



APPENDIX **A**

Sample AnyConnect Profile and XML Schema

This appendix contains a sample AnyConnect profile and a sample AnyConnect profile schema. Both of these are delivered with the client and are present in a client installation in the same directory. The profile defines the attributes configured for a particular user. The schema defines the profile format that is allowed. The schema is suitable for use as a validation mechanism.

- [Sample AnyConnect Profile, page A-1](#)
- [Sample AnyConnect Profile Schema, page A-3](#)



Caution

Do not cut and paste this example 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.

Use the template that appears after installing AnyConnect on a workstation:
\\Documents and Settings\\All Users\\Application Data\\Cisco\\Cisco AnyConnect VPN Client\\Profile\\AnyConnectProfile.tmpl

Sample AnyConnect Profile

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
  This is a sample of a Cisco AnyConnect VPN Client Profile XML file.

  This file is intended to be maintained by a Secure Gateway administrator
  and then distributed with the client software.  The xml file based on
  this schema can be distributed to clients at any time.  The distribution
  mechanisms supported are as a bundled file with the software distribution
  or as part of the automatic download mechanism.  The automatic download
  mechanism only available with certain Cisco Secure Gateway products.

  NOTE: Administrators are strongly encouraged to validate XML profile they
  create using an online validation tool or via the profile import
  functionality in ASDM.  Validation can be accomplished with the
  AnyConnectProfile.xsd found in this directory.

  AnyConnectProfile is the root element representing the AnyConnect Client
  Profile
-->
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
  <!--
```

The ClientInitialization section represents global settings for the client. In some cases (e.g. BackupServerList) host specific overrides are possible.

```

-->
<ClientInitialization>
  <!--
    The Start Before Logon feature can be used to activate the VPN as
    part of the logon sequence.

    UserControllable:
    Does the administrator of this profile allow the user to control
    this attribute for their own use. Any user setting associated
    with this attribute will be stored elsewhere.
  -->
  <UseStartBeforeLogon UserControllable="false">>false</UseStartBeforeLogon>
  <!--
    If user is importing a certificate using the enrollment feature,
    this attribute will enforce any pin application requirement.
  -->
  <CertEnrollmentPin>pinAllowed</CertEnrollmentPin>
  <!--
    This section enables the definition of various attributes that
    can be used to refine client certificate selection.
  -->
  <CertificateMatch>
    <!--
      Certificate Key attributes that can be used for choosing
      acceptable client certificates.
    -->
    <KeyUsage>
      <MatchKey>Non_Repudiation</MatchKey>
      <MatchKey>Digital_Signature</MatchKey>
    </KeyUsage>
    <!--
      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>
  <!--
    Collection of one or more backup servers to be used in case
    the user selected one fails.
  -->
  <BackupServerList>
    <!--

```

```

        Can be a FQDN or IP address.
    -->
    <HostAddress>cvc-asa-02.cisco.com</HostAddress>
    <HostAddress>10.94.146.172</HostAddress>
</BackupServerList>
</ClientInitialization>
<!--
    This section contains the list of hosts the user will be able to
    select from.
-->
<ServerList>
    <!--
        This is the data needed to attempt a connection to a specific
        host.
    -->
    <HostEntry>
        <!--
            Can be an alias used to refer to the host or an FQDN or
            IP address. If an FQDN or IP address is used, a
            HostAddress is not required.
        -->
        <HostName>CVC-ASA-02</HostName>
        <HostAddress>cvc-asa-02.cisco.com</HostAddress>
    </HostEntry>
    <HostEntry>
        <HostName>CVC-ASA-01</HostName>
        <HostAddress>10.94.146.172</HostAddress>
    <!--
        This backup server list represents an override to the
        global one defined previously.
    -->
    <BackupServerList>
        <HostAddress>cvc-asa-03.cisco.com</HostAddress>
        <HostAddress>10.94.146.173</HostAddress>
    </BackupServerList>
    </HostEntry>
</ServerList>
</AnyConnectProfile>

```

Sample AnyConnect Profile Schema

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- edited with XMLSpy v2006 rel. 3 sp1 (http://www.altova.com) by Chris Fitzgerald
(private) -->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:ns1="http://schemas.xmlsoap.org/encoding/"
targetNamespace="http://schemas.xmlsoap.org/encoding/" elementFormDefault="qualified"
attributeFormDefault="unqualified">
    <xs:annotation>
        <xs:documentation>pwd</xs:documentation>
    </xs:annotation>
    <xs:complexType name="HostEntry">
        <xs:annotation>
            <xs:documentation>This is the data needed to attempt a connection to a
specific host.</xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:element name="HostEntry" maxOccurs="unbounded">
                <xs:annotation>

```

```

        <xs:documentation>A HostEntry comprises the data needed to identify and
connect to a specific host.</xs:documentation>
    </xs:annotation>
    <xs:complexType>
        <xs:sequence>
            <xs:element name="HostName">
                <xs:annotation>
                    <xs:documentation>Can be an alias used to refer to the host
or an FQDN or IP address. If an FQDN or IP address is used, a HostAddress is not
required.</xs:documentation>
                </xs:annotation>
            </xs:element>
            <xs:element name="HostAddress" minOccurs="0">
                <xs:annotation>
                    <xs:documentation>Can be a FQDN or IP
address.</xs:documentation>
                </xs:annotation>
            </xs:element>
            <xs:element name="BackupServerList" type="ns1:BackupServerList"
minOccurs="0">
                <xs:annotation>
                    <xs:documentation>Collection of one or more backup servers
to be used in case the user selected one fails.</xs:documentation>
                </xs:annotation>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
<xs:complexType name="AnyConnectClientProfile">
    <xs:annotation>
        <xs:documentation>This is the XML schema definition for the Cisco AnyConnect
VPN Client Profile XML file. The VPN Client Initialization is a repository of information
used to manage the Cisco VPN client software. This file is intended to be maintained by a
Secure Gateway administrator and then distributed with the client software. The xml file
based on this schema can be distributed to clients at any time. The distribution
mechanisms supported are as a bundled file with the software distribution or as part of
the automatic download mechanism. The automatic download mechanism only available with
certain Cisco Secure Gateway products.</xs:documentation>
    </xs:annotation>
    <xs:sequence>
        <xs:element name="ClientInitialization" minOccurs="0">
            <xs:annotation>
                <xs:documentation>The ClientInitialization section represents global
settings for the client. In some cases (e.g. BackupServerList) host specific overrides
are possible.</xs:documentation>
            </xs:annotation>
            <xs:complexType>
                <xs:sequence>
                    <xs:element name="UseStartBeforeLogon" default="false"
minOccurs="0">
                        <xs:annotation>
                            <xs:documentation>The Start Before Logon feature can be used
to activate the VPN as part of the logon sequence.</xs:documentation>
                        </xs:annotation>
                    </xs:element>
                </xs:sequence>
            </xs:complexType>
            <xs:simpleContent>
                <xs:extension base="ns1:simpleBinary">
                    <xs:attribute name="UserControllable"
default="false">
                        <xs:annotation>

```

```

        <xs:documentation>Does the administrator of
this profile allow the user to control this attribute for their own use. Any user setting
associated with this attribute will be stored elsewhere.</xs:documentation>
    </xs:annotation>
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:enumeration value="true">
                <xs:annotation>
                    <xs:documentation>user is allowed
to control this setting.</xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="false">
                <xs:annotation>
                    <xs:documentation>user is not
allowed to control this setting.</xs:documentation>
                </xs:annotation>
            </xs:enumeration>
        </xs:restriction>
    </xs:simpleType>
</xs:attribute>
</xs:extension>
</xs:simpleContent>
</xs:complexType>
</xs:element>
<xs:element name="CertEnrollmentPin" default="pinAllowed"
minOccurs="0">
    <xs:annotation>
        <xs:documentation>If user is importing a certificate using
the enrollment feature, this attribute will enforce any pin application
requirement.</xs:documentation>
    </xs:annotation>
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:enumeration value="noPin">
                <xs:annotation>
                    <xs:documentation>user may not enter a pin when
enrolling a certificate.</xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="pinAllowed">
                <xs:annotation>
                    <xs:documentation>user may enter a pin when
enrolling a certificate.</xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="pinRequired">
                <xs:annotation>
                    <xs:documentation>user must enter a pin when
enrolling a certificate.</xs:documentation>
                </xs:annotation>
            </xs:enumeration>
        </xs:restriction>
    </xs:simpleType>
</xs:element>
<xs:element name="CertificateMatch" minOccurs="0">
    <xs:annotation>
        <xs:documentation>This section enables the definition of
various attributes that can be used to refine client certificate
selection.</xs:documentation>
    </xs:annotation>
    <xs:complexType>
        <xs:sequence>

```

```

        <xs:element name="KeyUsage" type="ns1:KeyUsage"
minOccurs="0">
            <xs:annotation>
                <xs:documentation>Certificate Key attributes
that can be used for choosing acceptable client certificates.</xs:documentation>
            </xs:annotation>
        </xs:element>
        <xs:element name="ExtendedKeyUsage"
type="ns1:ExtendedKeyUsage" minOccurs="0">
            <xs:annotation>
                <xs:documentation>Certificate Extended Key
attributes that can be used for choosing acceptable client
certificates.</xs:documentation>
            </xs:annotation>
        </xs:element>
        <xs:element name="DistinguishedName"
type="ns1:DistinguishedName" minOccurs="0">
            <xs:annotation>
                <xs:documentation>Certificate Distinguished Name
matching allows for exact match criteria in the choosing of acceptable client
certificates.</xs:documentation>
            </xs:annotation>
        </xs:element>
    </xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="BackupServerList" type="ns1:BackupServerList"
minOccurs="0">
    <xs:annotation>
        <xs:documentation>Collection of one or more backup servers
to be used in case the user selected one fails.</xs:documentation>
    </xs:annotation>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="ServerList" type="ns1:HostEntry" minOccurs="0">
    <xs:annotation>
        <xs:documentation>This section contains the list of hosts the user will
be able to select from.</xs:documentation>
    </xs:annotation>
</xs:element>
</xs:sequence>
</xs:complexType>
<xs:complexType name="BackupServerList">
    <xs:annotation>
        <xs:documentation>Collection of one or more backup servers to be used in case
the user selected one fails.</xs:documentation>
    </xs:annotation>
    <xs:sequence>
        <xs:element name="HostAddress" maxOccurs="unbounded">
            <xs:annotation>
                <xs:documentation>Can be a FQDN or IP address.</xs:documentation>
            </xs:annotation>
        </xs:element>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="KeyUsage">
    <xs:annotation>
        <xs:documentation>Certificate Key attributes that can be used for choosing
acceptable client certificates.</xs:documentation>
    </xs:annotation>
    <xs:sequence>
        <xs:element name="MatchKey" maxOccurs="9">

```

```

    <xs:annotation>
      <xs:documentation>One or more match key may be specified. A
certificate must match at least one of the specified key to be
selected.</xs:documentation>
    </xs:annotation>
    <xs:simpleType>
      <xs:restriction base="xs:string">
        <xs:enumeration value="Decipher_Only"/>
        <xs:enumeration value="Encipher_Only"/>
        <xs:enumeration value="CRL_Sign"/>
        <xs:enumeration value="Key_Cert_Sign"/>
        <xs:enumeration value="Key_Agreement"/>
        <xs:enumeration value="Data_Encipherment"/>
        <xs:enumeration value="Key_Encipherment"/>
        <xs:enumeration value="Non_Repudiation"/>
        <xs:enumeration value="Digital_Signature"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:element>
</xs:sequence>
</xs:complexType>
<xs:complexType name="ExtendedKeyUsage">
  <xs:annotation>
    <xs:documentation>Certificate Extended Key attributes that can be used for
choosing acceptable client certificates.</xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="ExtendedMatchKey" nillable="false" minOccurs="0"
maxOccurs="10">
      <xs:annotation>
        <xs:documentation>Zero or more extended match key may be specified. A
certificate must match all of the specified key(s) to be selected.</xs:documentation>
      </xs:annotation>
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:whiteSpace value="collapse"/>
          <xs:enumeration value="ServerAuth">
            <xs:annotation>
              <xs:documentation>1.3.6.1.5.5.7.3.1</xs:documentation>
            </xs:annotation>
          </xs:enumeration>
          <xs:enumeration value="ClientAuth">
            <xs:annotation>
              <xs:documentation>1.3.6.1.5.5.7.3.2</xs:documentation>
            </xs:annotation>
          </xs:enumeration>
          <xs:enumeration value="CodeSign">
            <xs:annotation>
              <xs:documentation>1.3.6.1.5.5.7.3.3</xs:documentation>
            </xs:annotation>
          </xs:enumeration>
          <xs:enumeration value="EmailProtect">
            <xs:annotation>
              <xs:documentation>1.3.6.1.5.5.7.3.4</xs:documentation>
            </xs:annotation>
          </xs:enumeration>
          <xs:enumeration value="IPSecEndSystem">
            <xs:annotation>
              <xs:documentation>1.3.6.1.5.5.7.3.5</xs:documentation>
            </xs:annotation>
          </xs:enumeration>
          <xs:enumeration value="IPSecTunnel">
            <xs:annotation>
              <xs:documentation>1.3.6.1.5.5.7.3.6</xs:documentation>
            </xs:annotation>
          </xs:enumeration>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
  </xs:sequence>

```

```

        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="IPSecUser">
        <xs:annotation>
            <xs:documentation>1.3.6.1.5.5.7.3.7</xs:documentation>
        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="TimeStamp">
        <xs:annotation>
            <xs:documentation>1.3.6.1.5.5.7.3.8</xs:documentation>
        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="OCSPSign">
        <xs:annotation>
            <xs:documentation>1.3.6.1.5.5.7.3.9</xs:documentation>
        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="DVCS">
        <xs:annotation>
            <xs:documentation>1.3.6.1.5.5.7.3.10</xs:documentation>
        </xs:annotation>
    </xs:enumeration>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name="CustomExtendedMatchKey" minOccurs="0" maxOccurs="10">
    <xs:annotation>
        <xs:documentation>Zero or more custom extended match key may be
specified. A certificate must match all of the specified key(s) to be selected. The key
should be in OID form (e.g. 1.3.6.1.5.5.7.3.11)</xs:documentation>
    </xs:annotation>
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:whiteSpace value="collapse"/>
            <xs:minLength value="1"/>
            <xs:maxLength value="30"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>
</xs:sequence>
</xs:complexType>
<xs:complexType name="DistinguishedName">
    <xs:annotation>
        <xs:documentation>Certificate Distinguished Name matching allows for exact
match criteria in the choosing of acceptable client certificates.</xs:documentation>
    </xs:annotation>
    <xs:sequence>
        <xs:element name="DistinguishedNameDefinition" maxOccurs="10">
            <xs:annotation>
                <xs:documentation>This element represents the set of attributes to
define a single Distinguished Name mathcing definition.</xs:documentation>
            </xs:annotation>
            <xs:complexType>
                <xs:sequence>
                    <xs:element name="Name">
                        <xs:annotation>
                            <xs:documentation>Distinguished attribute name to be used in
mathcing.</xs:documentation>
                        </xs:annotation>
                        <xs:simpleType>
                            <xs:restriction base="xs:string">
                                <xs:enumeration value="CN">
                                    <xs:annotation>

```

```

Name</xs:documentation>
    <xs:documentation>Subject Common
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="SN">
    <xs:annotation>
        <xs:documentation>Subject Sur
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="GN">
    <xs:annotation>
        <xs:documentation>Subject Given
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="N">
    <xs:annotation>
        <xs:documentation>Subject Unstruct
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="I">
    <xs:annotation>
        <xs:documentation>Subject
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="GENQ">
    <xs:annotation>
        <xs:documentation>Subject Gen
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="DNQ">
    <xs:annotation>
        <xs:documentation>Subject Dn
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="C">
    <xs:annotation>
        <xs:documentation>Subject
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="L">
    <xs:annotation>
        <xs:documentation>Subject
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="SP">
    <xs:annotation>
        <xs:documentation>Subject
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="ST">
    <xs:annotation>
        <xs:documentation>Subject
    </xs:annotation>
</xs:enumeration>
</xs:enumeration>

```



```

        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="ISSUER-C">
        <xs:annotation>
            <xs:documentation>Issuer
Country</xs:documentation>
        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="ISSUER-L">
        <xs:annotation>
            <xs:documentation>Issuer City</xs:documentation>
        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="ISSUER-SP">
        <xs:annotation>
            <xs:documentation>Issuer
State</xs:documentation>
        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="ISSUER-ST">
        <xs:annotation>
            <xs:documentation>Issuer
State</xs:documentation>
        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="ISSUER-O">
        <xs:annotation>
            <xs:documentation>Issuer
Company</xs:documentation>
        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="ISSUER-OU">
        <xs:annotation>
            <xs:documentation>Issuer
Department</xs:documentation>
        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="ISSUER-T">
        <xs:annotation>
            <xs:documentation>Issuer
Title</xs:documentation>
        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="ISSUER-EA">
        <xs:annotation>
            <xs:documentation>Issuer Email
Address</xs:documentation>
        </xs:annotation>
    </xs:enumeration>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name="Pattern" nillable="false">
    <xs:annotation>
        <xs:documentation>The string to use in the
match.</xs:documentation>
    </xs:annotation>
</xs:element>
<xs:simpleType>
    <xs:restriction base="xs:string">
        <xs:minLength value="1"/>
        <xs:maxLength value="30"/>
        <xs:whiteSpace value="collapse"/>
    </xs:restriction>
</xs:simpleType>

```

```

        </xs:element>
    </xs:sequence>
    <xs:attribute name="Wildcard" default="Disabled">
        <xs:annotation>
            <xs:documentation>Should the pattern include wildcard pattern
matching. With wildcarding enabled, the pattern can be anywhere in the
string.</xs:documentation>
        </xs:annotation>
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:enumeration value="Disabled">
                    <xs:annotation>
                        <xs:documentation>wildcard pattern match is not
enabled for this definition</xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="Enabled">
                    <xs:annotation>
                        <xs:documentation>wildcard pattern match is enabled
for this definition</xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
            </xs:restriction>
        </xs:simpleType>
    </xs:attribute>
    <xs:attribute name="Operator" default="Equal">
        <xs:annotation>
            <xs:documentation>The operator to be used in performing the
match</xs:documentation>
        </xs:annotation>
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:enumeration value="Equal">
                    <xs:annotation>
                        <xs:documentation>equivalent to
==</xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="NotEqual">
                    <xs:annotation>
                        <xs:documentation>equivalent to
!=</xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
            </xs:restriction>
        </xs:simpleType>
    </xs:attribute>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
<xs:element name="AnyConnectProfile" type="ns1:AnyConnectClientProfile">
    <xs:annotation>
        <xs:documentation>The root element representing the AnyConnect Client
Profile</xs:documentation>
    </xs:annotation>
</xs:element>
<xs:simpleType name="simpleBinary">
    <xs:restriction base="xs:string">
        <xs:enumeration value="true">
            <xs:annotation>
                <xs:documentation>enables the Start Before Logon
feature</xs:documentation>
            </xs:annotation>
        </xs:enumeration>
    </xs:restriction>
</xs:simpleType>

```

```
        </xs:enumeration>
        <xs:enumeration value="false">
          <xs:annotation>
            <xs:documentation>disables the Start Before Logon
feature.</xs:documentation>
          </xs:annotation>
        </xs:enumeration>
      </xs:restriction>
    </xs:simpleType>
  </xs:schema>
```

