Creating Geo/IP Files

This section describes the Geo/IP configuration file used by a Delivery Service to specify the geographic regions in which client requests are either allowed or denied.

The Geo/IP file is an XML file used to specify the geographic regions that are allowed or denied access to a Delivery Service, as well as the IP network that is allowed or denied access.

In addition to the allowed and denied geographical and network information, two optional elements are created for documentation purposes: a revision value to specify the version of the file and a customer name.

The Geo/IP files can be created using any ASCII text-editing tool. For information about uploading or importing a Geo/IP file, see the "Authorization Plugins" section on page 5-22.

The XML Schema file describes and dictates the content of the XML file. The CDSAuthorization.xsd file contains the XML schema. To view or download a copy of the CDSAuthorization.xsd, see the "Viewing or Downloading XML Schema Files" section on page 6-24.

Table D-1 defines the Geo/IP file elements.

Table D-1   Geo/IP File Elements

Tag	Element	Value	Description
Allow	pattern	file type suffix	Specifies a pattern that the client's URL request must match. The pattern can be any substring of the client's URL request. An asterisk (*) means all URLs.
	network	IP address	Specifies the IP address range of the subnet using classless inter-domain routing (CIDR) notation (A.B.C.D/N) for IPv4 addresses. Both IPv4 and IPv6 addresses are supported.
	Geo		Describes the geographic region by country, state, city, Netspeed, connection_type, line_speed, asn, carrier, anonymizer_status, and generic attribute.
Deny	pattern	file type suffix	Specifies a pattern that the client's URL request must match. The pattern can be any substring of the client's URL request. An asterisk (*) means all URLs.
	network	IP address	Specifies the IP address range of the subnet using classless inter-domain routing (CIDR) notation (A.B.C.D/N).
	Geo		Describes the geographic region by country, state, city, Netspeed, connection_type, line_speed, asn, carrier, anonymizer_status, and generic attribute.

Table D-1   Geo/IP File Elements (continued)

Tag	Element	Value	Description
Order	—	Allow, Deny	The order in which to apply the allow and deny rules. One of the following: • Allow • Deny • Allow, Deny • Deny, Allow
Geo	Country name	country name	Specifies the full name of the country.
	State name	state name	Specifies the full name of the state.
	City name	city name	Specifies the full name of the city.
	Netspeed	netspeed	Specifies the traffic in the specified network device.
	Connection_type	connection type	Specifies the connection type.
	Line_speed	line speed	Specifies the speed of the connection. The possible values are: • Low • Medium • High
	asn		Specifies the Autonomous System Number (ASN), that is corresponding to the senders IP address as retrieved from geo server/local geo cache. ASN value provided is a 32 bit integer.
	carrier		The carrier field provides the name of the organization responsible for the traffic carried on a particular network or set of networks designated as Autonomous System (AS).
CDSAuthorization	Revision	1.0	The revision of this file.
	CustomerName	customer name	The customer associated with this file.
	Allow	—	The CDSAuthorization tag can have one Allow element.
	Deny	—	The CDSAuthorization tag can have one Deny element.
	Order	—	The CDSAuthorization tag can have one Order element.

Note   For the Geo element, the country, state, and city names all must match what is used by the Geo-Location server. The names are case sensitive. If the country matches but the state and city names do not match, the request is denied. You can specify just the country, or the country and state, or the country, state, and city.

If the Geo element is defined, the Geo-Location servers are down or are not configured, and the client information is not found in the SE cache, a request denied message is returned to the client. The type of message that is returned depends on the protocol engine (for example, the Flash Media Streaming engine sends "Denied by auth server"). However, the client receives the same denied message from the protocol engine whether the client is denied based on the Authorization Service configuration, or based on the Geo-Location servers being down and the client information not being available in the SE cache.

Starting with Release 3.3, the Geo-Location servers support both IPv6 and IPv4 client configuration; therefore, geographic location authorization of client requests are supported for both IPv4 addresses and IPv6 addresses.

For more information on the Geo-Location server, see the "Geo-Location Servers" section on page 4-104.

Processing Order

When Geo/IP and Service Rules are configured, each client request goes through the following processing order:

1. SE bypass (this is used for multi-tiered SEs), no configuration is required

2. Service rules

3. Geo/IP Network element

4. Geo/IP Geo element

Service Rule Config File

If the Service Rule file exists for the Delivery Service, it is processed before the Geo/IP file. If after going through the Service Rule conditions the client request is allowed, and there is a Geo/IP file associated with the Delivery Service, the client request goes through all of the conditions defined in the Geo/IP file before the request is finally allowed.

Understanding the Allow and Deny Conditions

The Geo/IP file allows client requests based on the Pattern element defined and either the Network element defined or Geo element defined, or both the Network and Geo elements defined.

> **Note**   At least one Pattern element is required for the Allow tag and at least one Pattern element is required for the Deny tag.
>
> At least one Network element or Geo element is required for the Allow tag and at least one Network element or Geo element is required for the Deny tag.

Allow Conditions

Each element that is defined in the Allow tag (Pattern, Network, and Geo) must be matched for the client request to be allowed.

If only the Network element is defined for the Allow tag (no Geo element is defined), then the client request must only match the Network element for the request to be allowed. If only the Geo element tag is defined (no Network element is defined), then the client request must only match the Geo element for the request to be allowed.

If both the Network element and the Geo element are defined for the Allow tag, the client request must match both the Network and Geo element for the client request to be allowed.

If the Allow tag has multiple Network and Geo elements, at least one Network element must be matched and at least one Geo element must be matched for the client request to be allowed.

Deny Conditions

At least one of the elements that is defined in the Deny tag (Pattern, Network, and Geo) must be matched for the client request to be denied.

If both the Network element and the Geo element are defined for the Deny tag, the client request must only match one of the conditions (either Network or Geo), for the client request to be denied.

If the Deny tag has multiple Network and Geo elements, only one condition must be matched (either Network or Geo) for the client request to be denied.

Order Tag

The Order tag defines the order in which to apply the Allow and Deny tags. The Order tag can have the following settings:

- Allow, Deny
- Deny, Allow
- Allow
- Deny

Allow, Deny

If the Order tag is set to <Allow, Deny>, and both the Network element and the Geo element are defined for both the Allow tag and the Deny tag, first the request is compared to the Network element in the Allow tag, followed by the Network element in the Deny tag. Then the request is compared with the Geo element in the Allow tag, followed by the Geo element in the Deny tag.

Note If the request is denied during the comparison with the Network element (either by not matching the Allow condition or by matching the Deny condition), no further comparison is performed even if the Geo element is defined.

Deny, Allow

If the Order tag is defined as <Deny, Allow>, and both the Network element and the Geo element are defined for both the Allow tag and the Deny tag, first the request is compared to the Network element in the Deny tag, followed by the Network element in the Allow tag. Then the request is compared with the Geo element in the Deny tag, followed by the Geo element in the Allow tag.

Note If the request is denied during the comparison with the Network element (either by matching the Deny condition or by not matching the Allow condition), no further comparison is performed even if the Geo element is defined.

Allow

If the Order tag is only defined as Allow, and both the Allow tag and Deny tag are defined, the request is only compared with the Allow tag conditions. The Deny tag conditions are ignored. If the request does not match the Network element in the Allow tag, no further comparison is performed even if the Geo element is defined. If the request matches the Network element in the Allow tag, then the request is compared with Geo element next.

Deny

If the Order tag is only defined as Deny, and both the Allow tag and Deny tag are defined, the request is only compared with the Deny tag conditions. The Allow tag conditions are ignored. If the request matches the Network element in the Deny tag, no further comparison is performed even if the Geo element is defined.

Order Scenarios

Table D-2 lists the different Order tag settings and outcomes for single elements (Network or Geo) defined in each Allow and Deny tag, and multiple elements defined in each Allow and Deny tag. A reference to an XML example is provided for each scenario.

Table D-2   Geo/IP XML Order Scenarios

Case	Order	Single Element	Multiple Elements
1	Allow, Deny	If Allow element does not match, deny the request. See Example 3, page D-6.	If Allow Network element does not match, the request is denied and no further checking is performed. See Example 9, page D-9.
2	Allow, Deny	If Allow element matches, allow the request. SeeExample 1, page D-5.	If Allow Network element matches, check Allow Geo element. See Example 11, page D-10.
3	Deny, Allow	If Deny element does not match, check Allow element and take action. See Example 4, page D-7.	If Deny Network element does not match, check Allow Network element. If Allow Network element matches, check Deny Geo element. If Deny Geo element does not match, check Allow Geo element. If Allow Geo element matches, allow the request. If at any point along the above checking path, the Deny element matches, or the Allow element does not match; the request is denied.
4	Deny, Allow	If Deny element matches, deny the request. See Example 2, page D-6.	If Deny Network tag matches, request is denied. See Example 15, page D-12.
5	Allow	If Allow element does not match, deny the request. See Example 8, page D-8.	First check the Allow Network element, if it is configured. Then check the Allow Geo element if it is configure. See Example 14, page D-11.
6	Allow	If Allow element matches, allow the request. See Example 7, page D-8. First check the Allow Network element, if more than one Network element is configured, check each one. See Example 16, page D-12.	
7	Deny	If Deny element does not match, allow the request. SeeExample 6, page D-8.	First check the Deny Network element, if it is configured. Then check the Deny Geo element if it is configured. See Example 13, page D-11.
8	Deny	If Deny element matches, deny the request. See Example 5, page D-7.	

> **Note**   The allowed or denied results for the following examples are based on a client IP address of 209.165.201.30, which for the purposes of these examples belongs to India.

Example 1

The result in this example is that the client request is allowed.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
  <Revision>1.0</Revision>
  <CustomerName>Service Provider Ultra-CDN</CustomerName>
  <Allow>
    <Pattern>*</Pattern>
```

```
                                <Geo>
                                  <Country name="india"/>
                                  <Line_speed>high</Line_speed>
                                  <Field name="postal_code" value="200000" />
                                  <Field name="time_zone" value="8" />
                                </Geo>
                            </Allow>
                            <Deny>
                                <Pattern>*</Pattern>
                                <Geo>
                                  <Country name="ALL"/>
                                </Geo>
                            </Deny>
                            <Order>Allow,Deny</Order>
                        </CDSAuthorization>
```

Example 2

The result in this example is that the client request is denied.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
    <Revision>1.0</Revision>
    <CustomerName>Service Provider Ultra-CDN</CustomerName>
    <Allow>
        <Pattern>*</Pattern>
        <Geo>
          <Country name="india"/>
          <Line_speed>high</Line_speed>
          <Field name="postal_code" value="200000" />
          <Field name="time_zone" value="8" />
        </Geo>
    </Allow>
    <Deny>
        <Pattern>*</Pattern>
        <Geo>
          <Country name="ALL"/>
        </Geo>
    </Deny>
    <Order>Deny,Allow</Order>
</CDSAuthorization>
```

Example 3

The result in this example is that the client request is denied.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
    <Revision>1.0</Revision>
    <CustomerName>Service Provider Ultra-CDN</CustomerName>
    <Allow>
        <Pattern>*</Pattern>
        <Geo>
         <Country name="united states"/>
         <Line_speed>high</Line_speed>
         <Field name="postal_code" value="200000" />
          <Field name="time_zone" value="8" />
        </Geo>
    </Allow>
    <Deny>
        <Pattern>*</Pattern>
        <Geo>
            <Country name="ALL"/>
```

```
    </Geo>
  </Deny>
  <Order>Allow,Deny</Order>
</CDSAuthorization>
```

Example 4

The result in this example is that the client request is allowed.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
  <Revision>1.0</Revision>
  <CustomerName>Service Provider Ultra-CDN</CustomerName>
  <Allow>
    <Pattern>*</Pattern>
    <Geo>
      <Country name="ALL"/>
      <Line_speed>high</Line_speed>
      <Field name="postal_code" value="200000" />
      <Field name="time_zone" value="8" />
    </Geo>
  </Allow>
  <Deny>
  <Pattern>*</Pattern>
    <Geo>
      <Country name="united states"/>
    </Geo>
  </Deny>
  <Order>Deny,Allow</Order>
</CDSAuthorization>
```

Example 5

The result in this example is that the client request is denied.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
  <Revision>1.0</Revision>
  <CustomerName>Service Provider Ultra-CDN</CustomerName>
  <Allow>
    <Pattern>*</Pattern>
    <Geo>
      <Country name="ALL"/>
      <Line_speed>high</Line_speed>
      <Field name="postal_code" value="200000" />
      <Field name="time_zone" value="8" />
    </Geo>
  </Allow>
  <Deny>
    <Pattern>*</Pattern>
    <Geo>
      <Country name="india"/>
    </Geo>
  </Deny>
  <Order>Deny</Order>
</CDSAuthorization>
```

Example 6

The result in this example is that the client request is allowed.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
  <Revision>1.0</Revision>
  <CustomerName>Service Provider Ultra-CDN</CustomerName>
  <Allow>
    <Pattern>*</Pattern>
    <Geo>
     <Country name="ALL"/>
     <Line_speed>high</Line_speed>
     <Field name="postal_code" value="200000" />
     <Field name="time_zone" value="8" />
    </Geo>
  </Allow>
  <Deny>
    <Pattern>*</Pattern>
    <Geo>
     <Country name="united states"/>
    </Geo>
  </Deny>
  <Order>Deny</Order>
</CDSAuthorization>
```

Example 7

The result in this example is that the client request is allowed.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
  <Revision>1.0</Revision>
  <CustomerName>Service Provider Ultra-CDN</CustomerName>
  <Allow>
    <Pattern>*</Pattern>
    <Geo>
     <Country name="india"/>
     <Line_speed>high</Line_speed>
     <Field name="postal_code" value="200000" />
     <Field name="time_zone" value="8" />
    </Geo>
  </Allow>
  <Deny>
    <Pattern>*</Pattern>
    <Geo>
     <Country name="united states"/>
    </Geo>
  </Deny>
  <Order>Allow</Order>
</CDSAuthorization>
```

Example 8

The result in this example is that the client request is denied.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
  <Revision>1.0</Revision>
  <CustomerName>Service Provider Ultra-CDN</CustomerName>
  <Allow>
    <Pattern>*</Pattern>
    <Geo>
     <Country name="india"/>
```

```
    <Line_speed>high</Line_speed>
    <Field name="postal_code" value="200000" />
    <Field name="time_zone" value="8" />
  </Geo>
</Allow>
<Deny>
  <Pattern>*</Pattern>
  <Geo>
    <Country name="united states"/>
  </Geo>
</Deny>
<Order>Allow</Order>
</CDSAuthorization>
```

Example 9

The result in this example is that the client request is denied.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
  <Revision>1.0</Revision>
  <CustomerName>Service Provider Ultra-CDN</CustomerName>
  <Allow>
    <Pattern>*</Pattern>
    <Network>127.0.0.1/32</Network>
    <Geo>
      <Country name="india"/>
      <Line_speed>high</Line_speed>
      <Field name="postal_code" value="200000" />
      <Field name="time_zone" value="8" />
    </Geo>
  </Allow>
  <Deny>
    <Pattern>*</Pattern>
    <Geo>
      <Country name="ALL"/>
    </Geo>
  </Deny>
  <Order>Allow,Deny</Order>
</CDSAuthorization>
```

Example 10

The result in this example is that the client request is allowed.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
  <Revision>1.0</Revision>
  <CustomerName>Service Provider Ultra-CDN</CustomerName>
  <Allow>
    <Pattern>*</Pattern>
    <Network>209.165.201.0/27</Network>
    <Geo>
      <Country name="india"/>
      <Line_speed>high</Line_speed>
      <Field name="postal_code" value="200000" />
      <Field name="time_zone" value="8" />
    </Geo>
  </Allow>
  <Deny>
    <Pattern>*</Pattern>
    <Geo>
      <Country name="ALL"/>
```

```
        </Geo>
      </Deny>
      <Order>Allow,Deny</Order>
</CDSAuthorization>
```

Example 11

The result in this example is that the client request is denied. In the example below, first the Allow Network element is checked, which matches the client, so the intermediate result is the request is allowed, but the Allow Geo element is checked, which does not match the client request, so the final result is the request is denied.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
  <Revision>1.0</Revision>
  <CustomerName>Service Provider Ultra-CDN</CustomerName>
  <Allow>
    <Pattern>*</Pattern>
    <Network>209.165.201.0/27</Network>
    <Geo>
      <Country name="india"/>
      <Line_speed>high</Line_speed>
      <Field name="postal_code" value="200000" />
      <Field name="time_zone" value="8" />
    </Geo>
  </Allow>
  <Deny>
    <Pattern>*</Pattern>
    <Geo>
      <Country name="ALL"/>
    </Geo>
  </Deny>
  <Order>Allow,Deny</Order>
</CDSAuthorization>
```

Example 12

The result in this example is that the client request is denied. In the example below, first the Allow Network element is checked, which does not match the client, so the request is denied. No further checking is performed.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
  <Revision>1.0</Revision>
  <CustomerName>Service Provider Ultra-CDN</CustomerName>
  <Allow>
    <Pattern>*</Pattern>
    <Network>10.1.1.1/32</Network>
    <Geo>
      <Country name="india"/>
      <Line_speed>high</Line_speed>
      <Field name="postal_code" value="200000" />
      <Field name="time_zone" value="8" />
    </Geo>
  </Allow>
  <Deny>
    <Pattern>*</Pattern>
    <Network>1.1.1.1/32</Network>
    <Geo>
      <Country name="ALL"/>
    </Geo>
  </Deny>
```

```
  <Order>Allow,Deny</Order>
</CDSAuthorization>
```

Example 13

The result in this example is that the client request is denied. In the example below, first the Deny Network element is checked, which matches the client, so the request is denied. No further checking is performed.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
  <Revision>1.0</Revision>
  <CustomerName>Service Provider Ultra-CDN</CustomerName>
  <Allow>
    <Pattern>*</Pattern>
    <Network>10.1.1.1/32</Network>
    <Geo>
      <Country name="united states"/>
      <Line_speed>high</Line_speed>
      <Field name="postal_code" value="200000" />
      <Field name="time_zone" value="8" />
    </Geo>
  </Allow>
  <Deny>
    <Pattern>*</Pattern>
    <Network>209.165.201.0/27</Network>   --->Final result Deny (so don't process further)
    <Geo>
      <Country name="ALL"/>
    </Geo>
  </Deny>
  <Order>Deny</Order>
</CDSAuthorization>
```

Example 14

The result in this example is that the client request is denied. In the example below, first the Allow Network element is checked, which does not match the client, so the request is denied. No further checking is performed.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
  <Revision>1.0</Revision>
  <CustomerName>Service Provider Ultra-CDN</CustomerName>
  <Allow>
    <Pattern>*</Pattern>
    <Network>10.1.1.1/32</Network>
    <Geo>
      <Country name="united states"/>
      <Line_speed>high</Line_speed>
      <Field name="postal_code" value="200000" />
      <Field name="time_zone" value="8" />
    </Geo>
  </Allow>
  <Deny>
    <Pattern>*</Pattern>
    <Network>209.165.201.0/27</Network>
    <Geo>
      <Country name="ALL"/>
    </Geo>
  </Deny>
  <Order>Allow</Order>
</CDSAuthorization>
```

Example 15

The result in this example is that the client request is denied. In the example below, first the Deny Network element is checked, which matches the client, so the request is denied. No further checking is performed.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
<Revision>1.0</Revision>
<CustomerName>Service Provider Ultra-CDN</CustomerName>
<Allow>
<Pattern>*</Pattern>
<Network>10.1.1.1/32</Network>
<Geo>
<Country name="united states"/>
<Line_speed>high</Line_speed>
<Field name="postal_code" value="200000" />
<Field name="time_zone" value="8" />

</Geo>
</Allow>
<Deny>
<Pattern>*</Pattern>
<Network>209.165.201.0/27</Network>
<Geo>
<Country name="india"/>
</Geo>
</Deny>
<Order>Deny,Allow</Order>
</CDSAuthorization>
```

Example 16

The result in this example is that the client request is allowed. In the example below, first the Allow Network element is checked, the client IP address only has to match one Network element, so even though the first two Network elements do not match, the third Network element does match and the client request is allowed. No further checking is performed.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
<Revision>1.0</Revision>
<CustomerName>Service Provider Ultra-CDN</CustomerName>
<Allow>
<Pattern>*</Pattern>
<Network>10.1.1.1/32</Network>
<Network>10.2.2.2/32</Network>
<Network>209.165.201.0/27</Network>
</Allow>
<Deny>
<Pattern>*</Pattern>
<Geo>
<Country name="ALL"/>
</Geo>
</Deny>
<Order>Allow</Order>
</CDSAuthorization>
```

Geo/IP File Examples

The following is an example of the Authorization Service configuration file example.

```
<CDSAuthorization xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">
  <Revision>1.0</Revision>
  <CustomerName>ACompany</CustomerName>
  <Allow>
     <Pattern>*</Pattern>
     <Network>1.1.1.1/24</Network>
     <Network>2.2.2.2/24</Network>
     <Network>3.3.3.3/24</Network>
     <Network>4.4.4.4/8</Network>
     <Network>5.5.5.5/24</Network>
     <Geo>
        <Country name="united states">
           <State name="california">
              <City name="san francisco"/>
              <City name="san jose"/>
              <City name="sunnyvale"/>
           </State>
        </Country>
     </Geo>
     <Geo>
        <Country name="united states">
           <State name="california"/>
           <State name="arizona"/>
        </Country>
        <Country name="germany"/>
     </Geo>
  </Allow>
  <Deny>
     <Pattern>*</Pattern>
     <Geo>
        <Country name="france"/>
        <Country name="china">
           <State name="ALL">
           </State>
        </Country>
     </Geo>
  </Deny>
  <Order>Allow,Deny</Order>
</CDSAuthorization>
```

Following is an example of a Geo/Ip file with both IPv4 and IPv6 addresses:

```
<CDSAuthorization
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="schema\CDSAuthorization.xsd">

  <Revision>1.0</Revision>
  <CustomerName>Cisco Systems</CustomerName>
  <Allow>
     <Pattern>*</Pattern>
     <Network>1.1.1.1/24</Network>
     <Network>2001:0DB8:0000:0001::/64</Network>
  </Allow>
  <Deny>
     <Pattern>*</Pattern>
     <Network>2.2.2.2/24</Network>
     <Network>2001:0DB8:0000:0002::/64 </Network>
  </Deny>
  <Order>Allow,Deny</Order>
```

```
</CDSAuthorization>
```