Users API

This API provides access to a subset of functionality made available by the Users application, which allows you to manage your users, their roles and groups.

Users API manages the system entities User and Group but include additional logic to them.

To use this API simply reference the Users module using the References Window in the Development Environment.

Summary

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ChangePassword</td>
<td>Allows changing the user password.</td>
</tr>
<tr>
<td>EditMyInfo</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EncryptPassword</td>
<td>Returns the encrypted password for a specific username and password. This is the value kept in the Password attribute of the User system entity.</td>
</tr>
<tr>
<td>GetEffectiveUserProviderEspaceld</td>
<td>Returns the eSpace identifier of the effective user provider. Normally it returns the Users eSpaceld, in upgrade scenarios it returns the EnterpriseManager eSpaceld.</td>
</tr>
<tr>
<td>Group_CreateNew</td>
<td>Create a new system group. Requires the UserManager role to be invoked.</td>
</tr>
<tr>
<td>Group_Delete</td>
<td>Delete a system group. Requires the UserManager role to be invoked.</td>
</tr>
<tr>
<td>Group_Update</td>
<td>Updates a system group. Requires the UserManager role to be invoked.</td>
</tr>
<tr>
<td>IPAddress_GetBlockedStatus</td>
<td>Returns the blocking state of the IP address.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IPAddress_GetBlocks</td>
<td>Returns the blocking state of the IP address. If there are no blocks for this address, the list will be empty. If no IP address is given, information on all blocked IP addresses will be returned.</td>
</tr>
<tr>
<td>IPAddress_Unblock</td>
<td>Ends the blocking period for the specified IP address, allowing any user to login in that address.</td>
</tr>
<tr>
<td>PasswordAutocompleteValue</td>
<td>Depends on the site property PasswordAutocompleteValue</td>
</tr>
<tr>
<td>UseActiveDirectoryAuthentication</td>
<td>Returns the Users configuration that determines if the Active Directory is used for authentication</td>
</tr>
<tr>
<td>UseIntegratedAuthentication</td>
<td>Returns the Users configuration that determines if the Integrated Authentication is used to login.</td>
</tr>
<tr>
<td>UseLDAPAuthentication</td>
<td>Returns the Users configuration that determines if the Active Directory is used for authentication</td>
</tr>
<tr>
<td>User_CanChangePassword</td>
<td>Checks if the User is allowed to change a password. It is false for Active Directory users.</td>
</tr>
<tr>
<td>User_Create</td>
<td>Create a new user. Requires UserManager role to be invoked. Fails when the username is repeated.</td>
</tr>
<tr>
<td>User_CreateOrUpdate</td>
<td>Create or updates a user. Requires UserManager role to be invoked.</td>
</tr>
<tr>
<td>User_DeleteIfNoRoles</td>
<td>Deletes the User if there are no roles assigned to it.</td>
</tr>
<tr>
<td>User_GetBlockedStatus</td>
<td>Returns information regarding the blocking state of the user and the blocking reason, in the specified IP address. If no IP address is given, checks the last IP address from where the user attempted to login.</td>
</tr>
<tr>
<td>User_GetIdByUsername</td>
<td>Returns the user identifier for a specific user given the username</td>
</tr>
<tr>
<td>User_GetLastFailedLoginAttempts</td>
<td>Returns a list of last failed login attempts (one record for each IP address). This information can be used to invoke User_Unblock or IPAddress_Unblock.</td>
</tr>
<tr>
<td>User_GetName</td>
<td>Returns the name of the logged user.</td>
</tr>
<tr>
<td>User_GetUnifiedLoginUrl</td>
<td>Returns the Url used for custom unified login patterns. Includes Windows Integrated Authentication pattern.</td>
</tr>
<tr>
<td>User_IsExternalUser</td>
<td></td>
</tr>
<tr>
<td>User_Login</td>
<td>Action to login using username and password as credentials.</td>
</tr>
<tr>
<td>User_Logout</td>
<td>Logs out the current user. Session variables are cleared during the logout process.</td>
</tr>
<tr>
<td>User_Unblock</td>
<td>Ends the blocking period for the specified user, allowing the user to login in all IP addresses where the user was blocked.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>User Update</td>
<td>Updates a specific user.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Structure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LoginAttemptPublic</td>
<td>Represents the Login attempt record structure that is exposed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Static Entity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LoginAttemptResult</td>
<td>The alternative values that may appear in the LoginAttempt record Result column.</td>
</tr>
<tr>
<td>MenuItem</td>
<td>Menu item to be used in menu web block parameters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserManager</td>
<td></td>
</tr>
</tbody>
</table>

## Widgets

### ChangePassword

Allows changing the user password.

**Inputs**

- **UserId**
  - Type: optional, User Identifier.

### EditMyInfo
Actions

EncryptPassword

Returns the encrypted password for a specific username and password. This is the value kept in the Password attribute of the User system entity.

Inputs
Username
  Type: mandatory, Text.

Password
  Type: mandatory, Text.

Outputs
EncryptedPassword
  Type: Text.

GetEffectiveUserProviderEspaceId

Returns the eSpace identifier of the effective user provider. Normally it returns the Users eSpaceld, in upgrade scenarios it returns the EnterpriseManager eSpaceld.

Outputs
EspaceId
  Type: Espace Identifier.

Group_CreateNew

Create a new system group. Requires the UserManager role to be invoked.

Inputs
Group
Type: mandatory, Group.

Outputs
GroupId
Type: Group Identifier.

Group_Delete
Delete a system group. Requires the UserManager role to be invoked.

Inputs
GroupId
Type: mandatory, Group Identifier.

Group_Update
Updates a system group. Requires the UserManager role to be invoked.

Inputs
Group
Type: mandatory, Group.

IPAddress_GetBlockedStatus
Returns the blocking state of the IP address.

Inputs
IPAddress
Type: mandatory, Text.
IP address for which the blocking state should be evaluated.

Outputs
**LoginAttemptResult**

Type: `LoginAttemptResult`.

Blocking state for the given IP address.

---

**IPAddress_GetBlocks**

Returns the blocking state of the IP address. If there are no blocks for this address, the list will be empty. If no IP address is given, information on all blocked IP addresses will be returned.

**Inputs**

**IPAddress**

Type: optional, Text.

IP Address for which the current block information should be given.

**Outputs**

**BlockedAddresses**

Type: `LoginAttemptPublic` List.

Blocked login attempts associated to the given IP address, or all IP addresses, if no input is given.

---

**IPAddress_Unblock**

Ends the blocking period for the specified IP address, allowing any user to login in that address.

**Inputs**

**IPAddress**

Type: mandatory, Text.

The IP address to be unblocked.

---

**PasswordAutocompleteValue**

Depends on the site property `PasswordAutocompleteValue`

**Outputs**

**Value**

Type: Text.
UseActiveDirectoryAuthentication

Returns the Users configuration that determines if the Active Directory is used for authentication.

**Outputs**

**IsActive**
- Type: Boolean.

UseIntegratedAuthentication

Returns the Users configuration that determines if the Integrated Authentication is used to login.

**Outputs**

**IsActive**
- Type: Boolean.

UseLDAPAuthentication

Returns the Users configuration that determines if the Active Directory is used for authentication.

**Outputs**

**IsActive**
- Type: Boolean.

User_CanChangePassword

Checks if the User is allowed to change a password. It is false for Active Directory users.

**Inputs**

**UserId**
- Type: mandatory, User Identifier.

**Outputs**
IsAllowed
  Type: Boolean.

User_Create

Create a new user. Requires UserManager role to be invoked.
Fails when the username is repeated.

Inputs
User
  Type: mandatory, User.

Outputs
UserId
  Type: User Identifier.

User_CreateOrUpdate

Create or updates a user. Requires UserManager role to be invoked.

Inputs
User
  Type: mandatory, User.

Outputs
UserId
  Type: User Identifier.

User_DeleteIfNoRoles

Deletes the User if there are no roles assigned to it.

Inputs
UserId
  Type: mandatory, User Identifier.
User_GetBlockedStatus

Returns information regarding the blocking state of the user and the blocking reason, in the specified IP address. If no IP address is given, checks the last IP address from where the user attempted to login.

**Inputs**

**Username**
Type: mandatory, Text.
The username of the user whose information regarding the blocked/unblocked state will be retrieved.

**IPAddress**
Type: optional, Text.
The IP address for which the information regarding the blocked/unblocked user state will be retrieved.

**Outputs**

**LoginAttemptResult**
Type: LoginAttemptResult.
Blocking state and reason for the given username.

User_GetIdByUsername

Returns the user identifier for a specific user given the username

**Inputs**

**Username**
Type: mandatory, Text.

**Outputs**

**UserId**
Type: User Identifier.
User_GetLastFailedLoginAttempts

Returns a list of last failed login attempts (one record for each IP address). This information can be used to invoke User_Unblock or IPAddress_Unblock.

**Inputs**

**Username**
- **Type:** mandatory, Text.
- The username of the user whose failed login attempts are retrieved.

**Since**
- **Type:** optional, Date Time.
- Only the login attempts after this datetime are retrieved.

**Outputs**

**LoginAttempt**
- **Type:** LoginAttemptPublic List.
- List of last failed login attempts for the given username.

User_GetName

Returns the name of the logged user.

**Outputs**

**Name**
- **Type:** Text.

User_GetUnifiedLoginUrl

Returns the URL used for custom unified login patterns. Includes Windows Integrated Authentication pattern.

**Inputs**

**OriginalUrl**
- **Type:** mandatory, Text.

**Outputs**
User_IsExternalUser

**Inputs**

**UserId**
Type: mandatory, User Identifier.

**Outputs**

**IsExternal**
Type: Boolean.

User_Login

Action to login using username and password as credentials.

**Inputs**

**Username**
Type: mandatory, Text.
User's username

**Password**
Type: mandatory, Text.
User's password (should not be encrypted)

**RememberLogin**
Type: mandatory, Boolean.

User_Logout

Logs out the current user. Session variables are cleared during the logout process.
User_Unblock

Ends the blocking period for the specified user, allowing the user to login in all IP addresses where the user was blocked.

*Inputs*

**Username**
- Type: mandatory, Text.
- The username of the user that is being unblocked and that will be allowed to login again from the specified IP address.

**IPAddress**
- Type: optional, Text.
- The IP address that is being unblocked and from where the specified user will be allowed to login again.

User_Update

Updates a specific user.

*Inputs*

**User**
- Type: mandatory, User.

Structures

LoginAttemptPublic

Represents the Login attempt record structure that is exposed

*Attributes*

**Instant**
- Type: Date Time.

**Success**
- Type: Boolean.
IPAddress
  Type: Text (45).

UsernameFailureCount
  Type: Integer.

IPAddressFailureCount
  Type: Integer.

RequestKey
  Type: Text (36).

UserAgent
  Type: Text (200).

Visitor
  Type: Text (36).

Result
  Type: Text.

Static Entities

LoginAttemptResult

The alternative values that may appear in the LoginAttempt record Result column.

Attributes
Id
  Type: Text (50).

Records
• InvalidLDAPAuthentication
• BlockedIP
• Unblocked
• LoggedIn
• BlockedUser
• InvalidADAuthentication
• InvalidUser
• InvalidPassword
MenuItem

Menu item to be used in menu web block parameters.

Attributes

Id
  Type: Integer.

Order
  Type: Integer.

Caption
  Type: Text (50).

Records
  • Applications
  • Users
  • Groups