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.

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

This profile and the profile schema that follows are different from those for earlier AnyConnect client releases.

Caution This example profile contains enterprise-specific values that do not work for other networks. Set the values to those that are consistent with your network.

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

    Please refer to the Cisco AnyConnect VPN Client Administrator Guide
    for information regarding profile management and examples of all
    available options. In short:

      - A Profile should be uniquely named for your Company.  An example is:
        CiscoProfile.xml

      - The profile name should be the same even if different for individual
        group within the company.
```

```
    This file is intended to be maintained by a Secure Gateway administrator
    and then distributed with the client software.  The profile based on
    this XML 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>
        <!--
            This control enables an administrator to have a one time message
            displayed prior to a users first connection attempt.  As an example,
            the message could be used to remind a user to insert their smart
            card into it’s reader.

            The message to be used with this control is localizable and can be
            found in the AnyConnect message catalog.
            (default: "This is a pre-connect reminder message.")
          -->
        <ShowPreConnectMessage>false</ShowPreConnectMessage>
        <!--
            This setting allows an administrator to specify which certificate
            store AnyConnect will use for locating certificates.

            This setting only applies to the Microsoft Windows version of
            AnyConnect and has no effect on other platforms.
          -->
        <CertificateStore>All</CertificateStore>
        <!--
            This setting allows an administrator to direct AnyConnect to search
            for certificates in the Windows machine certificate store.  This is
            useful in cases where certificates are located in this store and
            users do not have administrator privileges on their machine.
          -->
        <CertificateStoreOverride>false</CertificateStoreOverride>
        <!--
            Controls AnyConnect client behavior when started.  By default, the
```

```
    client will attempt to contact the last Gateway a user connected
    to or the first one in the list from the AnyConnect profile.  In
    the case of certificate-only authentication, this will result in
    the establishment of a VPN tunnel when the client is started.
  -->
<AutoConnectOnStart UserControllable="true">true</AutoConnectOnStart>
<!--
    Controls AnyConnect GUI behavior when a VPN tunnel is established.
    By default, the GUI will minimize when the VPN tunnel is
    established.
  -->
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<!--
    If Local LAN access is enabled for remote clients on the Secure
    Gateway, this setting can be used to allow the user to accept or
    reject this access.
  -->
<LocalLanAccess UserControllable="true">true</LocalLanAccess>
<!--
    This setting allows an administrator to control how a client will
    behave when the VPN tunnel is interrupted.  Control can optionally
    be given to the user.
  -->
<AutoReconnect UserControllable="true">true
  <AutoReconnectBehavior>ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
<!--
    This setting allows the adminstrator to turn off the dynamic
    update functionality of AnyConnect.  Control of this can also be
    given to the user.
  -->
<AutoUpdate UserControllable="false">true</AutoUpdate>
<!--
    This setting allows the adminstrator to control how the user will
    interact with RSA.  By default, AnyConnect will determine the
    correct method of RSA interaction.  The desired setting can be
    locked down by the administrator or control can be given to the
    user.
  -->
<RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
<!--
    This setting allows the adminstrator to control if more than one
    user may be logged into the client PC during a VPN connection.
  -->
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<!--
    This setting allows the adminstrator to control if a VPN
    connection may be initiated by a remote user.
  -->
<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
<!--
    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>
            </ExtendedKeyUsage>
        </CertificateMatch>
        <MobilePolicy>
            <!--
            DeviceLockRequired indicates that a Windows Mobile device must
            be configured with a password or PIN prior to establishing a
            VPN connection.  This configuration is only valid on Windows
            Mobile devices that use the Microsoft Default Local
            Authentication Provider (LAP).

            The following attributes can be specified to check additional
            settings.  The platforms for which each additional check is
            performed as specified with "WM5AKU2+" for Windows Mobile 5 with
            the Messaging and Security Feature Pack delivered as part of
            Adaption Kit Upgrade 2 (AKU2).

                MaximumTimeoutMinutes - when set to non-negative
                    number, specifies the maximum number of minutes
                    that must be configured before device lock takes
                    effect.  (WM5/WM5AKU2+)
                MinimumPasswordLength - when set to a non-negative number,
                    specifies that any PIN/password used for device lock
                    must be equal to or longer than the specified value,
                    in characters.  This setting must be pushed down to
                    the mobile device by syncing with an Exchange server
                    before it can be enforced. (WM5AKU2+)
                PasswordComplexity - when present checks for the following
                    password subtypes:
                        "alpha"  - Requires an alphanumeric password
                        "pin"    - Numeric PIN required
                        "strong" - Strong alphanumeric password defined by
                                   Microsoft as containing at least 7
                                   characters, including at lesst 3 from
                                   the set of uppercase, lowercase,
                                   numerals, and punctuation.

                    This setting must be pushed down to the mobile device
                    by syncing with an Exchange server before it can be
                    enforced. (WM5AKU2+)

            Note that this configuration setting merely enforces policy -
            it does not actually change local device policy.
          -->
        <DeviceLockRequired
            MaximumTimeoutMinutes="60"
            MinimumPasswordLength="4"
            PasswordComplexity="pin"/>
        </MobilePolicy>
    </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>REPLACE_AsaName</HostName>
            <HostAddress>REPLACE_asa.address.com</HostAddress>
        </HostEntry>
        <HostEntry>
            <HostName>REPLACE_AsaName2</HostName>
            <HostAddress>REPLACE_10.94.146.172</HostAddress>
            <!--
                If present, UserGroup will be used in conjunction with
                HostAddress to form a Group based URL.
                NOTE: Group based URL support requires ASA version 8.0.3 or
                      later.
              -->
            <UserGroup>REPLACE_TunnelGroup</UserGroup>
        </HostEntry>
    </ServerList>
</AnyConnectProfile>
© 2009 Cisco Systems, Inc. - Internal Use Only
```

Sample AnyConnect Profile Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<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="UserGroup" minOccurs="0">
```

```
                        <xs:annotation>
                            <xs:documentation>The tunnel group to use when connecting to
the specified host.  This field is used in conjunction with the HostAddress value to form
a Group based URL.  NOTE: Group based URL support requires ASA version 8.0.3 or
later.</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:all>
                    <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:complexType>
                            <xs:simpleContent>
                                <xs:extension base="ns1:simpleBinary">
                                    <xs:attribute name="UserControllable"
type="ns1:UserControllableValues" default="true">
                                        <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:attribute>
                                </xs:extension>
                            </xs:simpleContent>
                        </xs:complexType>
                    </xs:element>
                    <xs:element name="ShowPreConnectMessage" default="false"
minOccurs="0">
                        <xs:annotation>
                            <xs:documentation>
```

```
                    This control enables an administrator to have a one time message
displayed prior to a users first connection attempt.  As an example, the message could be
used to remind a user to insert their smart card into it's reader.

                   The message to be used with this control is localizable and can be found
in the AnyConnect message catalog (default: "This is a pre-connect reminder message.").
                </xs:documentation>
                            </xs:annotation>
                            <xs:simpleType>
                                <xs:restriction base="xs:string">
                                    <xs:enumeration value="true">
                                        <xs:annotation>
                                            <xs:documentation>Show a pre-connect message
prior to users first connect attempt.</xs:documentation>
                                        </xs:annotation>
                                    </xs:enumeration>
                                    <xs:enumeration value="false">
                                        <xs:annotation>
                                            <xs:documentation>Do not show a pre-connect
message prior to users first connect attempt.</xs:documentation>
                                        </xs:annotation>
                                    </xs:enumeration>
                                </xs:restriction>
                            </xs:simpleType>
                        </xs:element>
                        <xs:element name="CertificateStore" default="All" minOccurs="0">
                            <xs:annotation>
                                <xs:documentation>
                    This setting allows an administrator to specify which certificate store
AnyConnect will use for locating certificates.

                    This setting only applies to the Microsoft Windows version of AnyConnect
and has no effect on other platforms.
                </xs:documentation>
                            </xs:annotation>
                            <xs:simpleType>
                                <xs:restriction base="xs:string">
                                    <xs:enumeration value="All">
                                        <xs:annotation>
                                            <xs:documentation>Use certificates from all
available certificate stores.</xs:documentation>
                                        </xs:annotation>
                                    </xs:enumeration>
                                    <xs:enumeration value="Machine">
                                        <xs:annotation>
                                            <xs:documentation>Use certificates only from the
Windows machine certificate store.</xs:documentation>
                                        </xs:annotation>
                                    </xs:enumeration>
                                    <xs:enumeration value="User">
                                        <xs:annotation>
                                            <xs:documentation>Use certificates only from the
Windows user certificate store.</xs:documentation>
                                        </xs:annotation>
                                    </xs:enumeration>
                                </xs:restriction>
                            </xs:simpleType>
                        </xs:element>
                        <xs:element name="CertificateStoreOverride" type="ns1:simpleBinary"
default="false" minOccurs="0">
                            <xs:annotation>
```

```
                            <xs:documentation>This setting allows an administrator to
direct AnyConnect to search for certificates in the Windows machine certificate store.
This is useful in cases where certificates are located in this store and users do not have
administrator privileges on their machine.</xs:documentation>
                        </xs:annotation>
                    </xs:element>
                    <xs:element name="AutoConnectOnStart" default="true" minOccurs="0">
                        <xs:annotation>
                            <xs:documentation>Controls AnyConnect client behavior when
started.  By default, the client will attempt to contact the last Gateway a user connected
to or the first one in the list from the AnyConnect profile.  In the case of
certificate-only authentication, this will result in the establishment of a VPN tunnel
when the client is started.</xs:documentation>
                        </xs:annotation>
                        <xs:complexType>
                            <xs:simpleContent>
                                <xs:extension base="ns1:simpleBinary">
                                    <xs:attribute name="UserControllable"
type="ns1:UserControllableValues" default="true">
                                        <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:attribute>
                                </xs:extension>
                            </xs:simpleContent>
                        </xs:complexType>
                    </xs:element>
                    <xs:element name="MinimizeOnConnect" default="true" minOccurs="0">
                        <xs:annotation>
                            <xs:documentation>Controls AnyConnect GUI behavior when a
VPN tunnel is established.  By default, the GUI will minimize when the VPN tunnel is
established.</xs:documentation>
                        </xs:annotation>
                        <xs:complexType>
                            <xs:simpleContent>
                                <xs:extension base="ns1:simpleBinary">
                                    <xs:attribute name="UserControllable"
type="ns1:UserControllableValues" default="true">
                                        <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:attribute>
                                </xs:extension>
                            </xs:simpleContent>
                        </xs:complexType>
                    </xs:element>
                    <xs:element name="LocalLanAccess" default="false" minOccurs="0">
                        <xs:annotation>
                            <xs:documentation>If Local LAN access is enabled for remote
clients on the Secure Gateway, this setting can be used to allow the user to accept or
reject this access.</xs:documentation>
                        </xs:annotation>
                        <xs:complexType>
                            <xs:simpleContent>
                                <xs:extension base="ns1:simpleBinary">
                                    <xs:attribute name="UserControllable"
type="ns1:UserControllableValues" default="true">
                                        <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:attribute>
                                    </xs:extension>
                                </xs:simpleContent>
                            </xs:complexType>
                        </xs:element>
                        <xs:element name="AutoReconnect" default="true" minOccurs="0">
                            <xs:annotation>
                                <xs:documentation>This setting allows an administrator to
control how a client will behave when the VPN tunnel is interrupted.  Control can
optionally be given to the user.</xs:documentation>
                            </xs:annotation>
                            <xs:complexType mixed="true">
                                <xs:sequence>
                                    <xs:element name="AutoReconnectBehavior"
default="DisconnectOnSuspend" minOccurs="0">
                                        <xs:complexType>
                                            <xs:simpleContent>
                                                <xs:extension base="ns1:AutoConnectValues">
                                                    <xs:attribute name="UserControllable"
type="ns1:UserControllableValues" 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:attribute>
                                                </xs:extension>
                                            </xs:simpleContent>
                                        </xs:complexType>
                                    </xs:element>
                                </xs:sequence>
                                <xs:attribute name="UserControllable"
type="ns1:UserControllableValues" 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:attribute>
                            </xs:complexType>
                        </xs:element>
                        <xs:element name="AutoUpdate" default="true" minOccurs="0">
                            <xs:annotation>
                                <xs:documentation>This setting allows the adminstrator to
turn off the dynamic update functionality of AnyConnect.  Control of this can also be
given to the user.</xs:documentation>
                            </xs:annotation>
                            <xs:complexType>
                                <xs:simpleContent>
                                    <xs:extension base="ns1:simpleBinary">
                                        <xs:attribute name="UserControllable"
type="ns1:UserControllableValues" 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:attribute>
                                    </xs:extension>
```

```
                            </xs:simpleContent>
                        </xs:complexType>
                    </xs:element>
                    <xs:element name="RSASecurIDIntegration" default="Automatic"
minOccurs="0">
                        <xs:annotation>
                            <xs:documentation>This setting allows the adminstrator to
control how the user will interact with RSA.  By default, AnyConnect will determine the
correct method of RSA interaction.  The desired setting can be locked down by the
administrator or control can be given to the user.</xs:documentation>
                        </xs:annotation>
                        <xs:complexType>
                            <xs:simpleContent>
                                <xs:extension base="ns1:RSAIntegrationValues">
                                    <xs:attribute name="UserControllable"
type="ns1:UserControllableValues" 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:attribute>
                                </xs:extension>
                            </xs:simpleContent>
                        </xs:complexType>
                    </xs:element>
                    <xs:element name="WindowsLogonEnforcement"
default="SingleLocalLogon" minOccurs="0">
                        <xs:annotation>
                            <xs:documentation>This preference allows an administrator to
control if more than one user may be logged into the client PC during the VPN connection
(Windows only).</xs:documentation>
                        </xs:annotation>
                        <xs:complexType>
                            <xs:simpleContent>
                                <xs:extension base="ns1:WindowsLogonEnforcementValues"/>
                            </xs:simpleContent>
                        </xs:complexType>
                    </xs:element>
                    <xs:element name="WindowsVPNEstablishment" default="LocalUsersOnly"
minOccurs="0">
                        <xs:annotation>
                            <xs:documentation>This preference allows an administrator to
control whether or not remote users may initiate a VPN connection (Windows
only).</xs:documentation>
                        </xs:annotation>
                        <xs:complexType>
                            <xs:simpleContent>
                                <xs:extension base="ns1:WindowsVPNEstablishmentValues"/>
                            </xs:simpleContent>
                        </xs:complexType>
                    </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:element name="MobilePolicy" minOccurs="0">
                        <xs:annotation>
                            <xs:documentation>Collection of policy settings specific to
the Windows Mobile version of AnyConnect that have no effect on other
platforms.</xs:documentation>
                        </xs:annotation>
                        <xs:complexType>
                            <xs:sequence>
                                <xs:element name="DeviceLockRequired" minOccurs="0">
                                    <xs:annotation>
                                        <xs:documentation>Indicates that a Windows
Mobile device must be configured with a password or PIN prior to establishing a VPN
connection.  This configuration is only valid on Windows Mobile devices that use the
Microsoft Default Local ation Provider (LAP).</xs:documentation>
                                    </xs:annotation>
                                    <xs:complexType>
                                        <xs:attribute name="MaximumTimeoutMinutes"
type="xs:unsignedInt">
                                            <xs:annotation>
                                                <xs:documentation>When set to
non-negative number, specifies the maximum number of minutes that must be configured
before device lock takes effect.  (WM5/WM5AKU2+)  </xs:documentation>
                                            </xs:annotation>
                                        </xs:attribute>
                                        <xs:attribute name="MinimumPasswordLength"
type="xs:unsignedInt">
                                            <xs:annotation>
                                                <xs:documentation>When set to a
non-negative number,  specifies that any PIN/password used for device lock must be equal
to or longer than the specified value, in characters. (WM5AKU2+)</xs:documentation>
                                            </xs:annotation>
                                        </xs:attribute>
                                        <xs:attribute name="PasswordComplexity">
                                            <xs:annotation>
```

```
                                                    <xs:documentation>When present checks for
the following password subtypes:  "alpha"  - Requires an alphanumeic password,  "pin"    -
Numeric PIN required, "strong" - Strong alphanumeric password defined by Microsoft as
containing at least 7 characters, including a minimum of 3 from the set of uppercase,
lowercase,  numerals, and punctuation characters. (WM5AKU2+)</xs:documentation>
                                                </xs:annotation>
                                                <xs:simpleType>
                                                    <xs:restriction base="xs:string">
                                                        <xs:enumeration value="alpha"/>
                                                        <xs:enumeration value="pin"/>
                                                        <xs:enumeration value="strong"/>
                                                    </xs:restriction>
                                                </xs:simpleType>
                                            </xs:attribute>
                                        </xs:complexType>
                                    </xs:element>
                                </xs:sequence>
                            </xs:complexType>
                        </xs:element>
                    </xs:all>
                </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: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>
                                            <xs:documentation>Subject Common
Name</xs:documentation>
                                        </xs:annotation>
                                    </xs:enumeration>
                                    <xs:enumeration value="DC">
                                        <xs:annotation>
                                            <xs:documentation>Domain
Component</xs:documentation>
                                        </xs:annotation>
                                    </xs:enumeration>
                                    <xs:enumeration value="SN">
                                        <xs:annotation>
                                            <xs:documentation>Subject Sur
Name</xs:documentation>
                                        </xs:annotation>
```

```
                                    </xs:enumeration>
                                    <xs:enumeration value="GN">
                                        <xs:annotation>
                                            <xs:documentation>Subject Given
Name</xs:documentation>
                                        </xs:annotation>
                                    </xs:enumeration>
                                    <xs:enumeration value="N">
                                        <xs:annotation>
                                            <xs:documentation>Subject Unstruct
Name</xs:documentation>
                                        </xs:annotation>
                                    </xs:enumeration>
                                    <xs:enumeration value="I">
                                        <xs:annotation>
                                            <xs:documentation>Subject
Initials</xs:documentation>
                                        </xs:annotation>
                                    </xs:enumeration>
                                    <xs:enumeration value="GENQ">
                                        <xs:annotation>
                                            <xs:documentation>Subject Gen
Qualifier</xs:documentation>
                                        </xs:annotation>
                                    </xs:enumeration>
                                    <xs:enumeration value="DNQ">
                                        <xs:annotation>
                                            <xs:documentation>Subject Dn
Qualifier</xs:documentation>
                                        </xs:annotation>
                                    </xs:enumeration>
                                    <xs:enumeration value="C">
                                        <xs:annotation>
                                            <xs:documentation>Subject
Country</xs:documentation>
                                        </xs:annotation>
                                    </xs:enumeration>
                                    <xs:enumeration value="L">
                                        <xs:annotation>
                                            <xs:documentation>Subject
City</xs:documentation>
                                        </xs:annotation>
                                    </xs:enumeration>
                                    <xs:enumeration value="SP">
                                        <xs:annotation>
                                            <xs:documentation>Subject
State</xs:documentation>
                                        </xs:annotation>
                                    </xs:enumeration>
                                    <xs:enumeration value="ST">
                                        <xs:annotation>
                                            <xs:documentation>Subject
State</xs:documentation>
                                        </xs:annotation>
                                    </xs:enumeration>
                                    <xs:enumeration value="O">
                                        <xs:annotation>
                                            <xs:documentation>Subject
Company</xs:documentation>
                                        </xs:annotation>
                                    </xs:enumeration>
                                    <xs:enumeration value="OU">
                                        <xs:annotation>
```

```
                                        <xs:documentation>Subject
Department</xs:documentation>
                                    </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="T">
                                    <xs:annotation>
                                        <xs:documentation>Subject
Title</xs:documentation>
                                    </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="EA">
                                    <xs:annotation>
                                        <xs:documentation>Subject Email
Address</xs:documentation>
                                    </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="ISSUER-CN">
                                    <xs:annotation>
                                        <xs:documentation>Issuer Common
Name</xs:documentation>
                                    </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="ISSUER-DC">
                                    <xs:annotation>
                                        <xs:documentation>Issuer Domain
Component</xs:documentation>
                                    </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="ISSUER-SN">
                                    <xs:annotation>
                                        <xs:documentation>Issuer Sur
Name</xs:documentation>
                                    </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="ISSUER-GN">
                                    <xs:annotation>
                                        <xs:documentation>Issuer Given
Name</xs:documentation>
                                    </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="ISSUER-N">
                                    <xs:annotation>
                                        <xs:documentation>Issuer Unstruct
Name</xs:documentation>
                                    </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="ISSUER-I">
                                    <xs:annotation>
                                        <xs:documentation>Issuer
Initials</xs:documentation>
                                    </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="ISSUER-GENQ">
                                    <xs:annotation>
                                        <xs:documentation>Issuer Gen
Qualifier</xs:documentation>
                                    </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="ISSUER-DNQ">
                                    <xs:annotation>
                                        <xs:documentation>Issuer Dn
Qualifier</xs:documentation>
                                    </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: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:attribute name="MatchCase" default="Enabled">
                        <xs:annotation>
                            <xs:documentation>Should the pattern matching applied to
"Pattern" be case sensitive?  Default is "Enabled" (case sensitive).</xs:documentation>
                        </xs:annotation>
                        <xs:simpleType>
                            <xs:restriction base="xs:string">
                                <xs:enumeration value="Enabled">
                                    <xs:annotation>
                                        <xs:documentation>perform case sensitive match with
pattern</xs:documentation>
                                    </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="Disabled">
                                    <xs:annotation>
                                        <xs:documentation>perform case in-sensitive match
with pattern</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>
           </xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="false">
                <xs:annotation>
                    <xs:documentation>
           </xs:documentation>
                </xs:annotation>
            </xs:enumeration>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="AutoConnectValues">
        <xs:restriction base="xs:string">
            <xs:enumeration value="DisconnectOnSuspend"/>
            <xs:enumeration value="ReconnectAfterResume"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="RSAIntegrationValues">
        <xs:restriction base="xs:string">
            <xs:enumeration value="Automatic"/>
            <xs:enumeration value="SoftwareToken"/>
            <xs:enumeration value="HardwareToken"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="UserControllableValues">
        <xs:restriction base="xs:string">
            <xs:enumeration value="true">
                <xs:annotation>
                    <xs:documentation source="user is allowed to control this setting."/>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="false">
                <xs:annotation>
                    <xs:documentation source="user is not allowed to control this
setting."/>
                </xs:annotation>
            </xs:enumeration>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="WindowsLogonEnforcementValues">
        <xs:restriction base="xs:string">
            <xs:enumeration value="SingleLogon">
                <xs:annotation>
                    <xs:documentation>Allows only one user during a VPN
connection</xs:documentation>
                </xs:annotation>
```

```
            </xs:enumeration>
            <xs:enumeration value="SingleLocalLogon">
                <xs:annotation>
                    <xs:documentation>Allows only one local user but many remote users
during a VPN connection</xs:documentation>
                </xs:annotation>
            </xs:enumeration>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="WindowsVPNEstablishmentValues">
        <xs:restriction base="xs:string">
            <xs:enumeration value="LocalUsersOnly">
                <xs:annotation>
                    <xs:documentation>Only local users may establish a VPN
connection</xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="AllowRemoteUsers">
                <xs:annotation>
                    <xs:documentation>Local and remote users may establish a VPN
connection</xs:documentation>
                </xs:annotation>
            </xs:enumeration>
        </xs:restriction>
    </xs:simpleType>
    <xs:element name="element1">
        <xs:complexType>
            <xs:sequence/>
        </xs:complexType>
    </xs:element>
</xs:schema>
```