# Configurer l'attribution d'adresses IP statiques pour les utilisateurs VPN clients sécurisés

# Table des matières

Introduction	
Conditions préalables	
Exigences	
Composants utilisés	
Informations générales	
Configurer	
Vérifier	
Dépannage	

## Introduction

Ce document décrit comment attribuer des adresses IP statiques aux utilisateurs VPN d'accès à distance à l'aide d'un mappage d'attributs LDAP.

# Conditions préalables

#### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Active Directory (AD)
- Protocole LDAP (Lightweight Directory Access Protocol)
- Cisco Secure Firewall Threat Defense
- Cisco Secure Firewall Management Center

#### Composants utilisés

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

- Windows Server 2022
- FTD version 7.4.2
- FMC version 7.4.2

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

Remarque : l'option permettant d'utiliser un domaine pour l'attribution d'adresses IP et de configurer les mappages d'attributs LDAP est prise en charge dans firepower version 6.7 ou ultérieure. Assurez-vous que la version de firepower est 6.7 ou ultérieure avant de continuer.

### Configurer

Étape 1. Accédez à Devices > Remote Access et sélectionnez la politique VPN d'accès à distance souhaitée. Sélectionnez le profil de connexion souhaité. Sous l'onglet AAA, sélectionnez un domaine pour Authentication Server et Authorization Server.

Edit Connection Profile		0
Connection Profile:* Group Policy:*	RAVPN_PROFILE	
Client Address Assignment	AAA Aliases	
Authentication Authentication Method: Authentication Server: Use secondary authenticat Authorization Authorization Server:	AAA Only   WINDOWS_2022_AD (AD)  Fallback to LOCAL Authentication ion Use same authentication server  Allow connection only if user exists in authorization database Configure LDAP Attribute Map	
Accounting Server: Advanced Settings		
	Cancel Sav	e

Étape 2. Accédez à Périphériques > Accès à distance et sélectionnez la stratégie VPN d'accès à distance souhaitée. Accédez à Advanced > Address Assignment Policy et vérifiez que l'option Use authorization server (Only for RADIUS or Realm) est activée.



Étape 3. Accédez à Advanced > LDAP Attribute Mapping et ajoutez un Name Map avec LDAP Attribute Name set to msRADIUSramedIPAddress et Cisco Attribute Name set to IETF-Radius-Framed-IP-Address.

Firewall Management	nt Center Overview Analysis F	Policies Devices Objects Integration	Deploy Q 💕 🌣 🔕 admin ~ 👘 SECURE
RAVPN_POLICY			Save Cancel
Enter Description			
			Policy Assignments (1)
Connection Drofile Assess Inte	orferen Advanced		Local Realm: None Dynamic Access Policy: None
Connection Prome Access in			
Secure Client Images	LDAP Attribute Mapping		
<ul> <li>Secure Client Customization</li> </ul>	LDAP attribute mapping can be configured to enable	LDAP server to perform authorization.	+
GUI Text and Messages			
Icons and Images	Realm	Map	
Binaries	WINDOWS_2022_AD		/ i
Custom Installer Transforms		Configure LDAP Attribute Man	
Localized Installer Transforms			
Address Assignment Policy		Realm:	
Certificate Maps		WINDOWS_2022_AD (AD) +	
Group Policies			
LDAP Attribute Mapping		LDAP attribute Maps: +	
Load Balancing		Name Map:	
✓ IPsec		LDAP Attribute Name Cisco Attribute Name	
Crypto Maps		mskADiUSFramediPAdoress v IETP-Radius-Framed-IP-Adoressv	
IKE Policy		Value Maps:	
IPsec/IKEv2 Parameters		LDAP Attribute Value Cisco Attribute Value	
		Add Value Map	
		Oreal OK	
		Cancer	

Étape 4. Sur votre serveur Windows AD, ouvrez le Gestionnaire de serveur et accédez à Outils > Utilisateurs et ordinateurs Active Directory. Cliquez avec le bouton droit sur un utilisateur, sélectionnez Propriétés > Accès commuté et cochez la case Attribuer des adresses IP statiques.

Jo	hn	Doe	Pro	perties

Remote control	Remote control Remote Desktop Services Profile COM+				
eneral Address	Account	Profile	Telephones	Organization	
Member Of	Dial-in	Envi	ronment	Sessions	
Vetwork Access Pe Allow access Deny access Control access t	mission	twork Polic	cy		
Verify Caller-ID: Callback Options No Callback Set by Caller (R Always Callback	outing and Rem < to:	ote Acces	s Service only)		
<ul> <li>Assign Static IP</li> <li>Define IP addresse</li> <li>Dial-in connection.</li> </ul>	Addresses	this	Static IP Addr	esses	
Apply Static Rou Define routes to er	ites nable for this Dia	ıl-in	Static F	outes	
Apply Static Rou Define routes to er	ites nable for this Dia	ıl-in	Static F	outes	

Étape 5. Sélectionnez Static IP Addresses et attribuez une adresse IP statique à l'utilisateur.

Static IP Addresses	>	<
Assign a static IPv4 address:	172 . 16 . 20 . 73	
Assign a static IPv6 address:		
Prefix:		
Interface ID:		
OK	Cancel	

Étape 6. Connectez-vous à la passerelle VPN et connectez-vous à l'aide du client sécurisé Cisco. L'adresse IP statique que vous avez configurée est attribuée à l'utilisateur.

S Cisco Secure Client		_		×
cisco Secure (	Client			0
General	Virtual Private Network (VPN)			
Status Overview	Preferences Statistics Route Details Firewall Message History			
AnyConnect VPN >	Connection Information		- •	^
Zero Trust Access	Tunnel Mode (IPv4): Tunnel All Traffic Tunnel Mode (IPv6): Drop All Traffic			
Network	Dynamic Tunnel Exclusion: None Dynamic Tunnel Inclusion: None			
ISE Posture	Duration: 00:00:26 Session Disconnect: None			
Umbrella	Management Connection State: Disconnected (user tunnel active) Address Information			
	Client (IPv4):         172.16.20.73           Client (IPv6):         Not Available           Server:         10.0.0.1			
Collect diagnostic information for all installed components. Diagnostics	Bytes Reset	Exp	port Stat	~

#### Vérifier

Activez debug Idap 255 et assurez-vous que l'attribut LDAP msRADIUSFramedIPAddress est récupéré :

```
[13] Session Start
[13] New request Session, context 0x000015371bf7a628, reqType = Authentication
[13] Fiber started
[13] Creating LDAP context with uri=ldap://192.168.2.101:389
[13] Connection to LDAP server: ldap://192.168.2.101:389, status = Successful
[13] supportedLDAPVersion: value = 3
[13] supportedLDAPVersion: value = 2
[13] Binding as (Administrator@test.example) [Administrator@test.example]
[13] Performing Simple authentication for Administrator@test.example to 192.168.2.101
[13] LDAP Search:
Base DN = [CN=Users,DC=test,DC=example]
Filter = [sAMAccountName=jdoe]
Scope = [SUBTREE]
[13] User DN = [CN=John Doe, CN=Users, DC=test, DC=example]
[13] Talking to Active Directory server 192.168.2.101
[13] Reading password policy for jdoe, dn:CN=John Doe,CN=Users,DC=test,DC=example
[13] Read bad password count 0
[13] Binding as (jdoe) [CN=John Doe, CN=Users, DC=test, DC=example]
[13] Performing Simple authentication for jdoe to 192.168.2.101
[13] Processing LDAP response for user jdoe
[13] Message (jdoe):
[13] Authentication successful for jdoe to 192.168.2.101
[13] Retrieved User Attributes:
[13] objectClass: value = top
[13] objectClass: value = person
[13] objectClass: value = organizationalPerson
[13] objectClass: value = user
[13] cn: value = John Doe
[13] sn: value = Doe
[13] givenName: value = John
[13] distinguishedName: value = CN=John Doe,CN=Users,DC=test,DC=example
[13] instanceType: value = 4
[13] whenCreated: value = 20240928142334.0Z
[13] whenChanged: value = 20240928152553.0Z
[13] displayName: value = John Doe
[13] uSNCreated: value = 12801
[13] uSNChanged: value = 12826
[13] name: value = John Doe
[13] objectGUID: value = .....fA.f...;.,
[13] userAccountControl: value = 66048
[13] badPwdCount: value = 0
[13] codePage: value = 0
[13] countryCode: value = 0
[13] badPasswordTime: value = 0
[13] lastLogoff: value = 0
[13] lastLogon: value = 0
[13] pwdLastSet: value = 133720070153887755
[13] primaryGroupID: value = 513
[13] userParameters: value = m: d.
[13] objectSid: value = .....Q=.S....=...Q...
[13] accountExpires: value = 9223372036854775807
[13] logonCount: value = 0
[13] sAMAccountName: value = jdoe
```

```
[13] sAMAccountType: value = 805306368
[13] userPrincipalName: value = jdoe@test.example
[13] objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=test,DC=example
[13] msRADIUSFramedIPAddress: value = -1408232375
[13] mapped to IETF-Radius-Framed-IP-Address: value = -1408232375
[13] msRASSavedFramedIPAddress: value = -1408232375
[13] dSCorePropagationData: value = 16010101000000.0Z
[13] lastLogonTimestamp: value = 133720093118057231
[13] Fiber exit Tx=522 bytes Rx=2492 bytes, status=1
[13] Session End
```

#### Dépannage

Commandes de débogage :

debug webvpn 255

debug Idap

Commande permettant de valider l'adresse IP statique attribuée à l'utilisateur VPN RA souhaité :

show vpn-sessiondb anyconnect filter name <username>

<#root>

firepower#

show vpn-sessiondb anyconnect filter name jdoe

Session Type: AnyConnect

Username : jdoe Index : 7 Assigned IP : 172.16.20.73 Public IP : 10.0.0.10 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384 Bytes Tx : 14664 Bytes Rx : 26949 Group Policy : DfltGrpPolicy Tunnel Group : RAVPN\_PROFILE Login Time : 11:45:48 UTC Sun Sep 29 2024 Duration : Oh:38m:59s Inactivity : Oh:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : cb0071820000700066f93dec Security Grp : none Tunnel Zone : 0

#### 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.