

ASA 8.x: 允許使用者通過Group-Alias和Group-URL方法在WebVPN登入時選擇組

目錄

[簡介](#)

[必要條件](#)

[配置別名並啟用下拉選單](#)

[ASDM](#)

[CLI](#)

[配置URL並啟用下拉選單](#)

[ASDM](#)

[CLI](#)

[問與答](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

SSL VPN使用者 (AnyConnect/SVC和無客戶端) 可以使用以下不同的方法選擇訪問哪個隧道組[自適應安全裝置管理器(ASDM)中的連線配置檔案lingo]:

- group-url
- group-alias (登入頁面上的隧道組下拉選單)
- certificate-maps (如果使用證書)

本文檔演示如何配置自適應安全裝置(ASA)，以允許使用者在登入到WebVPN服務時通過下拉選單選擇組。選單中顯示的組是在ASA上配置的實際連線配置檔案 (隧道組) 的別名或URL。本文檔說明了如何為連線配置檔案 (隧道組) 建立別名和URL，然後配置下拉選單以顯示。此配置使用運行軟體版本8.0(2)的ASA 6.0(2)執行。

注意：ASA 7.2.x版支援兩種方法：group-url和group-alias list。

注意：ASA 8.0.x版支援三種方法：group-url、group-alias和certificate-maps。

[必要條件](#)

基本WebVPN配置

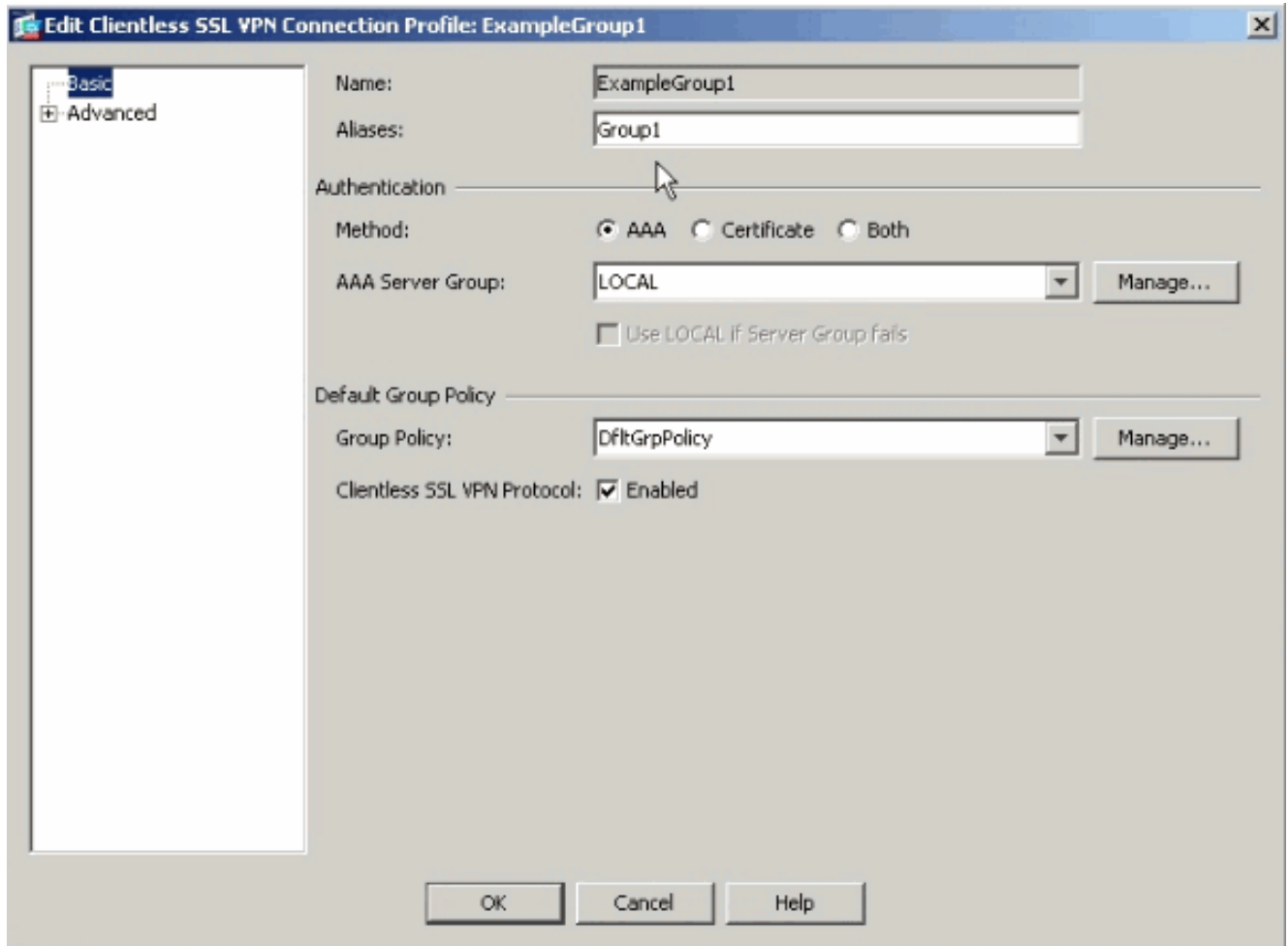
[配置別名並啟用下拉選單](#)

本節提供為連線配置檔案（隧道組）配置別名，然後配置這些別名以顯示在WebVPN登入頁面的Group下拉選單中的資訊。

ASDM

完成這些步驟，以便在ASDM中配置連線配置檔案（隧道組）的別名。根據需要對要為其配置別名的每個組重複上述步驟。

1. 選擇**Configuration > Clientless SSL VPN Access > Connection Profiles**。
2. 選擇連線配置檔案，然後按一下**Edit**。
3. 在「別名」欄位中輸入別名。



4. 按一下「OK」，然後「Apply」變更。
5. 在「連線配置檔案」視窗中，選中Allow user to select connection， identified by alias in the table above， at login page。

Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles

Configure Clientless SSL VPN access parameters.

Access Interfaces
 Enable interfaces for clientless SSL VPN access, and indicate whether to require a certificate for access.

Interface	Allow Access	Require Client Certificate
outside	<input checked="" type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>

Access Port:

[Click here to Assign Certificate to Interface.](#)

Connection Profiles
 Connection profile (tunnel group) table below contains records that determine connection policies. A record identifies a default group policy for the connection and contains protocol-specific connection parameters.

Name	Aliases	Clientless SSL VPN Protocol	Group Policy
DefaultRAGroup		Enabled	DfltGrpPolicy
DefaultWEBVPGGroup		Enabled	DfltGrpPolicy
ExampleGroup1	Group1	Enabled	DfltGrpPolicy
ExampleGroup2	Group2	Enabled	DfltGrpPolicy

Allow user to select connection, identified by alias in the table above, at login page
 Allow user to enter internal password at login page

CLI

在命令列使用這些命令為連線配置檔案（隧道組）配置別名並啟用隧道組下拉選單。根據需要對要為其配置別名的每個組重複上述步驟。

```
ciscoasa#configure terminal
ciscoasa(config)#tunnel-group ExampleGroup1 webvpn-att
ciscoasa(config-tunnel-webvpn)#group-alias Group1 enable
ciscoasa(config-tunnel-webvpn)#exit
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#tunnel-group-list enable
```

配置URL並啟用下拉選單

本節提供為連線配置檔案（隧道組）配置URL，然後配置這些URL以顯示在WebVPN登入頁面的Group下拉選單中的資訊。使用group-url而不是group-alias(group drop-down)的一個優點是，您不會像後一種方法那樣公開組名。

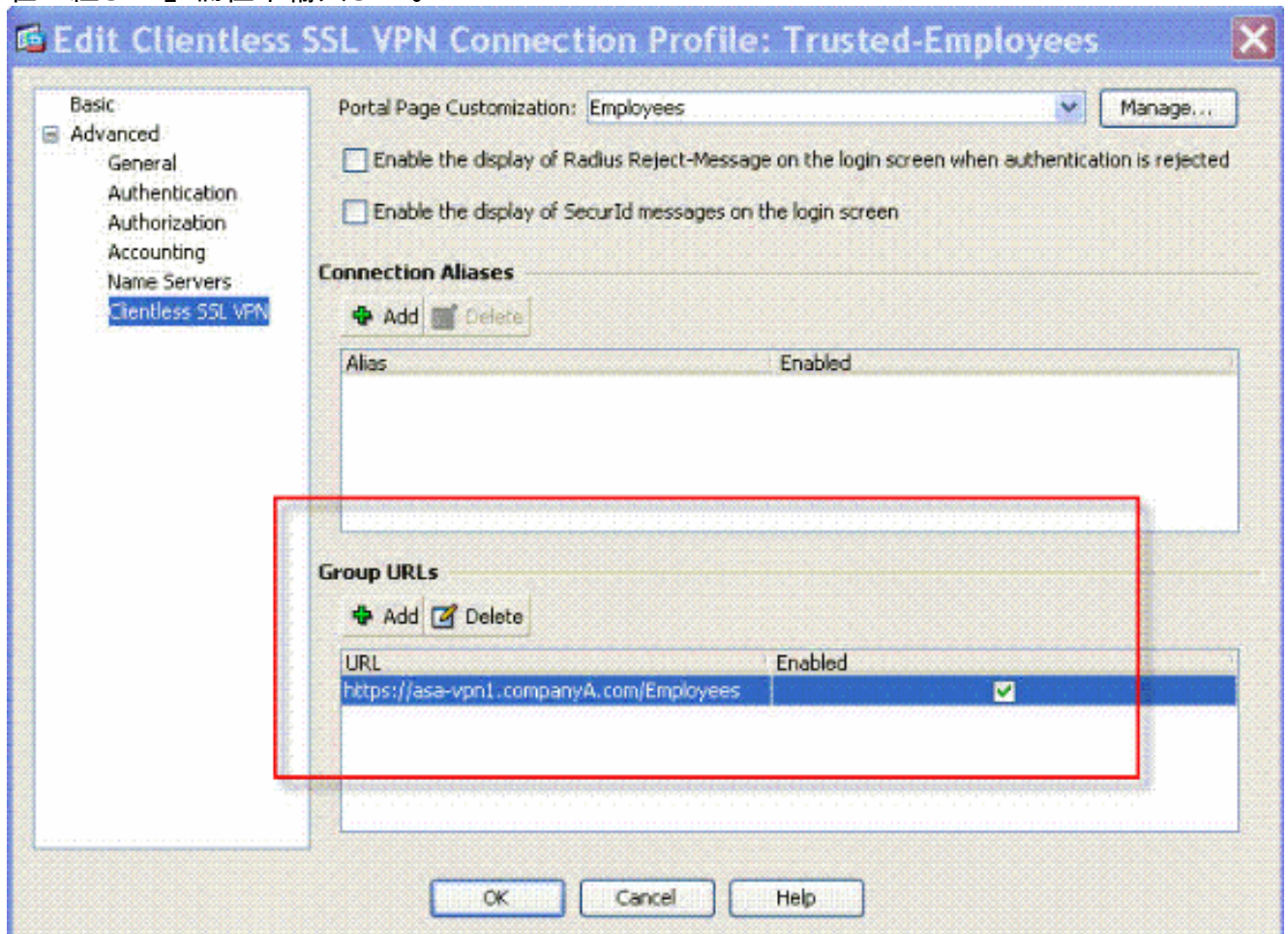
ASDM

在ASDM中指定組URL的方法有兩種：

- 配置檔案方法 — 完全操作編輯AC配置檔案並修改<HostAddress>欄位。在Windows 2000/XP上，預設配置檔案（例如CiscoAnyConnectProfile.xml）位於目錄中：C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\Profile。Vista的位置略有不同：C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\Profile。
- 在「連線到」欄位中輸入組URL字串。支援三種組URL字串格式：https://asa-vpn1.companyA.com/EmployeeSasa-vpn1.companyA.com/EmployeeSasa-vpn1.companyA.com（僅限域，無路徑）

完成這些步驟，以便在ASDM中配置連線配置檔案（隧道組）的URL。根據需要對要為其配置URL的每個組重複上述步驟。

1. 選擇Configuration > Clientless SSL VPN Access > Connection Profiles>Advanced>Clientless SSL VPN panel。
2. 選擇連線配置檔案，然後按一下Edit。
3. 在「組URL」欄位中輸入URL。



4. 按一下「OK」，然後「Apply」變更。

CLI

在命令列使用這些命令為連線配置檔案（隧道組）配置URL並啟用隧道組下拉選單。根據需要對要為其配置URL的每個組重複上述步驟。

```
ciscoasa#configure terminal
```

```
ciscoasa(config)#tunnel-group Trusted-Employees type remote-access
```

```
ciscoasa(config)#tunnel-group Trusted-Employees general-attributes
ciscoasa(config)#authentication-server-group (inside) LDAP-AD11
ciscoasa(config)#accounting-server-group RadiusACS12
ciscoasa(config)#default-group-policy Employees
ciscoasa(config)#tunnel-group Trusted-Employees webvpn-attributes
ciscoasa(config)#group-url https://asa-vpn1.companyA.com/Employees enable
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#tunnel-group-list enable
```

問與答

問題：

如果ASA VPN網關位於NAT裝置之後，如何配置group-url？

答案：

使用者輸入的主機/URL將用於組對映。因此，您必須使用NAT地址，而不是ASA外部介面上的實際地址。最佳替代方案是使用FQDN而不是IP地址進行組URL對映。

所有對映都在HTTP協定級別（基於瀏覽器傳送的資訊）實現，並且一個URL被組合成從傳入的HTTP報頭中的資訊對映。主機名或IP取自主機標頭，其餘URL取自HTTP請求行。這表示使用者輸入的主機/URL將用於群組對應。

驗證

導航到ASA的WebVPN登入頁面，驗證是否已啟用下拉選單以及是否顯示別名。



Login

Please enter your username and password.

USERNAME:

PASSWORD:

GROUP:

Group1
Group2

導航到ASA的WebVPN登入頁面，驗證是否已啟用下拉選單並顯示URL。



疑難排解

- 如果未顯示下拉選單，請確保您已啟用該清單並配置了別名。使用者經常做這些事情之一，但不會做其他事情。
- 請確保連線到ASA的基本URL。如果使用group-url連線到ASA，則不會顯示下拉選單，因為group-url的作用是執行組選擇。

相關資訊

- [Cisco ASA 5500系列調適型安全裝置](#)
- [技術支援與文件 - Cisco Systems](#)