

# Clientless-SSL-VPN (WebVPN) auf der ASA konfigurieren

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Hintergrundinformationen](#)

[Konfiguration](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Verfahren zur Fehlerbehebung](#)

[Befehle zur Fehlerbehebung](#)

[Häufige Probleme](#)

[Benutzer kann sich nicht anmelden](#)

[Verbindung von mehr als drei WebVPN-Benutzern mit der ASA nicht möglich](#)

[WebVPN-Clients können Lesezeichen nicht schlagen, und sie sind ausgegraut.](#)

[Citrix-Verbindung über WebVPN](#)

[Vermeidung einer zweiten Authentifizierung für Benutzer](#)

[Zugehörige Informationen](#)

## Einführung

Dieses Dokument enthält eine einfache Konfiguration für die Cisco Adaptive Security Appliance (ASA) 5500-Serie, um Clientless Secure Sockets Layer (SSL)-VPN-Zugriff auf interne Netzwerkressourcen zu ermöglichen. Clientless SSL Virtual Private Network (WebVPN) ermöglicht einen begrenzten, aber wertvollen sicheren Zugriff auf das Unternehmensnetzwerk von einem beliebigen Standort aus. Benutzer können jederzeit sicheren, browserbasierten Zugriff auf Unternehmensressourcen erhalten. Für den Zugriff auf interne Ressourcen ist kein weiterer Client erforderlich. Der Zugriff erfolgt über ein Hypertext Transfer Protocol über SSL-Verbindung.

Clientless-SSL-VPN bietet sicheren und einfachen Zugriff auf eine breite Palette von Webressourcen sowie sowohl webbasierte als auch ältere Anwendungen von fast jedem Computer aus, der Hypertext Transfer Protocol Internet (HTTP)-Websites erreichen kann. Dazu gehören:

- Interne Websites
- Microsoft SharePoint 2003, 2007 und 2010

- Microsoft Outlook Web Access 2003, 2007 und 2013
- Microsoft Outlook Web App 2010
- Domino Web Access (DWA) 8.5 und 8.5.1
- Citrix Metaframe Presentation Server 4.x
- Citrix XenApp Version 5 bis 6.5
- Citrix XenDesktop Version 5 bis 5.6 und 7.5
- VMware View 4

Eine Liste der unterstützten Software finden Sie unter [Unterstützte VPN-Plattformen der Cisco Serie ASA 5500](#).

## Voraussetzungen

### Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- SSL-fähiger Browser
- ASA mit Version 7.1 oder höher
- X.509-Zertifikat für den ASA-Domännennamen ausgestellt
- TCP-Port 443, der nicht entlang des Pfads vom Client zur ASA blockiert werden darf

Eine vollständige Liste der Anforderungen finden Sie in den [unterstützten VPN-Plattformen der Cisco Serie ASA 5500](#).

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ASA Version 9.4(1)
- Adaptive Security Device Manager (ASDM) Version 7.4(2)
- ASA 5515-X

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte begannen mit einer leeren (Standard-)Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Konfigurieren

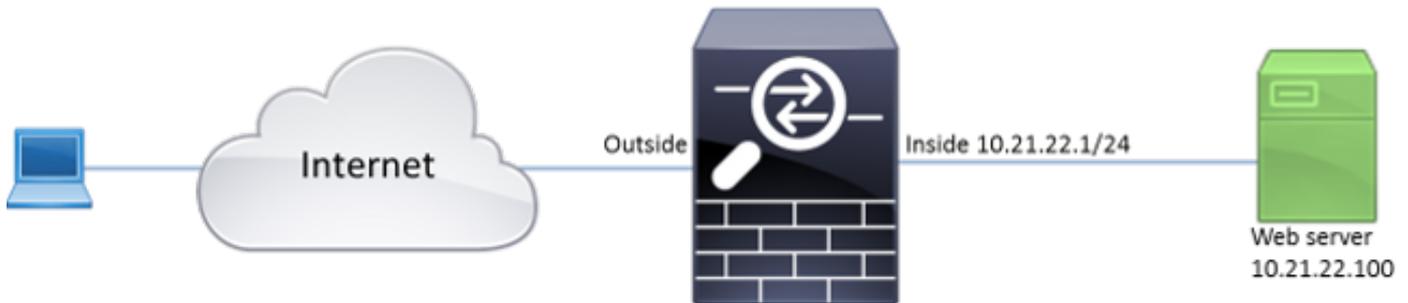
In diesem Artikel wird der Konfigurationsprozess für ASDM und CLI beschrieben. Sie können eines der Tools verwenden, um das WebVPN zu konfigurieren. Einige der Konfigurationsschritte können jedoch nur mit dem ASDM durchgeführt werden.

**Hinweis:** Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere

Informationen über die in diesem Abschnitt verwendeten Befehle zu erhalten.

## Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



## Hintergrundinformationen

WebVPN verwendet das SSL-Protokoll, um die zwischen Client und Server übertragenen Daten zu sichern. Wenn der Browser eine Verbindung zur ASA herstellt, legt die ASA das Zertifikat zur Authentifizierung vor. Um sicherzustellen, dass die Verbindung zwischen dem Client und der ASA sicher ist, müssen Sie der ASA das von der Zertifizierungsstelle signierte Zertifikat bereitstellen, dem der Client bereits vertraut. Andernfalls verfügt der Client nicht über die Mittel, um die Authentizität der ASA zu überprüfen, was zu einem möglichen Man-in-the-Middle-Angriff und einer schlechten Benutzererfahrung führt, da der Browser eine Warnung ausgibt, dass die Verbindung nicht vertrauenswürdig ist.

**Hinweis:** Standardmäßig generiert die ASA beim Start ein selbstsigniertes X.509-Zertifikat. Dieses Zertifikat wird standardmäßig verwendet, um Clientverbindungen bereitzustellen. Es wird nicht empfohlen, dieses Zertifikat zu verwenden, da seine Authentizität vom Browser nicht verifiziert werden kann. Außerdem wird dieses Zertifikat bei jedem Neustart neu generiert, sodass es nach jedem Neustart geändert wird.

Die Installation von Zertifikaten ist nicht Bestandteil dieses Dokuments.

## Konfiguration

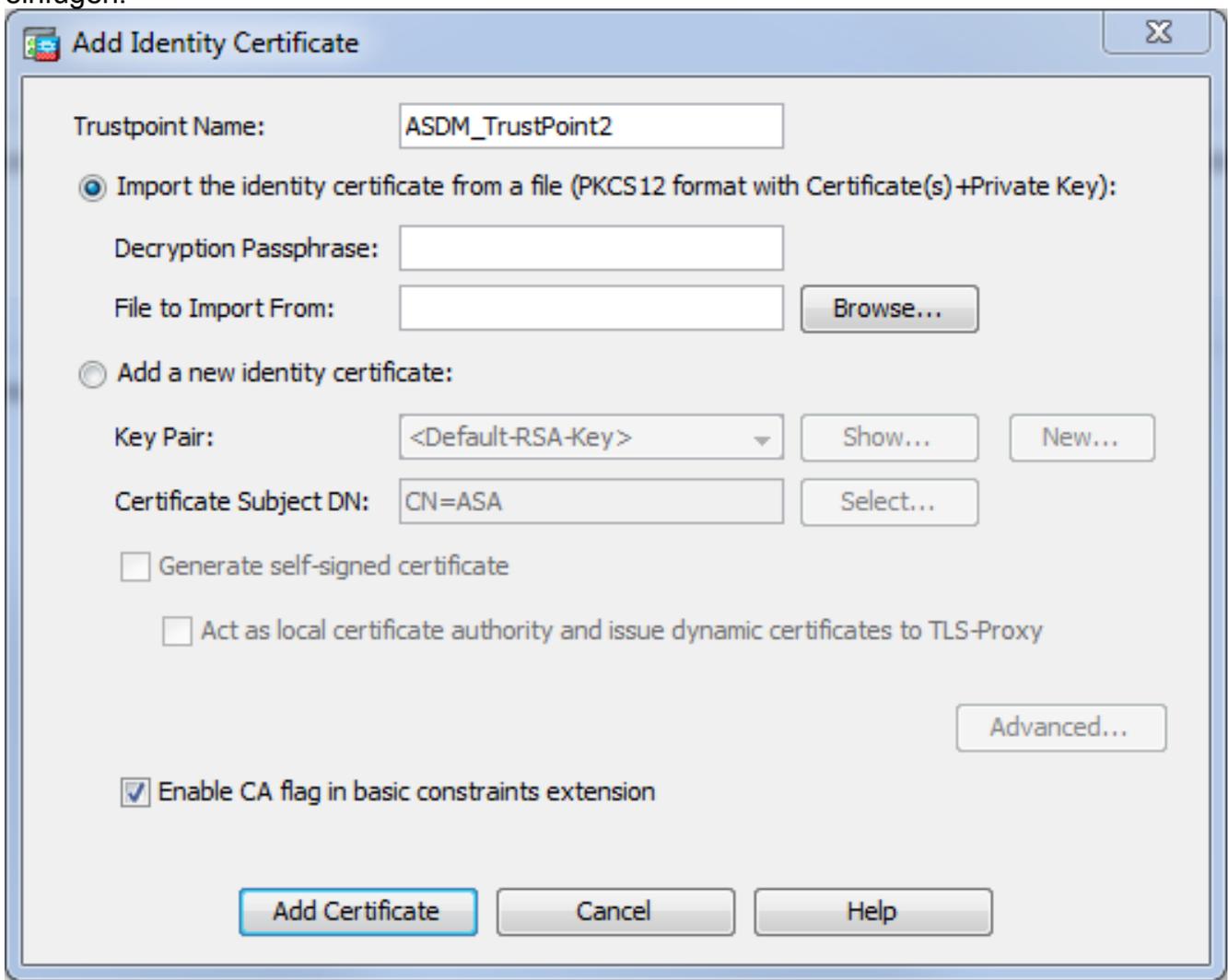
Konfigurieren Sie das WebVPN auf der ASA mit fünf Hauptschritten:

- Konfigurieren Sie das Zertifikat, das von der ASA verwendet wird.
- Aktivieren Sie das WebVPN auf einer ASA-Schnittstelle.
- Erstellen Sie eine Liste von Servern und/oder Uniform Resource Locator (URL) für den WebVPN-Zugriff.
- Erstellen Sie eine Gruppenrichtlinie für WebVPN-Benutzer.
- Wenden Sie die neue Gruppenrichtlinie auf eine Tunnelgruppe an.

**Hinweis:** In ASA-Versionen nach Version 9.4 wurde der Algorithmus zur Auswahl von SSL-

Verschlüsselungen geändert (siehe [Versionshinweise für die Cisco ASA-Serie, 9.4\(x\)](#)). Wenn nur elliptische, kurvenfähige Clients verwendet werden, ist es sicher, einen elliptischen Kurve-privaten Schlüssel für das Zertifikat zu verwenden. Andernfalls sollte die benutzerdefinierte Verschlüsselungssuite verwendet werden, um zu verhindern, dass die ASA ein selbst signiertes temporäres Zertifikat vorlegt. Sie können die ASA so konfigurieren, dass nur RSA-basierte Chiffren mit dem **SSL-Chip tlsv1.2 verwendet werden, der benutzerdefinierten "AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3 SHA:DES-CBC-SHA:RC4-SHA:RC4-MD5"**-Befehl.

1. **Option 1** - Importieren Sie das Zertifikat mit der Datei pkcs12. Wählen Sie **Configuration > Firewall > Advanced > Certificate Management > Identity Certificates > Add** aus. Sie können es mit der Datei pkcs12 installieren oder den Inhalt im Format Privacy Enhanced Mail (PEM) einfügen.



CLI:

```
ASA(config)# crypto ca import TrustPoint-name pkcs12 "password"
```

```
Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
MIIJUQIBAzCCCRcGCSqGSIB3DQEHAaCCCQgEggkEMIIJADCCBf8GCSqGSIB3DQEH
BqCCBfAwggXsAgEAMIIF5QYJKoZIhvcNAQcBMBwGCiqGSIB3DQEMAQYwDgQI8F3N
+vkvjUgCAggAgIIFuHFrv6enVflNv3sBBYB/yZswhELY5KpeALbXhfrFDpLNncAB
z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQpaBt8x30zo0JJxSAafmTWqDOEOS/
7mHsaKMoao+pv2LqKTWh007No4Ycx75Y5s0hyuQGPhLJRdionbils1ioe4Dplx1b
quit
```

--- output omitted ---

Enter the base 64 encoded pkcs12.

End with the word "quit" on a line by itself:

```
MIIJUQIBAzCCCRcGCSqGSIB3DQEHAAcCCQgEggkEMIIJADCCBf8GCSqGSIB3DQEH  
BqCCBfAwggXsAgEAMIIF5QYJKoZIhvcNAQcBMBwGCiqGSIB3DQEMAQYwDgQI8F3N  
+vkvjUgCAggAgIIFuHFrv6enVflNv3sBByB/yZswHEL5KpeALbXhfrFDpLNncAB  
z3xMfg6JkLYR6Fag1KjShg+o4qkDh8r9y9GQpaBt8x3Ozo0JJxSAafmTWqDOEOS/  
7mHsaKMoao+pv2LqKTWh007No4Ycx75Y5s0hyuQGPhLJRdionbi1slio4Dplx1b
```

quit

INFO: Import PKCS12 operation completed successfully

**Option 2** - Erstellen Sie ein selbstsigniertes Zertifikat. Wählen Sie **Configuration > Firewall > Advanced > Certificate Management > Identity Certificates > Add** aus. Klicken Sie auf das Optionsfeld **Neues Identitätszertifikat hinzufügen**. Aktivieren Sie das **Kontrollkästchen Eigensigniertes Zertifikat generieren**. Wählen Sie einen Common Name (CN) aus, der dem Domännennamen der ASA entspricht.

Trustpoint Name: ASDM\_TrustPoint1

Import the identity certificate from a file (PKCS12 format with Certificate(s) +Private Key):

Decryption Passphrase:

File to Import From:  Browse...

Add a new identity certificate:

Key Pair: <Default-RSA-Key> Show... New...

Certificate Subject DN: CN=ASA Select...

Generate self-signed certificate

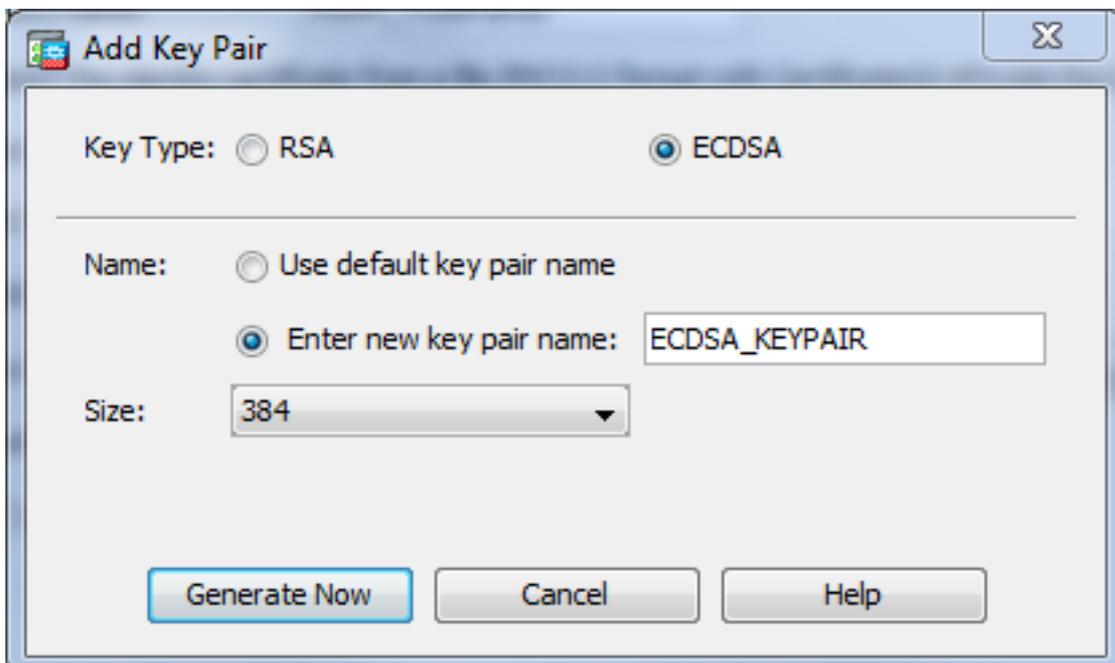
Act as local certificate authority and issue dynamic certificates to TLS-Proxy

Advanced...

Enable CA flag in basic constraints extension

Add Certificate Cancel Help

Klicken Sie auf **Neu**, um die Tastatur für das Zertifikat zu erstellen. Wählen Sie den Schlüsseltyp, den Namen und die Größe

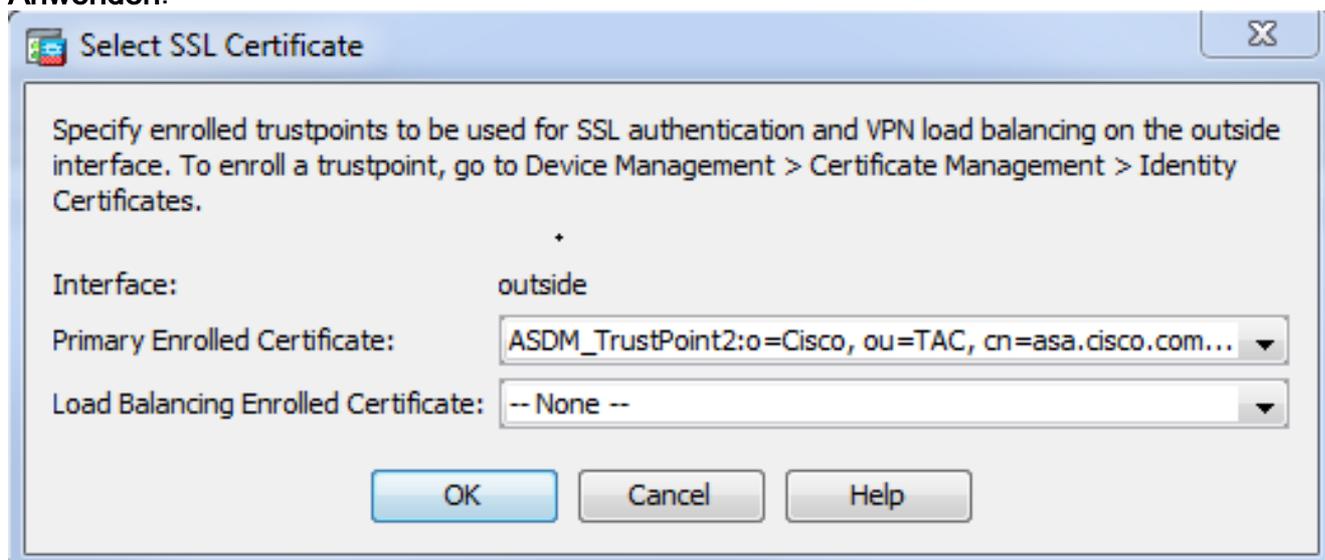


aus. CLI:

```
ASA(config)# crypto key generate ecdsa label ECDSA_KEYPAIR noconfirm
```

```
ASA(config)# crypto ca trustpoint TrustPoint1
ASA(config-ca-trustpoint)# revocation-check none
ASA(config-ca-trustpoint)# id-usage ssl-ipsec
ASA(config-ca-trustpoint)# no fqdn
ASA(config-ca-trustpoint)# subject-name CN=ASA
ASA(config-ca-trustpoint)# enrollment self
ASA(config-ca-trustpoint)# keypair ECDSA_KEYPAIR
ASA(config-ca-trustpoint)# exit
ASA(config)# crypto ca enroll TrustPoint1 noconfirm
```

2. Wählen Sie das Zertifikat aus, das für die Bereitstellung von WebVPN-Verbindungen verwendet wird. Wählen Sie **Configuration > Remote Access VPN > Advanced > SSL Settings** aus. Wählen Sie im Menü Certificates (Zertifikate) den Vertrauenspunkt aus, der dem gewünschten Zertifikat für die externe Schnittstelle zugeordnet ist. Klicken Sie auf **Anwenden**.



Entsprechende CLI-Konfiguration:

```
ASA(config)# ssl trust-point
```

3. (Optional) Aktivieren Sie DNS-Lookups (Domain Name Server). Der WebVPN-Server fungiert als Proxy für Clientverbindungen. Dies bedeutet, dass die ASA Verbindungen zu den Ressourcen im Namen des Clients erstellt. Wenn die Clients Verbindungen zu den Ressourcen benötigen, die Domännennamen verwenden, muss die ASA die DNS-Suche durchführen. Wählen Sie **Configuration > Remote Access VPN > DNS aus**. Konfigurieren Sie mindestens einen DNS-Server, und aktivieren Sie DNS-Lookups auf der Schnittstelle zum DNS-

**Configuration > Remote Access VPN > DNS**

Specify how to resolve DNS requests.

DNS Setup

**Configure one DNS server group**  Configure multiple DNS server groups

Primary DNS Server:

Secondary Servers:

Domain Name:

Server.

DNS Lookup

To configure DNS, enable DNS lookup on at least one interface.

Interface	DNS Enabled
inside	True
outside	False

DNS Guard

This function enforces one DNS response per query. If DNS inspection is configured, this option is ignored on that interface.

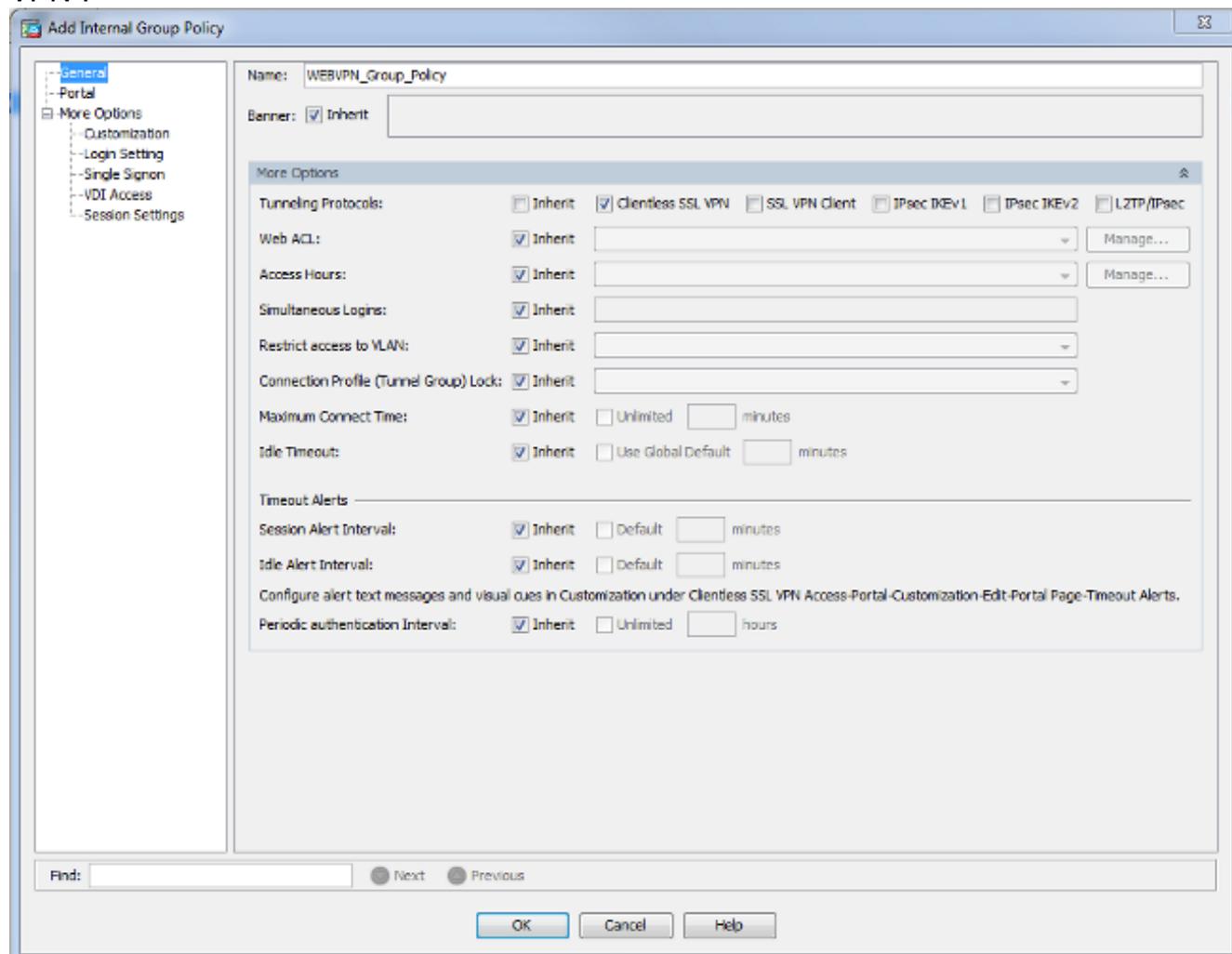
Enable DNS Guard on all interfaces.

CLI:

```
ASA(config)# dns domain-lookup inside
ASA(config)# dns server-group DefaultDNS
ASA(config-dns-server-group)# name-server 10.11.12.101
```

4. (Optional) Erstellen Sie Gruppenrichtlinien für WEBVPN-Verbindungen. Wählen Sie **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Add Internal Group Policy (Konfiguration > Remote-Access-VPN > Clientless-SSL-VPN-Zugriff > Gruppenrichtlinien > Interne Gruppenrichtlinie hinzufügen aus**. Unter Allgemeine Optionen

ändern Sie den Wert für das Abstimmungsprotokoll in "Clientless SSL VPN".



CLI:

```
ASA(config)# group-policy WEBVPN_Group_Policy internal
ASA(config)# group-policy WEBVPN_Group_Policy attributes
ASA(config-group-policy)# vpn-tunnel-protocol ssl-clientless
```

5. Konfigurieren Sie das Verbindungsprofil. Wählen Sie im ASDM **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles** aus.

Eine Übersicht über die Verbindungsprofile und die Gruppenrichtlinien finden Sie im [Konfigurationshandbuch zur VPN-CLI der Cisco ASA-Serie, 9.4 - Verbindungsprofile, Gruppenrichtlinien und Benutzer](#). Standardmäßig verwenden die WebVPN-Verbindungen das DefaultWEBVPNGroup-Profil. Sie können zusätzliche Profile erstellen. **Hinweis:** Es gibt verschiedene Möglichkeiten, Benutzer anderen Profilen zuzuweisen.

- Benutzer können das Verbindungsprofil manuell aus der Dropdown-Liste oder mit einer bestimmten URL auswählen. Siehe [ASA 8.x: Ermöglicht Benutzern die Auswahl einer Gruppe bei WebVPN-Anmeldung über Gruppen-Alias und Gruppen-URL-Methode](#).

- Wenn Sie einen LDAP-Server verwenden, können Sie das Benutzerprofil basierend auf den vom LDAP-Server erhaltenen Attributen zuweisen. Siehe [Konfigurationsbeispiel ASA-Verwendung von LDAP-Attributzuordnungen](#).

- Wenn Sie die zertifikatbasierte Authentifizierung der Clients verwenden, können Sie den Benutzer den Profilen zuordnen, die auf den im Zertifikat enthaltenen Feldern basieren.

Weitere Informationen finden Sie im [Cisco VPN CLI-Konfigurationshandbuch der ASA-Serie, 9.4 - Konfigurieren der Zertifikatsgruppenzuordnung für IKEv1](#).

- Informationen zum manuellen Zuweisen der Benutzer zur Gruppenrichtlinie finden Sie im [Konfigurationsleitfaden zur Cisco ASA VPN CLI der Serie 9.4 - Konfigurieren von Attributen für einzelne Benutzer](#). Bearbeiten Sie das DefaultWEBVPNGroup-Profil, und wählen Sie unter Default Group Policy (Standardgruppenrichtlinie) die Option WEBVPN\_Group\_Policy aus.

The screenshot shows the configuration window for the 'DefaultWEBVPNGroup' profile. The 'Authentication' section has 'Method' set to 'AAA' and 'AAA Server Group' set to 'LOCAL'. The 'DNS' section has 'Server Group' set to 'DefaultDNS', 'Servers' set to '10.21.22.101', and 'Domain Name' set to 'cisco.com'. The 'Default Group Policy' section has 'Group Policy' set to 'WEBVPN\_Group\_Policy' and the 'Enable clientless SSL VPN protocol' checkbox checked.

CLI:

```
ASA(config)# tunnel-group DefaultWEBVPNGroup general-attributes
ASA(config-tunnel-general)# default-group-policy WEBVPN_Group_Policy
```

- Um das WebVPN auf der externen Schnittstelle zu aktivieren, wählen Sie **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**. Aktivieren Sie das Kontrollkästchen **Zugriff zulassen** neben der externen Schnittstelle.

Access Interfaces

Enable interfaces for clientless SSL VPN access.

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

Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Device Certificate ...

Port Setting ...

CLI:

```
ASA(config)# webvpn
```

```
ASA(config-webvpn)# enable outside
```

7. (Optional) Erstellen Sie Lesezeichen für den Inhalt. Lesezeichen ermöglichen dem Benutzer das einfache Durchsuchen der internen Ressourcen, ohne sich die URLs merken zu müssen. Um ein Lesezeichen zu erstellen, wählen Sie **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks > Add**.

Add Bookmark List

Bookmark List Name:

Bookmark Title	URL
----------------	-----

Add

Edit

Delete

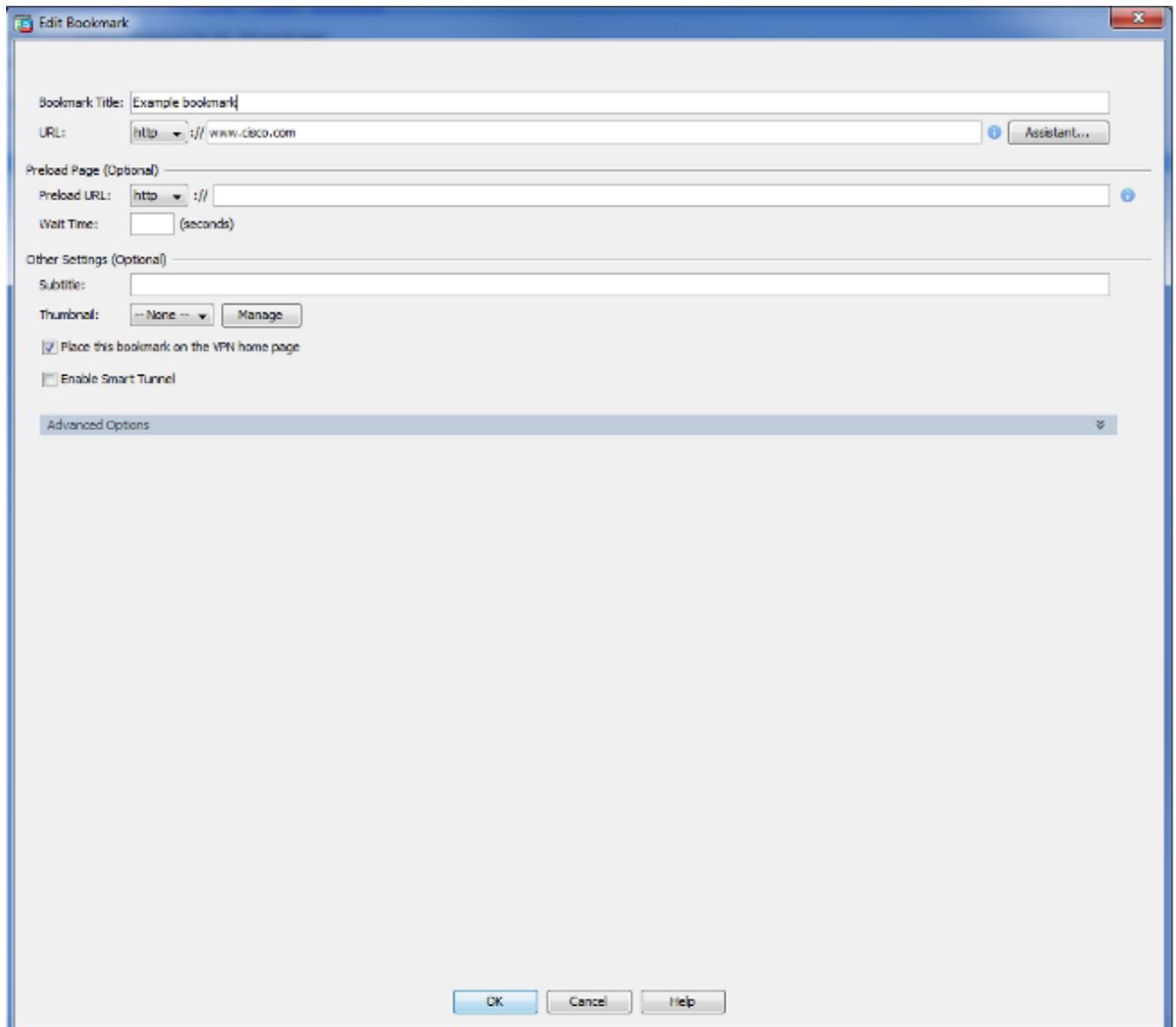
Move Up

Move Down

Find:     Match Case

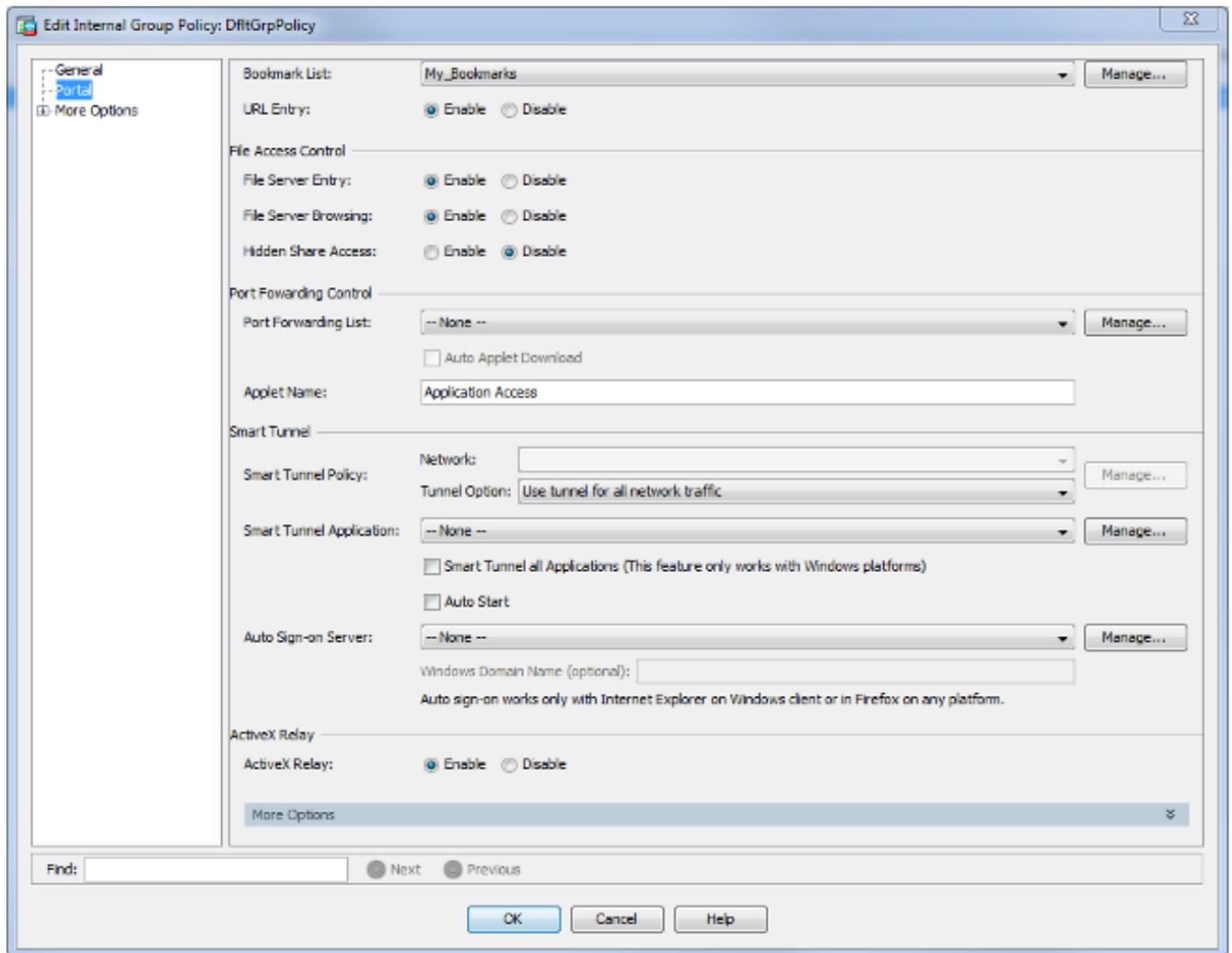
OK Cancel Help

Wählen Sie **Hinzufügen**, um ein bestimmtes Lesezeichen hinzuzufügen.



CLI:Lesezeichen können über die CLI nicht erstellt werden, da sie als XML-Dateien erstellt werden.

8. (Optional) Weisen Sie Lesezeichen einer bestimmten Gruppenrichtlinie zu. Wählen Sie **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies > Edit > Portal > Bookmark List** aus.

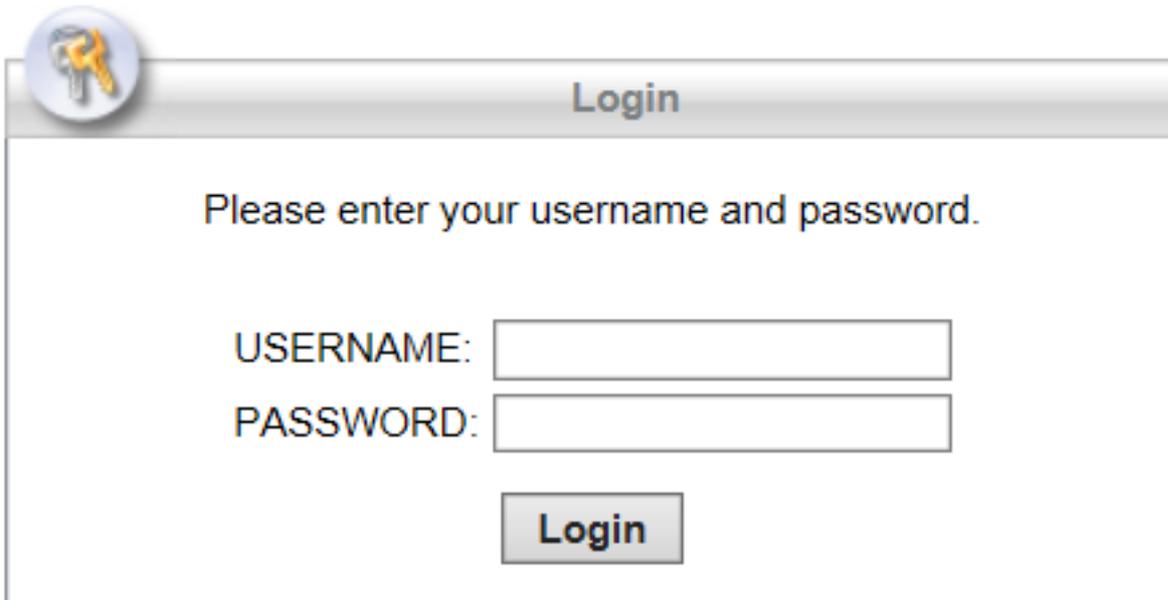


CLI:

```
ASA(config)# group-policy DfltGrpPolicy attributes  
ASA(config-group-policy)# webvpn  
ASA(config-group-webvpn)# url-list value My_Bookmarks
```

## Überprüfen

Nach der Konfiguration des WebVPN verwenden Sie die Adresse `https://<FQDN der ASA>` im Browser.



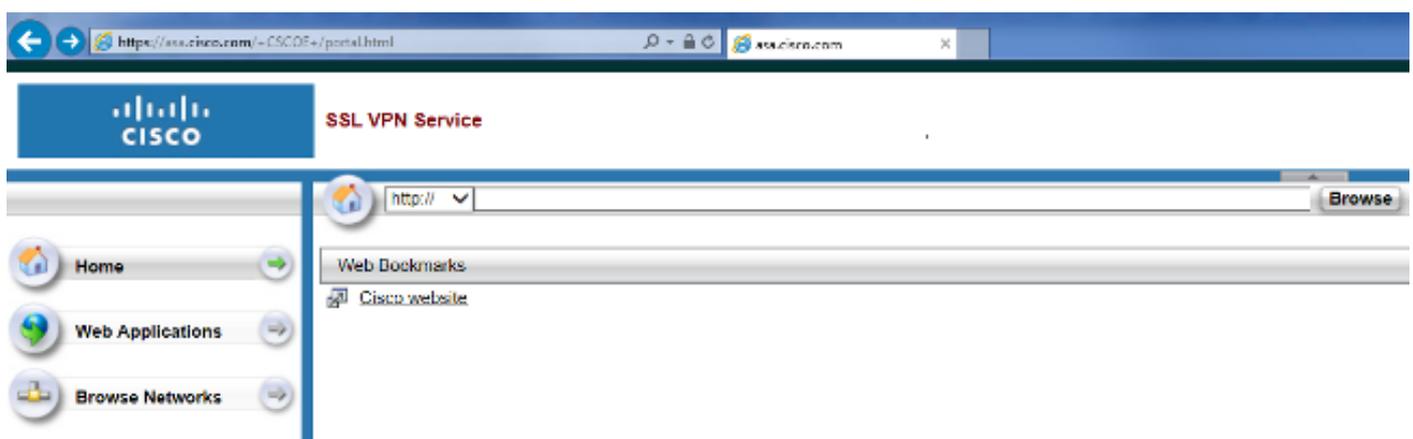
**Login**

Please enter your username and password.

USERNAME:

PASSWORD:

Nach der Anmeldung sollten Sie die Adressleiste sehen können, die zum Navigieren zu Websites und Lesezeichen verwendet wird.



## Fehlerbehebung

### Verfahren zur Fehlerbehebung

Befolgen Sie diese Anweisungen, um eine Fehlerbehebung für Ihre Konfiguration durchzuführen.

Wählen Sie im ASDM **Monitoring > Logging > Real-time Log Viewer > View (Überwachung > Protokollierung > Protokollanzeige in Echtzeit)** aus. Wenn ein Client eine Verbindung zur ASA herstellt, notieren Sie die Einrichtung einer TLS-Sitzung, die Auswahl der Gruppenrichtlinie und die erfolgreiche Authentifizierung des Benutzers.

```

Device completed SSL handshake with client outside:10.229.20.77/61307 to 10.48.66.179/443 for TLSv1.2 session
Device completed SSL handshake with client outside:10.229.20.77/61306 to 10.48.66.179/443 for TLSv1.2 session
SSL client outside:10.229.20.77/61307 to 10.48.66.179/443 request to resume previous session
Starting SSL handshake with client outside:10.229.20.77/61307 to 10.48.66.179/443 for TLS session
SSL client outside:10.229.20.77/61306 to 10.48.66.179/443 request to resume previous session
Starting SSL handshake with client outside:10.229.20.77/61306 to 10.48.66.179/443 for TLS session
Built inbound TCP connection 107 for outside:10.229.20.77/61307 (10.229.20.77/61307) to identity:10.48.66.179/443 (10.48.66.179/443)
Built inbound TCP connection 106 for outside:10.229.20.77/61306 (10.229.20.77/61306) to identity:10.48.66.179/443 (10.48.66.179/443)
Group <WEBVPN_Group_Policy> User <admin> IP <10.229.20.77> Authentication: successful, Session Type: WebVPN.
Device selects trust-point ASA-self-signed for client outside:10.229.20.77/53047 to 10.48.66.179/443
Group <WEBVPN_Group_Policy> User <admin> IP <10.229.20.77> WebVPN session started.
DAP: User admin, Addr 10.229.20.77, Connection Clientless: The following DAP records were selected for this connection: DfltAccessPolicy
AAA transaction status ACCEPT : user = admin
AAA retrieved default group policy (WEBVPN_Group_Policy) for user = admin
AAA user authentication Successful : local database : user = admin
Device completed SSL handshake with client outside:10.229.20.77/61304 to 10.48.66.179/443 for TLSv1.2 session
Device completed SSL handshake with client outside:10.229.20.77/61303 to 10.48.66.179/443 for TLSv1.2 session

```

CLI:

```

ASA(config)# logging buffered debugging
ASA(config)# show logging

```

Wählen Sie im ASDM **Monitoring > VPN > VPN Statistics > Sessions > Filter by: Clientless-SSL-VPN** Suchen Sie nach der neuen WebVPN-Sitzung. Wählen Sie den WebVPN-Filter aus, und klicken Sie auf **Filter**. Wenn ein Problem auftritt, umgehen Sie vorübergehend das ASA-Gerät, um sicherzustellen, dass die Clients auf die gewünschten Netzwerkressourcen zugreifen können. Überprüfen Sie die in diesem Dokument aufgeführten Konfigurationsschritte.

Username IP Address	Group Policy Connection Profile	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx	Cer Auth Int	Cer Auth Left
admin 10.229.20.77	WEBVPN_Group_Policy DefaultWEBVPNGroup	Clientless Clientless: (1)AES128	10:40:04 UTC Tue May 26 2015 0h:02m:50s	63991 166375		

CLI:

```

ASA(config)# show vpn-sessiondb webvpn

Session Type: WebVPN

Username : admin Index : 3
Public IP : 10.229.20.77
Protocol : Clientless
License : AnyConnect Premium
Encryption : Clientless: (1)AES128 Hashing : Clientless: (1)SHA256
Bytes Tx : 72214 Bytes Rx : 270241
Group Policy : WEBVPN_Group_Policy Tunnel Group : DefaultWEBVPNGroup
Login Time : 10:40:04 UTC Tue May 26 2015
Duration : 0h:05m:21s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a1516010000300055644d84
Security Grp : none

```

## Befehle zur Fehlerbehebung

Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des Befehls show anzuzeigen**.

**Hinweis:** Weitere Informationen [zu Debug-Befehlen](#) vor der Verwendung von **Debug**-Befehlen finden Sie unter [Wichtige Informationen](#).

- **show webvpn** - Mit WebVPN sind viele **show**-Befehle verknüpft. Weitere Informationen zur Verwendung der **show**-Befehle finden Sie im [Befehlsreferenz](#)-Abschnitt der Cisco Security Appliance.
- **debug webvpn**: Die Verwendung von **Debug**-Befehlen kann sich negativ auf die ASA auswirken. Weitere Informationen zur Verwendung von **Debug**-Befehlen finden Sie im [Befehlsreferenz](#)-Abschnitt der Cisco Security Appliance.

## Häufige Probleme

### Benutzer kann sich nicht anmelden

#### Problem

Die Meldung "Clientless (Browser) SSL VPN-Zugriff ist nicht zulässig." nach einem fehlgeschlagenen Anmeldeversuch im Browser angezeigt. Die AnyConnect Premium-Lizenz ist nicht auf der ASA installiert oder wird nicht verwendet, wie in "Premium AnyConnect-Lizenz ist auf der ASA nicht aktiviert" dargestellt.

#### Lösung

Aktivieren Sie die Premium AnyConnect-Lizenz mit folgenden Befehlen:

```
ASA(config)# webvpn
ASA(config-webvpn)# no anyconnect-essentials
```

#### Problem

Nach einem fehlgeschlagenen Anmeldeversuch wird im Browser die Meldung "Anmeldung fehlgeschlagen" angezeigt. Der Grenzwert für die AnyConnect-Lizenz wurde überschritten.

#### Lösung

Suchen Sie diese Meldung in den Protokollen:

```
%ASA-4-716023: Group <DfltGrpPolicy> User <cisco> IP <192.168.1.100>
Session could not be established: session limit of 2 reached.
```

Überprüfen Sie außerdem Ihre Lizenzgrenze:

```
ASA(config)# show version | include Premium
AnyConnect Premium Peers : 2 perpetual
```

#### Problem

Nach einem fehlgeschlagenen Anmeldeversuch wird im Browser die Meldung "AnyConnect ist auf dem VPN-Server nicht aktiviert" angezeigt. Das clientlose VPN-Protokoll ist in der Gruppenrichtlinie nicht aktiviert.

## Lösung

Suchen Sie diese Meldung in den Protokollen:

```
%ASA-6-716002: Group <DfltGrpPolicy> User <cisco> IP <192.168.1.100>  
WebVPN session terminated: Client type not supported.
```

Stellen Sie sicher, dass das Clientless-VPN-Protokoll für die gewünschte Gruppenrichtlinie aktiviert ist:

```
ASA(config)# show run all group-policy | include vpn-tunnel-protocol  
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-clientless
```

## Verbindung von mehr als drei WebVPN-Benutzern mit der ASA nicht möglich

### Problem

Nur drei WebVPN-Clients können eine Verbindung zur ASA herstellen. Die Verbindung für den vierten Client schlägt fehl.

### Lösung

In den meisten Fällen bezieht sich dieses Problem auf eine gleichzeitige Anmeldeeinstellung innerhalb der Gruppenrichtlinie. Verwenden Sie diese Abbildung, um die gewünschte Anzahl gleichzeitiger Anmeldungen zu konfigurieren. In diesem Beispiel ist der gewünschte Wert 20.

```
ASA(config)# group-policy Cisco attributes  
ASA(config-group-policy)# vpn-simultaneous-logins 20
```

## WebVPN-Clients können Lesezeichen nicht schlagen, und sie sind ausgegraut.

### Problem

Wenn diese Lesezeichen für Benutzer konfiguriert wurden, sich beim clientlosen VPN anzumelden, sie jedoch im Hauptbildschirm unter "Web Applications" (Webanwendungen) als ausgegraut angezeigt werden, wie kann ich diese HTTP-Links aktivieren, sodass die Benutzer auf sie klicken und auf die jeweilige URL zugreifen können?

### Lösung

Sie sollten zuerst sicherstellen, dass die ASA die Websites über DNS auflösen kann. Versuchen Sie, die Websites mit dem Namen zu pingen. Wenn der Name von der ASA nicht aufgelöst werden kann, ist der Link deaktiviert. Wenn die DNS-Server in Ihrem Netzwerk intern sind, konfigurieren Sie die private Schnittstelle für die DNS-Domänensuche.

## Citrix-Verbindung über WebVPN

## Problem

Die Fehlermeldung "Der ica-Client hat eine beschädigte ICA-Datei erhalten." tritt bei Citrix über WebVPN auf.

## Lösung

Wenn Sie den *sicheren Gateway*-Modus für Citrix-Verbindungen über WebVPN verwenden, kann die ICA-Datei beschädigt werden. Da die ASA nicht mit diesem Betriebsmodus kompatibel ist, erstellen Sie im Direktmodus (ungesicherter Modus) eine neue ICA-Datei.

## Vermeidung einer zweiten Authentifizierung für Benutzer

### Problem

Wenn Sie auf CIFS-Links im clientlosen WebVPN-Portal zugreifen, werden Sie nach dem Klicken auf das Lesezeichen zur Eingabe von Anmeldeinformationen aufgefordert. Das Lightweight Directory Access Protocol (LDAP) dient zur Authentifizierung der Ressourcen und der Benutzer, die bereits LDAP-Anmeldeinformationen eingegeben haben, um sich bei der VPN-Sitzung anzumelden.

### Lösung

In diesem Fall können Sie die Funktion für die automatische Anmeldung verwenden. Konfigurieren Sie unter der verwendeten Gruppenrichtlinie und unter den zugehörigen WebVPN-Attributen Folgendes:

```
ASA(config)# group-policy WEBVPN_Group_Policy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# auto-signon allow uri cifs://X.X.X.X/* auth-type all
```

wobei X.X.X.X=IP des CIFS-Servers und \*=restlicher Pfad, um die betreffende Freigabedatei/den betreffenden Ordner zu erreichen.

Ein Beispiel für einen Konfigurationsausschnitt wird hier angezeigt:

```
ASA(config)# group-policy ExamplePolicy attributes
ASA(config-group-policy)# webvpn
ASA(config-group-webvpn)# auto-signon allow uri
https://*.example.com/* auth-type all
```

Weitere Informationen hierzu finden Sie unter [Konfigurieren von SSO mit HTTP Basic- oder NTLM-Authentifizierung](#).

## Zugehörige Informationen

- [ASA: Smart Tunnel mit ASDM-Konfigurationsbeispiel](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)