Identity Server 2020.2 Release Notes

Release highlights

This release focuses on introduction of the following new features and improvements:

Time-based One-time Password

Ubisecure has always believed in two-factor authentications, with our original One-Time Password list being available in the very first release of SSO software in 2002. Since then, we have expanded the use of two-factor authentications to include other methods, such as SMS OTP/Mobile PKI and added the ability for the Identity Platform to use second factor as "step-up" authentication as well.

With this release, we extend the Identity Platform capabilities to include Time-based One-time Password (TOTP). In SSO you are now able to configure a new TOTP authentication method to be used for SSO directory users, similar to other OTP methods. You are also able to configure TOTP for external directory use, such as SQL directory. A new TOTP API application have been created for handling adding and removing of secrets for users when setting up their device. It should be noted, that you will need to facilitate ways for the users to setup their devices and utilise the TOTP API to insert the secret to the user's account as there is no self-service or QR code generation available within SSO in this initial release.

This initial release of TOTP complies with RFC 6238, which is a generic implementation for Time-based One-time Password and should function with any authenticator application that supports the RFC standard.

To get more information about how this can be setup and used, review the developer portal pages that explains it more in detail:

- **Installation**
  - TOTP API will be installed along with SSO. See TOTP API configuration instructions on how to enable TOTP API and swagger documentation
- **Method Configuration**
  - How to configure TOTP method - TOTP Authentication Method
  - How the login screen looks for TOTP - Login screens - SSO
  - Which language keys to change for localisation - Internationalisation
- **Application Configuration**

Per application, you are able to configure the required methods to be able to access, below is a table showing how the different configurations alternatives and how the affect the setup of TOTP

Use case	Functionality	password.1	totp.1	How to access
1	Not in use	Enabled	Disabled	• User is able to access application with username and password • User with TOTP secret available does not have to input code
2	Configurable	Enabled	Enabled	• User is able to access application with only username and password if no TOTP secret is set for the users account • User is able to access application with username and password + TOTP code if TOTP secret is available • NOTE: When set the User is unable to access application without entering TOTP code • Operators need to redirect users to their own self-service UI/application (might be the same application they are currently accessing or a different one) to enable TOTP for users through the TOTP API application

3	Required	Disabled	Enabled	• User is able to access application with username and password + TOTP code • User is unable to access application with only username and password • User needs to be able to have access to Operator's own self-service UI/application to enable TOTP for users through the TOTP API application before be able to access the application (or enable multiple step-up methods to choose from to access the application and enable TOTP)

- **Usage**
  - As mentioned above, this implementation enables the usage of TOTP for Google Authenticator and any other RFC 6238 compliant TOTP applications. In order to setup and use the method, your or your administrator will need to implement a self-service UI /application that the user can sign in to and add a secret to their account through the new TOTP API application
  - In use case 2 from above table, the user that has authenticated to the service (either only through password.1 or if there are other step-up methods available and already enabled for the user) should be provided a way of enabling the TOTP secret to their account. This use case can be used to add TOTP secrets to an existing system with existing users. After the user has authenticated to your application, they can be presented the TOTP secret, from your application UI and add that TOTP secret to their authenticator application (Google Authenticator or similar). Then for future authentications, the user will be required to enter both their password and the TOTP code.
  - In use case 3 from the above table, the user does not have access to the application before they have set their TOTP secret. This means that the administrator needs to provide a way of setting the TOTP secret outside of the application that the user is trying to access. This could be done through another application that does not require step-up method or if there are other step-up methods available for the application that the user can access with
- Information on how to use the TOTP API can be found from the Swagger documentation provided with the TOTP API application. See information on how to access documentation from TOTP API configuration

Note: The end user secrets are designed to be used through API, there is no user self-service UI offered for TOTP at this time. Future iterations may contain an improvement for this. Administrators are still able to set or (re)generate secrets for Ubilogin Directory users as needed through SSO Management UI.

Corrections and improvements

Related to the addition of TOTP there has been changes done for the two-factor authentication configurations in order to have TOTP as optional addition to other methods. With this change it is possible to have both password method as well as the step-up method(s) enabled for an application. This configuration is presented above as "Use case 2".

This means, for example, if your application has both password and SPI Mobile PKI enabled - this is currently an invalid configuration, that might be hidden to end-users as the SPI Mobile PKI will never been presented during authentication. When SSO 8.6.0 is installed and IF the user has the SPI Mobile PKI method configured for their account, then they will be required to use the configured step-up method - adding a second step to the users log-in process.

Additionally, you will find a listing of known issues, with internal ticket references at the bottom of this page.

Change log

SSO 8.6.0

New Features

- IDS-1885 - SSO now supports Time-based One-time Password as a new step-up method. See TOTP Authentication Method for more details
- IDS-2631 - TOTP API application has been created for handling of user TOTP secrets. These API calls allow Administrators to set and remove the secrets for users through their own self-service UI/application (this is not provided within the Ubisecure Identity Server). See TOTP API - SSO for more info how to setup and configure

Improvements

- IDS-2714 - Support for *PBKDF2-SHA256* password encoding has been added to SSO. All supported values can be found from Management UI authentication methods
- IDS-2571 - Improvement for handling multiple IPs in "*proxy.remote-addr-name = x-forwarded-for*" configuration. If there are multiple IPs included in the request, all of the IPs will be shown in the audit logs, separated by ",". This will need to be taken into consideration when parsing the audit logs. Previously multiple IPs caused issues with Ubilogin Management, Logviewer and Search applications.
- IDS-2717 - Changes to application configuration for two-factor authentication methods. If both password and a step-up method is enabled for an application, users who do not have the specific step-up method enabled on their account can log in to the application with password only. See Authentication and authorization process - SSO

CustomerID 5.6.0

Improvements

- IDS-2719 - ubixmlsec library has been updated to version 1.5.8.50494 to use same version as SSO

Here you can find links to previous version's change logs for SSO and CustomerID

Known Issues

SSO

Ticket number	External description
IDS-561	There is a known issue where SSO does not check the mappingURL value when creating or editing an inboundDirectoryMappings when using the SSO REST API. Directory Mappings are possible to be created, but then not opened or edited.
IDS-608	There is a known UI/UX issue where a very large site list is displayed within the SSO management UI. This results in hard to use UI if large lists of sites are present in the SSO deployment. A possible workaround is to use an ldap editor to configure the authorization policies and groups.
IDS-941	There is a known issue where unregistered SMTP OTP authentication will not permit TLS or any secure authentication. Documentation improvement will be made to ensure proper configuration is shown if unsecure SMTP servers are required.
IDS-1030	There is a known issue where running the CertAP setup.cmd in a windows environment will post errors of missing linux tags. While these errors are unsightly, they can be safely ignored. This issue will be corrected in a future release.
IDS-1039	There is a known issue where a user account will ask for a sixth OTP verification after five consecutive failed OTP verifications have occurred. The five consecutive failures results in a locked account, the user should be informed that they must wait for the OTP timeout to expire before they attempt to login again.
IDS-1127	There are known documentation issues within OpenLDAP clustering with SSO.
IDS-1171	There is a known issue when using OpenLDAP 2.4.44 when performing SSO session cleanup which will cause replication issues.
IDS-1499	There is a known issue where SSO will return http 401, rather than http 400 when token introspection without an authentication header or when invalid credentials are present.
IDS-1511	There is a known issue with the tokens used to reset your password. If a user requests multiple password reset tokens, the old ones are not invalidated, however they are not refreshed and will become invalid after expiration time.
IDS-1525	There is a known issue where SSO logs will contain a stopped search warning entry when tomcat is shutdown. This error can be safely ignored.
IDS-1526	There is a known issue where SSO logs will contain a unstopped thread warning entry when tomcat is shutdown. This error can be safely ignored.
IDS-1832	There is a known issue where editing an existing authorisation policy (example case added an attribute) resulted in the alteration of ubiloginNameValue. This affects SSO 8.3.0 and later. There is no work around at this time.
IDS-1893	There is a known issue if you use OpenID authentication, a user cannot access SAML or Ubilogin web applications. Work around use any other non-OpenID authentication method. If OpenID is required, then use OAuth 2.0 application.
IDS-1995	When using BankID and Safari, during initial login Safari displays a 0kb file being downloaded when there is no downloaded file
IDS-2059	There is a known issue where the authorisation endpoint may become corrupted if a URL contains "%b" in URL encoded format.
IDS-2089	There is a known issue where shutting down Ubisecure Accounting service on a windows server will show errors within the ids-accounting.log.
IDS-2090	There is a known issue where the SSO management UI will not filter results correctly if the filter expression is short, contains incorrect filter expressions and there are Scandinavian characters included.
IDS-2092	There is a known issue where the tomcat log will show a severe servlet warning for com.ubisecure.ss-ui. However, this warning is due to a user repeating the same action (double clicking an item or using the back button). This warning can be safely ignored and will be addressed in a future release.
IDS-2094	There is a known issue where disabling the main account in the SSO login directory does not disable the User Driven Federation accounts. Users are still able to login to services with the Federated account even while the main account is disabled. Work around: Administrators who are disabling a main login directory account should ensure that they check and disable any associated UDF accounts at the same time. This issue will be addressed in a future release.
IDS-2096	There is a known issue where attempting to use exceptionally long SAML Entity IDs will result in creation failure (larger than 64 characters) . There is no known work around and may not be possible to resolve due to LDAP field limitations. We will address this in a future release.

IDS-2120	There is a known issue where dual node SSO will require jndi.properties to be manually configured on the second node during SSO upgrade.
IDS-2121	There is a known issue where dual node SSO will require settings.sh to be manually configured on the second node during SSO upgrade.
IDS-2226	There is a known issue with using escape characters like '=' for a Site that causes the SSO management UI to be unable to map applications to the site. Workaround is to make sure not to use any Escape values for Site names (https://ldapwiki.com/wiki/DN%20Escape%20Values).
IDS-2247	There is a known issue with OTP_LOGIN_REMAINING_PASSWORD_AMOUNT configuration that prevents SSO from showing warning message to the end-user when OTP list is running out. Currently there is no workaround known.
IDS-2260	There is a known installation issue when using SSO Password reset. Using the installation instructions for password reset tool requires an administrator to run tomcat update. This occasionally results in an empty context.xml file being created which causes SSO to fail when being restarted. Workaround, repeat the run tomcat update step which will create a correct .xml file and SSO will restart.
IDS-2261	There are several known issues with javascript tools when using SSO Password reset. Similar javascript is used in UAS with no issue. If you are experiencing password reset javascript issue, please contact Ubisecure Support referencing this internal ticket for potential work arounds.
IDS-2314	There is a known issue with passing a refresh token to token endpoint results in "invalid_grant" error, if the refresh token has been issued to an unregistered user from an authentication method having a connected Directory Service.
IDS-2315	There is a known issue that SSO returns refresh token for un-registered users. This should not be done since there is no way of handling the lifecycle of the un-registered user's refresh token.
IDS-2332	There is a known issue when using OpenLDAP in SSO where slapd runs out of connections to process incoming requests.
IDS-2478	There is a known issue in SSO that it is not possible to have different localisations for access_denied returned by IdP and local access_denied, for example if directory user mapping fails after successful authentication
IDS-2498	There is a known issue with policy.password.history configuration. While setting this configuration for password.2 it does not have any effect on the history check of previous passwords used.
IDS-2663	There is a known issue where creating a new site via a Safari browser where the site as an @ symbol in the email address will cause an error and no site will be created. This error is not experiences with current Chrome or Firefox browsers. As a work around please use one of these alternate browsers.
IDS-2721	There is a known issue when using OAuth2 applications where the target application name is not shown, but should be by using the client_name parameter in the JSON metadata.
IDS-2750	There is a known issue where refresh tokens are invalid for Unregistered SMS with an Ubilogin Directory user. There is no work around for this item.

CustomerID

Ticket number	Description
IDS-693	There is a known issue with user approvals from Users view. If there are required attributes for the approval step, these are not validated if approval is done through the Users view.
IDS-1332	There is a known issue with CustomerID where it is not possible to use one email account for multiple UIDs created in CustomerID. Work around: It is possible for the system administrator to use custom attributes holding the same email address in the second or third CustomerID UID.
IDS-1358	There is a known issue within CustomerID where an administrator applying permissions across a whole organization will result in a failure of CustomerID to initialise. Work around: Admins should ensure that they do not apply permissions to an entire organisation, but apply the permission to a specific organisation class. All classes within an organisation may have the permission added, but not to the whole organisation at the same time, during the same commit.
IDS-1365	There is a known UI improvement for lists of Users and Roles for CustomerID administrators. Currently the lists are not ajax based, which means that cannot be called via popup, unlike other lists seen in CustomerID Admin UI. While this does not cause an error, it is not ideal from a usage point of view.
IDS-1373	There is a known issue in CustomerID when a new user is created in a non-virtual organisation, the invitation can contain a role when no role has been approved for that user.
IDS-1380	There is a known issue with CustomerID organisational attributes where the UI validation (validation.json) is not utilised. This impacts MOD001, POST100, PUT101 and MOD003. Using the API calls will result in good responses, but no organisational attribute change will be made.
IDS-1382	There is a known issue within CustomerID mandates where no email is sent to the user or organisation when the configuration is set to false (mandate.receiver.approval = false), even though the administrator requests a mail to be sent. No error or warning screen is displayed.

IDS-1389	There is a known usage limit in CustomerID Mandates. When viewing a mandate, currently only the role is shown. It would be more user friendly to show both the role and its organisation within the mandate view. There is no workaround.
IDS-1411	There is a known issue within the CustomerID XML schema ID, if an administrator makes an error and reuses and existing variable ID, this second use of the variable ID will not be assigned but the organisation will still be created. No error is reported. This can cause troubleshooting and usage errors. Workaround: Administrators should ensure that variable IDs are unique prior to creating new variable IDs within the system installation.
IDS-1413	There is a known error in CustomerID mandates if the mandate name is longer than 61 characters. If longer than 61 characters, creating the mandate will fail. Workaround: Do not create mandate names longer than 61 characters.
IDS-1418	There is a known issue with CustomerID REST API MOD008. If an administrator removes a single mandate role from a user with multiple mandate role, the original (removed) mandate template still exists within the LDAP database. This can result in troubleshooting errors and database checking errors (backup, etc).
IDS-1419	There is a known issue with CustomerID REST API MOD021 when creating a new user. Even when the API call appears to work, the user is not added to the organisation. Workaround: Do not use REST MOD021 (modification) during the creation of a new account. Please ensure you use create APIs when making new users.
IDS-1446	There is a known issue when using CustomerID REST API MOD009 to create a new user. The API will return 200 OK even when the new user password is not set; this results in a failed account creation. Workaround: Do not use REST API MOD009 (modification) to create a new user account. Please ensure you use create APIs when making new users.
IDS-1463	There is a known issue when using the CustomerID lost password recovery wizard where the wildfly server will log an exception in the error log. The password reset works correctly for the end user, but the resulting log file is cumbersome for large deployments where end users often reset their passwords. The error exceptions can be safely ignored, these will be corrected in a future release.
IDS-1468	There is a known issue caused by an Administrator altering the name of an Organisation when a new user has registered but not yet been approved. An application error occurs and is logged. Workaround: To avoid this only change an organization name when the pending user view is empty.
IDS-1474	There is a known issue that results in unsaved organisational custom attributes occurring when approval is set to false; attributes are saved when they should not be.
IDS-1476	There is a known issue within User DrivenFederation (UDF) of a social login during registration. If a user attempts to register more than one social login (UDF) against an external account a warning error message is presents. Resolution will be to provide the user a message explaining that they have already UDF'd a social account to this internal account and it is not possible to register a second social account.
IDS-1478	There is a known issue that results in a null pointer exception with stack trace if a user attempts Self Service User Driven Registration (UDF) of a social login account when UDF is not enabled within the CustomerID service.
IDS-1494	There is a known issue that causes occasional error pages to be displayed when a user logs out of their federated (User Driven Federation, UDF) social login account.
IDS-1500	There is a known issue where an error condition is caused if a user creates a password via the UI with 3 or more characters of their first or last name. Password verification does not permit this, and an error is raised. This error is not present if user passwords are created via API call.
IDS-1504	This known issue is a regression. When a user is invited to multiple roles, only one role appears in the invitation screen. This impacts both CustomerID Admin UI and user Self-Service.
IDS-1509	There is a known issue where a new user being invited to a virtual organisation the CustomerID administrator cannot approve the user; an internal server error occurs.
IDS-1555	There is a known issue where the mandate tab cannot be accessed on the CustomerID UI if the localisation information is incomplete. Workaround is to ensure that all localisation fields are completed.
IDS-1681	There is a known issue where the cursor focus remains in the mobile text field after a user has selected the email confirmation, when both email and mobile confirmations are required.
IDS-1706	There is a known issue with null values (DbAssignable.set and DbAssignable.isNull) which may result in NullPointer exceptions when using REST calls. This impacts Roles, Mandates and Invitations.
IDS-2033	Search response when using the CustomerID authoriser rule will return duplicate entries if capitalisation is present in the searched term or in the database field. In the future, no duplicates will be returned even if capitals are used or present in the naming field. Example: friendlyName and friendlyname.
IDS-2091	There is a known issue that the "New Organization" field in the "Open user applications" approval tab sometimes shows incorrect status
IDS-2093	There is a known issue that listing of users doesn't take into considerations users that are in locked status
IDS-2162	There is a known issue in CustomerID within Mandates, where no renotify email is sent to the administrator when an existing user requests a mandate for an existing additional organisation. No email is sent to Administrators for approval and no errors are logged. There is no workaround for this issue.
IDS-2201	There is a known issue in CustomerID where an email to a user with a single expiring or expired role will have all open roll invitations listed in the email, not just the expiring or expired role invitation.
IDS-2205	

IDS-2207	There is a known issue in CustomerID where interrupting the creation of a pending user will reset localisation of the browser session.
IDS-2231	There is a known issue when Administrator denies a role request for a user, that user gets two emails sent to them. One stating "Role invitation denied" and a second one stating "Role denied".
IDS-2233	There is a known issue in CustomerID API 1.2 REST call MOD025 "Create Role Invitation" related to email notification. If this REST call is used, the inviter mail address configured does not get a notification when the end-user approves the received role. The notification still works if role invitations are done through the GUI.
IDS-2234	There is a known issue where a user who has been invited to a role but not registered for that role within the defined time limit does not receive a reminder email that they have been invited to a role. See also: IDS-2235 below.
IDS-2235	There is a known issue where a user who has been invited to a role but not registered for that role within the defined time limit is not informed that the role invitation has expired. The user will have an email invitation with URL that does not function, they may become confused as they are not informed that the invitation has expired. See also: IDS-2234 above.
IDS-2290	There is an issue opening approval tab under main organization branch if there are around 10 000 sub-organizations. As a workaround, you can choose not to use recursive selection by adding "admin.approvals.recursive.selection.default = false" to you eidm2.properties file. See also: IDS-2310 below.
IDS-2310	There is an issue searching roles under main organization branch if there are around 10 000 sub-organizations. As a workaround, you can choose not to use recursive roles by adding "ui.organization.roles.recursive = false" to you eidm2.properties file. See also: IDS-2290 above.
IDS-2311	There is a known issue in approval view where changing main organization for a pending user in a sub-organization fails to create the new sub-organization in LDAP. This will need to manually be resolved by removing the invalid sub-organization in SQL
IDS-2312	There is a known issue in approval view where changing technical name of an organization to include Scandinavian letters doesn't work.
IDS-2420	There is a known issue in registration when pressing Enter without filling in all required fields causes registration to get cancelled instead of highlighting the required fields needed to complete the registration. Identified in CID 5.3.5
IDS-2649	There is a known issue with REST API 1.0 (MOD004b) & 2.1 (PUT103) when updating user's custom attribute to empty it does not remove the value for LDAP
IDS-2652	There is a known issue if a username attribute is removed via Admin or Self-Service UI then saved in an empty state, the UI will display an internal error.
IDS-2683	There is a known issue where CID REST API's 2.0 and 2.1 do not locate organisations with URL encoded characters in their names. Work around, if possible, ensure there are no URL encoded characters within organisation names. (example Ä Ö Å).
IDS-2703	There is a known issue where a role name with different case can be created which results in one LDAP entry and two SQL entries.
IDS-2709	There is a known issue where an installation which has defined custom attributes will cause a stack trace to be logged if a user is created without filling in all custom attributes. Work around: do not create users without all custom attributes configured.
IDS-2712	There is a known issue where an internal error is shown and stack trace is logged when a user registers with the same organisation name as an existing organisation but in a different case. Example. "UBISECURE" when "Ubisecure" already exists.
IDS-2713	There is a known issue impacting Windows server installations, where the import and export tools fail to move users between CustomerID 5.3.x and later versions.

Considerations and limitations

SameSite cookie changes in Google Chrome

In Google Chrome version 80 and above, the default behaviour of cookies that are used in cross-domain use cases have changed. If your applications or services are communicating between different top-level domains you need to take the following actions as described in our SameSite cookies changes technical announcement to ensure that they continue to operate as before.

Long Certificates Require Manual Installation in Linux Version

When a certificate is set in suffix.pfx, whose base64 encoded string is longer than about 4000 characters, the installation of SSO ends in a failure. This is due to an issue with an OpenLDAP tool *ldapmodify*, which is unable to read lines longer than 4096 characters long and the installation script writes the base64 encoded certificate in one line in *secrets.ldif*. To address this issue, a tool *ldiffold.sh* was included with SSO 7.1.0 linux version, which wraps given ldif file so that it no longer contains lines that are too long. It can be run as follows:

```
cd /usr/local/ubisecure/ubilogin-sso/ubilogin/ldap
../../tools/misc/ldiffold.sh < secrets.ldif > secrets.ldif.tmp
mv -f secrets.ldif.tmp secrets.ldif
```

Ubilogin Ticket Protocol Attribute Size Limits

The Ubilogin Ticket Protocol uses the HTTP GET method to send authentication and authorization information from UAS to Web Agents. The HTTP GET method has a size limit. The size limit affects the amount of information it is possible to successfully send from UAS to Web Agents. The SAML 2.0 protocol resolves this size limit by using the HTTP POST method to send information from UAS to Web Agents.

Ubilogin SAML Service Providers use SAML 2.0 protocol.

Ubisecure SSO, SAML 2.0 and High Availability

When installing Ubisecure SSO in High Availability mode, there are some restrictions due to some protocol requirements when using SAML 2.0. Please refer to the Ubisecure Clustering document for more information.

Backwards compatibility issues

Swedish BankID Authentication Adapter

As of Ubisecure SSO 8.4.1, the Swedish BankID Mobile authentication adapter has to be configured using the JWKS key id (kid) exposed in the SSO JWKS metadata. See Installing and configuring Swedish BankID - SSO for more details.