SAP Disclosure Management - RESTful APIs

Introduction

The RESTful APIs provided in SAP Disclosure Management can be used to create client applications that use SAP Disclosure Management functionality. Currently, the APIs are intended to work only with the authorization concepts in SAP Disclosure Management, and can be used for the following tasks:

- Get and set user information and also create new users in the SAP Disclosure Management system
- Get a list of entities from the SAP Disclosure Management system
- Get a list of the roles available in the SAP Disclosure Management system
- Get a list of the periods available in the SAP Disclosure Management system
- Get a list of the reports available in a period
- Get a list of the chapters available in a report
- Get a list of a user's global permissions and also assign new global permissions or delete existing global permissions
- Get a list of a user's local permissions and also assign new local permissions or delete existing local permissions at report or chapter level

List of APIs

1. POST /api/Authenticate

Description	:	Logs a user in to SAP Disclosure Management and gets a bearer access token that is to be used for all future API calls.
Input Parameters / Body	:	**Raw data:** *Basic Authentication:* username=XXXX&password=YYYY&grant_type=password XXXX is the SAP Disclosure Management login YYYY is the password for login XXXX *AD Authentication:* Leave the body field empty

Response Body	:	**On success:**
		{"services":
		{"Container":
		{"adapter":
		{"config":
		{
		"id": ID of the User,
		"UserName": "Login of the User in DM",
		"firstName": "User's Firstname",
		"lastName": "User's Lastname",
		"Password": null,
		"fullName": "User's Fullname"
		}
		}
		}
		}
		}
		
		On authorized:
		Status "401 Unauthorized" is send back to the client

Response Header		**On success:** access_token: This access token that is needed for every other API call. It is necessary to send this token in the header of each API call by using key="access_token", value="value of the received access token" **On authorized:** access_token: This field is missing
Note	:	To ensure the security of the bearer tokens, the APIs should be hosted and used in SSL (Secure Sockets Layer). SAP Disclosure Management ensures that insecure HTTP calls are unable to access the APIs. If an API call is made using an insecure HTTP connection, no response is returned from the server.

2. GET /api/Users

Description	:	Retrieves a list of users with user information.
Authentication Parameters / Header	:	access_token="the received access_token from /api/Authenticate"
Input Parameters / Body	:	-

Response Body	:	[
		{
		"Id": 1,
		"Login": "Admin",
		"FirstName": "Gandalf",
		"LastName": "De Grey",
		"IsActive": true,
		},
		{
		"Id": 2,
		"Login": "JSparrow",
		"FirstName": "Jack",
		"LastName": "Sparrow",
		"IsActive": true,
		}
		...
		]

Error Codes	:	401: Unauthorized 403: Not authorized for this action
Permissions needed	:	Security-Define Users OR Security-Assign Global Permissions OR Report-Manage

3. GET /api/Users/{id}

Description	:	Retrieves the information of a single user (the user's password value will be empty).
Authentication Parameters / Header	:	access_token="the received access_token from /api/Authenticate"
Input Parameters / Body	:	{id} – User ID

Response Body	:	{
		"Id": 1,
		"Login": "Admin",
		"FirstName": "Admin",
		"LastName": "Administrator",
		"IsActive": true,
		}

Error Codes	:	401: Unauthorized 403: Not authorized for this action 404: Not found (ID not found)
Permissions needed	:	Security-Define Users OR Security-Assign Global Permissions OR Report-Manage

4. POST /api/Users

Description	:	Creates a new user in the system.

Input Parameters / Body	:	Case 1: Basic Authentication (AuthenticationType 0)
		{
		"Login": "UserLogin",
		"Password": "Password",
		"FirstName": "Jack",
		"LastName": "Sparrow",
		"IsActive": true,
		"EMail": "jack@sparrow.com",
		"AuthenticationType": 0,
		"TimeZoneValue": "Mountain Standard Time"
		}
		
		Case 2: Active Directory Authentication (AuthenticationType 1)

```
{
  "Login": "DomainUser",
  "FirstName": "Gandalf",
  "LastName": "DeGrey",
  "IsActive": true,
  "EMail": "gandalf@degrey.com",
  "AuthenticationType": 1,
  "Domain": "GLOBAL",
  "TimeZoneValue": "Pacific Standard Time"
}
```

Response Body	:	
Error Codes	:	400: Bad request 401: Unauthorized 403: Not authorized for this action
Note	:	For a list of the TimeZone strings that are supported, see Appendix A. The 'IsActive' field is optional and set to 'false' by default. 'Domain' is mandatory if the AuthenticationType is 1 (Active Directory Authentication).
Permissions needed	:	Security-Define Users

5. PUT /api/Users/{id}

Description	:	Updates the details of an existing user. Currently only the IsActive state of the user can be updated.
Authentication Parameters / Header	:	access_token="the received access_token from /api/Authenticate"
Input Parameters / Body	:	{ "IsActive": true }
Response Body	:	
Error Codes	:	400: Bad request 401: Unauthorized 403: Not authorized for this action
Permissions needed	:	Security-Define Users

6. GET /api/Users/{id}/GlobalPermissions

Description	:	Retrieves a list of Role IDs that are assigned to a user.
Authentication Parameters / Header	:	access_token="the received access_token from /api/Authenticate"
Input Parameters / Body	:	{id} – User ID
Response Body	:	[{"EntityId": 1, "RoleId": 1} {"EntityId": 2, "RoleId": 2} {"EntityId": 2, "RoleId": 3}]
Error Codes	:	401: Unauthorized 403: Not authorized for this action 404: Not found (ID not found)
Permissions needed	:	Security-Assign Global Permissions

7. POST /api/Users/{id}/GlobalPermissions

Description	:	Assigns a specific entity and role to a user.

Authentication Parameters / Header	:	access_token=”the received access_token from /api/Authenticate”
Input Parameters / Body	:	{id} – User ID {“EntityId”: 3, “RoleId”: 1}
Response Body	:	
Error Codes	:	400: Bad request (Role ID /Entity ID is invalid) 401: Unauthorized 403: Not authorized for this action 404: Not found (ID not found) 409: Conflict (user already assigned to role and entity)
Permissions needed	:	Security-Assign Global Permissions

8. DELETE /api/Users/{id}/GlobalPermissions

Description	:	Removes a user from the specified entity and role.
Authentication Parameters / Header	:	access_token=”the received access_token from /api/Authenticate”
Input Parameters / Body	:	{id} – User ID {“EntityId”: 3, “RoleId”: 1}
Response Body	:	
Error Codes	:	400: Bad request (Role ID/ Entity ID is invalid) 401: Unauthorized 403: Not authorized for this action 404: Not found (ID not found)
Permissions needed	:	Security-Assign Global Permissions

9. GET /api/Roles

Description	:	Retrieves a list of all roles available in the system.
Authentication Parameters / Header	:	access_token=”the received access_token from /api/Authenticate”
Input Parameters / Body	:	-
Response Body	:	[{ "RoleId": "10", "RoleName" : "Standard-Admin", "Description" : "The standard admin role.", "Permissions" : [{ “Group”: “Report” , “Name”: “Manage”} { “Group”: “Security” , “Name”: “Define Users”}] }, …]
Error Codes	:	401: Unauthorized 403: Not authorized for this action.
Permissions needed	:	Security – Define Roles and workflows OR Security-Assign Global Permissions OR Report-Manage

10. GET /api/Roles/{id}

Description	:	Retrieves the details of the specified role.

Authentication Parameters / Header	:	access_token=”the received access_token from /api/Authenticate”
Input Parameters / Body	:	{id} – Role ID

Response Body	:	{
		"RoleId": "10",
		"RoleName" : "Standard-Admin",
		"Description”: "The standard admin role.”
		"Permissions" : {
		{ “Group”: “Report” , “Name”: “Manage”}
		{ “Group”: “Security” , “Name”: “Define Users”}
		}
		}

Error Codes	:	401: Unauthorized 403: Not authorized for this action 404: Not found (ID not found)
Permissions needed	:	Security – Define Roles and workflows OR Security-Assign Global Permissions OR Report-Manage

11. GET /api/Entities

Description	:	Retrieves a list of all entities in the system.
Authentication Parameters / Header	:	access_token=”the received access_token from /api/Authenticate”
Input Parameters / Body	:	-

Response Body	:	[
		{
		"EntityId": 1,
		"EntityName": "SAP",
		},
		{
		"EntityId": 2,
		"EntityName": "XYZ",
		},
		{
		"EntityId": 3,
		"EntityName": "ABCDE",
		}
		...
		]

Error Codes	:	401: Unauthorized 403: Not authorized for this action
Permissions needed	:	Administration – Define Entities OR Security-Assign Global Permissions

12. GET /api/CurrentUserEntities

Description	:	Retrieves a list of all entities that the logged in user is assigned to
Authentication Parameters / Header	:	access_token=”the received access_token from /api/Authenticate”
Input Parameters / Body	:	-

Response Body	:	[
		{
		"EntityId": 1,
		"EntityName": "SAP",
		},
		{
		"EntityId": 2,
		"EntityName": "XYZ",
		},
		{
		"EntityId": 3,
		"EntityName": "ABCDE",
		}
		...
		]

Error Codes	:	401: Unauthorized 403: Not authorized for this action
Permissions needed	:	Administration – Define Entities OR Security-Assign Global Permissions

13. GET /api/Periods

Description	:	Retrieves a list of periods in the system.
Authentication Parameters / Header	:	access_token="the received access_token from /api/Authenticate"
Input Parameters / Body	:	-
Response Body	:	[{ "PeriodId": 1, "PeriodName": "2015 Q1" }, { "PeriodId": 2, "PeriodName": "2015 Q2" }, ...]
Error Codes	:	401: Unauthorized 403: Not authorized for this action
Permissions needed	:	Period-Manage OR Report-Manage

14. GET /api/Periods/{id}/Reports

Description	:	Retrieves a list of reports that belong to the particular period.
Authentication Parameters / Header	:	access_token="the received access_token from /api/Authenticate"
Input Parameters / Body	:	{id} – Period ID

Response Body	:	[
		{
		"ReportId": 2,
		"ReportName": "Report 1"
		},
		{
		"ReportId": 7,
		"ReportName": "Another Report"
		}
		]

Error Codes	:	401: Unauthorized 403: Not authorized for this action 404: Not found (ID not found)
Permissions needed	:	Period-Manage OR Report-Manage

15. GET /api/Reports/{id}/LocalPermissions

Description	:	Retrieves a list of users and corresponding roles for the requested report.
Authentication Parameters / Header	:	access_token="the received access_token from /api/Authenticate"
Input Parameters / Body	:	{id} – Report ID
Response Body	:	[{"UserId":1, "RoleId": 1}, {"UserId":1, "RoleId": 2} {"UserId":2, "RoleId": 2} {"UserId":2, "RoleId": 4} ...]

Error Codes	:	401: Unauthorized 403: Not authorized for this action 404: Not found (ID not found)
Permissions needed	:	Report - Manage

16. POST /api/Reports/{id}/LocalPermissions

Description	:	Assigns roles to a user for the specified report.
Authentication Parameters / Header	:	access_token="the received access_token from /api/Authenticate"
Input Parameters / Body	:	{id} – Report ID {"UserId": 1, "RoleId": 1}
Response Body	:	
Authentication Parameters / Header	:	access_token="the received access_token from /api/Authenticate"
Error Codes	:	400: Bad request (UserId, RoleId values invalid) 401: Unauthorized 403: Not authorized for this action 404: Not found (ID not found) 409: Conflict (user already assigned to role)
Permissions needed	:	Report – Manage

17. DELETE /api/Reports/{id}/LocalPermissions

Description	:	Deletes a user's corresponding roles for the requested report.
Authentication Parameters / Header	:	access_token="the received access_token from /api/Authenticate"
Input Parameters / Body	:	{id} – Report ID {"UserId": 1, "RoleId": 1}
Response Body	:	
Error Codes	:	400: Bad request (UserId, RoleId values invalid) 401: Unauthorized 403: Not authorized for this action 404: Not found (ID not found)
Permissions needed	:	Report – Manage

18. GET /api/Reports/{id}/Chapters

Description	:	Retrieves a list of chapter IDs belonging to the specified report.
Authentication Parameters / Header	:	access_token="the received access_token from /api/Authenticate"
Input Parameters / Body	:	{id} – Report ID

Response Body	:	[{
		"ChapterId": 1,
		"ChapterName": "Contents"
		"Indent":" ㄴ"
		},
		{
		"ChapterId": 2,
		"ChapterName": "Introduction"
		"Indent":" ㄴ"
		}

]

Error Codes	:	401: Unauthorized 403: Not authorized for this action 404: Not found (ID not found)
Permissions needed	:	Report – Manage

19. GET /api/Reports/{id}/Users

Description	:	Retrieves a list of users that have access to the report specified.
Authentication Parameters / Header	:	access_token="the received access_token from /api/Authenticate"
Input Parameters / Body	:	{id} – Report ID

Response Body	:	[
		{
		"Id": 1357,
		"Login": "User 1",
		"FirstName": "User",
		"LastName": "One",
		"IsActive": true
		},
		{
		"Id": 1329,
		"Login": "User 2",
		"FirstName": "User",
		"LastName": "Two",
		"IsActive": true
		}
		]

Error Codes	:	401: Unauthorized 403: Not authorized for this action. 404: Not found (ID not found)
Permissions needed	:	Security-Define Users OR Security- Assign Global Permissions OR Report- Manage

20. GET /api/Chapters/{id}/LocalPermissions

Description	:	Retrieves a list of users and corresponding roles for the requested chapter.
Authentication Parameters / Header	:	access_token="the received access_token from /api/Authenticate"
Input Parameters / Body	:	{id} – Chapter ID
Response Body	:	[{"UserId":1, "RoleId": 1}, {"UserId":1, "RoleId": 2} {"UserId":2, "RoleId": 2} {"UserId":2, "RoleId": 4} …]
Error Codes	:	401: Unauthorized 403: Not authorized for this action 404: Not found (ID not found)
Permissions needed	:	Report – Manage

21. POST /api/Chapters/{id}/LocalPermissions

Description	:	Assigns roles to a new user or new roles to an existing user for the specified chapter.
Authentication Parameters / Header	:	access_token="the received access_token from /api/Authenticate"

Input Parameters / Body	:	{id} – Chapter ID {"UserId": 1, "RoleId": 1}
Response Body	:	
Error Codes	:	400: Bad request (UserId, RoleId values invalid) 401: Unauthorized 403: Not authorized for this action 404: Not found (ID not found) 409: Conflict (user already assigned to role)
Permissions needed	:	Report – Manage

22. DELETE /api/Chapters/{id}/LocalPermissions

Description	:	Deletes a user's corresponding roles for the requested chapter.
Authentication Parameters / Header	:	access_token="the received access_token from /api/Authenticate"
Input Parameters / Body	:	{id} – Chapter ID {"UserId": 1, "RoleId": 1}
Response Body	:	
Error Codes	:	400: Bad request (UserId, RoleId values invalid) 401: Unauthorized 403: Not authorized for this action 404: Not found (ID not found)
Permissions needed	:	Report – Manage

23. GET /api/GlobalPermissions

Description	:	Retrieves a list of entities, roles, and permissions of users in the system.
Authentication Parameters / Header	:	access_token="the received access_token from /api/Authenticate"
Input Parameters / Body	:	

Response Body	:	[{
		"UserId": 1,
		"UserLogin": "Admin",
		"RoleId": 1,
		"RoleName": "Standard-Admin",
		"EntityId": -2,
		"EntityName": "strGroup"
		},
		{
		"UserId": 1,
		"UserLogin": "Admin",
		"RoleId": 2,
		"RoleName": "Standard-Readonly",
		"EntityId": -2,
		"EntityName": "strGroup"
		}]

Error Codes	:	401: Unauthorized 403: Not authorized for this action
Permissions needed	:	Security-Assign Global Permissions

24. GET /api/GlobalPermissions/{id}

Description	:	Retrieves a list of entities, roles, and permissions of the specified user in the system.

Authentication Parameters / Header	:	access_token=”the received access_token from /api/Authenticate”
Input Parameters / Body	:	{id} – User ID

Response Body	:	[{
		"UserId": 1,
		"UserLogin": "Admin",
		"RoleId": 1,
		"RoleName": "Standard-Admin",
		"EntityId": -2,
		"EntityName": "strGroup"
		},
		{
		"UserId": 1,
		"UserLogin": "Admin",
		"RoleId": 2,
		"RoleName": "Standard-Readonly",
		"EntityId": -2,
		"EntityName": "strGroup"
		}]

Error Codes	:	401: Unauthorized 403: Not authorized for this action
Permissions needed	:	Security-Assign Global Permissions

25. GET /api/LocalPermissions

Description	:	Retrieves a list of roles, periods, reports, chapters, and permissions of users in the system to which the logged-in user has access to.
Authentication Parameters / Header	:	access_token=”the received access_token from /api/Authenticate”
Input Parameters / Body	:	
Response Body	:	[{ "UserId": 1, "UserName": "Admin", "RoleId": 1, "RoleName": "Standard-Admin", "ReportId": -2, "ReportName": "strGroup", “PeriodId” : 56, “PeriodName” : “PeriodName”, “ChapterId” : 23, “ChapterName” : “ChapterName” }]
Error Codes	:	401: Unauthorized 403: Not authorized for this action.
Note	:	If the ChapterId returned is -1, this denotes a report-level permission. In this case, the ChapterName will be set to ‘- - -‘.
Permissions needed	:	Report – Manage

26. GET /api/LocalPermissions/{id}

Description	:	Retrieves a list of roles, periods, reports, chapters, and permissions of the specified user in the system to which the logged-in user has access to.
Authentication Parameters / Header	:	access_token=”the received access_token from /api/Authenticate”
Input Parameters / Body	:	
Response Body	:	[{ "UserId": 1, "UserName": "Admin", "RoleId": 1, "RoleName": "Standard-Admin", "ReportId": -2, "ReportName": "strGroup", “PeriodId” : 56,

```
        "PeriodName" : "PeriodName",
        "ChapterId" : 23,
        "ChapterName" : "ChapterName"
}]
```

Error Codes	**:**	401: Unauthorized 403: Not authorized for this action
Note	**:**	If the ChapterId returned is -1, this denotes a report-level permission. In this case, the ChapterName will be set to '- - -'.
Permissions needed	**:**	Report – Manage

Example for authentication and use of APIs

The SAP Disclosure Management RESTful APIs use OAuth to authenticate users; a user must have an access token in order to make calls to the APIs. The timeout for the access token is 1 day.

The example below shows how to get the access token, followed by an example of a GET call to fetch a list of users from the SAP Disclosure Management system.

C# code snippet for authenticating user and getting bearer access token

```
// Login API - Authenticate and get an access token for future use
HttpResponseMessage response;
var httpHeader = new List<KeyValuePair<string, string>>
                  {
                    new KeyValuePair<string, string>( "grant_type", "password" ),
                    new KeyValuePair<string, string>( "username", UserName ),
                    new KeyValuePair<string, string> ( "password", Password )
                };
var content = new FormUrlEncodedContent(httpHeader);

using (var client = new HttpClient())
{
        var tokenEndpoint = new Uri(new Uri(HostUri), "api/login");
       response = await client.PostAsync(tokenEndpoint, content);
}

var responseContent = await response.Content.ReadAsStringAsync();
if (!response.IsSuccessStatusCode)
{
        throw new Exception(string.Format("Error: {0}", responseContent));
}

// Access Token for future calls
string accessToken = JsonConvert.DeserializeObject<Dictionary<string, string>>
                                                                    (responseContent)["access_token"];
```

Once an access token is obtained, future calls to any of the RESTful APIs can use this access token for authentication.

C# code snippet for getting user's information from the system with authentication using the bearer access token

```
// GET /api/Users – Get All User information from the Disclosure Management System
using (httpClient = new HttpClient())
{
        // Set the server details from which the API can be accessed
        httpClient.BaseAddress = new Uri("http://servername:8080/");
       httpClient.DefaultRequestHeaders.Accept.Clear();
       httpClient.DefaultRequestHeaders.Accept.Add(new
                                              MediaTypeWithQualityHeaderValue("application/json"));
        // Use the bearer token received earlier for authentication
        httpClient.DefaultRequestHeaders.Authorization = new AuthenticationHeaderValue(
                                                                                "Bearer", accessToken);

        // Call the API
        HttpResponseMessage response = await httpClient.GetAsync("api/Users");

        // Check status code returned by API call
       if (response.IsSuccessStatusCode)
       {
        string result = await response.Content.ReadAsStringAsync();
                // Tasks to perform when call is successful
        }
       else
       {
                // Handle cases when API returns error status code
        }
}

accessToken = “”;       // Destroy access token after use
```

Note: The bearer token should be deleted on the client after use. This prevents misuse of the token.

Appendix

A. Values supported for the TimeZone field while creating a new user

Name of Time Zone	Time
Dateline Standard Time	(GMT-12:00) International Date Line West
Samoa Standard Time	(GMT-11:00) Midway Island, Samoa
Hawaiian Standard Time	(GMT-10:00) Hawaii
Alaskan Standard Time	(GMT-09:00) Alaska
Pacific Standard Time	(GMT-08:00) Pacific Time (US and Canada); Tijuana
Mountain Standard Time	(GMT-07:00) Mountain Time (US and Canada)
Mexico Standard Time 2	(GMT-07:00) Chihuahua, La Paz, Mazatlan
U.S. Mountain Standard Time	(GMT-07:00) Arizona
Central Standard Time	(GMT-06:00) Central Time (US and Canada
Canada Central Standard Time	(GMT-06:00) Saskatchewan
Mexico Standard Time	(GMT-06:00) Guadalajara, Mexico City, Monterrey
Central America Standard Time	(GMT-06:00) Central America
Eastern Standard Time	(GMT-05:00) Eastern Time (US and Canada)
U.S. Eastern Standard Time	(GMT-05:00) Indiana (East)
S.A. Pacific Standard Time	(GMT-05:00) Bogota, Lima, Quito
Atlantic Standard Time	(GMT-04:00) Atlantic Time (Canada)
S.A. Western Standard Time	(GMT-04:00) Caracas, La Paz
Pacific S.A. Standard Time	(GMT-04:00) Santiago
Newfoundland and Labrador Standard Time	(GMT-03:30) Newfoundland and Labrador
E. South America Standard Time	(GMT-03:00) Brasilia
S.A. Eastern Standard Time	(GMT-03:00) Buenos Aires, Georgetown
Greenland Standard Time	(GMT-03:00) Greenland
Mid-Atlantic Standard Time	(GMT-02:00) Mid-Atlantic
Azores Standard Time	(GMT-01:00) Azores
Cape Verde Standard Time	(GMT-01:00) Cape Verde Islands
GMT Standard Time	(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
Greenwich Standard Time	(GMT) Casablanca, Monrovia
Central Europe Standard Time	(GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
Central European Standard Time	(GMT+01:00) Sarajevo, Skopje, Warsaw, Zagreb
Romance Standard Time	(GMT+01:00) Brussels, Copenhagen, Madrid, Paris
W. Europe Standard Time	(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
W. Central Africa Standard Time	(GMT+01:00) West Central Africa
E. Europe Standard Time	(GMT+02:00) Bucharest
Egypt Standard Time	(GMT+02:00) Cairo
FLE Standard Time	(GMT+02:00) Helsinki, Kiev, Riga, Sofia, Tallinn, Vilnius
GTB Standard Time	(GMT+02:00) Athens, Istanbul, Minsk
Israel Standard Time	(GMT+02:00) Jerusalem

Name of Time Zone	Time
South Africa Standard Time	(GMT+02:00) Harare, Pretoria
Russian Standard Time	(GMT+03:00) Moscow, St. Petersburg, Volgograd
Arab Standard Time	(GMT+03:00) Kuwait, Riyadh
E. Africa Standard Time	(GMT+03:00) Nairobi
Arabic Standard Time	(GMT+03:00) Baghdad
Iran Standard Time	(GMT+03:30) Tehran
Arabian Standard Time	(GMT+04:00) Abu Dhabi, Muscat
Caucasus Standard Time	(GMT+04:00) Baku, Tbilisi, Yerevan
Transitional Islamic State of Afghanistan Standard Time	(GMT+04:30) Kabul
Ekaterinburg Standard Time	(GMT+05:00) Ekaterinburg
West Asia Standard Time	(GMT+05:00) Islamabad, Karachi, Tashkent
India Standard Time	(GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi
Nepal Standard Time	(GMT+05:45) Kathmandu
Central Asia Standard Time	(GMT+06:00) Astana, Dhaka
Sri Lanka Standard Time	(GMT+06:00) Sri Jayawardenepura
N. Central Asia Standard Time	(GMT+06:00) Almaty, Novosibirsk
Myanmar Standard Time	(GMT+06:30) Yangon Rangoon
S.E. Asia Standard Time	(GMT+07:00) Bangkok, Hanoi, Jakarta
North Asia Standard Time	(GMT+07:00) Krasnoyarsk
China Standard Time	(GMT+08:00) Beijing, Chongqing, Hong Kong SAR, Urumqi
Singapore Standard Time	(GMT+08:00) Kuala Lumpur, Singapore
Taipei Standard Time	(GMT+08:00) Taipei
W. Australia Standard Time	(GMT+08:00) Perth
North Asia East Standard Time	(GMT+08:00) Irkutsk, Ulaanbaatar
Korea Standard Time	(GMT+09:00) Seoul
Tokyo Standard Time	(GMT+09:00) Osaka, Sapporo, Tokyo
Yakutsk Standard Time	(GMT+09:00) Yakutsk
A.U.S. Central Standard Time	(GMT+09:30) Darwin
Cen. Australia Standard Time	(GMT+09:30) Adelaide
A.U.S. Eastern Standard Time	(GMT+10:00) Canberra, Melbourne, Sydney
E. Australia Standard Time	(GMT+10:00) Brisbane
Tasmania Standard Time	(GMT+10:00) Hobart
Vladivostok Standard Time	(GMT+10:00) Vladivostok
West Pacific Standard Time	(GMT+10:00) Guam, Port Moresby
Central Pacific Standard Time	(GMT+11:00) Magadan, Solomon Islands, New Caledonia
Fiji Islands Standard Time	(GMT+12:00) Fiji Islands, Kamchatka, Marshall Islands
New Zealand Standard Time	(GMT+12:00) Auckland, Wellington
Tonga Standard Time	(GMT+13:00) Nuku'alofa