APPENDIX A

VPN XML Reference

Use this appendix only if you are not upgrading ASDM to 6.3(1) or later. AnyConnect 2.5 supports a profile editor that you can access to configure AnyConnect features. However, you can access it only with ASDM 6.3(1) or later. Earlier AnyConnect versions provided a standalone profile editor that you could install on Windows, but it was undocumented and unsupported and is no longer available as a standalone editor. We strongly recommend upgrading to ASDM because it is much easier to create, edit, and manage profiles directly with the AnyConnect profile editor than it is edit them with a conventional editor. The new profile editor is documented and supports and comes with its own online help. The minimum ASA software release supported by ASDM 6.3(1) with AnyConnect 2.5 is ASA 8.0(2). However, we recommend upgrading to ASA 8.3(1) or later to take full advantage of the new client features.

Read *Chapter 3, Configuring AnyConnect Client Features* for familiarity with the AnyConnect profile and features. This appendix provides an alternative to this chapter.

The following sections briefly describe each client feature and provide XML tag names, options, descriptions, and example code. AnyConnect uses the default value if the profile does not specify one. Consider case when entering all profile tags and the specific options within each value. You must match the upper or lowercase values presented in this chapter to avoid error conditions.

Note Do not cut and paste the examples from this document. Doing so introduces line breaks that can break your XML. Instead, open the profile template file in a text editor such as Notepad or Wordpad.

XML tags and values are case-sensitive. Using the wrong case can cause configurations to fail, for example, using IPSec instead of the correct IPsec.

- Local Proxy Connections, page A-2
- Optimal Gateway Selection (OGS), page A-2
- Trusted Network Detection, page A-3
- Always-on VPN and Subordinate Features, page A-4
- Always-on VPN With Load Balancing, page A-6
- AnyConnect Local Policy File Parameters and Values, page A-7
- Certificate Store on Windows, page A-10
- Restricting Certificate Store Use, page A-10
- SCEP Protocol to Provision and Renew Certificates, page A-10
- Automatic Certificate Selection, page A-17

- Backup Server List Parameters, page A-17
- Windows Mobile Policy, page A-17
- Server List, page A-20
- Scripting, page A-22
- Authentication Timeout Control, page A-23
- Allow AnyConnect Session from an RDP Session for Windows Users, page A-23
- AnyConnect over L2TP or PPTP, page A-25
- Other AnyConnect Profile Settings, page A-26

Local Proxy Connections

Table A-1 shows the tag name, options, and descriptions to configure support for local proxy connections.

Table A-1 Local Proxy Connection Settings

XML Tag Name	Options	Description
AllowLocalProxyConnections	true (default)	Enables local proxy connections.
	false	Disables local proxy connections.

Example:Disable Local Proxy Connections

Refer to the following example to disable AnyConnect support for local proxy connections:

```
<ClientInitialization>
<AllowLocalProxyConnections>false</AllowLocalProxyConnections>
</ClientInitialization>
```

Optimal Gateway Selection (OGS)

Table A-2 shows the tag names, options, and descriptions to configure OGS.

Table A-2 OGS Settings

XML Tag Name	Options	Description
EnableAutomaticServerSelection	true	Enables OGS by default.
	false	Disables OGS by default.
EnableAutomaticServerSelection UserControllable	true	Allows the user to enable or disable OGS in client preferences.*
	false	Reverts to the default where automatic server selection is not user-controllable.

Table A-2 OGS Settings

XML Tag Name	Options	Description
AutoServerSelectionImprovement	Integer. The default is 20 percent.	Percentage of performance improvement to trigger the client to connect to another secure gateway.
AutoServerSelectionSuspendTime	Integer. The default is 4 hours.	Specifies the elapsed time (in hours) since disconnecting from the current secure gateway and reconnecting to another secure gateway.

* When OGS is enabled, we recommend that you also make the feature user-controllable.

Example:OGS

Refer to the following example to configure OGS:

```
<ClientInitialization>
    <EnableAutomaticServerSelection UserControllable="true">
     true
         <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
         <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
     </EnableAutomaticServerSelection>
</ClientInitialization>
```

Trusted Network Detection

Table A-3 shows the tag names, options, and descriptions to configure trusted network detection.

Table A-3 Trusted Network Detection Settings

XML Tag Name	Options	Description
AutomaticVPNPolicy	true	Enables TND. Automatically manages when a VPN connection should be started or stopped according to the *TrustedNetworkPolicy* and *UntrustedNetworkPolicy* parameters.
	false	Disables TND. VPN connections can only be started and stopped manually.
TrustedNetworkPolicy	Disconnect	Disconnects the VPN connection in the trusted network.
	Connect	Initiates a VPN connection (if none exists) in the trusted network.
	DoNothing	Takes no action in a trusted network.
	Pause	Suspends the VPN session instead of disconnecting it if a user enters a network configured as trusted after establishing a VPN session outside the trusted network. When the user goes outside the trusted network again, AnyConnect resumes the session. This feature is for the user’s convenience because it eliminates the need to establish a new VPN session after leaving a trusted network.
UntrustedNetworkPolicy	Connect	Initiates a VPN connection upon the detection of an untrusted network.
	DoNothing	Initiates a VPN connection upon the detection of an untrusted network. This option is incompatible with always-on VPN. Setting both the Trusted Network Policy and Untrusted Network Policy to Do Nothing disables Trusted Network Detection.

Table A-3 Trusted Network Detection Settings (continued)

XML Tag Name	Options	Description
TrustedDNSDomains	String	A list of DNS suffixes (a string separated by commas) that a network interface may have when the client is in the trusted network. The following is an example of a TrustedDNSDomain string: *.cisco.com Wildcards (*) are supported for DNS suffixes.
TrustedDNSServers	String	A list of DNS server addresses (a string separated by commas) that a network interface may have when the client is in the trusted network. The following is an example of a TrustedDNSServers string: 161.44.124.*,64.102.6.247 Wildcards (*) are supported for DNS server addresses.

Example:Trusted Network Detection

Refer to the following example to configure trusted network detection. In the example, the client is configured to automatically disconnect the VPN connection when in the trusted network and to initiate the VPN connection in the untrusted network:

```
<AutomaticVPNPolicy>true
    <TrustedDNSDomains>*.cisco.com</TrustedDNSDomains>
    <TrustedDNSServers>161.44.124.*,64.102.6.247</TrustedDNSServers>
    <TrustedNetworkPolicy>Disconnect</TrustedNetworkPolicy>
    <UntrustedNetworkPolicy>Connect</UntrustedNetworkPolicy>
</AutomaticVPNPolicy>
```

Always-on VPN and Subordinate Features

If you choose always-on VPN, the fail-open policy permits network connectivity, and the fail-close policy disables network connectivity.

Table A-4 shows the tag names, options, and descriptions to configure always-on VPN.

Table A-4 Always-on VPN Settings

XML Tag Name	Options	Description
AutomaticVPNPolicy	true	Enables automatic VPN policy.
	false	Disables automatic VPN policy.
TrustedDNSDomains	string	Specifies possible DNS suffixes that a network interface may have when in a trusted network.
TrustedDNSServers	string	Specifies DNS server addresses that a network interface may have when the client is in a trusted network.
TrustedNetworkPolicy	disconnect	Disconnects from the VPN upon detection of a trusted network.
	connect	Connects to the VPN upon detection of a trusted network.
	donothing	Do not connect to the VPN or disconnect from the VPN upon detection of a trusted network.

Table A-4 Always-on VPN Settings (continued)

XML Tag Name	Options	Description
UntrustedNetworkPolicy	connect	Disconnects from the VPN upon detection of an untrusted network.
	disconnect	Connects to the VPN upon detection of an untrusted network.
	donothing	Do not connect to the VPN or disconnect from the VPN upon detection of an untrusted network.
AlwaysOn	true	Enables always-on VPN.
	false	Disables always-on VPN.
ConnectFailurePolicy	open	Does not restrict network access when AnyConnect cannot establish a VPN session (for example, when an adaptive security appliance is unreachable).
	closed	Restricts network access when the VPN is unreachable. The restricted state permits access only to secure gateways to which the computer is allowed to connect.
AllowCaptivePortalRemediation	true	Relaxes the network restrictions imposed by a closed connect failure policy for the number of minutes specified by the CaptivePortalRemediationTimeout tag so that the user can remediate a captive portal.
	false	Enforces the network restrictions imposed by a closed connect failure policy even if AnyConnect detects a captive portal.
CaptivePortalRemediationTimeout	Integer	The number of minutes AnyConnect lifts the network access restrictions.
ApplyLastVPNLocalResourceRules	true	Applies the last client firewall it received from the security appliance, which may include ACLs allowing access to resources on the local LAN.
	false	Does not apply the last client firewall received from the security appliance.
AllowVPNDisconnect	true	Displays a Disconnect button to provide users with the option to disconnect an always-on VPN session. Users might want to do so to select an alternative secure gateway before reconnecting.
	false	Does not display a Disconnect button. This option prevents the use of the AnyConnect GUI to disconnect from the VPN.

⚠

Caution A connect failure closed policy prevents network access if AnyConnect fails to establish a VPN session. It is primarily for exceptionally secure organizations where security persistence is a greater concern than always-available network access. It prevents all network access except for local resources such as printers and tethered devices permitted by split tunneling and limited by ACLs. It can halt productivity if users require Internet access beyond the VPN if a secure gateway is unavailable. AnyConnect detects most captive portals (described in Captive Portal Hotspot Detection, page 3-29). If it cannot detect a captive portal, a connect failure closed policy prevents all network connectivity.

If you deploy a closed connection policy, we highly recommend that you follow a phased approach. For example, first deploy always-on VPN with a connect failure open policy and survey users for the frequency with which AnyConnect does not connect seamlessly. Then deploy a small pilot deployment of a connect failure closed policy among early-adopter users and solicit their feedback. Expand the pilot program gradually while continuing to solicit feedback before considering a full deployment. As you deploy a connect failure closed policy, be sure to educate the VPN users about the network access limitation as well as the advantages of a connect failure closed policy.

Always-On VPN—XML Example

If you are using a release of ASDM that is earlier than 6.3(1), use the following example to edit the AnyConnect XML profile manually. This always-on VPN example does the following:

- Enables the Disconnect button (AllowVPNDisconnect) to let users establish a VPN session with another secure gateway.
- Specifies the connect failure policy is closed.
- Relaxes network restrictions imposed by the connect failure policy for five minutes to remediate a captive portal.
- Applies the ACL rules assigned during the last VPN session.

```
<ClientInitialization>
    <AutomaticVPNPolicy>true
        <TrustedDNSDomains>example.com</TrustedDNSDomains>
        <TrustedDNSServers>1.1.1.1</TrustedDNSServers>
        <TrustedNetworkPolicy>Disconnect</TrustedNetworkPolicy>
        <UntrustedNetworkPolicy>Connect</UntrustedNetworkPolicy>
        <AlwaysOn>true
            <AllowVPNDisconnect>true</AllowVPNDisconnect>
            <ConnectFailurePolicy>Closed
                <AllowCaptivePortalRemediation>true
                    <CaptivePortalRemediationTimeout>5</CaptivePortalRemediationTimeout>
                </AllowCaptivePortalRemediation>
                <ApplyLastVPNLocalResourceRules>true</ApplyLastVPNLocalResourceRules>
            </ConnectFailurePolicy>
        </AlwaysOn>
    </AutomaticVPNPolicy>
</ClientInitialization>
```

Always-on VPN With Load Balancing

Table A-5 shows the tag names, options, and descriptions to configure always-on VPN with load balancing.

Table A-5 Using Always-on VPN With Load Balancing Settings

XML Tag Name	Options	Description
LoadBalancingServerList	FQDN or IP address	Specify the backup devices of the cluster. Without this option, AnyConnect blocks access to backup devices in the load balancing cluster if always-on VPN is enabled.

Example:Always-on VPN With Load Balancing

```
<ServerList>
        <!--
            This is the data needed to attempt a connection to a specific
            host.
          -->
 <HostEntry>
```

```
   <HostName>ASA</HostName>
   <HostAddress>10.86.95.249</HostAddress>
  <LoadBalancingServerList>
     <!--
    Can be a FQDN or IP address.
        -->
      <HostAddress>loadbalancing1.domain.com</HostAddress>
      <HostAddress>loadbalancing2.domain.com</HostAddress>
      <HostAddress>11.24.116.172</HostAddress>
</LoadBalancingServerList>
  </HostEntry>
</ServerList>
```

Start Before Logon

Table A-6 shows the tag names, options, and descriptions to configure start before logon.

Table A-6 Start Before Logon Settings

XML Tag Name	Options	Description
UseStartBeforeLogon	true	Enables start before logon.
	false	Disables start before logon.
UseStartBeforeLogon UserControllable	true	Makes SBL user controllable.
	false	Reverts to the default where SBL is not user-controllable.

Example:Start Before Logon

Refer to the following example to configure SBL:

```
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
```

AnyConnect Local Policy File Parameters and Values

Table A-7 shows the tag names, options, and descriptions to configure local policy.

Table A-7 AnyConnect Local Policy Settings

XML Tag Name	Options	Description
acversion="<version number>"		Specifies the minimum version of the AnyConnect client capable of interpreting all of the parameters in the file. If a client older than the version specified reads the file, it issues an event log warning.
xmlns=http://schemas.xmlsoap.org/encoding/	Most administrators do not change this parameter.	The XML namespace specifier.
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/AnyConnectLocalPolicy.xsd">	Most administrators do not change this parameter.	The XML specifier for the schema location.

Table A-7 AnyConnect Local Policy Settings (continued)

XML Tag Name	Options	Description
xmlns:xsi=http://www.w3.org/2001/ XMLSchema-instance	Most administrators do not change this parameter.	The XML schema instance specifier.
FipsMode	true	Enables FIPS mode for the client. The client uses only algorithms and protocols approved by the FIPS standard.
	false	Disables FIPS mode for the client.
BypassDownloader	true	The client does not check for any dynamic content present on the ASA, including profile updates, translations, customization, optional modules, and core software updates.
	false	The client checks for dynamic content present on the ASA (default).
RestrictWebLaunch	true	WebLaunch attempts fail, and the client displays an informative message to the user.
	false	Permits WebLaunch (default—behavior consistent with AnyConnect 2.3 and earlier).
StrictCertificateTrust	true	The client fails to connect to security gateways that use invalid, mismatched, or untrusted certificates that require user interaction.
	false	The client prompts the user to accept the certificate (default—behavior consistent with AnyConnect 2.3 and earlier).
RestrictPreferenceCaching	Credentials	The user name and second user name are not cached.
	Thumbprints	The client and server certificate thumbprints are not cached.
	CredentialsAndThumbprints	Certificate thumbprints and user names are not cached.
	All	No automatic preferences are cached.
	false	All preferences are written to disk (default—behavior consistent with AnyConnect 2.3 and earlier).

Table A-7 AnyConnect Local Policy Settings (continued)

XML Tag Name	Options	Description
RestrictTunnelProtocols (currently not supported)	TLS	The client only uses IKEv2 and ESP to establish the tunnel and will not use TLS/DTLS to communicate information to the secure gateway.
	IPSec	The client only uses TLS/DTLS for authentication and tunneling.
	false	Any encrypted protocol may be used in connection establishment (default).
ExcludeFirefoxNSSCertStore (Linux and Mac)	true	Excludes the Firefox NSS certificate store.
	false	Permits the Firefox NSS certificate store (default).
ExcludePemFileCertStore (Linux and Mac)	true	Excludes the PEM file certificate store.
	false	Permits the PEM file certificate store (default).
ExcludeMacNativeCertStore (Mac only)	true	Excludes the Mac native certificate store.
	false	Permits the Mac native certificate store (default).
ExcludeWinNativeCertStore (Windows only, currently not supported)	true	Excludes the Windows Internet Explorer certificate store.
	false	Permits the Windows Internet Explorer certificate store (default).

Note If you omit a policy parameter in the profile file, the feature resorts to default behavior.

Example:AnyConnect Local Policy

Refer to the following example to configure the AnyConnect Local Policy file:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy acversion="2.4.140"
   xmlns=http://schemas.xmlsoap.org/encoding/
   xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd">
    <FipsMode>false</FipsMode>
    <BypassDownloader>false</BypassDownloader>
    <RestrictWebLaunch>false</RestrictWebLaunch>
    <StrictCertificateTrust>false</StrictCertificateTrust>
    <RestrictPreferenceCaching>false</RestrictPreferenceCaching>
    <RestrictTunnelProtocols>false</RestrictTunnelProtocols>
</AnyConnectLocalPolicy>
```

Certificate Store on Windows

Table A-8 shows the tag name, options, and descriptions to configure certificate store.

Table A-8 Certificate Store Settings

XML Tag Name	Options	Description
CertificateStore	All	(Default) Directs the AnyConnect client to use all certificate stores for locating certificates.
	Machine	Directs the AnyConnect client to restrict certificate lookup to the Windows local machine certificate store.
	User	Directs the AnyConnect client to restrict certificate lookup to the local user certificate stores.

Example:Certificate Store

Refer to the following example to configure certificate store:

```
<CertificateStore>Machine</CertificateStore>
```

Restricting Certificate Store Use

Table A-9 shows the tag names, options, and descriptions to restrict certificate store use.

Table A-9 Restricting Certificate Store Settings

XML Tag Name	Options	Description
ExcludeFirefoxNSSCertStore (Linux and Mac)	true	Excludes the Firefox NSS certificate store.
	false	Permits the Firefox NSS certificate store (default).
ExcludePemFileCertStore (Linux and Mac)	true	Excludes the PEM file certificate store.
	false	Permits the PEM file certificate store (default).
ExcludeMacNativeCertStore (Mac only)	true	Excludes the Mac native certificate store.
	false	Permits the Mac native certificate store (default).
ExcludeWinNativeCertStore (Windows only, currently not supported)	true	Excludes the Windows Internet Explorer certificate store.
	false	Permits the Windows Internet Explorer certificate store (default).

SCEP Protocol to Provision and Renew Certificates

Table A-10 shows the tag names, options, and descriptions to configure SCEP protocols to provision and renew certificates.

Table A-10 SCEP Protocol Settings

XML Tag Name	Options	Description
CertificateEnrollment		Starting tag for certificate enrollment.

Table A-10 SCEP Protocol Settings (continued)

CertificateExpirationThreshold	number of days	Specifies when AnyConnect should warn users that their certificate is going to expire.
AutomaticSCEPHost	fully qualified domain name of the ASA/group-alias	The host attempts automatic certificate retrieval if this attribute specifies the ASA host name and connection profile (tunnel group) for which SCEP certificate retrieval is configured.
	IP address of the ASA/group-alias	
CAURL	fully qualified domain name	
	IP address of CA server	
CertificateSCEP		Defines how the contents of the certificate will be requested.
CADomain		Domain of the certificate authority.
Name_CN		Common Name in the certificate.
Department_OU		Department name specified in certificate.
Company_O		Company name specified in certificate.
State_ST		State identifier named in certificate.
Country_C		Country identifier named in certificate.
Email_EA		Email address.
Domain_DC		Domain component.
SurName (SN)		The family name or last name.
GivenName (GN)		Generally, the first name.
UnstructName (N)		Undefined name.
Initials (I)		The initials of the user.
Qualifier (GEN)		The generation qualifier of the user. For example, "Jr." or "III."
Qualifier (DN)		A qualifier for the entire DN.
City (L)		The city identifier.
Title (T)		The person's title. For example, Ms., Mrs., Mr.
CA Domain		Used for the SCEP enrollment and is generally the CA domain.
Key Size		The size of the RSA keys generated for the certificate to be enrolled.
DisplayGetCertButton	true	Permits users to manually request provisioning or renewal of authentication certificates. Typically, these users will be able to reach the certificate authority without first needing to create a VPN tunnel.
	false	Does not permit users to manually request provisioning or renewal of authentication certificates.
ServerList		Starting tag for the server list. The server list is presented to users when they first launch AnyConnect. Users can choose which ASA to log into.
HostEntry		Starting tag for configuring an ASA.

Table A-10 SCEP Protocol Settings (continued)

HostName		Host name of the ASA.
HostAddress		Fully qualified domain name of the ASA.

Example:SCEP Protocols

Refer to the following example to configure SCEP elements in user profiles:

```
<AnyConnectProfile>
    <ClientInitialization>
        <CertificateEnrollment>
            <CertificateExpirationThreshold>14</CertificateExpirationThreshold>
            <AutomaticSCEPHost>asa.cisco.com/scep_eng</AutomaticSCEPHost>
            <CAURL PromptForChallengePW="true"
Thumbprint="8475B661202E3414D4BB223A464E6AAB8CA123AB">http://ca01.cisco.com</CAURL>
            <CertificateSCEP>
                <CADomain>cisco.com</CADomain>
                <Name_CN>%USER%</Name_CN>
                <Department_OU>Engineering</Department_OU>
                <Company_O>Cisco Systems</Company_O>
                <State_ST>Colorado</State_ST>
                <Country_C>US</Country_C>
                <Email_EA>%USER%@cisco.com</Email_EA>
                <Domain_DC>cisco.com</Domain_DC>
                <DisplayGetCertButton>false</DisplayGetCertButton>
            </CertificateSCEP>
        </CertificateEnrollment>
    </ClientInitialization>
    <ServerList>
        <HostEntry>
            <HostName>ABC-ASA</HostName>
            <HostAddress>ABC-asa-cluster.cisco.com</HostAddress>
        </HostEntry>
        <HostEntry>
            <HostName>Certificate Enroll</HostName>
            <HostAddress>ourasa.cisco.com</HostAddress>
            <AutomaticSCEPHost>ourasa.cisco.com/scep_eng</AutomaticSCEPHost>
            <CAURL PromptForChallengePW="false"
Thumbprint="8475B655202E3414D4BB223A464E6AAB8CA123AB">http://ca02.cisco.com</CAURL>
        </HostEntry>
    </ServerList>
</AnyConnectProfile>
```

Certificate Matching

Note If no certificate matching criteria is specified, AnyConnect applies the following certificate matching rules:

- Key Usage: Digital_Signature
- Extended Key Usage: Client Auth

If any criteria matching specifications are made in the profile, neither of these matching rules are applied unless they are specifically listed in the profile.

Table A-11 shows the tag names, options, and descriptions to configure certificate matching.

Table A-11 Certificate Matching

XML Tag Name	Options	Description
CertificateExpirationThreshold		Specifies the number of days prior to the certificate's expiration date. Users are warned that their certificate is expiring.
CertificateMatch	n/a	Defines preferences that refine client certificate selection. Include only if certificates are used as part of authentication. Only those CertificateMatch subsections (KeyUsage, ExtendedKeyUsage and DistinguishedName) that are needed to uniquely identify a user certificate should be included in the profile.
KeyUsage	n/a	Group identifier, subordinate to CertificateMatch. Use these attributes to specify acceptable client certificates.
MatchKey	Decipher_Only Encipher_Only CRL_Sign Key_Cert_Sign Key_Agreement Data_Encipherment Key_Encipherment Non_Repudiation Digital_Signature	Within the KeyUsage group, MatchKey attributes specify attributes that can be used for choosing acceptable client certificates. Specify one or more match keys. A certificate must match at least one of the specified key to be selected.
ExtendedKeyUsage	n/a	Group identifier, subordinate to CertificateMatch. Use these attributes to choose acceptable client certificates.
ExtendedMatchKey	ClientAuth ServerAuth CodeSign EmailProtect IPSecEndSystem IPSecUsers Timestamp OCSPSigns DVCS	Within the ExtendedKeyUsage group, ExtendedMatchKey specifies attributes that can be used for choosing acceptable client certificates. Specify zero or more extended match keys. A certificate must match all of the specified key(s) to be selected.
CustomExtendedMatchKey	Well-known MIB OID values, such as 1.3.6.1.5.5.7.3.11	Within the ExtendedKeyUsage group, you can specify zero or more custom extended match keys. A certificate must match all of the specified key(s) to be selected. The key should be in OID form (for example, 1.3.6.1.5.5.7.3.11).
DistinguishedName	n/a	Group identifier. Within the DistinguishedName group, Certificate Distinguished Name matching lets you specify match criteria for choosing acceptable client certificates.

Table A-11 Certificate Matching (continued)

XML Tag Name	Options	Description
DistinguishedNameDefinition	Bold text indicates default value. • Wildcard: **“Enabled”** “Disabled” • Operator: **“Equal”** (==) “NotEqual” (!==) • MatchCase: **“Enabled”** “Disabled”	DistinguishedNameDefinition specifies a set of operators used to define a single Distinguished Name attribute to be used in matching. The Operator specifies the operation to use in performing the match. MatchCase specifies whether the pattern matching is case sensitive.

Table A-11 Certificate Matching (continued)

XML Tag Name	Options	Description
Name	CN DC SN GN N I GENQ DNQ C L SP ST O OU T EA ISSUER-CN ISSUER-DC ISSUER-SN ISSUER-GN ISSUER-N ISSUER-I ISSUER-GENQ ISSUER-DNQ ISSUER-C ISSUER-L ISSUER-SP ISSUER-ST ISSUER-O ISSUER-OU ISSUER-T ISSUER-EA	A DistinguishedName attribute to be used in matching. You can specify up to 10 attributes.

Table A-11 Certificate Matching (continued)

XML Tag Name	Options	Description
Pattern	A string (1-30 characters) enclosed in double quotes. With wildcards enabled, the pattern can be anywhere in the string.	Specifies the string (pattern) to use in the match. Wildcard pattern matching is disabled by default for this definition.

Example:Certificate Matching

Refer to the following example to enable the attributes that you can use to refine client certificate selections:

Note In this example, the profile options for KeyUsage, ExtendedKeyUsage, and DistinguishedName are just examples. You should configure *only* the CertificateMatch criteria that apply to your certificates.

```
<CertificateMatch>
     <!--
         Specifies Certificate Key attributes that can be used for choosing
         acceptable client certificates.
       -->
    <KeyUsage>
        <MatchKey>Non_Repudiation</MatchKey>
        <MatchKey>Digital_Signature</MatchKey>
    </KeyUsage>
     <!--
         Specifies Certificate Extended Key attributes that can be used for
         choosing acceptable client certificates.
       -->
    <ExtendedKeyUsage>
        <ExtendedMatchKey>ClientAuth</ExtendedMatchKey>
        <ExtendedMatchKey>ServerAuth</ExtendedMatchKey>
        <CustomExtendedMatchKey>1.3.6.1.5.5.7.3.11</CustomExtendedMatchKey>
    </ExtendedKeyUsage>
     <!--
         Certificate Distinguished Name matching allows for exact
         match criteria in the choosing of acceptable client
         certificates.
       -->
    <DistinguishedName>
        <DistinguishedNameDefinition Operator="Equal" Wildcard="Enabled">
            <Name>CN</Name>
            <Pattern>ASASecurity</Pattern>
        </DistinguishedNameDefinition>
        <DistinguishedNameDefinition Operator="Equal" Wildcard="Disabled">
            <Name>L</Name>
            <Pattern>Boulder</Pattern>
        </DistinguishedNameDefinition>
    </DistinguishedName>
</CertificateMatch>
```

Automatic Certificate Selection

Table A-12 shows the tag names, options, and descriptions to configure automatic certificate selection.

Table A-12 Automatic Certificate Selection Settings

XML Tag Name	Options	Description
AutomaticCertSelection	true	Allows AnyConnect to automatically select the authentication certificate.
	false	Prompts the user to select the authentication certificate.

Example:AutomaticCertSelection

Refer to the following example to configure the client profile with AutomaticCertSelection:

```
<AnyConnectProfile>
    <ClientInitialization>
        <AutomaticCertSelection>false</AutomaticCertSelection>
    </ClientInitialization>
</AnyConnectProfile>
```

Backup Server List Parameters

Table A-13 shows the tag names, options, and descriptions to configure backup server list.

Table A-13 Backup Server List Settings

XML Tag Name	Options	Description
BackupServerList	n/a	Determines the group identifier.
HostAddress	An IP address or a Full-Qualified Domain Name (FQDN)	Specifies a host address to include in the backup server list.

Example:Backup Server List

Refer to the following example to configure backup server list parameters:

```
<BackupServerList>
   <HostAddress>bos</HostAddress>
   <HostAddress>bos.example.com</HostAddress>
</BackupServerList>
```

Windows Mobile Policy

Table A-14 shows the tag names, options, and descriptions to configure Windows Mobile policy.

Note

- This configuration merely validates the policy that is already present; it does not change it.
- AnyConnect version 3.0 and later does not support Windows Mobile devices. See *Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 2.5* for information related to Windows Mobile devices.

Table A-14 Windows Mobile Policy

XML Tag Name	Options	Description
MobilePolicy	n/a	Determines the group identifier.
DeviceLockRequired	n/a	Group identifier. Within the MobilePolicy group, DeviceLockRequired indicates that a Windows Mobile device must be configured with a password or PIN prior to establishing a VPN connection. This configuration is valid only on Windows Mobile devices that use the Microsoft Default Local Authentication Provider (LAP). **Note** The AnyConnect client supports Mobile Device Lock on Windows Mobile 5.0, WM5AKU2+, and Windows Mobile 6.0, but not on Windows Mobile 6.1.
MaximumTimeoutMinutes	Any non-negative integer	Within the DeviceLockRequired group, this parameter, when set to a non-negative number, specifies the maximum number of minutes that must be configured before device lock takes effect.
MinimumPasswordLength	Any non-negative integer	Within the DeviceLockRequired group, when set to a non-negative number, this parameter specifies that any PIN/password used for device locking must have at least the specified number of characters. This setting must be pushed down to the mobile device by synchronizing with an Exchange server before it can be enforced. (WM5AKU2+)
PasswordComplexity	"alpha"-Requires an alphanumeric password. "pin"-Requires a numeric PIN. "strong"-Requires a strong alphanumeric password, defined by Microsoft as containing at least 7 characters, including at least 3 from the set of uppercase, lowercase, numerals, and punctuation.	When present, checks for the password subtypes listed in the column to the left. This setting must be pushed down to the mobile device by synchronizing with an Exchange server before it can be enforced. (WM5AKU2+)

Example:Windows Mobile Policy

Refer to the following example to configure a Windows Mobile policy using XML:

```
<MobilePolicy>
<DeviceLockRequired>
    MaximumTimeoutMinutes=”60”
    MinimumPasswordLength=”4”
    PasswordComplexity=”pin”
</DeviceLockRequired>
</MobilePolicy>
```

Auto Connect On Start

Table A-15 shows the tag names, options, and descriptions to configure auto connect on start.

Table A-15 Auto Connect On Start Settings

XML Tag Name	Options	Description
AutoConnectOnStart	true	Starts the auto connect settings.
	false	Returns to the default auto connect settings.
AutoConnectOnStart UserControllable	true	Inserts user control attributes.
	false	Removes user control attributes.

Example:Auto Connect On Start

Refer to the following example to configure auto connect on start:

```
<AutoConnectOnStart>
true
</AutoConnectOnStart>
```

Auto Reconnect

Table A-16 shows the tag names, options, and descriptions to configure auto reconnect.

Table A-16 Auto Reconnect Settings

XML Tag Name	Options	Description
AutoReconnect	true	Client retains resources assigned to the VPN session if it is disrupted and attempts to reconnect.
	false	Client releases resources assigned to the VPN session if it is interrupted and does not attempt to reconnect.
AutoReconnectBehavior	DisconnectOnSuspend	AnyConnect releases the resources assigned to the VPN session upon a system suspend and does not attempt to reconnect after the system resume.
	ReconnectAfterResume	Client retains resources assigned to the VPN session during a system suspend. The client attempts to reconnect after the system resume.

Example:Auto Reconnect

Refer to the following example to configure AnyConnect VPN reconnect behavior in the client initialization section:

```
<AutoReconnect UserControllable=”true”>true
<AutoReconnectBehavior
UserControllable=”true”>ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
```

Server List

Table A-17 shows the tag names, options, and descriptions to configure server list.

Table A-17 Server List Settings

XML Tag Name	Options	Description
ServerList	n/a	Specifies a group identifier.
HostEntry	n/a	Group identifier, subordinate to ServerList. This is the data needed to attempt a connection to a specific host.
HostName	An alias used to refer to the host, FQDN, or IP address. If this is an FQDN or IP address, a HostAddress is not required.	Within the HostEntry group, the HostName parameter specifies a name of a host in the server list.
HostAddress	An IP address or Full-Qualified Domain Name (FQDN) used to refer to the host. If HostName is an FQDN or IP address, a HostAddress is not required.	Group identifier, subordinate to CertificateMatch. Use these attributes to choose acceptable client certificates.
PrimaryProtocol	SSL or IPsec	The encryption protocol for the VPN tunnel, either SSL (default) or IPsec with IKEv2. For IPsec, the client uses the proprietary AnyConnect EAP authentication method by default.
StandardAuthenticationOnly	n/a	Use the StandardAuthenticationOnly parameter to change the authentication method from the default proprietary AnyConnect EAP authentication method to a standards-based method. Be aware that doing this limits the dynamic download features of the client and disables some features and disables the ability of the ASA to configure session timeout, idle timeout, disconnected timeout, split tunneling, split DNS, MSIE proxy configuration, and other features.
AuthMethodDuringIKENegotiation	IKE-RSA, EAP-MD5, EAP-MSCHAPv2, EAP-GTC	Specifies the authentication method for standard-based authentication.

Table A-17 Server List Settings

XML Tag Name	Options	Description
IKEIdentity	An alpha-numeric string.	If you choose a standards-based EAP authentication method, you can enter a group or domain as the client identity in this field. The client sends the string as the ID_GROUP type IDi payload. By default, the string is *$AnyConnectClient$*. The string must not contain any terminators (for example, null or CR).
UserGroup	The connection profile (tunnel group) to use when connecting to the specified host. This parameter is optional.	If present, used in conjunction with HostAddress to form a Group-based URL. If you specify the Primary Protocol as IPsec, the User Group must be the exact name of the connection profile (tunnel group). For SSL, the user group is the group-url or group-alias of the connection profile. **Note** Group-based URL support requires ASA version 8.0.3 or later.

Example:Server List

Refer to the following example to configure a server list:

```
<ServerList>
    <HostEntry>
        <HostName>ASA-01</HostName>
        <HostAddress>cvc-asa01.cisco.com
         </HostAddress>
    </HostEntry>
    <HostEntry>
        <HostName>ASA-02</HostName>
         <HostAddress>cvc-asa02.cisco.com
         </HostAddress>
        <UserGroup>StandardUser</UserGroup>
        <BackupServerList>
            <HostAddress>cvc-asa03.cisco.com
            </HostAddress>
         </BackupServerList>
    </HostEntry>
</ServerList>
```

Scripting

Table A-18 shows the tag names, options, and descriptions to configure scripting.

Table A-18 Scripting Settings

XML Tag Name	Options	Description
EnableScripting	true	Launches OnConnect and OnDisconnect scripts if present.
	false	(Default) Does not launch scripts.
UserControllable	true	Lets users enable or disable the running of OnConnect and OnDisconnect scripts.
	false	(Default) Prevents users from controlling the scripting feature.
TerminateScriptOnNextEvent	true	Terminates a running script process if a transition to another scriptable event occurs. For example, AnyConnect terminates a running OnConnect script if the VPN session ends and terminates a running OnDisconnect script if AnyConnect starts a new VPN session. On Microsoft Windows, AnyConnect also terminates any scripts that the OnConnect or OnDisconnect script launched, as well as all their script descendents. On Mac OS and Linux, AnyConnect terminates only the OnConnect or OnDisconnect script; it does not terminate child scripts.
	false	(Default) Does not terminate a script process if a transition to another scriptable event occurs.
EnablePostSBLOnConnectScript	true	Prevents launching of the OnConnect script if SBL establishes the VPN session.
	false	(Default) When SBL establishes the VPN session, launches the OnConnect script, if present.

Example:Scripting

Refer to the following example to configure scripting:

```
<ClientInitialization>

<EnableScripting>true</EnableScripting>

</ClientInitialization>
```

This example enables scripting and overrides the default options for the other scripting parameters:

```
<ClientInitialization>

<EnableScripting UserControllable="true">true
    <TerminateScriptOnNextEvent>true</TerminateScriptOnNextEvent>
    <EnablePostSBLOnConnectScript>false</EnablePostSBLOnConnectScript>
</EnableScripting>

</ClientInitialization>
```

Authentication Timeout Control

By default, AnyConnect waits up to 12 seconds for an authentication from the secure gateway before terminating the connection attempt. AnyConnect then displays a message indicating the authentication timed out.

Table A-19 shows the tag name, options, and descriptions to change the authentication timer.

Table A-19 Authentication Timeout Control

XML Tag Name	Options	Description
AuthenticationTimeout	Integer in the range 10–120	Enter a number of seconds to change this timer.

Example:Authentication Timeout Control

The following example changes the authentication timeout to 20 seconds:

```
<ClientInitialization>
    <AuthenticationTimeout>20</AuthenticationTimeout>
</ClientInitialization>
```

Ignore Proxy

Table A-20 shows the tag name, options, and descriptions to configure ignore proxy.

Table A-20 Ignore Proxy Settings

XML Tag Name	Options	Description
ProxySettings	IgnoreProxy	Enables ignore proxy.
	native	Not supported.
	override	Not supported.

Example:Ignore Proxy

Refer to the following example to configure ignore proxy in the client initialization section:

```
<ProxySettings>IgnoreProxy</ProxySettings>
```

Allow AnyConnect Session from an RDP Session for Windows Users

Table A-21 shows the tag names, options, and descriptions to configure an RDP session.

Table A-21 Allow AnyConnect Session from an RDP Session

XML Tag Name	Options	Description
WindowsLogonEnforcement	SingleLocalLogon	Allows only one local user to be logged on during the entire VPN connection. With this setting, a local user can establish a VPN connection while one or more remote users are logged on to the client PC. If the VPN connection is configured for all-or-nothing tunneling, then the remote logon is disconnected because of the resulting modifications of the client PC routing table for the VPN connection. If the VPN connection is configured for split-tunneling, the remote logon might or might not be disconnected, depending on the routing configuration for the VPN connection. The SingleLocalLogin setting has no effect on remote user logons from the enterprise network over the VPN connection.
	SingleLogon	Allows only one user to be logged on during the entire VPN connection. If more than one user is logged on, either locally or remotely, when the VPN connection is being established, the connection is not allowed. If a second user logs on, either locally or remotely, during the VPN connection, the VPN connection is terminated.
WindowsVPNEstablishment	LocalUsersOnly	Prevents a remotely logged-on user from establishing a VPN connection. This is the same functionality as in prior versions of the AnyConnect client.
	AllowRemoteUsers	Allows remote users to establish a VPN connection. However, if the configured VPN connection routing causes the remote user to become disconnected, the VPN connection is terminated to allow the remote user to regain access to the client PC.

Example:Allow AnyConnect Session from an RDP Session for Windows Users

Refer to the following example to configure AnyConnect sessions from an RDP session:

```
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>

<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
```

AnyConnect over L2TP or PPTP

Table A-22 shows the tag names, options, and descriptions to configure AnyConnect over L2TP or PPTP.

Table A-22 AnyConnect Over L2TP or PPTP

XML Tag Name	Options	Description
PPPExclusion	automatic	Enables PPP exclusion. AnyConnect automatically uses the IP address of the PPP server. Instruct users to change the value only if automatic detection fails to get the IP address.
	override	Also enables PPP exclusion. If automatic detection fails to get the IP address of the PPP server, and the PPPExclusion UserControllable value is true, follow the steps in "Instructing Users to Override PPP Exclusion" on page 3-69.
	disabled	PPP exclusion is not applied.
PPPExclusionServerIP	true	Uses the IP address of the PPP server.
	false	Does not use the IP address of the PPP server.
PPPExclusion UserControllable=	true	Lets users read and change the PPP exclusion settings.
	false	Prevents users from viewing and changing the PPP exclusion settings.

Example:AnyConnect Over L2TP or PPTP

Refer to the following example to configure AnyConnect over L2TP or PPTP:

```
<ClientInitialization>
    <PPPExclusion UserControllable="true">Automatic
        <PPPExclusionServerIP UserControllable="true">127.0.0.1</PPPExclusionServerIP>
    </PPPExclusion>
    </ClientInitialization>
        <ServerList>
        <HostEntry>
            <HostName>DomainNameofASA</HostName>
            <HostAddress>IPaddressOfASA</HostAddress>
        </HostEntry>
         </ServerList>
</AnyConnectProfile>
```

Other AnyConnect Profile Settings

Table A-23 shows other parameters you can insert into the ClientInitialization section.

Table A-23 Other AnyConnect Profile Settings

XML Tag Name	Options	Description
CertificateStoreOverride	true	Allows an administrator to direct AnyConnect to search for certificates in the Windows machine certificate store. This tag becomes useful when certificates are located in this store and users do not have administrator privileges on their device. You must have a pre-deployed profile with this option enabled in order to connect with Windows 7 or VISTA using machine certificate. If this profile does not exist on a Windows 7 or VISTA device prior to connection, the certificate is not accessible in the machine store, and the connection fails.
	false	(Default) AnyConnect will not search for certificates in the Windows machine certificate store.
ShowPreConnectMessage	true	Enables an administrator to have a one-time message displayed prior to a users first connection attempt. For example, the message can remind users to insert their smart card into its reader. The message appears in the AnyConnect message catalog and is localized.
	false	(Default) No message displayed prior to a users first connection attempt.
MinimizeOnConnect	true	(Default) Controls AnyConnect GUI behavior when a VPN tunnel is established. By default, the GUI is minimized when the VPN tunnel is established.
	false	No control over AnyConnect GUI behavior.
LocalLanAccess	true	Allows the user to accept or reject Local LAN access when enabled for remote clients on the Secure Gateway.
	false	(Default) Disallows Local LAN access.
AutoUpdate	true	(Default) Installs new packages automatically.
	false	Does not install new pacakges.
RSASecurIDIntegration	automatic	(Default) Allows the administrator to control how the user interacts with RSA. By default, AnyConnect determines the correct method of RSA interaction. An administrator can lock down the RSA or give control to the user.
	software token	
	hardware token	
RetainVPNOnLogoff	true	Keeps the VPN session when the user logs off a Windows operating system.
	false	(Default) Stops the VPN session when the user logs off a Windows operating system.
UserEnforcement	AnyUser	Continues the VPN session even if a different user logs on. This value applies only if the RetainVPNPnLogoff is true and the original users logged off Windows when the VPN session was up.
	SameUserOnly	Ends the VPN session when a different user logs on.