APPENDIX C

Postprocessing Verification Errors

Command Usage Errors

Note Execution of the sscManagementUtility utility will result in either of the following:

- Success—No return message. Output file created with processed content.
- Failure—Error message returned. Output file created, but empty.

- Input file must have .xml file extension

  Command syntax example:

  ```
  sscManagementUtility validate -i distPkg
  ```

  Error message:

  ```
  Input file "distPkg" should have the ".xml" extension!
  ```

- Input file has an incorrect file extension

  Command syntax example:

  ```
  sscManagementUtility validate -i distPkg.txt
  ```

  Error message:

  ```
  Input file "distPkg.txt" should have the ".xml" extension!
  ```

- Command line syntax error

  Command syntax example:

  ```
  sscManagementUtility distPkg.xml distPkgSigned.xml
  ```

  Error message:

  ```
  Usage:
    sscManagementUtility [command] [command specific options]

  Command:
    help - print usage
    validate - check for validate configuration Xml file
    sign - validate and sign configuration Xml file
  ```

```
validate options:
  sscManagementUtility validate [-i <input file>]
  -i --in
     path to the original distribution package xml file
sign options:
  sscManagementUtility sign [-i <input file>] [-o <output file]
  -i --in
     path to the original distribution package xml file
  -o --out
     path to the processed and ready to deploy xml file
```

Most command syntax errors will display the command help information, as in this example.

XML Schema Validation Errors

Note Errors found by the utility's built-in XLM schema validation process are displayed as one of the following types:

parser error

Schema validity error

Some examples of schema validation errors are:

- An empty input file, distPkg.xml

  Error message:

  distPkg.xml:1: parser error : Document is empty

  distPkg.xml:1: parser error : Start tag expected, '<' not found

  failed to parse distPkg.xml

- Missing element closing tag (<credentialsStorage)

Tip Parsing errors are hierarchical in nature. Always resolve top-down. The actual error will most likely cause additional by-product errors to appear subsequently in the file.

In this case, fixing the single error in line 56, eliminates all of the reported parsing errors listed below.

Erroneous XML input text:

```
(line 54)   <collectionMethod>
(line 55)      <prompt>
(line 56)         <credentialsStorage
(line 57)            <logonSession/>
(line 58)         </credentialsStorage>
(line 59)      </prompt>
(line 60)    </collectionMethod>
```

Error message:

distPkg.xml:57: parser error : error parsing attribute name <logonSession/>

distPkg.xml:57: parser error : attributes construct error <logonSession/>

distPkg.xml:57: parser error : Couldn't find end of Start Tag credentialsStorage line 56 <logonSession/>

distPkg.xml:58: parser error : Opening and ending tag mismatch: prompt line 55 and credentialsStorage </credentialsStorage>

distPkg.xml:59: parser error : Opening and ending tag mismatch: collectionMethod line 54 and prompt </prompt>

distPkg.xml:60: parser error : Opening and ending tag mismatch: userAuthentication line 50 and collectionMethod </collectionMethod>

distPkg.xml:71: parser error : Opening and ending tag mismatch: authenticationNetwork line 49 and userAuthentication </userAuthentication>

distPkg.xml:83: parser error : Opening and ending tag mismatch: wifiNetwork line 44 and authenticationNetwork </authenticationNetwork>

distPkg.xml:84: parser error : Opening and ending tag mismatch: networks line 43 and wifiNetwork </wifiNetwork>

distPkg.xml:85: parser error : Opening and ending tag mismatch: configuration line 2 and networks </networks>

distPkg.xml:86: parser error : Extra content at the end of the document <stationSettings>

failed to parse distPkg.xml

- Missing attributes from base element

  Erroneous XML input text:

  ```
  <configuration>
  ```

  Error message:

  distPkg.xml:1: element configuration: Schema validity error : Element 'configuration': The attribute 'major_version' is required but missing.

  distPkg.xml:1: element configuration: Schema validity error : Element 'configuration': The attribute 'minor_version' is required but missing.

  distPkg.xml failed schema validation

- Elements out-of-order as required by schema

  Erroneous XML input text:

  ```
  <wifiNetwork>
    <ssid>MyCorpNet</ssid>
    <displayName>My Corporate Wi-Fi Network</displayName>
  ```

  Error message:

  distPkg.xml:45: element ssid: Schema validity error : Element 'ssid': This element is not expected. Expected is (displayName).

  distPkg.xml failed schema validation

- Missing a required element

  Erroneous XML input text:

  ```
  <userAuthentication>
    <autoConnect></autoConnect>
  ```

  Error message:

distPkg.xml:51: element autoConnect: Schema validity error : Element 'autoConnect': Missing child element(s). Expected is (connectBeforeLogon).

distPkg.xml failed schema validation

- Missing a required element value

  Erroneous XML input text:

  ```
  <wifiNetwork>
    <displayName></displayName>
    <ssid>MyCorpNet</ssid>
  ```

  Error message:

  distPkg.xml:45: element displayName: Schema validity error : Element 'displayName': [facet 'minLength'] The value has a length of '0'; this underruns the allowed minimum length of '1'.

  distPkg.xml:45: element displayName: Schema validity error : Element 'displayName': '' is not a valid value of the atomic type 'NonEmptyString'.

  distPkg.xml failed schema validation

- Element value data type error

  Erroneous XML input text:

  ```
  <allowedCredentialStorage>
    <duration>0</duration>
  </allowedCredentialStorage>
  ```

  Error message:

  distPkg.xml:38: element duration: Schema validity error : Element 'duration': '0' is not a valid value of the local atomic type.

  distPkg.xml failed schema validation

- Extra white space with an enumerated value

  Erroneous XML input text:

  ```
  <associationMode>
    <wpa-Enterprise>TKIP </wpa-Enterprise>
  </associationMode>
  ```

  Error message:

  distPkg.xml:81: element wpa-Enterprise: Schema validity error : Element 'wpa-Enterprise': [facet 'enumeration'] The value 'TKIP ' is not an element of the set{'AES', 'TKIP'}.

  distPkg.xml:81: element wpa-Enterprise: Schema validity error : Element 'wpa-Enterprise': 'TKIP ' is not a valid value of the atomic type 'WpaEncryption'.

  distPkg.xml failed schema validation

File Reference Error

The distribution package schema contains several elements that serve as a reference to an external file that is being designated for inclusion in the XML instance file.

Some examples of file reference errors are:

CA Certificate file:

- Incorrect path for file (designated file not present)

XML input text:

<caReference>E:\path\CaCertFile.pem</caReference>

Error message:

CA certificate file: "E:\path\CaCertFile.pem" doesn't exist

- Incorrect file type

  XML input text:

  <caReference>CaCertFile</caReference>

  Error message:

  CA certificate file: "CaCertFile" should be in .pem format

PAC file:

- Incorrect path for file (designated file not present)

  XML input text:

  <aIdReference>E:\path\pacRefFile</aIdReference>

  Error message:

  Pac file "E:\path\pacRefFile" processing error: can not open pac file E:\path\pacRefFile

- PAC password not provided or invalid

  XML input text: optional element, secretKey, not configured.

```
<reference>
  <aIdReference>pacRefFile</aIdReference>
</reference>
```

  XML input text: password value incorrect

```
<reference>
  <aIdReference>pacRefFile</aIdReference>
  <secretKey>1234</secretKey>
</reference>
```

  Error message:

  Pac file "pacRefFile" processing error: Invalid password to access pac file

Business Rules Verification Errors

The list of business rule verification errors, with examples, follows:

See the referenced element descriptions in Chapter 2, “Schema Elements” for more information.

- Rule 1.1 Limits on wired networks - only 1 allowed

  Erroneous XML input text:

```
<networks>
  <wiredNetwork>
    <displayName>Test 1.1-1</displayName>
    ...
  </wiredNetwork>
  <wiredNetwork>
    <displayName>Test 1.1-2</displayName>
```

```
    ...
  </wiredNetwork>
</networks>
```

Error message:

[Rule 1.1 violation] Only one wired network allowed!

See the description for element: *wiredNetwork.*

- Rule 1.2 Limits on networks with same SSID - only 1 allowed

  Erroneous XML input text:

```
<networks>
  <wifiNetwork>
    <displayName>Test 1.2-1</displayName>
    <ssid>SSID1</ssid>
    ...
  </wifiNetwork>
  <wifiNetwork>
    <displayName>Test 1.2-2</displayName>
    <ssid>SSID1</ssid>
    ...
  </wifiNetwork>
</networks>
```

  Error message:

  [Rule 1.2 violation] The following ssid(s) "SSID1" are duplicated!

  See the description for element: *ssid.*

- Rule 2.1.1 Authenticating wireless networks require the specification of at least one authentication method.

  Erroneous XML input text:

```
<wifiNetwork>
  <displayName>Test 2.1.2-1</displayName>
  ....
       <eapMethods/>
```

  Error message:

  [Rule 2.1.1 violation] Wifi authentication Networks "Test 2.1.1-1" should use at least one of the following methods: leap, eapTls, eapTtls, eapPeap or eapFast

  See the description for element: *eapMthods.*

- Rule 2.1.2 Authenticating wired networks require the specification of at least one authentication method.

  Erroneous XML input text:

```
<wiredNetwork>
  <displayName>Test 2.1.2-1</displayName>
  ....
       <eapMethods/>
```

  Error message:

  [Rule 2.1.2 violation] Wired authentication Network "Test 2.1.2-1" should use at least one of the following methods: eapMd5, eapMschapv2, eapGtc, leap, eapTls, eapTtls, eapPeap, eapFast

See the description for element: *eapMthods.*

- Rule 2.1.3 Authenticating networks using a tunneled authentication method require the specification of at least one corresponding inner method.

  Erroneous XML input text:

  Case 1—TTLS specific:

```
<displayName>Test 2.1.3-1</displayName>
...
   <eapMethods>
      <eapTtls>
         ...
         <innerMethods>
            <eap/>
         </innerMethods>
```

  Case 2—FAST, PEAP, TTLS:

```
<displayName>Test 2.1.3-5</displayName>
...
   <eapMethods>
      <eapPeap>
         ...
         <innerMethods/>
```

  Error message:

  [Rule 2.1.3 violation] Networks "Test 2.1.3-1", "Test 2.1.3-5" use a tunneled method without defining an inner method!

  See the description for element: *innerMethods, eap.*

- Rule 2.3 Static credentials (password) must be configured if the collection method is static.

  Erroneous XML input text:

```
<displayName>Test 2.2-2</displayName>
...
   <collectionMethod>
      <static/>
   </collectionMethod>
   <useAnonymousId>true</useAnonymousId>
   <staticIdentity encrypt="true">ItsMe</staticIdentity>
```

  Error message:

  [Rule 2.3 violation] Networks "Test 2.3-2" use static collection method without defining a static password!

  See the description for element: *static.*

- Rule 2.4a For user authentication, static credentials require a password-based EAP method.

  Erroneous XML input text:

  Case 1—Mismatch between settings for *collectionMethod* and *eapMethods*.

```
<displayName>Test 2.4a-1</displayName>
...
   <collectionMethod>
      <static/>
   </collectionMethod>
```

```
...
<eapMethods>
   <eapTls>
```

Case 2—Mismatch between settings for *collectionMethod* and *innerEapMethods*.

```
<displayName>Test 2.4a-3</displayName>
...
   <collectionMethod>
      <static/>
   </collectionMethod>
   ...
   <eapMethods>
      <eapFast>
         ...
         <innerEapMethods>
            <eapTls>
```

Error message:

> [Rule 2.4a violation] Networks "Test 2.4a-1", "Test 2.4a-3" use static credential collection for user authentication and should not define certificate based methods!

See the description for element: *static*.

- Rule 2.4b For machine authentication, static credentials require a password-based EAP method. Additionally, EAP FAST PACs can not be used.

  Erroneous XML input text:

  Case 1—Mismatch between settings for *collectionMethod* and *eapMethods*.

```
<displayName>Test 2.4b-1</displayName>
...
   <collectionMethod>
      <static/>
   </collectionMethod>
   ...
   <eapMethods>
      <eapTls>
      ...
      <eapFast>
```

  Case 2—Mismatch between settings for *collectionMethod* and *innerEapMethods*.

```
<displayName>Test 2.4b-3</displayName>
...
   <collectionMethod>
      <static/>
   </collectionMethod>
   ...
   <eapMethods>
      <eapPeap>
         ...
         <innerEapMethods>
            <eapTls>
```

  Error message:

  > [Rule 2.4b violation] Networks "Test 2.4b-1", "Test 2.4b-3" use static credential collection for machine authentication and should not define methods using pac(s) or certificates!

See the description for element: *static.*

- Rule 2.5 Client certificate usage requires configuring a certificate source.

  Erroneous XML input text:

```
<displayName>Test 2.5-1</displayName>
...
   <eapMethods>
      <eapFast>
         ...
         {Missing optional element certificateSource which is required in this case.}
         <innerEapMethods>
            <eapTls>
```

  Error message:

  [Rule 2.5 violation] Networks "Test 2.5-1" missing required certificate!

  See the description for element: *certificateSource.*

- Rule 2.6 In a user-only connection context configured for network connectivity before logon, client certificates are supported only through smartcards - client certificates in the Windows certificate store are not supported.

  Erroneous XML input text:

  Case 1—Outer method.

```
<displayName>Test 2.6-1</displayName>
...
   <userAuthentication>
      <autoConnect>
         <connectBeforeLogon>true</connectBeforeLogon>
      </autoConnect>
      ...
      <eapMethods>
         <eapTls>
            <certificateSource>
               <smartCardOrOsCertificate/> {Must be smartcard only.}
            </certificateSource>
```

  Case 2—Inner method.

```
<displayName>Test 2.6-2</displayName>
...
   <userAuthentication>
      <autoConnect>
         <connectBeforeLogon>true</connectBeforeLogon>
      </autoConnect>
      ...
      <eapMethods>
         <eapFast>
            <certificateSource>
               <smartCardOrOsCertificate/> {Must be smartcard only.}
            </certificateSource>
            <innerEapMethods>
               <eapTls>
```

  Error message:

[Rule 2.6 violation] Networks "Test 2.6-1", "Test 2.6-2" must be smartCardOnlyCertificate!

See the description for element: *connectBeforeLogon.*

- Rule 2.7 Mandating server validation requires the configuring of a trusted server certificate rule.

  Erroneous XML input text:

  Case 1—Outer method.

```
<displayName>Test 2.7-1</displayName>
...
      <eapMethods>
        <eapTls>
          <validateServerIdentity>true</validateServerIdentity>
          ...
    <serverValidation>
      {Missing optional element validationRules which is required in this case.}
      <trustAnyRootCaFromOs/>
    </serverValidation>
```

  Case 2—Inner method.

```
<displayName>Test 2.7-2</displayName>
...
      <eapMethods>
        <eapPeap>
          <validateServerIdentity>true</validateServerIdentity>
          ...
          <innerEapMethods>
            <eapTls>
    ...
    <serverValidation>
      {Missing optional element validationRules which is required in this case.}
      <trustAnyRootCaFromOs/>
    </serverValidation>
```

  Error message:

  [Rule 2.7 violation] Networks "Test 2.7-1", "Test 2.7-2" must be validated with either matchSubjectAlternateName or matchSubjectCommonName!

  See the description for element: *serverValidation.*

- Rule 2.8 Mandating server validation for FAST requires the configuring of either a trusted server certificate rule or a trusted server PAC rule.

  Erroneous XML input text:

```
<displayName>Test 2.8-1</displayName>
...
      <eapMethods>
        <eapFast>
          <validateServerIdentity>true</validateServerIdentity>
          ...
    <serverValidation>
      {Missing optional element validationRules or trustedServerIds, one of which is required
in this case.}
      <trustAnyRootCaFromOs/>
    </serverValidation>
```

Error message:

[Rule 2.8 violation] Networks "Test 2.8-1" must be validated with either matchSubjectAlternateName, matchSubjectCommonName or trustedServerIds!

See the description for element: *serverValidation.*

- Rule 2.9 Providing PACs for a network requires configuring FAST.

  Erroneous XML input text:

```
<displayName>Test 2.9-1</displayName>
...
      <pacs>
        <pac>
          <pacReference encrypt=”true”>pacFile</pacReference>
        </pac>
      </pacs>
      <eapMethods>
        <eapPeap> {Must be eapFast.}
      </eapMethods>
```

  Error message:

  [Rule 2.9 violation] Networks "Test 2.9-1" must have eapFast!

  See the description for element: *pacs.*

- Rule 2.11 Machine certificate must be from OS store.

  Erroneous XML input text:

```
<displayName>Test 2.11-2</displayName>
...
  <machineAuthentication>
    ...
        <certificateSource>
          <smartCardOnlyCertificate/> {Must be from OS.}
        </certificateSource>
```

  Error message:

  [Rule 2.11 violation] Networks "Test 2.11-2" must be configured to use the OS as a certificate source (machine authentication)!

  See the description for element: *smartCardOnlyCertificate.*

- Rule 2.12 The logical expression for the value of identity patterns must use the defined keywords and be properly bracketed.

  Case 1: Incorrect keyword

  Erroneous XML input text:

```
<displayName>Corporate User</displayName>
...
  <userAuthentication>
    ...
    <protectedIdentityPattern>&lt;user&gt;</protectedIdentityPattern>
```

  Error message:

  [Rule 2.12 violation] Network "Corporate User" protected identity pattern "<user>" is not valid: Unexpected token 'user' at character position 2.

Case 2: Incorrect bracketing

Erroneous XML input text:

```
<displayName>Corporate Machine</displayName>
...
   <machineAuthentication>
      ...
      <unprotectedIdentityPattern>host/&lt;fqhn&gt;&gt;</unprotectedIdentityPattern>
```

Error message:

[Rule 2.12 violation] Network "Corporate Machine" unprotected identity pattern "host/<fqhn>>" is not valid: Unexpected token '>' at the end of the identity pattern.

See the description for elements: *unprotectedIdentityPattern* and *protectedIdentityPattern.*

- Rule 2.13 & 2.14 Identity pattern keywords are connection-context and credential collection method dependent.

  Case 1: wrong connection context usage

  Erroneous XML input text:

```
<displayName>Test 2.13a</displayName>
...
   <machineAuthentication>
      ...
      <collectionMethod>
         <auto/>
      </collectionMethod>
      <unprotectedIdentityPattern>host/&lt;username&gt;</unprotectedIdentityPattern>
```

  Error message:

  [Rule 2.13a violation] Network "Test 2.13a" unprotected identity pattern "host/<username>" is not valid: token '<username>' at character position 6 may not be used with the configured machine connection context.

  Case 2: wrong credential collection method

  Erroneous XML input text:

```
<displayName>Test 2.14</displayName>
...
   <userAuthentication>
      ...
      <collectionMethod>
         <static/>
      </collectionMethod>
      <unprotectedIdentityPattern>&lt;username&gt;</unprotectedIdentityPattern>
```

  Error message:

  [Rule 2.14 violation] Network "Test 2.14" unprotected identity pattern "<username>" is not valid: token '<username>' at character position 1 may not be used with the static credential collection method with the configured user connection context.

  See the description for elements: *unprotectedIdentityPattern* and *protectedIdentityPattern.*

- Rule 2.15 Tunneled methods require a protected identity.

  Erroneous XML input text:

```
<displayName>Test 2.15</displayName>
...
   <userAuthentication>
      ...
      ...
      <unprotectedIdentityPattern>&lt;username&gt;@&lt;domain&gt;</unprotectedIdentityP
attern>
      <eapMethods>
         <eapFast>
```

Error message:

[Rule 2.15 violation] Network "Test 2.15" is not valid: a protected identity pattern must be supplied when configured for a tunneled EAP method but is not required when configured only for a non-tunneled method.

See the description for elements: *unprotectedIdentityPattern* and *protectedIdentityPattern.*

- Rule 3.1a Network policy for association mode must include *open* to support networks with no authentication or shared secrets.

  Erroneous XML input text:

```
<networkPolicy>
   <allowedAssociationModes>
      <wpa-Enterprise/> {No open networks configured.}
   </allowedAssociationModes>
....
<networks>
   <wifiNetwork>
      <displayName>Test 3.1a-1</displayName>
      ...
      <openNetworkUserConnection> {Not allowed}
      ...
   </wifiNetwork>
   <wiredNetwork>
      <displayName>Test 3.1a-2</displayName>
      <openNetworkMachineConnection/> {Not allowed}
   </wiredNetwork>
```

  Error message:

  [Rule 3.1a violation] Networks "Test 3.1a-1", "Test 3.1a-2" openNetworkMachineConnection or openNetworkUserConnection only allowed when Open mode is selected!

  See the description for element: *openNetworkUserConnection, openNetworkMachineConnection.*

- Rule 3.1b Network policy for association mode must include *wep* to support any WEP shared key network.

  Erroneous XML input text:

```
<networkPolicy>
   <allowedAssociationModes>
      <wpa-Enterprise/> {No WEP configured.}
   </allowedAssociationModes>
....
<networks>
   <wifiNetwork>
      <displayName>Test 3.1b-1</displayName>
```

```
...
<sharedKeyNetwork>
   ...
   <wep> {Not allowed}
```

Error message:

[Rule 3.1b violation] Networks "Test3.1b-1": wep with either ieee80211Authentication/open or ieee80211Authentication/shared only allowed when policy wep mode is selected!

See the description for element: *wep*.

- Rule 3.1c Network policy for association mode must include *wpa-Personal* to support a WPA-Personal shared key network.

  Erroneous XML input text:

```
<networkPolicy>
   <allowedAssociationModes>
      <wpa-Enterprise/> {No WPA-Personal configured.}
   </allowedAssociationModes>
....
<networks>
   <wifiNetwork>
      <displayName>Test 3.1c-1</displayName>
      ...
      <sharedKeyNetwork>
         ...
         <wpa> {Not allowed}
```

  Error message:

  [Rule 3.1c violation] Networks "Test 3.1c-1": keySettings/wpa only allowed when wpa-Personal mode is selected!

  See the description for element: *wpa*.

- Rule 3.1d Network policy for association mode must include *wpa2-Personal* to support a WPA2-Personal shared key network.

  Erroneous XML input text:

```
<networkPolicy>
   <allowedAssociationModes>
      <wpa-Enterprise/> {No WPA2-Personal configured.}
   </allowedAssociationModes>
....
<networks>
   <wifiNetwork>
      <displayName>Test 3.1d-1</displayName>
      ...
      <sharedKeyNetwork>
         ...
         <wpa2> {Not allowed}
```

  Error message:

  [Rule 3.1d violation] Networks "Test 3.1d-1": keySettings/wpa2 only allowed when wpa2-Personal mode is selected!

  See the description for element: *wpa2*.

- Rule 3.1e Network policy for association mode must include *wep* to support any dynamic WEP authenticating network.

  Erroneous XML input text:

  ```
  <networkPolicy>
    <allowedAssociationModes>
      <wpa-Enterprise/> {No WEP configured.}
    </allowedAssociationModes>
  ....
  <networks>
    <wifiNetwork>
      <displayName>Test 3.1e-1</displayName>
      ...
      <authenticationNetwork>
        ...
        <associationMode>
          <dynamicWep> {Not allowed}
  ```

  Error message:

  [Rule 3.1e violation] Network "Test 3.1e-1": associationMode/dynamicWep only allowed when policy wep mode is selected!

  See the description for element: *dynamicWep.*

- Rule 3.1f Network policy for association mode must include *wpa-Enterprise* to support a WPA-Enterprise network.

  Erroneous XML input text:

  ```
  <networkPolicy>
    <allowedAssociationModes>
      <wpa-Enterprise/> {No WPA-Enterprise configured.}
    </allowedAssociationModes>
  ....
  <networks>
    <wifiNetwork>
      <displayName>Test 3.1f-1</displayName>
      ...
      <authenticationNetwork>
        ...
        <associationMode>
          <wpa-Enterprise>TKIP</wpa-Enterprise> {Not allowed}
  ```

  Error message:

  [Rule 3.1f violation] Network "Test 3.1f-1": associationMode/wpa-Enterprise only allowed when wpa-Enterprise mode is selected!

  See the description for element: *wpa-Enterprise.*

- Rule 3.1g Network policy for association mode must include *wpa2-Enterprise* to support a WPA2-Enterprise network.

  Erroneous XML input text:

  ```
  <networkPolicy>
    <allowedAssociationModes>
      <wpa-Enterprise/> {No WPA2-Enterprise configured.}
    </allowedAssociationModes>
  ```

```
....
<networks>
   <wifiNetwork>
      <displayName>Test 3.1g-1</displayName>
      ...
      <authenticationNetwork>
         ...
         <associationMode>
            <wpa2-Enterprise>AES</wpa2-Enterprise> {Not allowed}
```

Error message:

[Rule 3.1g violation] Network "Test 3.1g-1": associationMode/wpa2-Enterprise only allowed when wpa2-Enterprise mode is selected!

See the description for element: *wpa2-Enterprise.*

- Rule 3.2a Network policy for EAP methods must include *eapMd5* to support authenticating wired networks configured for EAP-MD5.

  Erroneous XML input text:

```
<networkPolicy>
   <allowedEapMethods>
      <eapFast/> {No EAP-MD5 configured.}
   </allowedEapMethods>
....
<networks>
   <wiredNetwork>
      <displayName>Test 3.2a</displayName>
      ...
      <authenticationNetwork>
         ...
         <eapMethods>
            <eapMd5> {Not allowed}
```

  Error message:

  [Rule 3.2a violation] Network "Test 3.2a" : eapMethod/eapMd5 requires allowedEapMethods/eapMd5.

  See the description for element: *eapMethod/eapMd5.*

- Rule 3.2b Network policy for EAP methods must include *eapMschapv2* to support authenticating wired networks configured for EAP-MSCHAPv2.

  Erroneous XML input text:

```
<networkPolicy>
   <allowedEapMethods>
      <eapFast/> {No EAP-MSCHAPv2 configured.}
   </allowedEapMethods>
....
<networks>
   <wiredNetwork>
      <displayName>Test 3.2b</displayName>
      ...
      <authenticationNetwork>
```

```
...
<eapMethods>
   <eapMschapv2> {Not allowed}
```

Error message:

[Rule 3.2b violation] Network "Test 3.2b" : eapMethod/eapMschapv2 requires allowedEapMethods/eapMschapv2.

See the description for element: *eapMethod/eapMschapv2*.

- Rule 3.2c Network policy for EAP methods must include *eapGtc* to support authenticating wired networks configured for EAP-GTC.

  Erroneous XML input text:

```
<networkPolicy>
   <allowedEapMethods>
      <eapFast/> {No EAP-GTC configured.}
   </allowedEapMethods>
....
<networks>
   <wiredNetwork>
      <displayName>Test 3.2c</displayName>
      ...
      <authenticationNetwork>
         ...
         <eapMethods>
            <eapGtc> {Not allowed}
```

  Error message:

  [Rule 3.2c violation] Network "Test 3.2c" : eapMethod/eapGtc requires allowedEapMethods/eapGtc.

  See the description for element: *eapMethod/eapGtc*.

- Rule 3.2d Network policy for EAP methods must include *leap* to support authenticating wired or wireless networks configured for EAP-LEAP.

  Erroneous XML input text:

```
<networkPolicy>
   <allowedEapMethods>
      <eapFast/> {No EAP-LEAP configured.}
   </allowedEapMethods>
....
<networks>
   <wiredNetwork>
      <displayName>Test 3.2d</displayName>
      ...
      <authenticationNetwork>
         ...
         <eapMethods>
            <leap> {Not allowed}
```

  Error message:

  [Rule 3.2d violation] Network "Test 3.2d" : eapMethod/leap requires allowedEapMethods/leap.

  See the description for element: *eapMethod/leap*.

- Rule 3.2e Network policy for EAP methods must include *eapTls* to support authenticating wired or wireless networks configured for EAP-TLS.

  Erroneous XML input text:

  ```
  <networkPolicy>
    <allowedEapMethods>
      <eapFast/> {No EAP-TLS configured.}
    </allowedEapMethods>
  ....
  <networks>
    <wiredNetwork>
      <displayName>Test 3.2e</displayName>
      ...
      <authenticationNetwork>
        ...
        <eapMethods>
          <eapTls> {Not allowed}
  ```

  Error message:

  [Rule 3.2e violation] Network "Test 3.2e" : eapMethod/eapTls requires allowedEapMethods/eapTls.

  See the description for element: *eapMethod/eapTls.*

- Rule 3.2f Network policy for EAP methods must include *eapTtls* to support authenticating wired or wireless networks configured for EAP-TTLS.

  Erroneous XML input text:

  ```
  <networkPolicy>
    <allowedEapMethods>
      <eapFast/> {No EAP-TTLS configured.}
    </allowedEapMethods>
  ....
  <networks>
    <wiredNetwork>
      <displayName>Test 3.2f</displayName>
      ...
      <authenticationNetwork>
        ...
        <eapMethods>
          <eapTtls> {Not allowed}
  ```

  Error message:

  [Rule 3.2f violation] Network "Test 3.2f" : eapMethod/eapTtls requires allowedEapMethods/eapTtls.

  See the description for element: *eapMethod/eapTtls.*

- Rule 3.2g Network policy for EAP methods must include *eapPeap* to support authenticating wired or wireless networks configured for EAP-PEAP.

  Erroneous XML input text:

  ```
  <networkPolicy>
    <allowedEapMethods>
      <eapFast/> {No EAP-PEAP configured.}
    </allowedEapMethods>
  ```

```
....
<networks>
   <wiredNetwork>
      <displayName>Test 3.2g</displayName>
      ...
      <authenticationNetwork>
         ...
         <eapMethods>
            <eapPeap> {Not allowed}
```

Error message:

[Rule 3.2g violation] Network "Test 3.2g" : eapMethod/eapPeap requires allowedEapMethods/eapPeap.

See the description for element: *eapMethod/eapPeap.*

- Rule 3.2h Network policy for EAP methods must include *eapFast* to support authenticating wired or wireless networks configured for EAP-FAST.

  Erroneous XML input text:

```
<networkPolicy>
   <allowedEapMethods>
      <eapPeap/> {No EAP-FAST configured.}
   </allowedEapMethods>
....
<networks>
   <wiredNetwork>
      <displayName>Test 3.2h</displayName>
      ...
      <authenticationNetwork>
         ...
         <eapMethods>
            <eapFast> {Not allowed}
```

  Error message:

  [Rule 3.2h violation] Network "Test 3.2h" : eapMethod/eapFast requires allowedEapMethods/eapFast.

  See the description for element: *eapMethod/eapFast.*

- Rule 3.3a Network policy for credential storage must include *forever* to support networks with credentials that are to be saved across logins.

  Erroneous XML input text:

```
<networkPolicy>
   <allowedCredentialStorage>
       {forever not configured.}
   </allowedCredentialStorage>
....
<networks>
   <wiredNetwork>
      <displayName>Test 3.3a</displayName>
      ...
      <authenticationNetwork>
```

```
...
   <credentialsStorage>
      <forever> {Not allowed}
```

Error message:

[Rule 3.3a violation] Networks "Test 3.3a": credentialStorage/forever requires that networkPolicy/allowedCredentialStorage/forever be selected.

See the description for element: *credentialStorage.*

- Rule 3.3b Network policy for credential storage must include *logonSession* to support networks with credentials that are to be saved only during the current login session.

  Erroneous XML input text:

```
<networkPolicy>
   <allowedCredentialStorage>
       {logonSession not configured.}
   </allowedCredentialStorage>
....
<networks>
   <wiredNetwork>
      <displayName>Test 3.3b</displayName>
      ...
      <authenticationNetwork>
         ...
            <credentialsStorage>
               <logonSession> {Not allowed}
```

  Error message:

  [Rule 3.3b violation] Networks "Test 3.3b": credentialStorage/logonSession requires that networkPolicy/allowedCredentialStorage/logonSession be selected.

  See the description for element: *credentialStorage.*

- Rule 3.3c Network policy for credential storage must include *duration* to support networks with credentials that are to be saved for a preconfigured time period.

  Erroneous XML input text:

```
<networkPolicy>
   <allowedCredentialStorage>
       {duration not configured.}
   </allowedCredentialStorage>
....
<networks>
   <wiredNetwork>
      <displayName>Test 3.3c</displayName>
      ...
      <authenticationNetwork>
         ...
            <credentialsStorage>
               <duration> {Not allowed}
```

  Error message:

  [Rule 3.3c violation] Networks "Test 3.3c": credentialStorage/duration requires that networkPolicy/allowedCredentialStorage/duration be selected.

  See the description for element: *credentialStorage.*

- Rule 3.4 If the network policy requires server validation, then all networks must be configured accordingly.

  Erroneous XML input text:

```
<networkPolicy>
   <serverValidationPolicy>
      <alwaysValidate> {Validation required.}
....
<networks>
   <wifiNetwork>
      <displayName>Test 3.4-1</displayName>
      ...
      <authenticationNetwork>
         ...
         <eapMethods>
            <eapFast>
               <validateServerIdentity>false</validateServerIdentity> {Not allowed}
...
   <wifiNetwork>
      <displayName>Test 3.4-2</displayName>
      ...
      <authenticationNetwork>
         ...
         <eapMethods>
            <eapFast>
               <validateServerIdentity>true</validateServerIdentity>
               ...
                  <innerEapMethods>
                     <eapTls>
                        <validateServerIdentity>false</validateServerIdentity> {Not allowed}
```

  Error message:

  [Rule 3.4 violation] Networks "Test 3.4-1", "Test 3.4-2": each Tls, Ttls, Peap, Fast method should require server identity validation in conformance with the policy.

  See the description for element: *validateServerIdentity.*

- Rule 3.5 The logical expression for the client certificate Extended Key Usage filtering must use the defined keywords and be properly parenthesized.

  Case 1—Incorrect keyword

  Erroneous XML input text:

```
<networkPolicy>
   ...
   <allowedClientCertificates>
      <certificateEkuFilterExpression>(SmartCardLogon or not
IpsecTunnel1)</certificateEkuFilterExpression> {keyword misspelled}
   </allowedClientCertificates>
</networkPolicy>
```

  Error message:

  [Rule 3.5 violation] The certificate Extended Key Usage (EKU) expression is not valid: Unexpected token 'IpsecTunnel1' at character position 24

  Case 2—Errored expression

Erroneous XML input text:

```
<networkPolicy>
   ...
   <allowedClientCertificates>
      <certificateEkuFilterExpression>(SmartCardLogon or not
IpsecTunnel</certificateEkuFilterExpression> {missing closing parenthesis}
   </allowedClientCertificates>
</networkPolicy>
```

Error message:

[Rule 3.5 violation] The certificate Extended Key Usage (EKU) expression is not valid: Expected ')' at the end of the expression.

See the description for element: *certificateEkuFilterExpression.*

- Rule 4 End-user is not permitted to override an initial setting of a single-homed network.

  Erroneous XML input text:

  ```
  <networkPolicy>
     <allowUserSimultaneousConnectionsControl>true</allowUserSimultaneousConnectionsCo
  ntrol> {Not allowed.}
  ....
  <stationSettings>
     <simultaneousConnections>singleHomed</simultaneousConnections>
  ```

  Error message:

  [Rule 4 violation] If stationSettings/simultaneousConnections is singleHome, networkPolicy/allowUserSimultaneousConnectionsControl must be false!

  See the description for element: *allowUserSimultaneousConnectionsControl.*

- Rule 5a SSC must be configured for at least one media type.

  Erroneous XML input text:

  ```
  <userControlPolicy>
     ...
     <allowedMedia></allowedMedia> {Missing a child element.}
  ```

  Error message:

  [Rule 5a violation] At least one media type must be specified for userControyPolicy/allowedMedia!

  See the description for element: *allowedMedia.*

- Rule 5b The general policy must be configured to allow wired media to support the configuring of a wired network.

  Erroneous XML input text:

  ```
  <networks>
     <wiredNetwork> {Not allowed.}
        <displayName>Test 5b</displayName>
  ...
  <userControlPolicy>
     ...
     <allowedMedia>
        <wifi/> {Wired not configured.}
     </allowedMedia>
  ```

Error message:

[Rule 5b violation] Network "Test 5b": (wired) may not be present unless userControlPolicy/allowedMedia/wired is present.

See the description for element: *wiredNetwork*.

- Rule 5c The general policy must be configured to allow wireless media to support the configuring of a Wi-Fi network.

  Erroneous XML input text:

```
<networks>
   <wifiNetwork> {Not allowed.}
      <displayName>Test 5c</displayName>
...
<userControlPolicy>
   ...
   <allowedMedia>
      <wired/> {Wireless not configured.}
   </allowedMedia>
```

  Error message:

  [Rule 5c violation] Network "Test 5c": (wifi) may not be present unless userControlPolicy/allowedMedia/wifi is present.

  See the description for element: *wifiNetwork*.

Scripting Errors

Return codes are implemented for identification of failures at each phase of processing. The following lists all the application return codes:

- 0 Success
- 1 Wrong arguments
- 2 Unknown configuration file version
- 3 Schema validation failed
- 4 Business rules validation failed
- 5 Referenced files cannot be found
- -1 Unexpected error (see stderr for details)