SAML SSO Configuration

Overview of Single Sign-On

Federated single sign-on (SSO) standards such as SAML 2.0 provide secure mechanisms for passing credentials and related information between different web sites that have their own authorization and authentication systems. SAML 2.0 is an open standard developed by the OASIS Security Services Technical Committee.

The SAML 2.0 protocol has seen significant success, gaining momentum in financial services, higher education, government, and other industry segments. SAML 2.0 support has been implemented by all major web-access management vendors. The U.S. Government General Services Administration (GSA) requires all vendors participating in the U.S. E-Authentication Identity Federation program to be SAML 2.0-compliant.

SAML 2.0-compliant web sites exchange user credential information using SAML assertions. A SAML assertion is an XML document that contains trusted statements about a subject including, for example, a username and privileges. SAML assertions are usually digitally signed to ensure their authenticity.

Many large enterprises have deployed federated Identity and Access Management (IAM) and Identity Provider (IdP) systems, such as Ping Identity Ping Federate, CA SiteMinder, Open AM, and Windows ADFS 2.0 on their corporate intranets. These IAM and IdP systems handle the user authentication and SSO requirements for employees and partners. IAM and IdP systems use the SAML protocols to interoperate with partner websites outside their firewalls. Users can utilize their IAM and IdP systems to automatically authenticate their users to Cisco WebEx meeting services. This increases efficiency because users do not have to remember their usernames and passwords to start or join meetings on their Cisco WebEx sites.

Note WebEx Meetings Server supports SAML 2.0 IdPs only. It does not support IdPs based on the older SAML 1.1 and WS-Federate standards. This restriction stands in contrast to the cloud-based Cisco WebEx meeting services which continue to support SAML 1.1 and WS-Federate. The following is a list of SAML 2.0 IdPs that have been validated to work with Cisco WebEx Meetings Server:

- Microsoft ADFS 2.0 (a free add-on to Microsoft Windows Server 2008/Windows Server 2008 R2 or AD FS server role in Windows Server 2012)
- Ping Identity Ping Federate 6.6.0.17
- Forgerock Open AM 10.0.0
- CA SiteMinder 6.0 SP5

Because SAML 2.0 is an open standard, other SAML 2.0 IdPs might also operate with Cisco WebEx Meetings Server. However, other SAML 2.0 IdPs have not been tested by Cisco. It is therefore the user's responsibility to make any such integration operational.

Benefits of Single Sign-On

Single sign-on (SSO) can benefit you in the following ways:

- Simplified user authentication—Out of the box, Cisco WebEx Meetings Server requires users to sign in using email addresses and self-selected passwords specific to the Meetings Server system. Users select their passwords upon activating their Meetings Server accounts. While this approach works well for most small- and mid-sized organizations, larger organizations prefer user authentication using corporate credentials—that is, Active Directory—for enhanced security. You can accomplish this goal by using SAML 2.0 SSO.

  Note One added security benefit of SSO is that the corporate password is never actually sent to or stored in Cisco WebEx Meetings Server after the user authenticates successfully.

- Simplified user management—Large organizations with changing workforces due to normal attrition prefer to automate the process of user management when integrating with WebEx Meetings Server. This means automating the following:
  - User account creation when employees join the organization
  - User account updates when employees take on different roles within the organization
  - User account deactivation when employees leave the organization

  You can achieve automation for these events by configuring **Auto Account Creation** and **Auto Account Update** in the SSO section of the Cisco WebEx Meetings Server Administration site. We recommend that you turn on these features if they are also supported by your SAML IdPs. User accounts are automatically created and updated "on demand" when users authenticate successfully, thereby eliminating the need to create users manually using Cisco WebEx Administration. Similarly, users can no longer sign into their accounts after they leave the organization because the SAML 2.0 IdP blocks those users from signing in after they are removed from the SAML 2.0 IdP user database, which is usually a proxy for the underlying corporate directory.

Overview of Setting Up SAML 2.0 Single Sign-On

Important Unless you or someone in your organization has experience with SAML 2.0 single sign-on (SSO), we recommend that you engage the services of a qualified Cisco AUC partner or Cisco Advanced Services. We make this recommendation because SAML SSO configuration can be fairly complicated.

Review these general steps for setting up SAML 2.0 SSO:

1. Ensure that your SAML 2.0 SSO infrastructure is in place and is integrated with your corporate directory. This implies setting up SAML 2.0 IdP software and the SSO authentication website. The authentication website is a portal where users enter their corporate credentials.
2. Ensure that users can access the SSO authentication website. This step is important because, as part of the sign-in process, Cisco WebEx Meetings Server redirects users to this authentication website.

Note If your Cisco WebEx Meetings Server system is enabled for public access—allowing users to sign in and join meetings from the Internet—then it is critical to ensure that the SSO authentication website is also accessible from the Internet. This usually implies deploying the SAML 2.0 IdP in your DMZ. Without this extra step, users will see "404 site not found" errors when signing in to Cisco WebEx Meetings Server from the Internet.

3. Connect WebEx Meetings Server to the SAML 2.0 IdP using both of these methods:
   - Select **Settings** > **Security** > **Federated SSO** on your Cisco WebEx Meetings Server Administration site.
   - Follow the instructions in your SAML 2.0 IdP documentation. Note that these instructions vary from vendor to vendor and might even change from version to version of the SAML 2.0 IdP. This is another reason to ensure that you contact a qualified Cisco AUC partner or Cisco Advanced Services to help you implement the solution.

     Note Do not use the instructions found on the Cisco Developer Network to set up SAML 2.0 IdPs because those instructions are intended for cloud-based Cisco WebEx meeting services and therefore do not work optimally with Cisco WebEx Meetings Server.

SAML SSO for End-User and Administration Sign In

SAML SSO is typically configured only for sign-in purposes on the End-User site and not the Administration site. On SAML 2.0 SSO-integrated Cisco WebEx Meetings Server sites the behavior mirrors SaaS WebEx behavior when it comes to user authentication. A Cisco WebEx Meetings Server administrator (and an SaaS

WebEx administrator) can sign in to an end-user account using SAML SSO but must sign in to an administrator account on the same system using a separate password. This ensures that in the event of catastrophic failures on the SAML SSO iDP, an administrator will still be able to access the Administration site. Without this failsafe, you might encounter a situation in which the Administration site becomes inaccessible not because of a product failure but because of a problem with the SAML SSO IdP software. The SAML SSO IdP software is on a server that is external to Cisco WebEx Meetings Server (or SaaS WebEx) and therefore outside of our control.

SAML 2.0 Single Sign-On Differences Between Cloud-Based WebEx Meeting Services and WebEx Meetings Server

While the cloud-based Cisco WebEx meeting services employ unique user IDs when creating users accounts, Cisco WebEx Meetings Server uses email addresses as the basis for creating user accounts. This has the following important implications for SAML 2.0 single sign-on (SSO):

- It is mandatory for the SAML Assertion to carry the email address in the NameID field. Without this step, user authentication and account creation fail because Cisco WebEx Meetings Server does not permit the creation of user accounts without an associated email address.
- The cloud-based Cisco WebEx meeting services permit removal of the email domain, such as "@cisco.com," from the UPN (User Principal Name) when auto account creation is turned on. This results in the creation of a user account that resembles a user ID. Because WebEx Meetings Server uses a complete email address to create user accounts, you cannot remove the email domain from the UPN.

In practice, you can initially deploy Cisco WebEx Meetings Server without SAML 2.0 SSO and turn on SSO later. Doing so has the following important effects on the user authentication, auto account creation, and auto account update features:

Scenario	User Authentication Behavior	Auto Account Creation (AAC) On	AAC Off	Auto Account Update (AAU) On	AAU Off
You have not turned on SSO. User accounts were created in the system.	Users sign in using their email addresses and self-selected passwords.	N/A	N/A	N/A	N/A

Scenario	User Authentication Behavior	Auto Account Creation (AAC) On	AAC Off	Auto Account Update (AAU) On	AAU Off
Next you turn on SSO. Users with existing accounts sign in to their WebEx site, WebEx Productivity Tools, or the Cisco WebEx Meetings app on their mobile devices.	Users are redirected to the SAML 2.0 IdP authentication website and asked to sign in using their corporate credentials, instead of email addresses and self-selected passwords. The users sign in successfully because they are recognized by the SAML 2.0 IdP as valid users. If they are not valid users, they will be informed by the SAML 2.0 IdP that they cannot use WebEx Meetings Server or that they are invalid users.	N/A	N/A	N/A	N/A

Scenario	User Authentication Behavior	Auto Account Creation (AAC) On	AAC Off	Auto Account Update (AAU) On	AAU Off
SSO is turned on. Users do not have existing accounts in the system.	Same as the previous scenario.	User accounts in Cisco WebEx Meetings Server are created "on-demand" after users sign in. Prerequisite: The SAML Assertion contains a valid email address in the NameID field.	Users do not have existing accounts in the system. They can sign in but will not be able to use Cisco WebEx Meetings Server. The easiest way to remedy this situation is to do one of the following: • Leave AAC on. • Before users sign in, manually create user accounts using "CSV File Import" or "Create user" from the Cisco WebEx Administration site.	N/A	N/A

Scenario	User Authentication Behavior	Auto Account Creation (AAC) On	AAC Off	Auto Account Update (AAU) On	AAU Off
SSO is turned on. Users previously signed in using SSO and are now signing in again.	Same as the second scenario.	N/A	N/A	Existing user accounts are automatically updated with any changes to the user credentials (usually first name or last name) as long as the NameID remains unchanged.	N/A
Subsequently you turn off SSO. This is an uncommon scenario because customers tend to leave SSO on after turning it on. Users previously signed in using SSO and are now signing in again.	If users enter their corporate credentials, they cannot sign in because WebEx Meetings Server expects them to enter their email addresses and self-selected passwords. In this situation, educate the users about resetting the self-selected passwords in their WebEx accounts and allow them enough time to act before you turn off SSO. After resetting their passwords, users can sign in using their email addresses and self-selected passwords.	N/A	N/A	N/A	N/A

Scenario	User Authentication Behavior	Auto Account Creation (AAC) On	AAC Off	Auto Account Update (AAU) On	AAU Off
Special case: A user is also a system administrator. Scenario A: The user signs in to the WebEx Site. Scenario B: The user signs in to the Cisco WebEx Administration site.		Scenario A: Same results as the previous scenario. Scenario B: N/A.	Scenario A: Same results as the previous scenario. Scenario B: N/A.	Scenario A: Same results as the previous scenario. Scenario B: N/A.	Scenario A: Same results as the previous scenario. Scenario B: N/A.

Scenario	User Authentication Behavior	Auto Account Creation (AAC) On	AAC Off	Auto Account Update (AAU) On	AAU Off
	Scenario A: Same results as the previous scenario Scenario B: In contrast to the behavior on a WebEx site, when the user signs in to the Cisco WebEx Administration site, he or she is always prompted to enter the email address and self-selected password. In other words, SSO has no effect when you sign in to the Cisco WebEx Administration site. This is a security measure built into the product because of the need to ensure that systems administrators can always sign in to the Cisco WebEx Administration site. If the Cisco WebEx Administration site also supports SSO, then malfunctions in				

Scenario	User Authentication Behavior	Auto Account Creation (AAC) On	AAC Off	Auto Account Update (AAU) On	AAU Off
	the SAML 2.0 IdP or a loss of network connectivity between Cisco WebEx Meetings Server and the SAML 2.0 IdP might result in a situation in which systems administrators can no longer sign in and manage the product. This is the reason why SSO is not supported for the Cisco WebEx Administration site.				

SAML Assertion Attributes

The following table lists the SAML assertion attributes supported by Cisco WebEx Meetings Server. Make sure to configure the lastname, firstname, email, and updatetimestamp attributes. Automatic update does not work unless the updatetimestamp attribute is configured.

Supported SAML Assertion Attributes

Attribute Name	Attribute Meaning	Mandatory for Auto Create User	Input Value Range	Comments
lastname		Yes		
firstname		Yes		
email		Yes	Valid email format	

Attribute Name	Attribute Meaning	Mandatory for Auto Create User	Input Value Range	Comments
updatetimestamp	The user information update time	No	Support format **long format:** sample: System.currentTimeMillis() **LDIF format:** yyyyMMddHHmmss yyyy-MM-dd HH:mm:ss sample: 20090115213256 **UTC format** ("2009-10-09T06:00:32Z")	If the updateTimeStamp is missing, you cannot perform an auto update user, normally mapped to the whenChanged item if the IdP is linked to AD.
optionalparams		No		Optional parameters can be set in the formats described in the "Optional Parameters" section below.
OPhoneCountry		No		Office phone country code
OPhoneArea		No		Office phone area
OPhoneLocal		No	Enter numerical characters only. For example, 5551212. Do not enter non-numerical characters such as dashes or parentheses.	Office phone local
OPhoneExt		No		Office phone extension
FPhoneCountry		No		Alternate phone country code
FPhoneArea		No		Alternate phone area
FPhoneLocal		No		Alternate phone local
FPhoneExt		No		Alternate phone extension
PPhoneCountry		No		Alternate phone 2 country code
PPhoneArea		No		Alternate phone 2 area
PPhoneLocal		No		Alternate phone 2 local

Attribute Name	Attribute Meaning	Mandatory for Auto Create User	Input Value Range	Comments
PPhoneExt		No		Alternate phone 2 extension
MPhoneCountry		No		Mobile phone country code
MPhoneArea		No		Mobile phone area
MPhoneLocal		No		Mobile phone local
MPhoneExt		No		Mobile phone extension
TimeZone		No		Time zone (see the "Time Zones" section below)
Address1		No		Address1
Address2		No		Address2
City		No		City
State		No		State
ZIP Code		No		ZIP code
Country		No		Country (see the "Country Values" section below)
Region		No		Region (see the "Region Values" section below)
Language		No		Language (see the "Language Values" section below)
TC1	String	No	Tracking Code Group 1 entered by user on the Administration site	Index 1
TC2	String	No	Tracking Code Group 2 entered by user on the Administration site	Index 2
TC3	String	No	Tracking Code Group 3 entered by user on the Administration site	Index 3
TC4	String	No	Tracking Code Group 4 entered by user on the Administration site	Index 4

Attribute Name	Attribute Meaning	Mandatory for Auto Create User	Input Value Range	Comments
TC5	String	No	Tracking Code Group 5 entered by user on the Administration site	Index 5
TC6	String	No	Tracking Code Group 6 entered by user on the Administration site	Index 6
TC7	String	No	Tracking Code Group 7 entered by user on the Administration site	Index 7
TC8	String	No	Tracking Code Group 8 entered by user on the Administration site	Index 8
TC9	String	No	Tracking Code Group 9 entered by user on the Administration site	Index 9
TC10	String	No	Tracking Code Group 10 entered by user on the Administration site	Index 10

Optional Parameters

You can set the optionalparams setting as follows:

- <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic' Name="optionalparams">
- <saml:AttributeValue xsi:type="xs:string">City=Toronto</saml:AttributeValue >
- <saml:AttributeValue xsi:type="xs:string">AA=OFF</saml:AttributeValue >
- <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic' Name="City">
- <saml:AttributeValue xsi:type="xs:string">Toronto</saml:AttributeValue>
- <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic' Name="AA">
- <saml:AttributeValue xsi:type="xs:string">OFF</saml:AttributeValue>

Time Zone Values

The following table provides the values for the TimeZone attribute.

Time Zone	Value
Marshall Islands (Dateline Time, GMT-12:00)	0
Samoa (Samoa Time, GMT-11:00)	1

Time Zone	Value
Honolulu (Hawaii Time, GMT-10:00)	2
Anchorage (Alaska Daylight Time, GMT-08:00)	3
San Francisco (Pacific Daylight Time, GMT-07:00)	4
Arizona (Mountain Time, GMT-07:00)	5
Denver (Mountain Daylight Time, GMT-06:00)	6
Chicago (Central Daylight Time, GMT-05:00)	7
Mexico City (Mexico Daylight Time, GMT-05:00)	8
Saskatchewan (Central Time, GMT-06:00)	9
Bogota (S. America Pacific Time, GMT-05:00)	10
New York (Eastern Daylight Time, GMT-04:00)	11
Indiana (Eastern Daylight Time, GMT-04:00)	12
Halifax (Atlantic Daylight Time, GMT-03:00)	13
La Paz (S. America Western Time, GMT-04:00)	14
Newfoundland (Newfoundland Daylight Time, GMT-02:30)	15
Brasilia (S. America Eastern Standard Time, GMT-03:00)	16
Buenos Aires (S. America Eastern Time, GMT-03:00)	17
Mid-Atlantic (Mid-Atlantic Time, GMT-02:00)	18
Azores (Azores Summer Time, GMT)	19
Reykjavik (Greenwich Time, GMT)	20
London (GMT Summer Time, GMT+01:00)	21
Amsterdam (Europe Summer Time, GMT+02:00)	22
Paris (Europe Summer Time, GMT+02:00)	23
Berlin (Europe Summer Time, GMT+02:00)	25
Athens (Greece Summer Time, GMT+03:00)	26
Cairo (Egypt Time, GMT+02:00)	28
Pretoria (South Africa Time, GMT+02:00)	29
Helsinki (Northern Europe Summer Time, GMT+03:00)	30
Tel Aviv (Israel Daylight Time, GMT+03:00)	31
Riyadh (Saudi Arabia Time, GMT+03:00)	32

Time Zone	Value
Moscow (Russian Time, GMT+04:00)	33
Nairobi (Nairobi Time, GMT+03:00)	34
Tehran (Iran Daylight Time, GMT+04:30)	35
Abu Dhabi, Muscat (Arabian Time, GMT+04:00)	36
Baku (Baku Daylight Time, GMT+05:00)	37
Kabul (Afghanistan Time, GMT+04:30)	38
Ekaterinburg (West Asia Time, GMT+06:00)	39
Islamabad (West Asia Time, GMT+05:00)	40
Mumbai (India Time, GMT+05:30)	41
Colombo (Colombo Time, GMT+05:30)	42
Almaty (Central Asia Time, GMT+06:00)	43
Bangkok (Bangkok Time, GMT+07:00)	44
Beijing (China Time, GMT+08:00)	45
Perth (Australia Western Time, GMT+08:00)	46
Singapore (Singapore Time, GMT+08:00)	47
Taipei (Taipei Time, GMT+08:00)	48
Tokyo (Japan Time, GMT+09:00)	49
Seoul (Korea Time, GMT+09:00)	50
Yakutsk (Yakutsk Time, GMT+10:00)	51
Adelaide (Australia Central Standard Time, GMT+09:30)	52
Darwin (Australia Central Time, GMT+09:30)	53
Brisbane (Australia Eastern Time, GMT+10:00)	54
Sydney (Australia Eastern Standard Time, GMT+10:00)	55
Guam (West Pacific Time, GMT+10:00)	56
Hobart (Tasmania Standard Time, GMT+10:00)	57
Vladivostok (Vladivostok Time, GMT+11:00)	58
Solomon Is (Central Pacific Time, GMT+11:00)	59
Wellington (New Zealand Standard Time, GMT+12:00)	60
Fiji (Fiji Time, GMT+12:00)	61

Time Zone	Value
Stockholm (Sweden Summer Time, GMT+02:00)	130
Tijuana (Mexico Pacific Daylight Time, GMT-07:00)	131
Chihuahua (Mexico Mountain Daylight Time, GMT-06:00)	132
Caracas (S. America Western Time, GMT-04:30)	133
Kuala Lumpur (Malaysia Time, GMT+08:00)	134
Recife (S. America Eastern Time, GMT-03:00)	135
Casablanca (Morocco Daylight Time, GMT+01:00)	136
Tegucigalpa (Honduras Time, GMT-06:00)	137
Nuuk (Greenland Daylight Time, GMT-02:00)	138
Amman (Jordan Daylight Time, GMT+03:00)	139
Istanbul (Eastern Europe Summer Time, GMT+03:00)	140
Kathmandu (Nepal Time, GMT+05:45)	141
Rome (Europe Summer Time, GMT+02:00)	142
West Africa (West Africa Time, GMT+01:00)	143
Madrid (Europe Summer Time, GMT+02:00)	144

Country Values

The following table provides the values for the Country attribute.

Country	Value
Afghanistan	93
Albania	355
Algeria	213
American Samoa	1684
Andorra	376
Angola	244
Anguilla	1264
Antarctica	672_1
Antigua (including Barbuda)	1268
Argentina	54
Armenia	374

Country	Value
Aruba	297
Ascension Islands	247
Australia	61
Austria	43
Azerbaijan	994
Bahamas	1242
Bahrain	973
Bangladesh	880
Barbados	1246
Belarus	375
Belgium	32
Belize	501
Benin	229
Bermuda	1441
Bhutan	975
Bolivia	591
Bosnia_Herzegovina	387
Botswana	267
Brazil	55
British Virgin Islands	1284
Brunei	673
Bulgaria	359
Burkina Faso	226
Burundi	257
Cambodia	855
Cameroon	237
Canada	1_1
Cape Verde Island	238
Cayman Islands	1_9
Central African Republic	236
Chad Republic	235

Country	Value
Chile	56
China	86
Colombia	57
Comoros	269_1
Cook Islands	682
Costa Rica	506
Croatia	385
Cuba	53
Cyprus	357
Czech Republic	420
Denmark	45
Diego Garcia	246
Djibouti	253
Dominica	1767
Dominican Republic	1809
Ecuador	593
Egypt outside Cairo	20
El Salvador	503
Equatorial Guinea	240
Eritrea	291
Estonia	372
Ethiopia	251
Faeroe Islands	298
Falkland Islands	500
Fiji Islands	679
Finland	358
France	33
French Depts. (Indian Ocean)	262
French Guiana	594
French Polynesia	689
Gabon Republic	241

Country	Value
Gambia	220
Georgia	995
Germany	49
Ghana	233
Gibraltar	350
Greece	30
Greenland	299
Grenada	1473
Guadeloupe	590
Guantanamo (U.S. Naval Base)	53_1
Guatemala	502
Guinea	224
Guinea-Bisau	245
Guyana	592
Haiti	509
Honduras	504
Hong Kong	852
Hungary	36
Iceland	354
India	91
Indonesia	62
Iran	98
Iraq	964
Ireland	353
Israel	972
Italy	39_1
Ivory Coast	225
Jamaica	1876
Japan	81
Jordan	962
Kazakhstan	7_1

Country	Value
Kenya	254
Kiribati	686
Korea (North)	850
Korea (South)	82
Kuwait	965
Kyrgyzstan	996
Laos	856
Latvia	371
Lebanon	961
Lesotho	266
Liberia	231
Libya	218
Liechtenstein	423
Lithuania	370
Luxembourg	352
Macao	853
Macedonia	389
Madagascar	261
Malawi	265
Malaysia	60
Maldives	960
Mali	223
Malta	356
Marshall Islands	692
Mauritania	222
Mauritius	230
Mayotte Island	269
Mexico	52
Micronesia	691
Moldova	373
Monaco	377

Country	Value
Mongolia	976
Montserrat	1664
Morocco	212
Mozambique	258
Myanmar	95
Namibia	264
Nauru	674
Nepal	977
Netherlands	31
Netherlands Antilles	599_2
New Caledonia	687
New Zealand	64
Nicaragua	505
Niger	227
Niue	683
Norfolk Island	672
Northern Mariana Islands	1670
Norway	47
Oman	968
Pakistan	92
Palau	680
Panama	507
Papua New Guinea	675
Paraguay	595
Peru	51
Philippines	63
Poland	48
Portugal	351
Puerto Rico	1787
Qatar	974
Romania	40

Country	Value
Russia	7
Rwanda	250
San Marino	378
Sao Tome	239
Saudi Arabia	966
Senegal Republic	221
Serbia	381
Seychelles Islands	248
Sierra Leone	232
Singapore	65
Slovakia	421
Slovenia	386
Solomon Islands	677
Somalia	252
South Africa	27
Spain	34
Sri Lanka	94
St. Helena	290
St. Kitts and Nevis	1869
St. Lucia	1758
St. Pierre and Miguelon	508
St. Vincent	1784
Sudan	249
Suriname	597
Swaziland	268
Sweden	46
Switzerland	41
Syria	963
Taiwan	886
Tajikistan	992
Tanzania	255

Country	Value
Thailand	66
Togo	228
Tonga Islands	676
Trinidad and Tobago	1868
Tunisia	216
Turkey	90
Turkmenistan	993
Turks and Caicos	1649
Tuvalu	688
Uganda	256
Ukraine	380
United Arab Emirates	971
United Kingdom	41
United States of America	1
Uruguay	598
Uzbekistan	998
Vanuatu	678
Vatican City	39
Venezuela	58
Vietnam	84
Wallis and Futuna Islands	681
Western Samoa	685
Yemen	967
Zambia	260
Zimbabwe	263

Region Values

The following table provides the values for the Region attribute.

Region	Value
U.S.	2
Australia	3

Region	Value
Canada	4
French Canada	5
China	6
France	7
Germany	8
Hong Kong	9
Italy	10
Japan	11
Korea	12
New Zealand	13
Spain	14
Switzerland	16
Taiwan	17
U.K.	18
Mexico	19
Argentina	20
Chile	21
Colombia	22
Venezuela	23
Brazil	24
Portugal	25
Belgium	26
Netherlands	27
Russia	28
India	29

Language Values

The following table provides the values for the Language attribute.

Language	Value
Castilian Spanish	11
Dutch	14

Language	Value
English	1
French	7
German	9
Italian	10
Japanese	5
Korean	6
Latin American Spanish	12
Portuguese	15
Russian	16
Simplified Chinese	3
Traditional Chinese	4