在Anyconnect/远程接入VPN客户端上配置与 Active Directory和ISE的双核集成,以实现双因素 身份验证

目录
先决条件
使用的组件
<u>网络图和场景</u>
通信过程
<u>Active Directory配置</u>
Duo配置
<u>Duo Auth代理配置</u>
<u>Cisco ISE配置</u>
<u>Cisco ASA RADIUS/ISE配置</u>
<u>Cisco ASA远程访问VPN配置</u>
测试
<u>故障排除</u>
<u>工作调试</u>

简介

本文档介绍作为连接到ASA的AnyConnect客户端的双因素身份验证与AD和ISE集成的双重Push。

先决条件

要求

Cisco 建议您了解以下主题:

- 自适应安全设备(ASA)上的RA VPN配置
- ASA上的RADIUS配置
- 身份服务引擎 (ISE)
- Active Directory (AD)
- Duo应用程序

使用的组件

本文档中的信息基于以下软件和硬件版本:

- Microsoft 2016服务器
- ASA 9.14(3)18
- ISE服务器3.0
- Duo服务器
- Duo认证代理管理器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

网络图和场景



通信过程

Cisco ISE的双重RADIUS身份验证

- 1. 主身份验证启动到Cisco ISE。
- 2. Cisco ASA向Duo身份验证代理发送身份验证请求。
- 3. 主身份验证使用Active Directory或RADIUS。
- 4. 已建立Duo Authentication Proxy连接,以通过TCP端口443实现Duo Security。
- 5. 通过Duo Security的服务进行辅助身份验证。
- 6. Duo认证代理接收认证响应。
- 7. 已授予思科ISE访问权限。

用户帐户:

• Active Directory管理员:此帐户用作目录帐户,以允许双重身份验证代理绑定到Active Directory服务器进行主要身份验证。

- Active Directory测试用户
- Duo测试用户进行辅助身份验证

Active Directory配置

Windows服务器预配置了Active Directory域服务。

注意:如果RADIUS Duo Auth代理管理器在同一Active Directory主机上运行,则必须卸载/删除网络策略服务器(NPS)角色。如果两个RADIUS服务都运行,则可能会发生冲突并影响性能。

要在远程访问VPN用户上实现身份验证和用户身份的AD配置,需要几个值。

必须先在Microsoft服务器上创建或收集所有这些详细信息,然后才能在ASA和Duo Auth代理服务器 上进行配置。

主要值包括:

- 域名.这是服务器的域名。在本配置指南中,agarciam.cisco是域名。
- 服务器IP/完全限定域名(FQDN)地址。用于连接Microsoft服务器的IP地址或FQDN。如果使用 FQDN,则必须在ASA和双重身份验证代理中配置DNS服务器以解析FQDN。

在本配置指南中,此值为agarciam.cisco(解析为10.28.17.107)。

- 服务器端口.LDAP服务使用的端口。默认情况下,LDAP和STARTTLS对LDAP使用TCP端口 389, LDAP over SSL (LDAPS)使用TCP端口636。
- 根 CA.如果使用LDAPS或STARTTLS,则需要用于签署LDAPS使用的SSL证书的根CA。
- 目录用户名和密码。这是Duo Auth代理服务器用于绑定到LDAP服务器并对用户进行身份验证 以及搜索用户和组的帐户。
- 基本和组可分辨名称(DN)。基础DN是Duo Auth代理的出发点,它告知Active Directory开始搜索和验证用户。

在本配置指南中,根域agarciam.cisco用作基础DN,组DN为Duo-USERS。

1. 为了添加新的Duo用户,请在Windows Server上导航到左下方的Windows图标,然后单击 Windows管理工具,如图所示。



2. 在"Windows管理工具"窗口中,导航到Active Directory用户和计算机。

在Active Directory用户和计算机面板上,展开域选项并导航到用户文件夹。

在此配置示例中,Duo-USERS用作辅助身份验证的目标组。

Name Date modified Type Size Could access Therminal Services The 2016 623 AM File fielder Downloads Active Directory Administrates Center The 2016 623 AM Shortcut 248 Downloads Active Directory Mainistrates Center The 2016 619 AM Shortcut 248 Documents Active Directory Mainistrates The 2016 619 AM Shortcut 248 Pictures Active Directory Uses and Computers The 2016 619 AM Shortcut 248 System32 Space Sing The 2016 619 AM Shortcut 248 System32 Space Sing The 2016 619 AM Shortcut 248 Source Comparets The 2016 619 AM Shortcut 248 System32 Space Sing The 2016 619 AM Shortcut 248 Source Comparets Sconnaction Manage Administration Kat The 2016 619 AM Source Comparets Connaction Manage Administration Kat The 2016 619 AM Source Comparets Sconnaction Manage Administration Kat The 2016 619 AM Source Comparets Sconnaction Manage Administration Kat The 2016 619 AM Source Comparets Sconnaction Manage Administration Kat The 2016 619 AM Source Comparets Sconnaction Manage Administration Kat The 2016 619 AM	→ ~ ↑ ៉ ៉ Cor	trol Panel > System and Security > Administra	tive Tools			Active Directory Users and Comp	outers		- C		ŝ
■ Active Directory Administrate Center 7/16/2016 619 AM Shortcut 216 ■ Documents ■ Active Directory Monains and Turk 7/16/2016 619 AM Shortcut 216 ■ Defuest ■ Active Directory Monains and Turk 7/16/2016 619 AM Shortcut 216 ■ Dig ■ Active Directory Monains and Turk 7/16/2016 619 AM Shortcut 216 ■ Dig ■ Active Directory Monains and Turk 7/16/2016 619 AM Shortcut 216 ■ System2 ■ Active Directory Monains and Turk 7/16/2016 619 AM Shortcut 216 ■ Distance 7/16/2016 619 AM Shortcut 216 > ■ Directory Administration Controllers > ■ Computers ■ Distance 7/16/2016 619 AM Shortcut 216 > ■ Distance Managed Service Accord ■ Desktop ● Component Services 7/16/2016 618 AM Shortcut 216 > ■ Distance Managed Service Accord ■ Downloads ● Defragment and Optimize Drives 7/16/2016 618 AM Shortcut 216 ■ Downloads ● Defragment and Optimize Drives 7/16/2016 618 AM Shortcut 216 ■ Downloads ● Defragment and Optimize Drives <	Quick access Desktop	Name	Date modified 7/16/2016 6:23 AM	Type File folder	Size	File Action View Help) @ 🕞 🛛 🗂 🗏 📚 🐿 '	🕈 🔟 📚			^
Pictures Active Directory Sites and Services 7/16/2016 6:19 AM Shortcut 2 KB I log Active Directory Sites and Computers 7/16/2016 6:19 AM Shortcut 2 KB Salando User System32 Active Directory Sites and Computers 7/16/2016 6:19 AM Shortcut 2 KB Salando User This PC Scomponent Services 7/16/2016 6:19 AM Shortcut 2 KB Salando User Dotation Directory Sites and Computers 7/16/2016 6:19 AM Shortcut 2 KB Salando User This PC Scomponent Services 7/16/2016 6:19 AM Shortcut 2 KB Managed Service Accore Members in this group c Members in this group c Dotation Dotation Scomponent Services 7/16/2016 6:19 AM Shortcut 2 KB Sometoin Members in this group c Members in this group c Dotation Dotation Scomponent Services 7/16/2016 6:19 AM Shortcut 2 KB Sometoin Members in this group c Not cut analyse Downloads Scomponent Services 7/16/2016 6:19 AM Shortcut 2 KB Sometoin Sometoin Controllers Sometoin Controlle	Downloads # Documents	Active Directory Administrative Center Active Directory Domains and Trusts Active Directory Module fee Windows Po	7/16/2016 6:19 AM 7/16/2016 6:20 AM 7/16/2016 6:19 AM	Shortcut Shortcut Shortcut	2 KB 2 KB 2 KB	> Saved Queries	& Administrator User & agarciam User	Built-in account for ad			
Image: Security Group. Security Group. Members of this group L. Image: Security Group. Members of this group L. Ausre account manage. Image: Security Group. Members of this group L. Ausre account manage. Image: Security Group. Members of this group L. Ausre account manage. Image: Security Group. Members of this group L. Ausre account manage. Image: Security Group. Members of this group L. Ausre account manage. Image: Security Group. Members of this group L. Members of this group L. Image: Security Group. Members of this group L. Members of this group L. Image: Security Group. Members of this group L. Members of this group L. Image: Security Group. Members of this group L. Members of this group L. Image: Security Group. Members of this group L. Members of this group L. Image: Security Group. Members of this group L. Members of this group L. Image: Security Group. Members of this group L. Members of this group L. Image: Security Group. Members of this Group C. Members of this group L. Image: Security Group. Members of this group L. Members of this group L. Image: Security Group. Members of this group L. Members of this group L. Image: Security Group	Pictures #	Active Directory Sites and Services Active Directory Users and Computers ADSI Edit	7/16/2016 6:19 AM 7/16/2016 6:20 AM 7/16/2016 6:19 AM	Shortcut Shortcut Shortcut	2 KB 2 KB 2 KB	Computers S Domain Controllers ForeignSecurityPrincipal:	る alanad User 名 alanduo User 単Allowed RO Security Group 第 Cert Publish Security Group	Members in this group c Members of this group			
Bit Consection Manager Administration Xi 7/16/2016 6/19 AM Shortcut 2 K8 Downloads Downloads Dis Cleanup 7/16/2016 6/18 AM Shortcut 2 K8 Downloads Dis Cleanup 7/16/2016 6/18 AM Shortcut 2 K8 Downloads Dis Cleanup 7/16/2016 6/18 AM Shortcut 2 K8 Downloads Dis Cleanup 7/16/2016 6/19 AM Shortcut 2 K8 Dis Cleanup 7/16/2016 6/19 AM Shortcut 2 K8 Dis Cleanup 7/16/2016 6/19 AM Shortcut 2 K8 Pictures Group Policy Management 7/16/2016 6/19 AM Shortcut 2 K8 Videos Security Group All domain courts All domain courts Videos Internet Information Services (IIS) Manager 7/16/2016 6/19 AM Shortcut 2 K8 DVD Drive (D) SSS: Jaccest Security Group All domain courts All domain courts Divide Divide Divis (D) SSS: Security Group All domain courts All domain courts Divide Divis (D) SSS: All domain courts Security Group All domain courts Divide Divis (D) SSS: Microsoft Azure Services Shortcut 2 K8 Divide Divis (D) SSS: Microsoft Azure Services Shortcut 2 K8 <td>This PC</td> <td>Certification Authority Component Services Computer Management</td> <td>7/16/2016 6:19 AM 7/16/2016 6:18 AM 7/16/2016 6:18 AM</td> <td>Shortcut Shortcut Shortcut</td> <td>2 KB 2 KB 2 KB</td> <td>Service Account</td> <td>Cloneable D Security Group Coneable D User Denied ROD Security Group</td> <td>Members of this group t A user account manage Members in this group c</td> <td></td> <td></td> <td></td>	This PC	Certification Authority Component Services Computer Management	7/16/2016 6:19 AM 7/16/2016 6:18 AM 7/16/2016 6:18 AM	Shortcut Shortcut Shortcut	2 KB 2 KB 2 KB	Service Account	Cloneable D Security Group Coneable D User Denied ROD Security Group	Members of this group t A user account manage Members in this group c			
Music Music Music No. 7/16/2016 619 AM Shortcut 2.K8 Music Music Music Music Shortcut 2.K8 Pictures Music Music Shortcut 2.K8 Videos Internet Information Services (IIS) Manager 7/16/2016 619 AM Shortcut 2.K8 Videos Internet Information Services (IIS) Manager 7/16/2016 619 AM Shortcut 2.K8 DVD Drive (D) SSS Accil Scientify Group All domain quests DVD Drive (D) SSS Accil Scientify Folicy All domain quests DVD Drive (D) SSS Accil Scientify Folicy Shortcut 2.K8	Documents Downloads Downloads on Mac	Connection Manager Administration Kit befragment and Optimize Drives Disk Cleanup	7/16/2016 6:19 AM 7/16/2016 6:18 AM 7/16/2016 6:19 AM	Shortcut Shortcut Shortcut	2 KB 2 KB 2 KB		DonsAdmins Security Group DonsUpdateP Security Group Domain Ad Security Group	DNS Administrators Gro DNS clients who are permitted to Designated administrato	perform dynamic u	updates or	n bi
Image: Security Policy 7/16/2016/619.AM Shortcut 2 K8 Image: Security Group Designated administrato Bit Interprint A Image: Security Group Policy Security Group Nembers of this group	Music	A DNS Event Viewer Group Policy Management	7/16/2016 6:19 AM 7/16/2016 6:18 AM 7/16/2016 6:19 AM	Shortcut Shortcut Shortcut	2 KB 2 KB 2 KB		Domain Co Security Group Domain Con Security Group	All workstations and ser All domain controllers i All domain guests			1
DVD Drive (D) SSS } B Local Security Policy 7/16/2016 6:19 AM Shortcut 2 KB DVD Drive (D) SSS / B Local Security Policy Designated administrato Designated administrato Designated administrato Designated administrato Designated administrato Designated administrato	Videos	Internet Information Services (IIS) Manager Si SCSI Initiator	7/16/2016 6:19 AM 7/16/2016 6:18 AM	Shortcut	2 KB 2 KB		DUO-USERS Security Group DUO-USERS Security Group duo2 Ser	All domain users			
Addition Addition	DVD Drive (D:) SSS_; Network	Local Security Policy Microsoft Azure Services ODBC Data Sources (32-bit)	7/16/2016 6:19 AM 7/16/2016 6:19 AM 7/16/2016 6:18 AM	Shortcut Shortcut Shortcut	2 KB 2 KB 2 KB	۲ ک	Enterprise A Security Group Enterprise K Security Group Enterprise R Security Group	Designated administrato Members of this group Members of this group			*

3. 右键单击用户文件夹,然后选择新建>用户,如图所示。

Active Directory Users and Comp	uters			-	×
File Action View Help		1 🛠 🗽 în 🖷	7 🖸 🖓		
Active Directory Users and Com Saved Queries Saved Queries Builtin Computers Domain Controllers Sign Domain Controllers Managed Service Accour Users Delegate Controllers	Name Administrator agarciam alanad alanduo Allowed RO Cert Publish Concable D rol D	Type User User User Security Group Security Group Security Group User Security Group	Description Built-in account for ad Members in this group c Members of this group Members of this group t A user account manage Members in this group c		^
New All Tasks View Refresh Export List Properties Help < >>>	> > Enterprise	Computer Contact Group InetOrgPerson msDS-KeyCreden msDS-ResourceP msDS-ShadowPri msImaging-PSPs MSMQ Queue Ali Printer	tial ropertyList ncipalContainer		v
Create a new object		User 🗲			
		Shared Folder			

4. 在"新建对象-用户"窗口中,指定此新用户的身份属性,然后单击下一步,如图所示。

New Object - User	×	
Create in: agarciam.cisco/Users		on
First name: duovpn Initials:		зсс
Last name:		
Full name: duovpn		s ir
User logon name:		s o s o
duovpn @agarciam.cisco v		cc
User logon name (pre-Windows 2000):		s ir nir
AGARCIAM\ duovpn		nts
		ed
Canad		sta ain
		ain

5. 确认口令并单击下一步,然后在验证用户信息之后单击完成。

New Object - User	\times
Create in: agarciam.cisco/Users	0
Password: Confirm password:]
 User must change password at next logon User cannot change password Password never expires Account is disabled 	s s c s n
< Back Next >	nt je st Cancel jii

6. 将新用户分配给特定组,右键单击该用户并选择添加到组,如图所示。

Active Directory Users and Comp	puters			-	×
File Action View Help					
♦ ♦ 2 📰 4 🖬 🗙 🛙	i 🧟 🔒 🔽 🖬	1 🗏 🐮 🕯 🦷	1 🔟 🐍		
Active Directory Users and Com Saved Queries Saved Queries Builtin Builtin Computers Domain Controllers ForeignSecurityPrincipal: Managed Service Accour Users	Name Administrator agarciam alanad alanad alanduo Allowed RO Cert Publish Cort Publish Cloneable D DefaultAcco DefaultAcco Denied ROD DnsAdmins DnsUpdateP Domain Ad Domain Co Domain Con Domain Gue Domain Gue Domain Users duo2	Type User User User Security Group Security Group	Description Built-in account for ad Members in this group c Members of this group Members of this group t A user account manage Members in this group c DNS Administrators Gro DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain users		
	duovpn Enterprise	Copy Add to a group	d administrato		0
Allows you to add the selected object	s to a group yo	Disable Account	of this group		Ŷ

7. 在"选择组"面板上,键入所需组的名称,然后单击检查名称。

然后,选择符合条件的名称,然后单击Ok。

Select Groups	×	
Select this object type:		_
Groups or Built-in security principals	Object Types	۱.
From this location:		:01
agarciam.cisco	Locations	
Enter the object names to select (examples):	\frown	
DUO-USERS	Check Names) †
	\sim	of 1
		of 1
Advanced OK	Cancel	bu n t
		n t

8. 此用户是本文档中使用的示例。

Duo配置

1. 登录您的Duo管理员门户。

Admin Login	
Enter your admin credentials	
Password Terrererererererererererererererererere	
Log in Confirm your identity	
o o mining your raomary	

2. 在左侧面板上,导航到用户,单击添加用户并键入与我们的Active Domain用户名匹配的用户名 ,然后单击添加用户。

	Q Search for users, groups, a	applications, or devices
Dashboard	Dashboard > Users > Add Us	er
Device Insight	Add User	
Policies	Most applications allow users	s to enroll themselves after they complete primary authentication.
Applications	Learn more about adding use	ers 🖸
Single Sign-On		
Users ┥	Username	duovpn
Add User		Should match the primary authentication username.
Pending Enrollments Bulk Enroll Users		
Import Users	(
Directory Sync		Add User

3. 在"新用户"面板中,填写所有必要信息。

Policies	Uasnboard > Users > duovpn		
Applications	duovpn		Logs Send Enrollment Email
Single Sign-On			
Users Add User Pending Enroliments Bulk Enroll Users	(i) This user has not en	duovpn	
Directory Sync Bypass Codes	Username aliases	+ Add a username alias Users can have up to 8 aliases.	
Groups		Optionally, you may choose to reserve using an alias number for a specific alias (e.g., Username alias 1 should only be used for Employee ID).	
Endpoints			
2FA Devices	Full name	test vpn user	
Trusted Endpoints			
Trust Monitor	5		
Reports	Email	com	
Settings	Status	Active	
Need Help? Chat with Tech Support C Email Support Call us at 1-855-386-2884 Versioning Core Authentication Service: D235.6 Admin Panel:	Surg.	 Require multi-factor authentication (default). Bypass Allow users to skip two-factor authentication and log in with only a password. Passwordless. Disabled Automatically deny access This controls the user's two-factor authentication process. 	authentication is not skipped.
D235.6 Read Release Notes C ² Account ID 2910-6030-53	Groups	You don't have any editable groups. Add one. Groups can be used for management, reporting, and policy. Learn more about groups ☐	
Deployment ID DU063 cf Helpful Links Documentation cf User Guide cf Knowledge Base cf	Notes	For internal use.	

4. 在"用户设备"下,指定辅助身份验证方法。

Subscription State Sta

单击Add Phone。

		\frown
Phones ou may rearrange the phones by dragging and dropping in the table. Lear	n more about activating a replacement phone ⊡.	Add Phone
Th	nis user has no phones. Add one.	
ndpoints		
	This user has no devices.	
lardware Tokens		Add Hardware Token
This us	ser has no hardware tokens. Add one.	
Sypass Codes		Add Bypass Code
This u	user has no bypass codes. Add one.	
VebAuthn & U2F		Add Security Key

5. 键入用户电话号码并单击Add Phone。

Dashboard > Users > duovpn > Add Phone

Add Phone



6. 在左侧"Duo管理员"面板上,导航到用户,然后单击新用户。

Dashboard	Dashboard > Users						
Device Insight	Llooro			Director	Suna L Import	Llaara Dulk En	
Policies	Users			Directory	Sync 1 Import	Users I Buik En	roll Users Add User
Applications	i You have users w	ho have not activated Duo N	obile. Click here to send them a	ctivation links.			
Single Sign-On	Need to activate a	a replacement phone? Learn	more about Reactivating Duo Mo	obile 🖆.			
Users ┥							
Add User	5	0	2	1	0		0
Pending Enrollments	Total Users	Not Enrolled	Inactive Users	Trash	Bypass	Users	Locked Out
Bulk Enroll Users							
Directory Sync	Select (0) ∽ ····				Export 🛩	Q Search	
Bypass Codes							
Groups	Username 🔺	Name	Email	Phones	Tokens	Status	Last Login
Endpoints				1		Active	Mar 8, 2022 6:50 PM
2FA Devices				1		Active	Mar 5, 2022 7:04 PM
Trusted Endpoints							
Trust Monitor	-			1		Active	Never authenticated
Reports	duovpn		.com	1		Active	Never authenticated
Settings			e e e.com	1		Active	Mar 5, 2022 7:16 PM
Need Help? Chat with Tech Support 🗅							

💊 注意:如果您目前无权访问您的电话,可以选择电邮选项。

7. 导航到电话部分并单击激活Duo Mobile。

Phones You may rearrang	e the phones by dragging and d	ropping in the table. I	Learn more about activating a	replacement phone 🗗.		Add Phone
Alias	Device	Platform	Model	Security Warnings		
phone1	2 C 2 C 2 C	Android 10	0,0,0,0,0,0	✓ No warnings	Activate Duo Mobile	Ē

8. 单击Generate Duo Mobile Activation Code。



9. 选择电子邮件以便通过电子邮件接收说明,键入您的电子邮件地址,然后单击通过电子邮件发送 说明。

Activate Duo Mobile

This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allow: 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 r

Phone	a di ka Utabili - 666		
Send links via	 SMS Email 		
Email	aya mine il norma com		

10. 您会收到一封包含说明的电子邮件,如图所示。

This is an automated email from Duo Security.

Your organization invites you to set up Duo Mobile on your phone. You will find instructions from your Duo administrator below. If you have questions, please reach out to your organization's IT or help desk team.

This email will help you add your Cisco account to Duo Mobile on this device:

Just tap this link from + r copy and paste it into Duo Mobile manually:

If you're not reading this from +



Don't have Duo Mobile yet? Install it first:

iPhone: https://itunes.apple.com/us/app/duo-mobile/id422663827

Android: https://play.google.com/store/apps/details?id=com.duosecurity.duomobile

11. 从移动设备打开Duo Mobile App,然后单击Add,然后选择Use QR code并从说明邮件扫描代码

o

12. 新用户将添加到您的Duo移动应用。

Duo Auth代理配置

1. 从<u>Cisco Duo Authentication</u>下载并安装Duo Auth Proxy Manager

✤ 注意:在本文档中,Duo Auth代理管理器安装在承载Active Directory服务的同一Windows服务器上。

2. 在Duo管理面板上,导航至"应用程序",然后单击保护应用程序。



3. 在搜索栏中,查找Cisco ISE Radius。

Pro	tect an Application						
0	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 will see it, until you decide to add others. Documentation: Getting Started C Choose an application below to get started.						
ise							
Applica	tion	Protection Type					
CAkamal	Akamai Enterprise Application Access	2FA	Documentation 🗗 Protect				
ahaha cisco	Cisco ISE RADIUS	2FA	Documentation E Protect				

4. 复制集成密钥、密钥和API主机名。Duo认证代理配置需要此信息。

Successfully added Cisco ISE RADIUS to protected applications. Add another.

Dashboard > Applications > Cisco ISE RADIUS 1

Cisco ISE RADIUS 1

Follow the Cisco ISE RADIUS instructions ⊡.

Details

~



5. 运行Duo Authentication Proxy Manager应用程序并完成Active Directory客户端和ISE Radius服 务器的配置,然后单击Validate。

💊 注意:如果验证不成功,请参阅调试选项卡了解详细信息并相应更正。

Duo Authentication Proxy Manager			- 🗆 X
Authentication Proxy is running Up since: 3/5/2022, 9:	23:04 AM <u>Update</u>	rsion: 5.6.0 your Authentication Proxy	Restart Service Stop Service
Validation passed Configuration has passed validation and is ready to be saved	←		
Configure: authproxy.cfg	Unsaved Changes	Output	
<pre>18 ; number to the section name (e.g. [ad_client2]) 19 20 [ad_client] 21 host=10.28.17.107 22 service_account_username=Administrator 23 service_account_password= HEVTH11/1 24 search_dn=DC=agarciam,DC=cisco 25 [26 [radius_server_auto] 27 ikey=Untrining[Untrining] 28 skey=K0nd7xtRiA2D14H17p77idA16SaHn112pa904C2dp 29 api_host=api_udft47bd.cumturf1y.tom 30 radius_ip_1=10.28.17.101 31 radius_secret_1=HMAXpn117! 32 failmode=safe 33 client=ad_client 34 port=1812 35 36</pre>		Running The Duo Authentication Proxy Co several minutes [info] Testing section 'main' with con [info] {'debug': 'True', 'log_max_files': '10', 'log_max_size': '20971520', 'test_connectivity_on_startup' [info] There are no configuration prob [info]	<pre>nnectivity Tool. This may take figuration: : 'true'} lems h configuration: isco', *****', dministrator'} lems auto' with configuration: orurity com! now to configure the Authentication Prove.</pre>
Valitate		Learn h	low to configure the Authentication Proxy

Cisco ISE配置

1. 登录ISE管理员门户。

2. 展开Cisco ISE选项卡并导航到Administration,然后单击Network Resources,再单击External RADIUS Servers。

Cisco ISE ┥	(Q What page are you looking for	х?		
Dashb	oard	Context Visibility	Operations	-Policy-	Administration
Recent Pag External I Policy Se	es dentity Sources ts	System Deployment Licensing		Network Resources	Ins
Network External I RADIUS S Live Logs	Device Profiles RADIUS Servers Server Sequences	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore		Network Device Prof External RADIUS Server RADIUS Server Sequence NAC Managers External MDM Location Services	iles vers Jeness

3. 在外部Radius服务器选项卡上,单击添加。

E Cisco ISE Administration • Network Resources						
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences		
External R	ADIUS Servers		1			
	🗍 Duplicate 🌐 Delete					
Name Name:	Currently Sorted	Description				

4. 使用Duo Authentication Proxy Manager中使用的RADIUS配置填写空白并单击Submit。

Network Devices Networ	k Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers	External MDM	More
* Name	DUO_NEW						
Description							
* Host IP	10.28.17.107						
* Shared Secret	······· -	Show)				
Enable KeyWrap							
* Key Encryption Key		Show					
* Message Authenticator Code Key		Show					
Key Input Format	• ASCII O HEXA	DECIMAL					
* Authentication Port	1812	(Valid Range 1 to	65535)				
* Accounting Port	1813	(Valid Range 1 to	65535)				
* Server Timeout	5	Seconds (Valid R	lange 1 to 120)				
* Connection Attempts	3	(Valid Range 1 to	9)				
Radius ProxyFailover Expiration	300	(i)(valid Range	1 to 600)				

5. 导航到RADIUS Server Sequences选项卡,然后单击Add。

≡ Cisco ISE		inistration · Network Resour	ces	
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences
RADIUS S For Policy Export go to Adm	erver Sequence	S Policy Export Page		1

6. 指定序列名称并分配新的RADIUS外部服务器,单击Submit。

RADIUS Server Sequences List > New RADIUS Server Sequence

RADIUS Server Sequence



✓ User Selected Service Type

Select the set of external RADIUS servers to use to process requests. Servers are accessed in sequence until a response is r



7. 从"控制面板"菜单定位至策略, 然后单击策略集。



✤ 注意:在本文档中,将应用所有连接的Duo序列,因此使用默认策略。策略分配可能因要求而 异。

Policy Sets					Reset	Reset Policyset Hi	tcount
+ Status	Policy Set Name	Description	Con	ditions	Allowed Proto	ocols / Server Sequence	Hits
Q Search	'n						
0	w. 1919		Ŧ	Radius-User-Name EQUALS isevpn	Default Netw	ork Access $\overline{\ \ } $	3
0	1 m - 1		D	Radius-NAS-Port-Type EQUALS Virtual	DUO_Sequer	nce 🛛 🗸 +	22
0	Default	Default policy set			Default Netw	ork Access $\ \ \boxtimes \ \land +$	0
	Î				<u>=q</u>		
	1				Allowed Prot	tocols	eset
					Default I	Network Access	
					Proxy Seque	nce	
					DUD_M	~~~~	
					DUO_Se	quence	

Cisco ASA RADIUS/ISE配置

1. 要在AAA服务器组下配置ISE RADIUS服务器,请导航到配置,然后单击设备管理,展开用户 /AAA部分,然后选择AAA服务器组。

o t avi	Home Configuration Monitoring Save Device Lip Beokmarks Bookmarks bookmark a page, right-click on a node in the agation tree and select "Add to bookmarks".	Refresh Ba AAA Server Group Server Group ISE LOCAL ad-agarciam	ack () ation : ips Pro RA LO
0	O O Device Management		
>	Management Access		
>	8 Licensing		
>	System Image/Configuration		
>	High Availability and Scalability		
>	Logging	Find:	
	Smart Call-Home		
	Security	Servers in the Se	elected
	Service Module Settings	Server Name or IP	Addres
¢.	🕼 Users/AAA 🚽	10.28.17.101	Addre.
	讓 AAA Server Groups		
	S LDAP Attribute Map		
	🔓 AAA Kerberos		
	Sa Authentication Prompt		
	🗛 AAA Access		
	🛱 Dynamic Access Policies		
	😴 User Accounts		
	A Password Policy		
	Thange My Password		
	Login History		
>	Certificate Management		
>	P DHCP		
	B DNS		
\geq	MATERIAL CONTRACTOR AND A DESCRIPTION OF		

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。