Configuration de l'intégration Duo avec Active Directory et ISE pour l'authentification à deux facteurs sur les clients VPN Anyconnect/Remote Access

Table des matières

Introduction Conditions préalables Exigences Composants utilisés Informations générales Schéma de réseau et scénario Processus de communication **Configurations Active Directory Configurations Duo** Configuration du proxy Duo Auth **Configurations Cisco ISE** Configuration de Cisco ASA RADIUS/ISE Configuration VPN d'accès à distance Cisco ASA Essai Dépannage Débogages de travail

Introduction

Ce document décrit l'intégration de la transmission Duo avec AD et ISE en tant qu'authentification à deux facteurs pour les clients AnyConnect connectés à ASA.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration VPN RA sur ASA
- Configuration RADIUS sur ASA
- ISE
- Active Directory
- Applications duo

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Microsoft 2016 Server
- ASA 9.14(3)18
- Serveur ISE 3.0
- Serveur Duo
- Duo Authentication Proxy Manager

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Ce document décrit comment configurer l'intégration Duo Push avec Active Directory (AD) et Cisco Identity Service Engine (ISE) en tant qu'authentification à deux facteurs pour les clients AnyConnect qui se connectent à Cisco Adaptive Security Appliance (ASA).

Schéma de réseau et scénario



Processus de communication

https://duo.com/docs/ciscoise-radius

- 1. Authentification principale initiée vers Cisco ISE
- 2. Cisco ISE envoie une demande d'authentification au proxy d'authentification duo
- 3. L'authentification principale utilise Active Directory ou RADIUS
- 4. Connexion proxy d'authentification duo établie avec Duo Security sur le port TCP 443
- 5. Authentification secondaire via le service de Duo Security
- 6. Le proxy d'authentification duo reçoit une réponse d'authentification
- 7. Accès Cisco ISE accordé

Comptes utilisateurs:

- Active Directory Admin : compte d'annuaire permettant au proxy d'authentification Duo de se lier au serveur Active Directory pour l'authentification principale.
- Utilisateur de test Active Directory
- Utilisateur de test duo pour authentification secondaire

Configurations Active Directory

Le serveur Windows est préconfiguré avec les services de domaine Active Directory.

Remarque : si le Gestionnaire proxy d'authentification RADIUS Duo s'exécute sur le même ordinateur hôte Active Directory, les rôles NPS (Network Policy Server) doivent être désinstallés/supprimés. Si les deux services RADIUS s'exécutent, ils peuvent créer des conflits et affecter les performances.

Afin d'obtenir la configuration AD pour l'authentification et l'identité d'utilisateur sur les utilisateurs VPN d'accès à distance, quelques valeurs sont requises.

Tous ces détails doivent être créés ou collectés sur le serveur Microsoft avant que la configuration puisse être effectuée sur le serveur proxy ASA et Duo Auth.

Les principales valeurs sont les suivantes :

- le nom de domaine. Il s'agit du nom de domaine du serveur. Dans ce guide de configuration, agarciam.cisco est le nom de domaine.
- Adresse IP/FQDN du serveur. Adresse IP ou nom de domaine complet (FQDN) utilisé pour atteindre le serveur Microsoft. Si un nom de domaine complet est utilisé, un serveur DNS doit être configuré au sein du proxy ASA et Duo Auth pour résoudre le nom de domaine complet.

Dans ce guide de configuration, cette valeur est agarciam.cisco (qui correspond à 10.28.17.107).

- Port du serveur. Port utilisé par le service LDAP. Par défaut, LDAP et STARTTLS utilisent le port TCP 389 pour LDAP, et LDAP sur SSL (LDAPS) utilise le port TCP 636.
- CA racine. Si LDAPS ou STARTTLS est utilisé, l'autorité de certification racine utilisée pour signer le certificat SSL utilisé par LDAPS est requise.

- Nom d'utilisateur et mot de passe du répertoire II s'agit du compte utilisé par le serveur proxy Duo Auth pour se lier au serveur LDAP et authentifier les utilisateurs et rechercher des utilisateurs et des groupes.
- Nom distinctif (DN) de base et de groupe. Le DN de base est le point de départ du proxy Duo Auth et il indique à Active Directory de commencer la recherche et l'authentification des utilisateurs.

Dans ce guide de configuration, le domaine racine agarciam.cisco est utilisé comme DN de base et le DN de groupe est Duo-USERS.

1. Afin d'ajouter un nouvel utilisateur Duo, sur Windows Server, naviguez vers l'icône Windows en bas à gauche et cliquez sur Outils d'administration Windows, comme illustré dans l'image.

| = | Recent | lly added | Windows Server | | |
|---|--------|----------------------------------|----------------|-----------------------|---------------------------|
| | | Notepad++ | | | |
| | Z | PuTTYgen | L | Σ | 2 |
| | | PSFTP | Server Manager | Windows PowerShell | Windows PowerShell ISE |
| | Expand | 1 v | | | |
| | Most u | ised | Windows | | |
| | 240 | Duo Authentication Proxy Manager | Administrativ | Task Manager | Control Panel |
| | | Command Prompt | | | |
| | 9 | Snipping Tool | Remote | ė, | |
| | 4 | Wireshark | Desktop | Event Viewer | File Explorer |
| | Ń | Paint | | | |
| | 9 | Google Chrome | | | |
| | D | | | | |
| | | Duo Security V New | | | |
| 8 | G | | | | |
| ٢ | 9 | Google Chrome New | | | |
| Φ | N | | | | |
| | | Notepad++ | | | |
| - | Q | • 🤌 🥫 💆 | 🧧 🔼 🚦 | • | |

2. Dans la fenêtre Outils d'administration de Windows, accédez à Utilisateurs et ordinateurs Active Directory.

Dans le panneau Utilisateurs et ordinateurs Active Directory, développez l'option de domaine et accédez au dossier Utilisateurs.

Dans cet exemple de configuration, Duo-USERS est utilisé comme groupe cible pour l'authentification secondaire.

| → ↑ 倍 > Con | trol Panel > System and Security > Administra | tive Tools | | | Active Directory Users and Compute | ers | | - C | 1 X |
|---|--|---|---|--|--|--|---|---------------------|------------|
| Control C | trol Panel » System and Security » Administra Name Attive Directory Administrative Center Active Directory Domains and Trusts Active Directory Domains and Trusts Active Directory Domains and Trusts Active Directory Stess and Services Active Directory Stess and Services Active Directory Stess and Services Active Directory Users and Computers Active Directory Users and Computers Active Directory Users and Computers Active Directory Users and Computers Component Services Component Services Computer Management Defragment and Optimize Drives Disk Cleanup Disk Cleanup Active Directory | tive Tools Tr/14/2016 623 AM 7/16/2016 623 AM 7/16/2016 623 AM 7/16/2016 620 AM 7/16/2016 619 AM 7/16/2016 619 AM 7/16/2016 619 AM 7/16/2016 618 AM | Type File folder Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut | Size 2 KB 2 KB 2 KB 2 KB 2 KB 2 KB 2 KB 2 KB | Active Directory Users and Computer File Action View Help Active Directory Users and Com Saved Queries Builtin Buil | ers | | o perform dynamic u | ipdates on |
| Pictures Videos Local Disk (C:) DVD Drive (D:) SSS_; | Event Viewer Group Policy Management Group Policy Management Signature formation Services (IIS) Manager Jocal Security Policy Microsoft Azure Services | 7/16/2016 &18 AM 7/16/2016 &19 AM 7/16/2016 &19 AM 7/16/2016 &19 AM 7/16/2016 &18 AM 7/16/2016 &19 AM | Shortcut Shortcut Shortcut Shortcut Shortcut Shortcut | 2 KB 2 KB 2 KB 2 KB 2 KB 2 KB | | Domain Gue. Security Group Domain Users Security Group DUO-USERS Security Group duo2 Security Group Security Group Enterprise K Security Group | All domain guests All domain users Designated administrato Members of this group | | |
| 🧼 Network | Microsoft Azure Services ODBC Data Sources (32-bit) ODBC Data Sources (64-bit) | 7/16/2016 6:19 AM 7/16/2016 6:18 AM 7/16/2016 6:18 AM | Shortcut Shortcut | 2 KB 2 KB 2 KB | | Enterprise R Security Group | Members of this group | | |

3. Cliquez avec le bouton droit sur le dossier Users et sélectionnez New > User, comme illustré dans l'image.

| Active Directory Users and Comp | outers | | | - | × |
|--|---|--|---|---|---|
| File Action View Help | | | | | |
| 🗢 🔿 🙍 🚾 🔏 🖬 🗙 🗑 |] @ 🔒 🛛 🖬 | 1 🙎 🔌 🛍 🦷 | r 🗾 🕱 | | |
| Active Directory Users and Com Saved Queries Saved Queries Save | Name Administrator agarciam alanad alanduo Allowed RO Cert Publish Cloneable D rol D | Type User User User 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 | | ~ |
| Create a new object | | User 🗲 | | | |
| | | Shared Folder | | | |

4. Dans la fenêtre Nouvel objet-utilisateur, spécifiez les attributs d'identité pour ce nouvel utilisateur et cliquez sur Suivant, comme indiqué dans l'image.

| New Object - User | × |
|--------------------------------------|---------|
| Create in: agarciam.cisco/Users | on |
| First name: duovpn Initials: | |
| Last name: | |
| Full name: duovpn | s ir |
| | s o |
| User logon name: | s o |
| duovpn @agarciam.cisco | ~ :cc |
| Liser logon name (pre-Windows 2000): | s ir |
| | nir |
| AGARCIAM | nts |
| | ed |
| | sta |
| < Back Next > | Cancel |
| | jin ain |

5. Confirmez le mot de passe et cliquez sur Next, puis sur Finish une fois que les informations utilisateur sont vérifiées.

| New Object - User | × |
|---|-----------------------|
| Create in: agarciam.cisco/Users | 0 |
| Password: Confirm password: | ac |
| User must change password at next logon User cannot change password Password never expires Account is disabled | s s c s n |
| < Back Next > C | ancel aii |

6. Affectez le nouvel utilisateur à un groupe spécifique, cliquez dessus avec le bouton droit et sélectionnez Ajouter à un groupe, comme illustré dans l'image.

| Active Directory Users and Com | puters | - | | | - | × |
|---|---|--|---|--|---|-------|
| File Action View Help | | | | | | |
| 🗢 🔿 🙋 📅 🖌 🖬 🗡 🕼 | 1 🖬 📑 🖬 🖬 | 1 🙎 🐮 🗊 🦷 | ' 🗾 🗿 | | | |
| Active Directory Users and Com Saved Queries Saved Queries Builtin Builtin Computers Domain Controllers Sim ForeignSecurityPrincipal: Managed Service Accour Users | Name Administrator agarciam alanad alanduo Allowed RO Cert Publish Cort Publish Coneable D DefaultAcco DefaultAcco Denied ROD Donain ROD Donain Ad Domain Ad Domain Co Domain Co Domain Gue Domain Gue Domain Users duo2 DUO-USERS | Type User User User Security Group Security Group | Description Built-in a Members Members A user ac Members DNS Adm DNS clier Designato All works All doma All doma | on ccount for ad s in this group c s of this group s of this group t count manage s in this group c ninistrators Gro ed administrato tations and ser in controllers i in guests in users | | |
| < > | R Enterprise | Add to a group Disable Account | | of this group | | ~ |
| Allows you to add the selected object | ts to a group yo | a static Account | | | | |

7. Dans le panneau Sélectionner des groupes, tapez le nom du groupe souhaité et cliquez sur Vérifier les noms.

Sélectionnez ensuite le nom qui correspond à vos critères et cliquez sur Ok.

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

8. Il s'agit de l'utilisateur utilisé dans ce document à titre d'exemple.

Configurations Duo

1. Connectez-vous à votre portail d'administration Dudo.

| | Admin Login | |
|----------|--|--|
| E | Enter your admin credentials .com Log in as someone else | |
| Pi Fc | assword orgot password? | |
| | Log in | |
| C | Confirm your identity | |

2.Sur le panneau latéral gauche, naviguez vers Users, cliquez sur Add User et tapez le nom de l'utilisateur qui correspond à votre nom d'utilisateur Active Domain, puis cliquez sur Add User.

| DUO | Q Search for users, groups, a | pplications, or devices |
|---------------------|-------------------------------|--|
| Dashboard | Dashboard > Users > Add Use | r |
| Device Insight | Add User | |
| Policies | Most applications allow users | to enroll themselves after they complete primary authentication. |
| Applications | Learn more about adding use | 's [] |
| 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. Sur le nouveau panneau de l'utilisateur, remplissez le vide toutes les informations nécessaires.

| Policies | Uasnboard > Users > duovpn | | |
|---|----------------------------|---|--------------------------------|
| Applications | duovpn | | Logs Send Enrollment Email |
| Single Sign-On | | | |
| Users | (i) This user has not en | olled yet. See our enrollment documentation [2] to learn more about enrolling users. | |
| Add User | | | |
| Pending Enrollments | | | |
| Bulk Enroll Users | Username | duovpn | |
| Import Users | | | |
| Directory Sync | Username aliases | + Add a username alias | |
| Bypass Codes | | Users can have up to 8 aliases. | |
| Groups | | (e.g., Username alias 1 should only be used for Employee ID). | |
| Endpoints | | | |
| 2FA Devices | Full name | test ypn user | |
| Trusted Endpoints | | | |
| Trust Monitor | | | |
| Reports | Email | .com | |
| Settings | | | |
| | Status | Active Bequire multi-factor authentication (default) | |
| Need Help? Chat with Tech Support I? | | | |
| Email Support | | Bypass Allow users to skip two-factor authentication and log in with only a password. Passwordless | authentication is not skipped. |
| Call us at 1-855-386-2884 | | | |
| Versioning | | Automatically deny access | |
| Core Authentication Service: | | This controls the user's two-factor authentication process | |
| Admin Panel: | | | |
| D235.6 | | | |
| Read Release Notes | Groups | You don't have any editable groups. Add one. | |
| Account ID | | Groups can be used for management, reporting, and policy. Learn more about groups 🗳 | |
| 2910-6030-53 | | | |
| Deployment ID | | | |
| | Notes | | |
| Documentation | | | |
| <u>User Guide</u> 다 | | For internal use | |
| Knowledge Base | | | |

4. Sous user devices, spécifiez la méthode d'authentification secondaire.

Remarque : dans ce document, la méthode « Duo push for mobile devices » est utilisée. Un appareil téléphonique doit donc être ajouté.

Cliquez sur Ajouter un téléphone.

| | \sim |
|--|---------------------------|
| Phones | |
| four may rearrange the phones by dragging and dropping in the table. Learn more about activation | ng a replacement phone 🖆. |
| This user has no phone | es. Add one. |
| Endpoints | |
| This user has no d | levices. |
| Hardware Tokens | Add Hardware Token |
| This user has no hardware t | okens. Add one. |
| Bypass Codes | Add Bypass Code |
| This user has no bypass c | odes. Add one. |
| NobAutha & LICE | â del Consultu Vau |

5. Tapez le numéro de téléphone de l'utilisateur et cliquez sur Ajouter un téléphone.

Dashboard > Users > duovpn > Add Phone

Add Phone



6. Dans le panneau d'administration Duo de gauche, accédez à Utilisateurs et cliquez sur le nouvel utilisateur.

| Dashboard | Dashboard > Users | | | | | | |
|--|---------------------|---------------------------|------------------------------------|------------------|-----------------|------------------|---------------------|
| Device Insight | Llooro | | | Director | Suno Import I | Isora Bulk En | |
| Policies | Users | | | Directory | y Sync T Import | JSUIS I DUIK EII | Add User |
| Applications | i You have users wh | to have not activated Duo | Mobile. Click here to send them ad | ctivation links. | | | |
| Single Sign-On | Need to activate a | replacement phone? Lear | rn 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 U | Jsers | Locked Out |
| Bulk Enroll Users | | - | | | | | |
| Import Users | Select (0) V ···· | | | | Export ~ | Q Search | |
| Directory Sync | | | | | | | |
| Bypass Codes | Litername - | Name | Email | Phones | Tokono | Status | Last Logia |
| 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 | | | .com | 1 | | Active | Mar 5, 2022 7:16 PM |
| Need Help? Chat with Tech Support 🗅 | | | | | | | |

Remarque : si vous n'avez pas accès à votre téléphone pour le moment, vous pouvez sélectionner l'option e-mail.

7. Accédez à la section Téléphones et cliquez sur Activer Duo Mobile.

| Phones You may rearrang | e the phones by dragging and dr | a replacement phone 🖒. | | Add Phone | | |
|----------------------------|---------------------------------|------------------------|----------------------|-------------------|---------------------|---|
| Alias | Device | Platform | Model | Security Warnings | | |
| phone1 | 2 8 2 7 2 9 | Android 10 | $(0,1,2,\ldots,2,1)$ | 🗸 No warnings | Activate Duo Mobile | Ē |

8. Cliquez sur Generate Duo Mobile Activation Code.



9. Sélectionnez Email afin de recevoir les instructions par e-mail, tapez votre adresse e-mail et cliquez sur Send Instructions by email.

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 Wasaka |
|----------------|-------------------------|
| Send links via | SMS Email |
| Email | ay i mian ilin ven avan |

10. Vous recevez un e-mail contenant les instructions, comme illustré dans l'image.



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. Ouvrez l'application mobile Duo à partir de votre appareil mobile et cliquez sur Ajouter, puis sélectionnez Utiliser le code QR et numérisez le code à partir de l'e-mail des instructions.

12. Un nouvel utilisateur est ajouté à votre application mobile Duo.

Configuration du proxy Duo Auth

1. Téléchargez et installez Duo Auth Proxy Manager à partir de <u>https://duo.com/docs/authproxy-reference.</u>

Remarque : dans ce document, le Duo Auth Proxy Manager est installé sur le même serveur Windows que celui qui héberge les services Active Directory.

2. Dans le panneau d'administration Duo, accédez à Applications et cliquez sur Protect an Application.

| | Q Search for users, groups, applications, or devices | tools. | Cisco ID: 31/ 6-6006-65 | alan 🗸 |
|------------------------|--|----------|---------------------------|----------|
| Dashboard | Dashboard > Applications | | | - |
| Device Insight | Applications | | Protect an App | lication |
| Policies | Applications | | | |
| Applications 🚽 | _ | | | \times |
| Protect an Application | Manage view undets to the new Universal Drawnt | | | \times |
| Single Sign-On | experience, all in one place. | | | \sim |
| Users | | 0 | | |
| Groups | Get Started Get More Information | | | |
| Endpoints | | • | | |
| 2FA Devices | | | 0 | |
| Trusted Endpoints | | Export V | C Search | |

3. Dans la barre de recherche, recherchez Cisco ISE Radius.

Protect 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 IS Choose an application below to get started. | | | | | | | |
|------------------|--|-----------------|--------------------------|--|--|--|--|--|
| ise Applica | tion | Protection Type | | | | | | |
| Cakamai | Akamai Enterprise Application Access | 2FA | Documentation Id Protect | | | | | |
| alialia cisco | Cisco ISE RADIUS | 2FA | Documentation D | | | | | |

4. Copiez la clé d'intégration, la clé de sécurité et le nom d'hôte de l'API. Vous avez besoin de ces informations pour la configuration Duo Authentication Proxy.

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. Exécutez l'application Duo Authentication Proxy Manager et terminez la configuration du client Active Directory et du serveur RADIUS ISE, puis cliquez sur Valider.

Remarque : si la validation échoue, reportez-vous à l'onglet debug pour plus de détails et corrigez-les en conséquence.

| Duo Authentication Proxy Manager | | - 🗆 × |
|---|--|--|
| Authentication Proxy is running Up since: 3/5/2022, 9:23:0 | 4 AM Version: 5.6.0 Update your Authentication Proxy | Restart Service Stop Service |
| Validation passed Configuration has passed validation and is ready to be saved | | |
| Configure: authproxy.cfg | Insaved 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= HEVMIN H*1 24 search_dn=DC=agarciam,DC=cisco 25 26 [radius_server_auto] 27 ikey=EurorNPICELCATENLEC 28 skey=VGmaTriPicELCATENLEC 28 skey=VGmaTriPicELCATENLEC 29 api_host=api dfT4710.clreatenTifyEtcm 30 radius_ip_1=10.28.17.101 31 radius_secret_1=MmatriPitE1 34 port=1812 35 36 36 37 38 39 39 39 39 30 30 30 30 30 30 30 30 30 30 30 30 30</pre> | Running The Duo Auth several minu [info] Testing sect [info] {'debug': 'T 'log_max_fi 'log_max_si 'test_conne [info] There are no [info] There are no [info] Testing sect [info] {'debug': 'T 'host': 'l0 'search_dn' 'service_acc 'service_acc [info] There are no [info] There are no [info] There are no [info] There are no [info] There are no | <pre>entication Proxy Connectivity Tool. This may take tes ion 'main' with configuration: rue', les': '10', ze': '20971520', ctivity_on_startup': 'true'} configuration problems</pre> |
| Validate Save | | Learn how to configure the Authentication Proxy |

Configurations Cisco ISE

1. Connectez-vous au portail d'administration ISE.

2.Développez l'onglet Cisco ISE et accédez à Administration, puis cliquez sur Network Resources et cliquez sur External RADIUS Servers.

| Cisco ISE - | Q What page are you looking for? | | | | | |
|--|--|------------|--|----------------|--|--|
| Dashboard | Context Visibility | Operations | -Policy- | Administration | | |
| Recent Pages External Identity Sources Policy Sets Network Device Profiles External RADIUS Servers RADIUS Server Sequences Live Logs | System Deployment Licensing Certificates Logging Maintenance Upgrade | | Network Resources Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers | | | |
| | Health Checks Backup & Restore | | External MDM Location Services | | | |

3. Dans l'onglet Serveurs Radius externes, cliquez sur Ajouter.

| ■ Cisco ISE | | Admi | Administration · Network Resources | | | | |
|-------------------------|-----------------------|-------------------------|------------------------------------|-------------------------|--|--|--|
| Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | | | |
| External RADIUS Servers | | | | | | | |
| | 🗍 Duplicate 🌐 Delete | | | | | | |
| Name Name: | Currently Sorted | Description | | | | | |

4. Complétez la zone vide avec la configuration RADIUS utilisée dans le Duo Authentication Proxy Manager et cliquez sur Submit.

| Network Devices Networ | rk Device Groups | Network Device Profil | les External RADIUS Servers | RADIUS Server Sequences | NAC Managers | External MDM | More |
|----------------------------------|------------------|-----------------------|-----------------------------|-------------------------|--------------|--------------|------|
| * Name | DUO_NEW ┥ | | | | | | |
| Description | | | | | | | |
| * Host IP | 10.28.17.107 | | | | | | |
| * Shared Secret | ········ - | Show | N | | | | |
| Enable KeyWrap | | | | | | | |
| * Key Encryption Key | | Show | | | | | |
| * Message Authenticator Code Key | | Show | | | | | |
| Key Input Format | O ASCII O HEXAL | DECIMAL | | | | | |
| * Authentication Port | 1812 | (Valid Range | e 1 to 65535) | | | | |
| * Accounting Port | 1813 | (Valid Range | e 1 to 65535) | | | | |
| * Server Timeout | 5 | Seconds (V | Valid Range 1 to 120) | | | | |
| * Connection Attempts | 3 | (Valid Rang | ge 1 to 9) | | | | |
| Radius ProxyFailover Expiration | 300 | (valid Ra | ange 1 to 600) | | | | |
| | | | | | | Su | bmit |

5. Accédez à l'onglet Séquences de serveur RADIUS et cliquez sur Ajouter.

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

6. Spécifiez le nom de la séquence et affectez le nouveau serveur externe RADIUS, cliquez sur Submit.

RADIUS Server Sequences List > New RADIUS Server Sequence

RADIUS Server Sequence



\sim 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. Accédez à Policy à partir du menu Tableau de bord et cliquez sur Policy Sets.

| 8 | Cisco ISE | Q. What page are you looking for? | | | | | |
|---|---|-----------------------------------|-------------|---------------------|-----|--|--|
| | Dashboard | Context Visibility | Operations- | Policy | Adm | | |
| | Recent Pages | Policy Sets | | Profiling | | | |
| | Policy Sets External RADIUS Servers External Identity Sources | Posture | | Client Provisioning | | | |
| | Network Device Profiles Live Logs | Policy Elements | | | | | |
| | | Dictionaries Conditions | | | | | |

8. Affectez la séquence RADIUS à la stratégie par défaut.

Remarque : dans ce document, la séquence Duo est appliquée à toutes les connexions. La stratégie par défaut est donc utilisée. L'affectation des stratégies peut varier selon les besoins.

| Policy | Sets | | | | | Reset | t Policyset Hi | tcount |
|--------|--------|-----------------|--------------------|-----|-------------------------------------|-------------------------|----------------|--------|
| ÷ | Status | Policy Set Name | Description | Cor | nditions | Allowed Protocols / Ser | ver Sequence | Hits |
| Q | Search | | | | | | | |
| | 0 | 81 D I N | | Ŧ | Radius-User-Name EQUALS isevpn | Default Network Access | • • • • | 3 |
| | 0 | 1 m 1 | | ۲ | Radius-NAS-Port-Type EQUALS Virtual | DUO_Sequence | <u> </u> | 22 |
| | 0 | Default | Default policy set | | | Default Network Acces | s 🛛 ^ + | 0 |
| | | Ĩ | | | | EQ | | |
| | | I | | | | Allowed Protocols | | eset |
| | | | | | | Default Network Ac | cess | |
| | | | | | | DUO_NEW | | |
| | | | | | | DUO Sequence | | |

Configuration de Cisco ASA RADIUS/ISE

1. Configurez le serveur RADIUS ISE sous les groupes de serveurs AAA, accédez à Configuration, cliquez sur Device Management et développez la section Users/AAA, sélectionnez AAA Server Groups.

| 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". Go The Delete | Refresh Ba | ack () ation : ips Pro RA LO |
|------------|--|-------------------|---|
| 0 | O O Device Management | | |
| > | Management Access | | |
| > | 8 Licensing | | |
| > | System Image/Configuration | | |
| > | High Availability and Scalability | | |
| > | | Find: | |
| | Smart Call-Home | | |
| | Security | Servers in the Se | elected |
| | Service Module Settings | Server Name or IP | Addres |
| 0 | | 10 28 17 101 | Addre: |
| | 19 AAA Server Groups | 10.20.17.101 | |
| | Se I DAP Attribute Map | | |
| | AAA Kerberos | | |
| | Authentication Prompt | | |
| | 🗣 AAA Access | | |
| | Dvnamic Access Policies | | |
| | User Accounts | | |
| | A Password Policy | | |
| | G Change My Password | | |
| | Login History | | |
| 5 | Certificate Management | | |
| > | P DHCP | | |
| | B DNS | | |
| Σ | UND TO THE REAL PROPERTY OF TH | | |

, sélectionnez le nom de l'interface, spécifiez l'adresse IP du serveur ISE et tapez la clé secrète RADIUS et cliquez sur Ok.

Remarque : toutes ces informations doivent correspondre à celles spécifiées dans le Duo Authentication Proxy Manager.

| • • | Edit AAA Server |
|-------------------------------------|---------------------------|
| Server Group: IS Interface Name: | SE outside |
| Server Name or IP Address: | 10.28.17.101 |
| Timeout: | 10 seconds |
| RADIUS Parameters | |
| Server Authentication Port: | 1645 |
| Server Accounting Port: | 1646 |
| Retry Interval: | 10 seconds |
| Server Secret Key: | ••••• |
| Common Password: | |
| ACL Netmask Convert: | Standard 📀 |
| Microsoft CHAPv2 Capable | : 🔽 |
| SDI Messages | |
| Message Table | × |
| Help | Cancel OK |

Configuration CLI.

```
aaa-server ISE protocol radius
dynamic-authorization
aaa-server ISE (outside) host 10.28.17.101
key *****
```

Configuration VPN d'accès à distance Cisco ASA

ip local pool agarciam-pool 192.168.17.1-192.168.17.100 mask 255.255.255.0
group-policy DUO internal
group-policy DUO attributes
banner value This connection is for DUO authorized users only!
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split-agarciam
address-pools value agarciam-pool
tunnel-group ISE-users type remote-access
tunnel-group ISE-users general-attributes
address-pool agarciam-pool
authentication-server-group ISE

```
default-group-policy DUO
tunnel-group ISE-users webvpn-attributes
group-alias ISE enable
dns-group DNS-CISCO
```

Essai

1. Ouvrez l'application Anyconnect sur votre appareil PC. Spécifiez le nom d'hôte de la tête de réseau VPN ASA et connectez-vous avec l'utilisateur créé pour l'authentification secondaire Duo et cliquez sur OK.

| 000 | Sec | AnyConnect ure Mobility Client | cisco | |
|-----|-------------------------|-----------------------------------|------------|----|
| | VPN: Please enter yo | ur username and pass | word. | |
| | | | | |
| | Cisco A | nyConnect 192.16 | 58.100.100 | |
| | Please enter your | username and pass | word. | |
| | Group: | ISE - | - | 0 |
| | msgstringESMEX | duovpn 🔶 | | |
| | MEX-PASS | •••• | | |
| | | | Cancel | ок |

2. Vous avez reçu une notification de transmission Duo sur l'appareil Duo Mobile de l'utilisateur spécifié.

3. Ouvrez la notification de l'application mobile Duo et cliquez sur Approuver.





4. Acceptez la bannière et la connexion est établie.





Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Duo Authentication Proxy est fourni avec un outil de débogage qui affiche les raisons de l'erreur et de l'échec.



Remarque : les informations suivantes sont stockées dans le fichier C:\Program Files\Duo Security Authentication Proxy\log\connectivity_tool.log.

| Output | |
|---------|---|
| Running | The Duo Authentication Proxy Connectivity Tool. This may take several minutes |
| [info] | Testing section 'main' with configuration: |
| [info] | {'debug': 'True', |
| | 'log_max_files': '10', |
| | 'log_max_size': '20971520', |
| | 'test_connectivity_on_startup': 'true'} |
| [info] | There are no configuration problems |
| [info] | |
| [info] | Testing section 'ad_client' with configuration: |
| [info] | {'debug': 'True', |
| | 'host': '10.28.17.107', |
| | 'search_dn': 'DC=agarciam,DC=cisco', |
| | 'service_account_password': '*****', |
| | <pre>'service_account_username': 'Administrator'}</pre> |
| [info] | There are no configuration problems |

```
[info]
        Testing section 'radius_server_auto' with configuration:
[info]
        {'api_host': 'apl affect?'Laboratelly.com',
[info]
         'client': 'ad_client',
         'debug': 'True',
         'failmode': 'safe',
         'ikey': Lange Los AN BHALL'
         'port': '1812',
         'radius_ip_1': '10.28.17.101',
         'radius_secret_1': '******',
         'skey': '********[40]'}
        There are no configuration problems
[info]
[info] Testing section 'main' with configuration:
[info] {'debug': 'True',
         'log_max_files': '10',
         'log_max_size': '20971520',
         'test_connectivity_on_startup': 'true'}
[info] There are no connectivity problems with the section.
```

```
[info]
       There are no connectivity problems with the section.
[info]
[info] Testing section 'ad_client' with configuration:
[info] {'debug': 'True',
         'host': '10.28.17.107',
         'search_dn': 'DC=agarciam,DC=cisco',
         'service_account_password': '******',
         'service_account_username': 'Administrator'}
       The LDAP Client section has no connectivity issues.
[info]
[info]
[info] Testing section 'radius_server_auto' with configuration:
[info] {'api_host': 'asi_adicate dissecurity.cmp',
         'client': 'ad_client',
         'debug': 'True',
         'failmode': 'safe',
         'ikey': 'n marchner wordstate'
         'port': '1812',
         'radius_ip_1': '10.28.17.101',
         'radius_secret_1': '******',
         'skey': '****** [40]'}
       The RADIUS Server has no connectivity problems.
[info]
[info]
[info] SUMMARY
[info] No issues detected
```

1. Problèmes de connectivité, adresse IP incorrecte, nom de domaine complet/nom d'hôte non résolu dans la configuration Active Directory.

Output

'host': '10.28.17.106', 'search_dn': 'DC=agarciam,DC=cisco', 'service_account_password': '*****', 'service_account_username': 'Administrator'} [warn] The LDAP Client section has connectivity problems. [warn] The LDAP host clear connection to 10.28.17.106:389 has connectivity problems. [error] The Auth Proxy was not able to establish a connection to 10 .28.17.106:389.

2. Mot de passe incorrect pour l'utilisateur Administrateur sur Active Directory.



Débogages.

| .107:389. | 10 |
|--|----|
| fiefal The Auth Drawy use ship to actablish an LDAD connection to | 10 |
| [info] the Auth Proxy was able to establish an LDAP connection to | |
| .28.17.107:389. | |
| [error] The Auth Proxy was unable to bind as Administrator. | |
| [error] Please ensure that the provided service account credential | |
| are correct. | |
| [debug] Exception: invalidCredentials: 8009030C: LdapErr: DSID | |
| -0C090516, comment: AcceptSecurityContext error, data 52e, | |
| v3839 <mark>-</mark> | |
| [warn] The Auth Proxy did not run the search check because of the | |
| problem(s) with the bind check. Resolve that issue and rer | in |
| the tester. | |

3. Domaine de base incorrect.



Débogages.



4. Valeur RADIUS ikey incorrecte.

| [radius_server_auto] |
|--|
| ikey=U_NUU KHRNZ6EZ1 |
| skey=Jacking - Italia 🖓 🛛 🖓 🖓 👘 👘 👘 🖓 |
| api_host=apl = 🗖 📲 🖬 🖬 🖛 🖜 ity.com |
| radius_ip_1=10.28.17.101 |
| <pre>radius_secret_1=!Mexvpn!17!</pre> |
| failmode=safe |
| <pre>client=ad_client</pre> |
| port=1812 |
| |

Déboguages

| | and a sussifier t |
|---------|---|
| [error] | The ikey value provided is invalid. |
| [info] | |
| [info] | SUMMARY |
| [warn] | Checks for external connectivity were not run. Please fix the |
| | configuration and try again. |

5. Vérifiez que le serveur ISE envoie des paquets de demande d'accès.

*Ethernet0

| File | e Edi | t View | Go | Capture | Analyze | Statistics | Telephony | Wirele | ss Tools | Hel | P | | | |
|---------|--------|---------|---------|----------|-----------------------|------------|-------------|---------|----------|--------|-------|---------------|--------------|------------|
| 1 | • | . 💿 | | | ۹ 👄 🕫 |) 🗟 🖗 | £ 🗐 🔳 | ର୍ ପ୍ | ۹. 🖽 | | | | | |
| | radius | | | | 1 | | | | | | | | | |
| No. | | Time | | Source | | | Destination | | Proto | col L | ength | Terio | <hr/> | |
| | 1511. | . 6020. | 521457 | 10.20 | 8.17.101 | | 10.28.17.10 | 97 | RADI | US | 877 | Access-Reque | st 刘 - 31 | |
| <u></u> | 1513. | . 6024. | 344735 | 10.2 | 8.17.107 | | 10.28.17.10 | 91 | RADI | US | 191 | Access Accep | t id=31 | |
| > | Frame | 15111 | 5: 877 | bytes o | on wire (| 7016 bit: | ;), 877 byt | es cap | tured (7 | 016 b | its) | on interface | \Device\NPF | CA092CEE-5 |
| > | Ether | net II, | Src: | Where_ | b3:a4:2f | (00:50:5 | 6:b3:a4:2f |), Dst | : Wheare | _b3:b | 4:3e | (00:50:56:b3: | :b4:3e) | |
| > | Inter | net Pro | otocol | Version | 4, Src: | 10.28.17 | 7.101, Dst: | 10.28 | .17.107 | | | | | |
| > | User | Datagra | am Pro | tocol, S | inc Port: | 42022, 0 | Ost Port: 1 | 812 | | | | | | |
| ~ | RADIU | S Prote | col | | | | | | | | | | | |
| | Co | de: Acc | ess-R | equest (| 1) | | | | | | | | | |
| | Pa | cket id | dentif: | ier: 0x1 | f (31) | | | | | | | | | |
| | Le | ngth: 8 | 335 | | | | | | | | | | | |
| | Au | thentio | ator: | 38a28ca | 3ca6bbc26 | 51819c530 | Mb1be6e3 | | | | | | | |
| | 11 | he resp | onse | to this | request i | is in fra | me 151332] | | | | | | | |
| | ✓ At | tribute | e Valu | e Pairs | | | - | | | | | | | |
| | 2 | AVP: t | =User | Name(1) | 1=8 val= | duovpn | | | | | | | | |
| | > | AVP: t | =User | Passwor | d(2) 1=18 | 3 val=Enc | rypted | | | | | | | |
| | 2 | AVP: t | =NAS- | (P-Addre | ss(4) 1=6 | 5 val=192 | .168.100.1 | 99 | | | | | | |
| | 2 | AVP: t | =NAS-I | Port(5) | 1=6 val=3 | 44064 | | | | | | | | |
| | 2 | AVP: t | =Call(| d-Stati | on-1d(30) | 1=17 va | 1=192.168. | 100.100 | , | | | | | |
| | 2 | AVP: t | =Call: | ing-Stat | 10n-1d(31 | () 1=13 v | a1 10.11.c | 1.11 | | | | | | |
| | 2 | AVP: 1 | =Proxy | -State(| 33) 1=25 | va1=4069 | 72/3/450/2 | 01/8/93 | 0001302e | 435382 | e313/ | 20313031 | 06363303434 | 165633463 |
| | | AVP: T | -Prox | -state(| 55) 1=/6 0(61) 1-6 | val=4369 | 1/3030T2053 | 0303/5/ | 2052041 | 43533 | /3665 | 3332373561203 | 90302302031: | 103032003- |
| | | AVP: 1 | -7-00-1 | -ore-typ | e(or) rec | +/66) 1- | 13 val-10 | 00 65 9 | | | | | | |
| | | AVP: 1 | -Tunne | inclien. | c-enupoir | r(00) 1 | 15 Val=10. | 55.05.5 | | | | | | |

6. Afin de confirmer que le serveur proxy d'authentification Duo fonctionne, Duo fournit l'outil <u>NTRadPing</u> pour simuler les paquets de demande d'accès et la réponse avec Duo.

6.1 Installation de NTRadPing sur un autre PC et génération de trafic

Remarque : dans cet exemple, la machine Windows 10.28.17.3 est utilisée.

6.2 Configuration à l'aide des attributs utilisés dans la configuration ISE Radius

| INTRadPing Test Utility | – 🗆 X | | | |
|--------------------------------------|--|--|--|--|
| RADIUS Server/port 10.28.17.107 | NTRadPing 1.5 - RADIUS Server Testing Tool © 1999-2003 Master Soft SpA - Italy - All rights reserved | | | |
| Reply timeout (sec.): 3 Retries: 6 | http://www.dialways.com/ | | | |
| RADIUS Secret key: | THE LOS | | | |
| User-Name: duovpn | | | | |
| Password CHAP | MASTERSOFT DIALWAYS | | | |
| Request type: Authentication Request | RADIUS Server reply: | | | |
| Additional RADIUS Attributes: | Source of the first interpret is some 22 20.52 W23/22 Instantianes, and source in which is non-will in a source of the object area should be included from the contract in 20.52 Hills interpret www.areat.com/source.com/source area.com/source/source/ area source in a company area source in a comp and areas for the contract area source. | | | |
| Add Remove Clear list Load Save | Send Help Close | | | |

6.3 Configurez le Duo Authentication Proxy Manager comme suit.

| [radius_server_auto] |
|--|
| ikey="million:new"ikey |
| skey=Jac3 |
| api_host=ani_nd7c172n.chmarch_nity.com |
| radius_ip_1=10.28.17.101 |
| <pre>radius_secret_1=!Mex.u!17!</pre> |
| radius_ip_2=10.28.17.3 |
| <pre>radius_secret_2=!Mex 7! </pre> |

6.4. Accédez à votre outil NTRadPing et cliquez sur Send (Envoyer). Vous recevez une notification de transmission Duo sur l'appareil mobile attribué.

| INTRadPing Test | Utility | | - 🗆 X |
|-----------------------|---|---------|--|
| RADIUS Server/port: | 10.28.17.107 | 1812 | NTRadPing 1.5 - RADIUS Server Testing Tool © 1999-2003 Master Soft SpA - Italy - All rights reserved |
| Reply timeout (sec.): | 3 Ret | ries: 6 | http://www.dialways.com/ |
| RADIUS Secret key: | !Mexvpn!17! | | ms |
| User-Name: | duovpn | | |
| Password: | XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX | CHAP | MASTERSOFT DIALWAYS |
| Request type: | Authentication Request 💌 | 0 | RADIUS Server reply: |
| Additional RADIUS A | ttributes: | _ | Sending authentication request to server 10.28.17.107:1812 Transmitting packet, code=1 id=12 length=46 no response from server (uned out), non-ottempt (#1) received response from the server in 4000 millisecords reply packet code=2 id=12 length=49 response: Access:Accept attribute dump Reply-Message=Success. Logging you in |
| Add Remove | e Clear list Load | Save | Send Help Close |

| | 700 20.866684 | 10.28.17.3 | 10.28.17.107 | RADIUS | 88 Access-Request id=13, | , Duplicate Request | |
|----|--------------------|----------------------|------------------------|---------------|---------------------------|------------------------------------|---------|
| ąL | 737 22.184895 | 10.28.17.107 | 10.28.17.3 | RADIUS | 90 Access-Accept id=13 | ← | |
| | | | | | | | |
| > | Frame 700: 88 byte | s on wire (704 bit: | s), 88 bytes captured | (704 bits) on | interface \Device\NPF {CA | 092CEE-5528-4E0A-9310-2D523160DD60 | }, id 0 |
| > | Ethernet II, Src: | VMware_b3:f2:72 (00 | 0:50:56:b3:f2:72), Dst | : VMware_b3:b | 4:3e (00:50:56:b3:b4:3e) | | |
| > | Internet Protocol | Version 4, Src: 10 | .28.17.3, Dst: 10.28.1 | 7.107 | | | |
| > | User Datagram Prot | cocol, Src Port: 51 | 188, Dst Port: 1812 | | | | |
| ~ | RADIUS Protocol | | | | | | |
| | Code: Access-Re | quest (1) | | | | | |
| | Packet identifi | er: 0xd (13) | | | | | |
| | Length: 46 | | | | | | |
| | Authenticator: | 2020202020203136343 | 36393335333230 | | | | |
| | [Duplicate Requ | est Frame Number: 5 | 532] | | | | |
| | [The response t | to this request is i | in frame 737] | | | | |
| | ✓ Attribute Value | Pairs | | | | | |
| | > AVP: t=User- | Name(1) l=8 val=duc | ovpn | | | | |
| | > AVP: t=User- | Password(2) l=18 va | al=Encrypted | | | | |
| | | | | | | | |
| 1 | | | | | | | |

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.