ISE管理アクセス用のDuo Two Factor Authenticationの設定

内容

<u>概要</u>
<u>前提条件</u>
<u>要件</u>
<u>使用するコンポーネント</u>
<u>ネットワーク図</u>
<u>コンフィギュレーション</u>
<u>Duo設定</u>
<u>ISE の設定</u>
<u>確認</u>
<u>トラブルシュート</u>
<u>関連情報</u>

概要

このドキュメントでは、Identity Services Engine(ISE)管理アクセスの外部2要素認証を設定するために必要な手順について説明します。この例では、ISE管理者がRADIUSトークンサーバに対して認証を行い、プッシュ通知の形式の追加認証がDuo Authentication Proxyサーバによって管理者の モバイルデバイスに送信されます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

• RADIUS プロトコル

• ISE RADIUSトークンサーバとIDの設定

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Identity Services Engine (ISE)
- Active Directory (AD)
- Duo認証プロキシサーバ
- Duo Cloud Service

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

ネットワーク図



コンフィギュレーション

Duo設定

ステップ1:WindowsまたはLinuxマシンでのDuo認証プロキシサーバのダウンロードとインストール: <u>https://duo.com/docs/ciscoise-radius#install-the-duo-authentication-proxy</u>

注:このマシンは、ISEおよびDuoクラウド(インターネット)にアクセスできる必要があ ります

ステップ2:authproxy.cfgファイルを設定します。

このファイルをメモ帳++やワードパッドなどのテキストエディタで開きます。

注:デフォルトの場所はC:\Program Files (x86)\Duo Security Authentication Proxy\conf\authproxy.cfg

ステップ 3 Duo Admin Panelで「Cisco ISE RADIUS」アプリケーションを作成します。 https://duo.com/docs/ciscoise-radius#first-steps

ステップ4:authproxy.cfgファイルを編集し、この設定を追加します。

ステップ5:ad_clientをActive Directoryの詳細で設定します。Duo認証プロキシは、プライマリ認 証に対してADに対して認証するために次の情報を使用します。

```
[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

注:ネットワークでインターネットアクセスにHTTPプロキシ接続が必要な場合は、 authproxy.cfgにhttp_proxyの詳細を追加します。

ステップ6: Duo Security Authentication Proxy Serviceを再起動します。ファイルを保存し、 Windowsマシン上でDuoサービスを再起動します。Windowsサービスコンソール(services.msc)を 開き、サービスのリストでDuo Security Authentication Proxy Serviceを見つけ、図に示すように Restartをクリックします。

			Services				-	• ×	
File Action View	w Help								
🕈 🔿 🔝 🗊	a 🗟 🛛 🖬 🕨 🖬 🕪 👘								
🔍 Services (Local)	Services (Local)								
	Duo Security Authentication Proxy	Name *	Description	Status	Startup Type	Log On As			^
	Service	COM Server Process Laun	The DCOMLAUNCH se	Running	Automatic	Local System			
		Device Association Service	Enables pairing betwee		Manual (Trigger Start)	Local System			
	Stop the service	Device Install Service	Enables a computer to		Manual (Trigger Start)	Local System			
	Restart the service	Device Setup Manager	Enables the detection,		Manual (Trigger Start)	Local System			
		CFS Namespace	Enables you to group s	Running	Automatic	Local System			=
		DFS Replication	Enables you to synchro	Running	Automatic	Local System			-
		Client	Registers and updates I	Running	Automatic	Local Service			
		C DHCP Server	Performs TCP/IP confi	Running	Automatic	Network Service			
		Diagnostic Policy Service	The Diagnostic Policy S	Running	Automatic (Delayed	Local Service			
		Diagnostic Service Host	The Diagnostic Service		Manual	Local Service			
		Diagnostic System Host	The Diagnostic System		Manual	Local System			
		Diagnostics Tracking Service	The Diagnostics Tracki	Running	Automatic	Local System			
		Distributed Link Tracking Cl	Maintains links betwee		Manual	Local System			
		Distributed Transaction Co	Coordinates transactio	Running	Automatic (Delayed	Network Service			
		Client 000 Client	The DNS Client service	Running	Automatic (Trigger S	Network Service			
		C DNS Server	Enables DNS clients to r	Running	Automatic	Local System			
		C DS Role Server	This service hosts the D		Manual	Local System			
		😪 Duo Security Authenticatio		Running	Automatic	Local System			
		Encrypting File System (EFS)	Provides the core file e		Manual (Trigger Start)	Local System			
		Extensible Authentication P	The Extensible Authenti		Manual	Local System			
		File Replication	Synchronizes folders wi		Disabled	Local System			
		FileZilla Server FTP server		Running	Automatic	Local System			v

Extended Standard

ステップ7:ユーザ名を作成し、エンドデバイスでDuo Mobileをアクティブにします。 <u>https://duo.com/docs/administration-users#creating-users-manually</u>

Duo Admin Panelでユーザを追加します。図に示すように、[Users] > [add users]に移動します。



エンドユーザにDuoアプリが電話機にインストールされていることを確認します。

Phones You may rearrange the phones by dragging and dropping in the table. Add Phone				
This user has no phones. Add one.				
Due	۹ Search for users, groups,	applications, or devices		
Dashboard	Dashboard > Users > duoadr	min > Add Phone		
Policies	Add Phone			
Applications	Add Flidile			
Users	Туре	Phone		
Add User		Tablet		
Pending Enrollments				
Bulk Enroll Users	Phone number	▶ +1 201-555-5555	Show extension field	
Import Users				
Directory Sync				
Bypass Codes		Add Phone		
2FA Devices				

図に示すように[Activate Duo Mobile]を選択します。

Device Info



図に示すように、[Generate Duo Mobile Activation Code]を選択します。

Dashboard	Dashboard > Phone: Generic S	martphone > Activate Duo Mobile			
Policies	Activate Duo	Mobile			
Applications		Activate Buo mobile			
Users	This form allows you to gene mobile device or authenticate	rate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to generate passcodes on their e via Duo Push.			
2FA Devices	Note: Generating an activation	on code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.			
Phones	Note: Constanting an activation				
Hardware Tokens	-				
WebAuthn & U2F	Phone	Generic Smartphone			
Groups					
Administrators	Expiration	24 hours • after generation			
Reports					
Settings		Generate Duo Mobile Activation Code			

図に示すように、[Send Instructions by SMS]を選択します。

Policies Applications Users An ew 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. ZFA Devices Phones Hardware Tokens WebAuth & U2F Groups Administrators Reports Settings Billing Activation instructions Centerions via SMS To activation instructions via SMS To activation instructions Settings Settings Centerions Centeri	Dashboard	Dashboard > Phone: Generic Sn	nartphone > Activate Duo Mobile		
Applications Activate Dub 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. ZFA Devices Phone Generic Smartphone Hardware Tokens Phone Generic Smartphone Medulth & U2F Installation instructions Image: Smartphone Groups Installation instructions Image: Smartphone Administrators Selfings Image: Smartphone Billing Activation instructions Image: Smartphone Activation instructions Image: Smartphone Image: Smartphone Administrators Selfings Image: Smartphone Image: Smartphone Billing Image: Smartphone Image: Smartphone Image: Smartphone Image: Smartphone Settings Image: Smartphone Image: Smartphone Image: Smartphone Image: Smartphone Image: Smartphone Billing Image: Smartphone Image: Smartphone Image: Smartphone Image: Smartphone Image: Smartphone Image: Smartphone Sectored Billing Image: Smartphone Image: Smartphone Image: Smartphone Image: Smartphone Image: Smartphone	Policies	Activate Due Mahila			
Users 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. 2FA Devices Phone Phones Generic Smartphone NetAuthin & U2F Installation instructions Groups Installation instructions Administrators Settings Settings Velcome to Duol Please install Duo Mobile from your app store. Billing Activation instructions Support Settings Support Setivate the app, tap and open this link with Duo Mobile: Upgrade your plan for support. Activate the app, tap and open this link with Duo Mobile:	Applications	Activate Duc	Activate Duo Mobile		
2FA Devices Phone Generic Smartphone Hardware Tokens Phone Generic Smartphone WebAuthn & U2F Installation instructions Send installation instructions via SMS Groups Installation instructions Welcome to Duol Please install Duo Mobile from your app store. Reports Installation instructions Instructions Settings Instructions Send activation instructions via SMS Billing Instructions Send activation instructions via SMS Support Veloame to pupper to activate the app, tap and open this link with Duo Mobile: Devicement ID Instructions	Users	A new Duo Mobile activation	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		
Phones Hardware Tokens WebAuthn & U2F Groups Administrators Reports Settings Billing Support Upgrade your plan for support. Activation instructions Constructions	2FA Devices	activation instructions to the			
WebAuthn & U2F Groups Administrators Reports Settings Billing Activation instructions Veloceme to Duol Please install Duo Mobile from your app store.	Phones Hardware Tokens	Phone	Generic Smartphone		
Groups Administrators Reports Settings Billing Activation instructions Velcome to Duol Please install Duo Mobile from your app store. Reports Settings Activation instructions Velcome to Duol Please install Duo Mobile from your app store.	WebAuthn & U2F	Installation instructions	Send installation instructions via SMS		
Reports Settings Billing Activation instructions Vpgrade your plan for support. Account ID	Groups		Welcome to Duo! Please install Duo Mobile from your app store.		
Settings Billing Activation instructions Activation instructions Image: Construction instruction instruction instructions via SMS Support Upgrade your plan for support. Account ID	Reports				
Billing Activation instructions Support Upgrade your plan for support. Account ID	Settings		li.		
Activation instructions Send activation instructions via SMS Support To activate the app, tap and open this link with Duo Mobile: Upgrade your plan for support. Account ID	Billing		-		
Parlownert ID	Support <u>Upgrade your plan</u> for support. Account ID	Activation instructions	Send activation instructions via SMS To activate the app, tap and open this link with Duo Mobile:		
	Deployment ID		li.		
Helpful Links Documentation Cf Send Instructions by SMS or skip this step	Helpful Links Documentation C		Send Instructions by SMS or skip this step		

SMS内のリンクをクリックすると、Duoアプリは次の図に示すように、[Device Info]セクションの ユーザアカウントにリンクされます。



ISE の設定

ステップ1:ISEとDuo認証プロキシを統合します。

[Administration] > [Identity Management] > [External Identity Sources] > [RADIUS Token]に移動し 、[Add]をクリックして新しいRADIUSトークンサーバを追加します。図に示すように、 [general]タブでサーバ名、[IP address]タブで共有キーを定義します。

[Server Timeout]60

Identity Services Engine Home	Context Visibility → Operations → Policy ✓ Administration → Work Centers
System Identity Management Network Re	sources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
Identities Groups External Identity Sources	Identity Source Sequences
External Identity Sources	RADIUS Token List > DUO
⟨- ▼ E-▼ _ @ _▼	RADIUS Token Identity Sources General Connection Authentication Authorization
Certificate Authentication Profile	
 Active Directory 	▼ Server Connection
	Safeword Server
COBC	Enable Secondary Server Always Access Primary Server First
RADIUS Token	Failback to Primary Server after 5 Minutes (0-99)
RSA SecuriD	
SAML Id Providers	▼ Primary Server ▼ Secondary Server
Social Login	* Host IP to 127 tos 220
	Shared Secret Show Shared Secret Show
	* Authentication Port 1812 () Authentication Port 1812 ()
	* Server Timeout 60 Seconds (i) Server Timeout 5 seconds (i)
	* Connection Attempts 3 () Connection Attempts 3 ()
	Save Reset

ステップ2:図に示すように、[Administration] > [System] > [Admin Access] > [Authentication] > [Authentication Method]に移動し、以前に設定したRADIUSトークンサーバを[Identity Source]とし て選択します。



ステップ3:図に示すように、[Administration] > [System] > [Admin Access] > [Administrators] > [Admin Users]に移動し、管理ユーザを[External]として作成し、スーパー管理者権限を付与します。

Identity Services Engine	Home → Context Visibility → Operations → Policy → Administration → Work Centers
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
Deployment Licensing + Certificat	es Logging Maintenance Upgrade Backup & Restore Admin Access Settings
Authentication	Administrators List > New Administrator
Authorization	▼ Admin User
- Administrators	Status Z Enabled -
Admin Users	Email Include system alarms in emails
Admin Groups	External 🗹 👔
 Settings 	Read Only
	Inactive account never disabled 📝
	▼ User Information
	First Name
	Last Name
	Account Options
	▼ Admin Groups
	* II Super Admin 📀 🕂
	Submit Cancel

確認

ここでは、設定が正常に機能しているかどうかを確認します。

ISE GUIを開き、[ID Source]として[RADIUS Token Server]を選択し、adminユーザでログインします。

uluilu cisco

Identity Services Engine

Username	duoadmin
Password	••••••
Identity Source	DUO -
	Login

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

クラウドまたはActive DirectoryとのDuoプロキシ接続に関連する問題をトラブルシューティング するには、authproxy.cfgのメインセクションに「debug=true」を追加して、Duo認証プロキシの デバッグを有効にします。

ログは次の場所にあります。

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

メモ帳++やWordPadなど、テキストエディタでauthproxy.logファイルを開きます。

ISEから要求を受信してDuo Cloudに送信するDuo Auth Proxyのログスニペット。

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 Duo Auth ProxyのログスニペットがDuo Cloudに到達できません。

```
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 gotResult
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-
xxxxxxx.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

```
関連情報
```

・<u>DUOを使用したRA VPN認証</u>

・テクニカル サポートとドキュメント – Cisco Systems