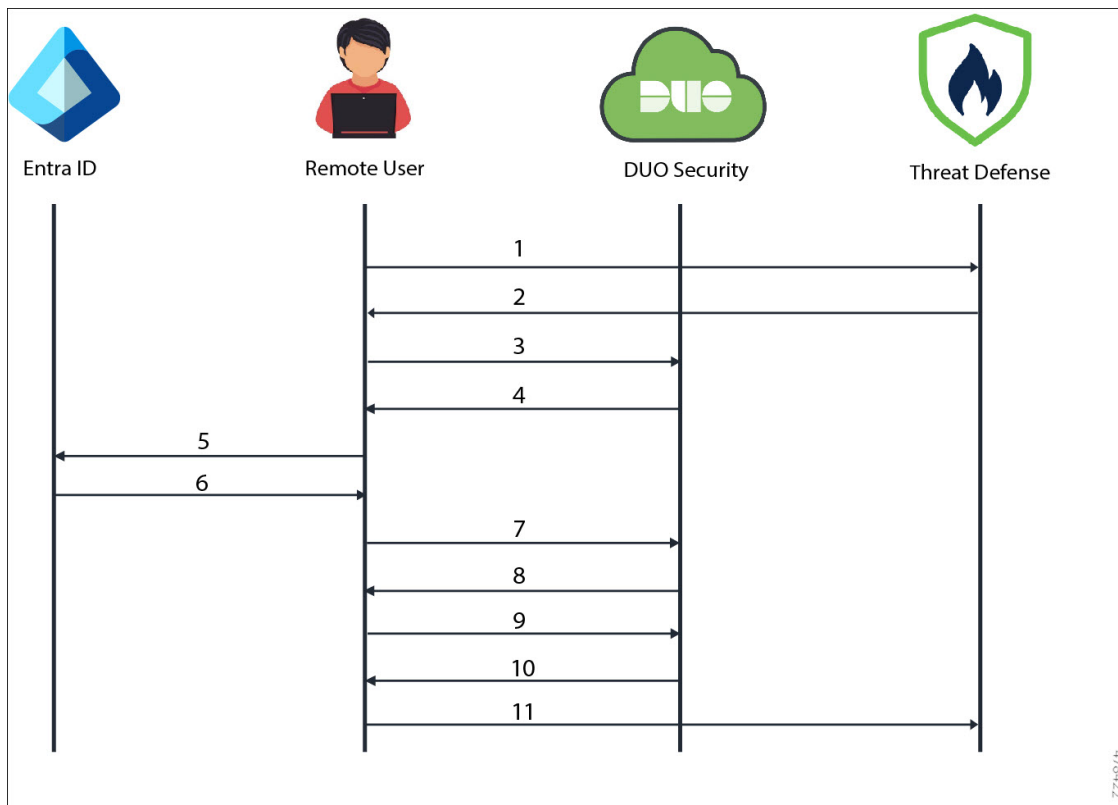
**How does Duo SSO solve the problem?**

- Improved security: Duo SSO can improve security by reducing the number of passwords users must remember. Fewer passwords mean lower chances of password-related security breaches, such as weak passwords or password reuse.
- Seamless login experience: Duo SSO simplifies the login process for users by allowing them to authenticate once and gain access to multiple applications and services without the need to re-enter their credentials for each one.
- Reduced IT helpdesk efforts: Fewer password-related issues help to minimize the load on the IT helpdesk team, allowing them to focus on other business initiatives.

## How Does Duo Single-Sign-On Work?

The following diagram illustrates the workflow that occurs when a remote user authenticates to use the remote access VPN using Duo SSO.

**Figure 1: Duo SSO Authentication Workflow**



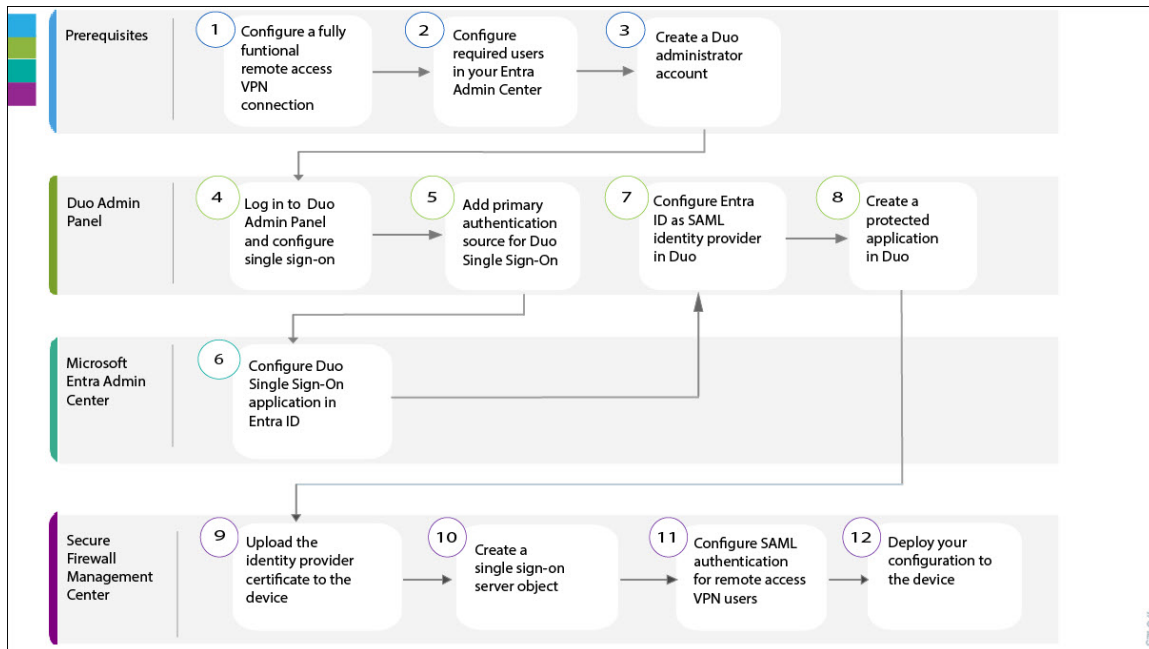
### Workflow

1. A remote user uses Secure Client and initiates a remote access VPN connection request to the threat defense device.
2. The threat defense device redirects the user's browser to Duo SSO with an SAML request message.
3. User's browser gets redirected to Duo SSO.
4. Duo SSO redirects the user's browser to Entra ID with an SAML request message.
5. User's browser gets redirected to Entra ID SSO login page.
6. User logs in with primary credentials. Entra ID generates the SAML assertion and redirects the user's browser to Duo SSO with the SAML assertion.  
  
SAML assertions are the messages that are exchanged between the SAML identity provider and the SAML service provider that confidentially identify the remote user and what the remote user is authorized to access. SAML assertions also specify security conditions and assurances that the assertions are valid.
7. User's browser gets redirected to Duo SSO.
8. Duo requests the user to authenticate using Duo two-factor authentication.
9. User completes Duo two-factor authentication.
10. Duo SSO redirects the user's browser to the threat defense with an SAML response message.
11. User's browser gets redirected to the threat defense device with the SAML response and completes the remote access VPN authentication.

## End-to-End Procedure to Configure Duo Single Sign-On

The following flowchart illustrates the end-to-end workflow of configuring Duo SSO for your remote workers.

Figure 2: End-to-End Workflow: Configuring Duo SSO



Step	Application	Description
1	Prerequisites	Configure a fully functional remote access VPN connection. See <a href="#">Prerequisites for Configuring Duo Single Sign-On</a> .
2	Prerequisites	Configure the required users in your Entra Admin Center. See <a href="#">Prerequisites for Configuring Duo Single Sign-On</a> .
3	Prerequisites	Create a Duo administrator account. See <a href="#">Prerequisites for Configuring Duo Single Sign-On</a> .
4	Duo Admin Panel	Log in to your Duo Admin Panel and configure single sign-on. See <a href="#">Configure Duo Single Sign-On and Authentication Source, on page 5</a> .
5	Duo Admin Panel	Add a primary authentication source for Duo SSO. See <a href="#">Configure Duo Single Sign-On and Authentication Source, on page 5</a> .
6	Microsoft Entra Admin Center	<a href="#">Configure Duo Single Sign-On Application in Entra ID, on page 6</a> .
7	Duo Admin Panel	<a href="#">Configure Entra ID As the Identity Provider in Duo, on page 8</a> .
8	Duo Admin Panel	<a href="#">Create a Protected Application in Duo, on page 9</a> .
9	Secure Firewall Management Center	<a href="#">Upload the Identity Provider Certificate to the Threat Defense Device, on page 10</a> .
10	Secure Firewall Management Center	<a href="#">Create a Single Sign-On Server Object, on page 11</a> .

Step	Application	Description
11	Secure Firewall Management Center	<a href="#">Configure SAML Authentication for Remote Access VPN Users, on page 12.</a>
12	Secure Firewall Management Center	<a href="#">Deploy Your Configuration to the Threat Defense Device, on page 12.</a>

## Prerequisites for Configuring Duo Single Sign-On

Ensure that you have met the following prerequisites before you begin the Duo SSO configuration described in this guide:

- An active Entra ID subscription with the required user configuration. For more information on getting started with Entra ID, see [Microsoft Entra ID Documentation](#).
- A Duo admin account with **Owner** role. For more information, see [Getting Started with Duo Security](#).
- A fully functional remote access VPN configuration on the threat defense device managed by the management center.
- Secure Firewall Management Center Version 7.0.0 or later.
- Secure Firewall Threat Defense Version 6.7.0 or later on the managed devices.
- Secure Client Version 4.6 or later.

### System Requirements

- Secure Firewall Management Center Version 7.0.0 or later.
- Secure Firewall Threat Defense Version 6.7.0 or later on the managed devices.
- Secure Client Version 4.6 or later.

## Configure Duo Single Sign-On and Authentication Source

Duo SSO is a cloud-hosted SAML 2.0 identity provider that provides secure access to web applications with an existing user directory such as Entra ID. Duo SSO supports local Active Directory (AD) and SAML Identity Providers (IdP) as authentication sources. This sample configuration uses Microsoft Entra ID as the primary authentication source.

For more information about configuring Duo SSO and the authentication source, see [Duo documentation](#).

### Procedure

- 
- Step 1** Log in to your Duo Admin Panel and click **Single Sign-On**.
- Step 2** (Optional) If you are configuring Duo Single Sign-On for the first time, review the information on the **Single Sign-On** page and the Duo privacy statements. Agree to the user terms and click **Activate and Start Setup**.

- Step 3** On the **Customize your SSO subdomain** page, specify a subdomain that you want your users to see when they log in with Duo SSO. For example, you can enter *example* and users will see *example.login.duosecurity.com* in the URL when logging into Duo SSO.
- Click **Save and continue** to use the subdomain or click **Skip for now** to customize your subdomain later.
- Step 4** On the **Add Authentication Source** page, click **Add SAML Identity Provider**.
- The Duo SSO metadata information that you need to provide the SAML identity provider is displayed under the **Configure the SAML Identity Provider** section.
- 

## Configure Duo Single Sign-On Application in Entra ID

SAML delegates authentication from a service provider to an identity provider. In this configuration, Duo SSO acts as the SAML service provider that uses Microsoft Entra ID as the SAML identity provider for primary authentication. For more information, see the instructions for using Entra ID described in the [SAML Identity Provider](#) section of the *Duo documentation*.

### Before you begin

Ensure that you have a Microsoft Entra ID account with the required user configuration.

### Procedure

---

- Step 1** Log in to your Microsoft Azure Portal and click **Microsoft Entra ID**.
- Step 2** On the left pane, click **Enterprise applications**, and then click **+ New application**.
- Step 3** Click **+ Create your own application** to create a new application for Duo SSO configuration.
- Step 4** Specify a display name to uniquely identify your application, for example, *Duo SSO*.
- Step 5** Choose the option **Integrate any other application you don't find in the gallery** and click **Create**.
- Step 6** On the *Duo SSO* application **Overview** page, click **Users and groups**.
- Step 7** Click **+ Add user/group** and choose the users and groups that you want to provide access to log in to Duo SSO using Entra ID credentials. After selecting the users and groups, click **Assign** at the bottom of the page.
- Step 8** On the left pane, click **Single sign-on**, and then click **SAML** from the **Select a single sign-on method** page.
- Step 9** On the **Set up Single Sign-On with SAML** page, click **Edit** next to **Basic SAML Configuration**.
- Step 10** Provide the Duo SSO metadata information that is available under the **Configure the SAML Identity Provider** section of your Duo Admin Panel.

Figure 3: Duo SSO Metadata

- a) Copy the **Entity ID** from the Duo Admin Panel and paste it into the **Identifier (Entity ID)** field in the Entra admin center.
- b) Copy the **Assertion Consumer Service URL** from the Duo Admin Panel and paste it into the **Reply URL (Assertion Consumer Service URL)** field in the Entra admin center.
- c) Leave all other fields empty, and click **Save**.

**Step 11**

Click **Edit** next to the **Attributes & Claims** section to configure the attribute names to use while sending SAML responses to Duo.

With these attribute names in the SAML responses, Duo automatically selects the correct attributes when signing in users into their applications. When configuring an SAML application, you can pick any of these five bridge attributes and additional custom bridge attributes, if any, that you have configured. If you pick a bridge attribute on the application's configuration page in the Duo Admin Panel, it will automatically map to the appropriate attribute for the enabled authentication source.

- a) Delete all the default claims available under the **Additional Claims**.
- b) Click + **Add new claim** and use the following bridge attributes to add a total of five additional claims.

Note that the attribute names are case-sensitive.

**Table 1: Microsoft Entra ID Attribute Names**

Name	Namespace	Source	Source Attribute
Email	Leave empty	Attribute	user.mail
Username	Leave empty	Attribute	user.userprinciplename
FirstName	Leave empty	Attribute	user.givenname

Name	Namespace	Source	Source Attribute
LastName	Leave empty	Attribute	user.surname
DisplayName	Leave empty	Attribute	user.displayname

c) After adding all the five claims, click the **Close (x)** icon at the top-right side to close the view.

**Note** Duo SSO does not support the option to test your single sign-on connection from Entra ID.

## Configure Entra ID As the Identity Provider in Duo

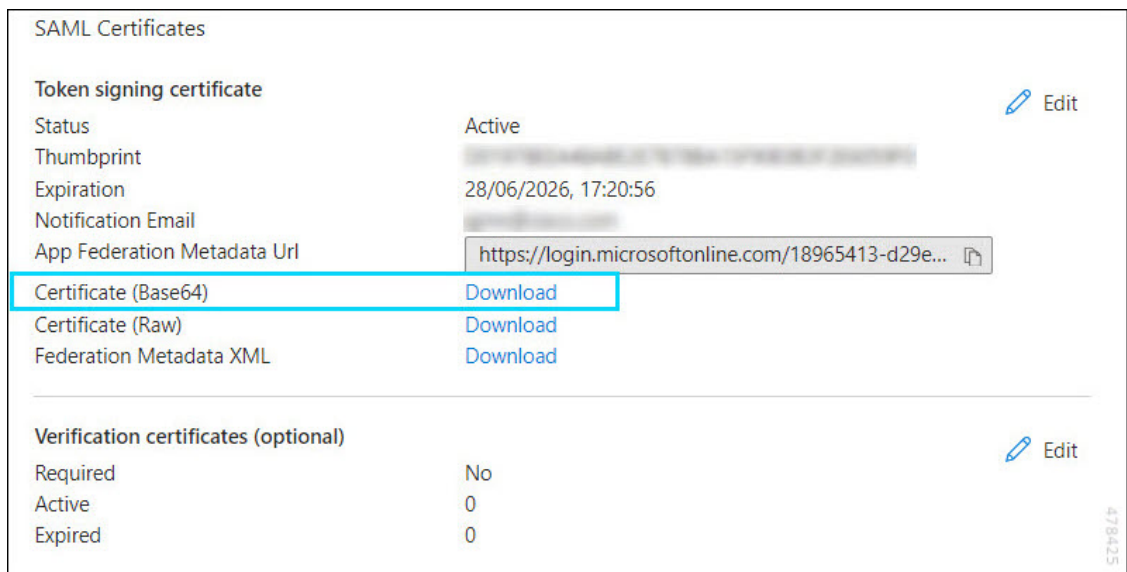
### Procedure

#### Step 1

When a user authenticates through Microsoft Entra ID by using SAML, Entra ID issues a token to Duo. Instead of prompting for a username and password, Duo uses the token to sign in the user. Microsoft Entra ID signs these SAML tokens with a unique certificate. Follow these steps to download the SAML certificate from Entra ID that Duo can use for decrypting the tokens:

- In your Microsoft Entra Admin Center, choose the application *Duo SSO* that you have created for Duo, and click **Single Sign-on**.
- Under the **SAML Certificates** section, click **Download** next to **Certificate (Base64)** to download the SAML certificate.

**Figure 4: Download the SAML Certificate**



#### Step 2

Copy the metadata information for Entra ID that is available under **Set up Duo SSO** (or the name you specified).



Figure 5: Entra ID Metadata

Set up Duo SSO

You'll need to configure the application to link with Microsoft Entra ID.

Login URL	https://login.microsoftonline.com/18965413-d29e...
Microsoft Entra ID Identifier	https://sts.windows.net/18965413-d29e-40cb-a6e...
Logout URL	https://login.microsoftonline.com/18965413-d29e...

- Step 3** Return to your Duo Admin Panel and scroll down to the **Configure Duo Single Sign-On** section on the **SAML Identity Provider Configuration** page.
- Step 4** Specify a unique display name to identify the SAML identity provider, for example, *Entra ID*.
- Step 5** Copy and paste the **Microsoft Entra ID Identifier** from the Entra ID into the **Entity ID** field in the Duo Admin Panel.
- Step 6** Copy and paste the **Login URL** from Entra ID into the **Single Sign-On URL** field in the Duo Admin Panel.
- Step 7** Upload the SAML certificate that you downloaded from Entra ID to the **Certificate** section in the Duo Admin Panel.
- Step 8** Leave the **Username Normalization** option set to **Simple**. The username normalization determines whether the username entered for primary authentication needs to be altered before matching it to a Duo user account.
- Step 9** Click **Save**.

## Create a Protected Application in Duo

A protected application in Duo is a service that integrates Duo and a threat defense remote access VPN. See [Protecting Applications](#) for more information about protecting applications in Duo and additional application options.




### Before you begin

Enable Duo SSO for your Duo account and configure a working authentication source as described in the [Configure Duo Single Sign-On and Authentication Source](#).

### Procedure

- Step 1** Log in to your Duo Admin Panel and choose **Applications**.
- Step 2** Click **Protect an Application**.
- Step 3** Scroll down and locate the entry **Cisco Firepower Threat Defense VPN** with the protection type **2FA with SSO hosted by Duo (Single Sign-On)** in the applications list, and click **Protect** next to the application.

Figure 6: Cisco Firepower Threat Defense VPN Application

Application	Protection Type		
 Cisco Firepower Threat Defense VPN	2FA with SSO hosted by Duo (Single Sign-On)	<a href="#">Documentation</a>	<input type="button" value="Protect"/>
 Cisco ISE Administrative Web Login	2FA with SSO hosted by Duo (Single Sign-On)	<a href="#">Documentation</a>	<input type="button" value="Protect"/>
 Cisco ISE RADIUS	2FA	<a href="#">Documentation</a>	<input type="button" value="Protect"/>

- Step 4** Enter the publicly resolvable hostname of your Cisco Secure Firewall Threat Defense as the **Cisco Firepower Base URL**.
- Step 5** Enter the name of the connection profile of your remote access VPN for which you want to configure SSO as the **Connection Profile Name**.
- Step 6** Scroll to the bottom of the page and click **Save**.

## Upload the Identity Provider Certificate to the Threat Defense Device

### Procedure

- Step 1** Log in to your Duo Admin panel and choose **Applications**.
- Step 2** Under the list of applications, choose the **Cisco Firepower Threat Defense VPN** application that you have configured, as described in [Create a Protected Application in Duo, on page 9](#).
- Step 3** Click **Download certificate** next to **Identity Provider Certificate** under **Downloads** on the details page for your application.
- Step 4** Log in to your management center and choose **Devices > Certificates**.
- Step 5** Click **Add**.
- Step 6** Choose the threat defense device in which you are configuring Duo SSO.
- Step 7** Click + next to **Cert Enrollment**.
- Step 8** Specify a name for the certificate, for example, *duo\_sso\_cert*.
- Step 9** From the **Enrollment Type** drop-down list, choose **Manual**.
- Step 10** Check the **CA Only** check box.
- Step 11** Open the certificate file that you downloaded earlier in a text editor (such as Notepad) and copy the entire contents of the file (including the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- lines). Paste the certificate file text into the **CA Certificate** field in the management center.
- Step 12** Check the **Skip Check for CA flag in basic constraints of the CA Certificate** check box to skip checking the basic constraints extension and the CA flag in the trustpoint certificate.
- Step 13** Click **Save**.
- Step 14** Click **Add**.

## Create a Single Sign-On Server Object

### Before you begin

Ensure that you have the following information from your Duo Admin Panel.

**Table 2: Duo SSO Server Metadata**

Metadata	Description
Identity Provider Entity ID	The URL that is defined in SAML IdP to uniquely identify a service provider. Example: <i>https://sso-rbdef4.sso.duosecurity.com/saml2/sp/DIABC1367234567/metadata</i>
SSO URL	The URL for signing into the SAML identity provider server. Example: <i>https://sso-rbdef4.sso.duosecurity.com/saml2/sp/DIABC1367234567/sso</i>
Logout URL	This field is optional. After users are logged out of Duo SSO, they will be redirected to the URL in this field.
Identity Provider Certificate	Certificate of the IdP enrolled with the threat defense to verify the messages signed by the IdP.

### Procedure

- 
- Step 1** In your management center, choose **Objects > Object Management > AAA Server > Single Sign-on Server**.
  - Step 2** Click **Add Single Sign-on Server**.
  - Step 3** Enter the name as **Duo SSO** in the **Name** field.
  - Step 4** Copy the **Identity Provider Entity ID** from the **Duo Admin Panel Metadata** section and paste it into the management center's **Identity Provider Entity ID** field.
  - Step 5** Copy the SSO URL from the **Duo Admin Panel Metadata** section and paste it into the management center's **SSO URL** field.
  - Step 6** (Optional) Copy the Logout URL from the **Duo Admin Panel Metadata** section and paste it in the management center's **Logout URL** field.
  - Step 7** Specify the publicly resolvable hostname of the threat defense as the **Base URL**. This URL redirects the user back to Secure Firewall Threat Defense after the identity provider authentication is complete.
  - Step 8** Choose the identity provider certificate *duo\_sso\_cert* from the **Identity Provider Certificate** drop-down list.
  - Step 9** Leave the **Request Signature** set to **No Signature**.
  - Step 10** Ensure that you uncheck the **Request IdP re-authentication on Login** check box.
  - Step 11** Leave all the other options to the default setting and click **Save**.
-

## Configure SAML Authentication for Remote Access VPN Users

### Procedure

---

- Step 1** In your management center, choose **Devices** > **Remote Access**.
  - Step 2** Click the **Edit** (✎) icon next to the remote access VPN that you want to update.
  - Step 3** Click the **Edit** (✎) icon next to the connection profile for which you want to use Duo single sign-on.
  - Step 4** Click the **AAA** tab.
  - Step 5** Choose **SAML** from the **Authentication Method** drop-down list.
  - Step 6** Choose the Duo single sign-on server **Duo SSO** from the **Authentication Server** drop-down list.
  - Step 7** Click the **Aliases** tab and add an alias name for this connection profile to map the connections to this connection profile. Users can see this alias name in the drop-down list that appears in the Secure Client.
  - Step 8** Save your changes.
- 

## Deploy Your Configuration to the Threat Defense Device

After you complete all the configurations, deploy them to the managed device.

### Procedure

---

- Step 1** On the management center menu bar, click **Deploy**.
- Step 2** Click **Advanced Deploy**.
- Step 3** Check the check box next to the threat defense device in which you want to deploy the configurations and click **Deploy**.

For more information about configuration deployment, see the Configuration Deployment section of the [Cisco Secure Firewall Management Center Device Configuration Guide](#).

---

## Verify Your Configuration

### Procedure

---

- Step 1** Open the Secure Client, choose the VPN connection profile that uses SAML SSO authentication, and click **Connect**.
- Step 2** The Secure Client redirects you to the Microsoft Entra ID login page for primary authentication. Log in using your credentials.

**Step 3** Upon successful verification of the user credentials, you will be redirected to Duo for two-factor authentication. When prompted, complete the Duo two-factor authentication.

After you successfully complete the authentication, you will be connected to the VPN tunnel.

---

## Troubleshoot the Duo Single Sign-On Configuration

After the deployment, use the following CLIs to troubleshoot issues related to Duo SSO authentication configuration on your Secure Firewall Threat Defense device.



---

**Caution** Proceed with caution when you run **debug** commands on the threat defense device in production environments. You can set various debug levels on the device that may have verbose outputs; by default, level 1 is used.

---

*Table 3: Duo SSO Troubleshooting*

Troubleshooting Task	Command
Debug the remote access VPN related information.	<b>debug webvpn 255</b>
Debug the remote access VPN Secure Client-related information.	<b>debug webvpn anyconnect 255</b>
Debug the remote access VPN session-related information.	<b>debug webvpn session 255</b>
Debug the common IKE-related transactions.	<b>debug webvpn request 255</b>
Debug SAML authentication-related information.	<b>debug aaa authentication</b>

---

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.