Change log - SSO

Please see the current Release Notes (here - scroll down to change log) for the active release change log

Ubisecure SSO 8.x.x

SSO 8.5.1 (07/10/2020)

Improvements

- IDS-2719 - ubixmlsec library has been updated to version 1.5.8.50494 to support http://www.w3.org/2009/xmlenc11#aes128-gcm encryption algorithm that will be taken into use by Suomi.fi service in the near future

SSO 8.5.0 (17/06/2020)

New Features

- IDS-1303 - Mobile Connect integration has been extended with support related to logging and consent. This enables Mobile Operators to take Mobile Connect Authentication and Authentication Plus product into commercial use. The items that have been updated for this feature can be found in the improvements section.

Improvements

- IDS-2516 - OAuth 2.0 applications can be extended with compatibility flag *ExtendedOAuth2AuditLogging*. This enables additional log entries to the audit log to facilitate Mobile Connect billing use cases. This can also be use for other OpenID Connect use cases. More detailed information can be found from Additional audit logging for OAuth 2.0
- IDS-1304 - Authorisation policies have been updated with scope field. This will allow Administrators to specify which scopes should be evaluated for OpenID Connect and OAuth 2.0 applications. You can read more about how to Manage authorization policies - SSO here
- IDS-2522 - Improved consent page includes requested scopes and confirm/cancel buttons instead of previous static text and checkbox. This improvement can be used for OpenID Connect methods and OAuth 2.0 applications. For other applications and methods, an updated static page of consent information will be shown to the end user. Read more about how to configure the consent screen from our Login screens - SSO and Internationalization - SSO documentation pages.
- IDS-1591 - Mobile ID (Mobiilivarmenne) phone number input field has been changed from '*text*' to '*tel*' to improve the user experience on mobile devices. Users default screen will show number keypad rather than alphabet keyboard, easing use of the service
- IDS-2486 - Optimisation of LDAP search in Password Reset application related to lookup of available methods
- IDS-2014 - Additional information for the different entry types has been added to our Audit log description - SSO
- IDS-2034 - Improved documentation how to setup authentication methods using SSO Management API can be found from OpenID Connect authentication method - SSO
- IDS-750 - Improved documentation related to handling of error situation not to expose any sensitive server or software information. Read more about how to use reverse proxy in our Security considerations for production environments - SSO
- IDS-1487 - Improved version handling of SSO components in order to have a better understanding of which version is currently installed. Logging of correct version (i.e. same as the release version) during SSO startup
- IDS-2445 - Improvement to how threads are handled for Health check API. In clustered environments it was noticed that the health check calls could go into a deadlock due to timing issue when connection was shutting down
- IDS-2615 - OAuth2 / OpenID Connect Token responses have been changed to exclude the id_token for refresh requests. This is to make sure that no additional information is shared with the application that the user has not approved to be shared. Read more about Access Token and ID Token from Authorization code grant and web single sign-on - SSO
- IDS-2608 - Updated audit log field "Web Application User ID" to get username sent to the application in the log entries that have this field available. More information can be found from Audit log description - SSO

Corrections

- IDS-2158 - Version number in the footer of SSO Management UI now correctly displays the installed version of the application
- IDS-2317 - UsernameUserMappingIdentityFactory flag has been set to disabled as default as specified in SSO 8.4.1 release notes. If this functionality needs to be enabled follow the Enabling UsernameUserMappingIdentityFactory instructions
- IDS-2032 - Changing log levels in SSO management UI will now come into affect without restarting SSO application, this would previously require a restart
- IDS-1182 & IDS-1469 - Documentation has been updated related to how to configure your reverse proxy in order not to expose any sensitive server or software information. Read more about how to use reverse proxy in our Security considerations for production environments - SSO page
- IDS-2537 - Correction to jQuery call that broke WS-Federation logout in 8.4.0 and 8.4.1. If using WS-Federation methods, we suggest to upgrade to SSO 8.5.0 to resolve this issue

SSO 8.4.1 (06/02/2020)

Improvements

- IDS-2161 - Merged changes made in SSO 8.3.8 that did not make it into SSO 8.4.0 release (see Change log - SSO)
- IDS-2058 - Addition of compatibility flag for UsernameUserMapping legacy feature in order to prevent exhaustion of LDAP connections. This will be disabled by default in upcoming SSO 8.5.0 release (Disabling UsernameUserMappingIdentityFactory)
- IDS-2166 - Inclusion of KeyID in metadata generated by SSO Management API (OpenID Connect authentication method - SSO)
- IDS-2283 - Client metadata extension *ubisecure_request_parameters* / *acr_values* has been updated to have highest priority in outbound requests in order to ensure that correct values are sent (OpenID Connect authentication method - SSO)
- IDS-1999 - Ability to configure *RequestedAuthnContext* through *AuthnContextClassRef* or *AuthnContextDeclRef* together with *comparision* for SAML authentication methods (SAML IDP Proxy - SSO)
- IDS-2303 - Ability to configure the thread pool size of Mobile PKI authentication method (Installing and configuring ETSI MSS Mobile PKI - SSO)

Corrections

- IDS-2208 - Fix for *StrictAudiencePolicy* to be able to set the compatibility flag system-wide, this did not overwrite application or authentication method flags set in SSO 8.3.8 (OpenID Connect authentication method - SSO)

SSO 8.4.0 (12/11/2019)

New Features

- IDS-1103 - Accounting Service
  - More information about this feature can be found from our Developer portal (Accounting Service - SSO)
- IDS-994 - Per user authentication matching
  - More information about this JavaScript based frontend user interface extension can be found from our public Github repository (https://github.com/ubisecure/per-user-authentication-matching)

Improvements

- IDS-58 - Server side session storage/Redis product documentation (Use Redis with Identity Server)
- IDS-79 - NameIDPolicy must be set for AuthnRequest sent by SSO
- IDS-110 - Updated SSO external library (3rd party) dependencies (3rd party licenses - SSO)
- IDS-684 - AuthnContextClassRef from a SAML Identity Provider to SSO (IdP Proxy) should also be possible to be forwarded to SP
- IDS-930 - SSO management API for persistentID (PCR) name mapping
- IDS-1080 - Identity Server supports BCrypt for password encoding

Corrections

- IDS-653 - Name change: Agent has been replaced with Application in SSO UI
- IDS-683 - Fix for deadlock in JLDAP
- IDS-712 - Fix usability on Unregistered SMS login screens. Focus set to OTP field
- IDS-1106 - Fix for SSO server jwks interoperability issue in Chrome
- IDS-1190 - Fix for one time feature not working for OAuth applications when there is SSO session available
- IDS-1412 - Fix for REDIS failover when the node configured in SSO goes offline

Ubisecure SSO 8.3.8 (24/10/2019)

This release improves the compatibility with Finnish Trust Network. It also includes improvements on general OpenID Connect compatibility.

Improvements

- IDS-2037: OpenID Connect: Ability to duplicate parameters outside the request object when sending Authorization requests as JWTs
- IDS-2107: OpenID Connect: Implementation of Key ID in JWKs, JWS and JWE
- IDS-2108: OpenID Connect: Send client_id as a request parameter in Token requests when using client assertions
- IDS-2110: OpenID Connect: Ability to perform relaxed or strict JWT aud claim validation
- IDS-2113: OpenID Connect: Improved UI locale handling
- IDS-2114: OpenID Connect: Ability to perform Authentication request with HTTP POST instead of GET
- IDS-2115: OpenID Connect:: Include the aud claim in client assertions
- IDS-2164: OpenID Connect: Ability to define static `ubisecure_request_parameters` to be sent with Authorization requests

Ubisecure SSO 8.3.7

- This version was omitted from public consumption due to limited use functionality

Ubisecure SSO 8.3.6 (12/04/2019)

Improvements

- IDS-1412: Improvements in support for Redis Cluster failover during server startup and runtime.
  - SSO now supports configuring more than one initial seed nodes which are used during SSO startup. Instructions on setting the initial seed nodes can be found here.
  - SSO now recovers from changes in the Redis cluster's topology during runtime, such as nodes going down and back up.

- IDS-1460: The errors "User not found" and "Invalid credentials" are no longer revealed in "subStatus" attribute of the JSON object "view", which can be found when viewing the *page source* of the login page.

Ubisecure SSO 8.3.5 (01/03/2019)

Corrections

- IDS-1354: Fixed warning of missing library file `commons-daemon.jar` in application server log during startup
  - This issue occurred in version 8.3.4 but does not cause regression other than the warning note in the logs

Ubisecure SSO 8.3.4 (21/02/2019)

New Features

- IDS-1308: Finnish Trust Network: Support for SAML2 LG extension as specified in FTN SAML2 Profile v1.0 chapter 3.5.3.1.
  - SSO is now able to read the LG extension from inbound SAML 2.0 Authentication Requests and use it as the login UI locale; and write it to outbound SAML 2.0 Authentication Requests.
  - For SAML 2.0 Authentication Methods, writing the extension in an Authentication Request requires a new Compatibility Flag `FinnishTrustNetwork` set for the method.
  - For SAML 2.0 Applications, the Extension is read from an Authentication Request automatically if one is available.

Corrections

- IDS-1326: Running the setup.sh for Enterprise Linux doesn't require high system entropy.
  - This was an errored requirement used only in 8.3.2 and 8.3.3
- IDS-1279: Mobile Connect Authentication v1.1: Error responses for Mobile Connect authentication requests are now compatible with the updated Authentication 1.1 profile.

Ubisecure SSO 8.3.3 (17/01/2019)

New Features

- IDS-1146: One-time password format in OAuth SMS/SMTP grant can be freely formatted.
  - Check the documentation from Configuration of unregistered SMTP - SSO and Installing SMS authentication method - SSO.

Ubisecure SSO 8.3.2 (14/01/2019)

New Features

- IDS-1117: Support for HTML emails in OAuth SMTP-OTP Grant.
  - You can set a new parameter in OAuth and our language files to set an explicit content type for emails and if omitted then plain text will be used for backward compatibility.
  - Check the documentation from Configuration of unregistered SMTP - SSO and Password Reset application internationalization - SSO.

Corrections

- IDS-947: Corrected ForceAuthn authentications when user has already an existing authentication.
- IDS-1037: Made it possible to update Tomcat version.
  - Check the *RefreshServlet security* chapter from Security considerations for production environments - SSO and Configuring CORS with credentials - SSO.
- IDS-1106: Corrected JWK interoperability issue with Chrome browser.

Ubisecure SSO 8.3.0 (12/10/2018)

New Features

- IDS-270: Password Reset - A new web application for resetting a forgotten password.
  - More information in the documentation.
- IDS-639: Support for Swedish BankID via external Authentication Adapter using *Ubisecure Backchannel Authentication Adapter* (UBAA) Authentication Method.
  - Technical information, installing and configuring Swedish BankID Authentication Adapter is described here
  - Installing the Ubisecure Backchannel Authentication Adapter Authentication Method is described here
    - SSO Management UI supports configuration by providing new method type *Backchannel Authentication Adapter*

Impovements

- IDS-963: The LDAP search for finding a ubiloginAuthMapping entry in the Ubilogin Directory, that is performed each time a user is authenticated, consumes less resources
- IDS-78: LDAPS support for SSO install.sh, export.sh and import.sh
- IDS-388: The default font size for error messages is increased from *0.8em* to *1.1em*

Corrections

- IDS-60: Disabled users cannot log in to applications with accounts that are linked by User Driven Federation.
  - When a user authenticates with a federated identity and a matching local account is returned by a FederationManager implementation (i. e. CIDFederationManager or UbiloginFederationTable), the local account status is now verified and the access is denied if the status is not valid.
  - The workaround fix *Preventing disabled users from logging in with user driven federation* as described in the page User driven federation is not needed anymore.
- IDS-1014: SSO management doesn't disclose the client_secret for OAuth2 application agents
  - When uploading a client metadata to an OAuth 2.0 application agent using the SSO Management Console, if the metadata contains a `client_secret`, the `client_secret` is now removed before storing the metadata in the agent configuration in Ubilogin Directory.
    - Prior to 8.3, the `client_secret` was not removed, but stored as is in the agent configuration in Ubilogin Directory.
  - Furthermore, even if the `client_secret` has already been stored in the agent configuration, as may be the case for agents that have already been activated prior to SSO 8.3, the `client_secret` will now not be shown in the SSO Management Console nor in the SSO Management API.
    - Prior to 8.3, the `client_secret`, if set in the client metadata, was shown in SSO Management Console.
- IDS-1052: OTP lists for UbiloginDirectory users created from SSO Management Console are not invalid randomly
- IDS-945: Execute flag is set for the bash scripts in the Linux version
- IDS-723: The SMTP message that is sent by SMTP OTP method sets the Date header as specified in RFC 822
- IDS-821: Some errors (such as LDAP read timeout) during password/reset don't deactivate the servlet that catches it
- IDS-437: Main Class in the MANIFEST.MF of sso-pkipolicy.jar is correct
- IDS-1074: Linux version: OpenLDAP installation script (ldap/openldap/install.sh) doesn't show an unnecessary error message *ldap_modify: No such attribute (16)*

Ubisecure SSO 8.2.25-1 (06/2018)

Corrections

- IDS-782: Added missing OTP Server files to installation package.

Ubisecure SSO 8.2.25

Improvements for Finnish MobileID (Mobile Certificate / Mobiilivarmenne) Authentication Method

- IDS-578: Configurable status request delay.
  - The delays between the transaction request and the initial status request, as well as the delay between consecutive status requests after the first one, are configurable. The configuration parameters are `initialStatusRequestDelay` and `consecutiveStatusRequestDelay`. Refer also to the method configuration guide.
- IDS-658: Separate error message when authentication times out.
  - There is a new error message `LOGIN_EXPIRED` that is shown whenever authentication timeout occurs. The timeout is set in the `ae.timeout` configuration parameter. The possible error messages are listed under *ETSI MSS Mobile PKI Unregistered Screen* in Login Screens.

Corrections

- IDS-589: Chrome: Forms submitted using POST to SSO's browser endpoints don't work.
  - SSO 8.2.19 and 8.2.24 had the issue with Chrome browser, that Forms submitted using POST method to SSO's browser endpoint return 403 Forbidden HTTP status. This caused problems for example with SAML 2.0 login sequence with Ubisecure SAML SP module, because it uses SAML HTTP-POST binding by default, which is based on send a form using POST. That issue is now fixed.

Ubisecure SSO 8.2.24

Improvements and Corrections for Finnish Mobile ID (Mobile Certificate / Mobiilivarmenne) Authentication Method

- IDS-89: Configurable length of Event Identifier
  - Length of the event identifier used for matching the authentication event in the mobile device and the browser can now be configured to be 4 to 8 digits long. This is done by setting the new configuration parameter `eventIdLength`, which is also described in the method configuration documentation.
- IDS-555: Show the error message for missing or invalid NoSpamCode
  - When NoSpamCode has been asked from a user, but the NoSpamCode the user has given is invalid or missing, error message is now shown to the user to indicate what went wrong.
- IDS-556: NoSpamCode field being visible or not is preserved when error message is shown
  - NoSpamCode field is hidden in login screen with error message, if the field was also hidden before the error. Conversely, the field is shown, if it was also shown before the error.
- IDS-582: Correct text in the label for the phone number is shown in the wait screen

    - The wait screen (the screen where the Event Identifier is shown) shows now correct text `MPKI_UNREGISTERED_MOBILENUMBER` in the label for the phone number.

Other Changes

- IDS-464: Mobile Connect / OpenID Connect: SSO decrypts an encrypted Mobile Connect login_hint when passed to OpenID Connect Authentication Provider
    - SSO passes login_hint to an Open ID Connect Authentication Provider as a generic unencrypted OpenID Connect login_hint also, if the login_hint originates from a Mobile Connect Authentication Request that contains an encrypted login_hint.

Ubisecure SSO 8.2.19

Improvements and Corrections

- IAM-2304: OpenID Connect authentication method
    - OpenID Connect authentication providers can now be used as authentication methods in SSO. For more information, please see the documentation in OpenID Connect authentication method - SSO.
- IAM-1038: OpenID Connect: Support for configuration of essential JSON Web Algorithms in encryption and signing
    - Along with the previously supported RS256 digital signing algorithm, we have added support for HS256, in which the signing key is derived from client_secret value. For encryption, there are also options for algorithms in key management and content encryption.
      Complete list of supported algorithms for the various endpoints can be found in the OpenID Connect provider metadata (see documentation for OAuth 2.0 and OpenID Connect metadata - SSO).
      Reference: https://tools.ietf.org/html/rfc7518
- IAM-2156: OpenID Connect: Configurable idtoken encryption and signing
    - Added support for enabling encryption for idtokens, which can be configured by setting *id_token_encrypted_response_alg* and *id_token_encrypted_response_enc* configuration parameters in the client metadata. The digital signing algorithm used for idtokens can respectively be configured by setting *id_token_signed_response_alg* (by default it is "RS256").
      Complete list of supported values is provided in the *id_token_encryption_alg_values_supported*, *id_token_encryption_enc_values_supported* and *id_token_signing_alg_values_supported* attributes in the OpenID Connect provider metadata (see documentation for OAuth 2.0 and OpenID Connect metadata - SSO).
- IAM-2157: OpenID Connect: Configurable userinfo response encryption and signing
    - Added support for enabling encryption for userinfo endpoint responses, which can be configured by setting *userinfo_encrypted_response_alg* and *userinfo_encrypted_response_enc* configuration parameters in the client metadata. The digital signing algorithm used for userinfo response can respectively be configured by setting *userinfo_signed_response_alg* (by default no signature is added to userinfo response).
      Complete list of supported values is provided in the *userinfo_encryption_alg_values_supported*, *userinfo_encryption_enc_values_supported* and *userinfo_signing_alg_values_supported* attributes in the OpenID Connect provider metadata (see documentation for OAuth 2.0 and OpenID Connect metadata - SSO).
- IAM-2303: OpenID Connect client integrations: JSON Web Token (JWT) Profile for Client Authentication
    - Added support for JWT based methods *client_secret_jwt* and *private_key_jwt* for client authencation. The method to be used by the client integration can be configured by setting *token_endpoint_auth_method* and *token_endpoint_auth_signing_alg* configuration parameters in the client metadata.
      Complete list of supported values is provided in the *token_endpoint_auth_methods_supported* attribute in the OpenID Connect provider metadata (see documentation for OAuth 2.0 and OpenID Connect metadata - SSO).
      References:
        https://tools.ietf.org/html/rfc7521#section-4.2
        https://tools.ietf.org/html/rfc7523#section-2.2
        http://openid.net/specs/openid-connect-core-1_0.html#ClientAuthentication
        https://tools.ietf.org/html/rfc7519
- IAM-2364: OpenID Connect client integrations: Any port is allowed for Loopback URI Redirection
    - When a loopback URI (such as "http://localhost/app") is set in the redirect_uri or redirect_uris attribute of the client metadata of an OAuth2 application, then it is allowed use any port in the redirect_uri of the Authorization Request.
      Reference: https://tools.ietf.org/html/draft-ietf-oauth-native-apps-09#section-7.3
- IAM-2363: OpenID Connect client integrations: App-declared Custom URI Scheme Redirection
    - Applications can register customer URI schemes, such as "com.example.app", as their redirect_uris.
      Reference: https://tools.ietf.org/html/draft-ietf-oauth-native-apps-09#section-7.1
- IAM-1435: OpenID Connect client integrations: Support for scope in client metadata
    - Use the client metadata scope setting to restrict and white list the set of allowed scopes for a OAuth client.
      Scopes "openid", "userinfo" and the client_id of the metadata's owner cannot be disallowed, so they are always implicitly included in the scope list (if set in the client metadata in the first place).
      Reference: https://tools.ietf.org/html/rfc7591#section-2
- IAM-1847: Java Runtime Environment is no longer provided in the SSO installation package
    - Ubisecure SSO uses now an existing JRE installation provided in the standard JRE_HOME environment variable. This must be taken into account for all upgrades from pre-8.2 SSO's.
- IAM-2353: SSO writes information of the system environment in the diag log during start up
    - When starting up, SSO writes a comprehensive information printout in the diagnostics log about the system environment it's running on. The printout includes JRE version, environment variables, Java security providers, trusted certificates etc. This is crucial for our support, as with the JRE now removed, it would otherwise be difficult and time consuming to gain knowledge of the exact details of the environment SSO is running on.
- IAM-2873: OpenID Connect: Access token lifetime follows SSO session's lifetime
    - Access token lifetime follows the lifetime of the associated SSO session, in which the token was issued. This means that an access token's lifetime can be extended by extending SSO session's lifetime. Conversely, if an SSO session is terminated, all access tokens issued during that session are revoked.
- IAM-2982: OpenID Connect: Second use of authorization code revokes the access token that was previously issued for the authorization code
    - When authorization code replay is detected, the access token, that has been issued for the replayed authorization code during its first use, is revoked.
- IAM-2891: Error page without authentication methods is now shown also for SAML and Tupas agents

    - The plain error page, that is shown when there are no visible authentication methods to be shown, was previously skipped when the application agent was of type SAML or Tupas whereas for other agent types it was visible. This behaviour is now unified so that the error page is visible with all agents.
      Any other page (such as authentication method list also known as "menu" page) that happened to contain an error message was shown with all agents even in previous versions.
- IDS-22: Improved support for UI template setting in Password Change and Password Reset
    - There are some UI template settings, that hasn't been shown properly in the Password application. These setttings are logo.ico, logolink, logoalt, HEADER_TEXT_1, HEADER_TEXT_2 and COPYRIGHT. Now they are shown and updated correctly based on the selected UI template also in the Password Application.
      Secondly, if user changes the locale in the Password Application, the changed locale is now included in the URL that is sent in the password reset mail. Also, if the password reset was initiated from SSO login page, the changed locale is propagated back to the SSO page when user is returned there after finishing or canceling the reset.

Ubisecure SSO 8.1.2 (15/05/2017)

Corrections

- IAM-2376: The rules specified in methodmenu.rules are now applied correctly

Ubisecure SSO 8.1.1 (26/04/2017)

New Features

- IAM-2320: Tupas IDP: If A01Y_RETLINK contains query part, the query part is now included also in the tupas response.

Corrections

- IAM-2300: In fresh SSO installation, user can now define "allowed to" -group for SSO API agent
- IAM-2308: Agent type of SSO API agent is now correctly OAuth agent
- IAM-2326: WS-Federation: Continue button is now shown after successful IDP initated logout, if there's active WS-Federation session
- IAM-2311: Url is corrected for Nordea TUPAS test method (tupas.nordea.1) in methods-tupas.ldif

Ubisecure SSO 8.1.0 (28/03/2017)

New Features

- IAM-1374: SSO support for wreply and wfresh paraneters in WS-Federation
- IAM-2019: SSO support for wauth and whr parameters in WS-Federation
- IAM-1352: SSO Management API - New functionality to add/remove/modify users
- IAM-1457: SSO Management API - New functionality to create mapping configuration (persistentId, refreshtokenPolicy)
- IAM-1735: Sms-mt-otp and smtp-otp grant, added error description to Error Response explaining the error situation
- IAM-1907: OTP Timout for Sms-mt-otp and smtp-otp grant,is now configurable in minutes. By default, there is no timeout.
- IAM-2073: TUPAS IDP A01Y_RETLINK parameter allows ignoring of query parameters from the URL(s)
- IAM-2110: Type and attribute names in SSO Management API calls for input are now case in-sensitive. Type and attribute names in responses are now in CamelCase.
- IAM-2204: Java updated to version jdk-8u121
- IAM-2197: Tomcat updated to version 8.0.42

Corrections

- IAM-2066: SSO Linux UbiloginDirectory does not fail to start after reboot (because the OS changes /var/run/ubilogin ownership to root:root)
- IAM-2075: Agents with empty template field, no longer show the wrong template in login page
- IAM-2018: Agent activation file download now works also in new Chrome browser

Ubisecure SSO 8.0.1 (02/12/2016)

Corrections

- IAM-1833: MPKI authentication now works with mobileconnectloginhint-compabilityflag and ENCR_MSIDN

Ubisecure SSO 8.0.0 (25/11/2016)

New Features

- IAM-1320: SSO Server acts as a TUPAS IDP
- IAM-1478: PCR generation - an option to use new kind of UUID format as specified in RFC 4122[9]
- IAM-1493: It is now possible to prevent SSO on server side by using agent setting (using either Forceauthn, oneTimeUse or both parameters)

- IAM-1736: New Ubisecure look and feel to SSO
- IAM-1770: New tomcat version 8.0.38

Corrections

- IAM-1685: SAML agent metadata configuration fixed - agentlogo is not mandatory when clientname is used

Ubisecure SSO 7.x.x

Ubisecure SSO 7.7.1 (03/10/2016)

New Features

- IAM-1506: SSO authorization policy can decrypt values

Corrections

- IAM-1538: SSO password app doesn't show errors for all users

Ubisecure SSO 7.7.0 (26/08/2016)

New Features

- IAM-1032: OpenID Provider Metadata, tokeninfo_endpoint replaced with introspection_endpoint (RFC 7662)
- IAM-1384: Token Introspection updates for RFC 7662
- IAM-1066: MPKI login screen can be configured so that it does not ask a spam code and tries automatically to login if mobile connect crypted loginhint is provided.
- IAM-1451: OAuth2 and SAML2 metadata agent logo, based on locale, can be set visible in the login screen, with or without the default SSO logo
- IAM-1474: SSO openldap version upgrade to openldap-2.4.44 (OpenLDAP is now compiled without DDS overlay and with both BDB (default) and new MDB backends)

Corrections

- IAM-1420: SSO management GUI copyright message is changed to state GlobalSign instead of Ubisecure

Ubisecure SSO 7.6.0 (29/05/2016)

New Features

- IAM-712: OAuth 2.0 Token Revocation (RFC 7009).
- IAM-1124: SAML Profile for OAuth 2.0 Authorization Grants (RFC 7522)
- IAM-1354: SSO Management API new functionality to allow Relying Party specified client_id and secret for OAuth2 metadata (RFC-7591 Dynamic client registration protocol)
- IAM-1364: OAuth2 and SAML2 metadata client name can be set visible in the login screen, id addition, or to replace to current hostname
- IAM-1365: SSO Login screen templates can contain also javascript resources
- IAM-1366: Username in login screen cannot be changed if mobile connect login_hint is encrypted (ENCR_MSISDN)
- IAM-1384: Oauth2 Token Introspection token_type supports refresh_token
- IAM-1448: OAuth2 OpenID Provider Metadata changes, tokeninfo_endpoint is replaced with introspection_endpoint. Note that tokeninfo_endpoint and /uas/oauth2/tokeninfo are deprecated (will be removed in the version after 7.6)
- IAM-1395: SSO can return grant type and refresh token create time to application using authorization policy
- IAM-1428: AuthnStatementSessionNotOnOrAfter interop flag to leave SessionNotOnOrAfter unassigned in SAML2 response
- IAM-1403: OpenID Connect idtoken contains azp attribute in Mobile Connect
- IAM-1404: OAuth2 idtoken attribute aud is now always array to fully support Mobile Connect
- IAM-1406: OAuth2 authorization endpoint error page now sets http status 400 to indicate error condition (Does not return user to relying party)

Corrections

- IAM-1402: OpenID Connect idtoken nonce updates correctly to new auth. requests (From same client using authorization code grant)
- IAM-1455: Password application url parameter "method" now handles the NUL character (= %00 url encoded) for password/reset application without error situation

Ubisecure SSO 7.5.0 (26.02.2016)

New Features

- IAM-5: OAuth2-extension for confirming Email and Phone number

- IAM-823: SSO Management REST API Phase 1
- IAM-873: Compability flag SendAssertionConsumerServiceURL for sending AssertionConsumerServiceURL in SAML-AuthnRequest
- IAM-1170: New compabilityflag ExplicitUnspecifiedAuthnContextClassRef for sending authnContextClassRef in SAML-response
- IAM-941: OTP server support for external SQL user database
- IAM-1060: Unregistered SMS OTP Authentication method
- IAM-1208: Unregistered SMTP OTP Authentication method
- IAM-1147: Login_hint now works also with unregistered authentication methods (unregistered MPKI, SMS and SMTP)
- IAM-1253: SSO Management UI to GlobalSign branding
- IAM-1296: OAuth request scope now ignored as long as the correct scope in use is returned in Token Endpoint response
- IAM-1297: Only password, authorization_code and refresh_token are allowed OAuth grant_types By default.
- IAM-1295: Template property useloginhint for showing OAuth2 login_hint in SSO
- IAM-1294: Support for Mobile Connect encrypted login_hint with prefix ENCR_MSISDN

Corrections

- IAM-183: Audit contains information after user tries with incorrect username

Ubisecure SSO 7.4.0 (27.11.2015)

New Features

- IAM-805: Upgrade SSO JVM to Java 8
- IAM-884: SSO Tomcat updated, version 8.0.27
- IAM-910: OpenID Connect/Mobile Connect Identity Provider
- IAM-966: Support multivalue SAML2 AuthnContextClassRef in methods
- IAM-995: updated OpenSSL version to 1.0.1p, used by OpenLDAP in linux installations

Ubisecure SSO 7.3.4 (30.9.2015)

Corrections

- IAM-997: Some button texts not visible in management UI
- IAM-998: Service cant be deleted if name contains "<>"

Ubisecure SSO 7.3.3 (29.9.2015)

New features

- IAM-817: SSO login flow should double check UDF linking need after registration and not ask for user consent if linking has be done
- IAM-895: Autocomplete for password input forms settable in UI-template (affects screens in SSO and password application)
- IAM-946: If address tracking (netmask) is disabled then a AuthnStatement/SubjectLocality element is no longer created in SAML Assertion
- IAM-948: If directory user mapping is successful for a user then UDF process will be skipped
- IAM-951: Backchannel messages (SOAP Logout) are now secured with TLS 1.2

Corrections

- IAM-25: SSO Management: Form inputs should be sanitized to prevent Cross-Site Scripting
- IAM-883: OAuth: Malformed JWT causes error "Unexpected char 127 (line no=1, column no=1, offset=0) at ...)"
- IAM-943: Session injection in Password application doesn't work in a reverse proxy deployment
- IAM-969: Methodmenu rules don't change when a template is changed

Ubisecure SSO 7.3 (29.5.2015)

New Features

- IAM-9: After a successfull password reset, a SSO session is created for the user and the user is redirected to a predefined url
- IAM-49: SSO Management UI for oAuth2.0 authorization server
- IAM-44: OAuth 2.0 Authorization Server
- IAM-73: Password application to use the SSO UI templates
- IAM-601: Keytool to support SHA256WithRSA in certificate signatures

Corrections

- IAM-743: Password reset token email link broken

Ubisecure SSO 7.2.1 (16.4.2015)

Corrections

- IAM-270: Redirect URL for OAuth2 Authentication Method shown in SSO Management UI is invalid

- IAM-266: "Logout failed" is shown when using iframelogout and more than one sp-session is active

Ubisecure SSO 7.2.0 (2.4.2015)

New Features

- IAM-19: Support for OAuth2 protocol in Authentication Methods
- IAM-18: Support for Facebook authentication using OAuth2
- IAM-15: Support for Google+ authentication using OAuth2
- IAM-14: Support for Vkontakte authentication using OAuth2
- IAM-24: New password encryption methods: SHA256,SSHA256,SHA384,SSHA384,SHA512,SSHA512,PKCS5S2,PBKDF2

Improvements

- IAM-27: Value of NameID/@Format can now be explicitly set or asserted in Method
- IAM-36: Support for RHEL/CentOS 7
- IAM-7: Support for user setting the new password when using Password-reset

Ubisecure SSO 7.1.0 (31.12.2014)

New Features

- SSO-574: User Driven Federation
- SSO-583: Support for Salesforce integration
- SSO-590: Support for setting emailAddress as NameID Format in Authorization Policy

Improvements

- SSO-472: Robots.txt search engine hiding
- SSO-556: NameIDPolicy format emailaddress not supported in authrequest
- SSO-565: Termplate API
- SSO-596: Improved NameIDPolicy processing

Corrections

- SSO-71: Columns messed up
- SSO-231: Exception stacktrace thrown to user's face when trying to log in after the login window has been open for a long time
- SSO-437: Web Agent activation fails on Chrome
- SSO-597: OpenID Yadis handling fails with no logging

Ubisecure SSO 7.0.0 (10.3.2014)

New Features

- SSO-482: Feature to embed encryption key with encrypted message
- SSO-536: Health check support
- SSO-535: Web Agent can change the used template when doing AuthnRequest
- SSO-539: Support for template switching in SSO's 'resume' interface
  See: Login UI Customization, Chapter 6. Returning to SSO login page from external applications

Improvements

- SSO-531: Support for Zendesk (missing ProtocolBinding caused ticket validation error)
- SSO-541: Unsolicited SAML message can be initiated from SSO UI
  See: Login UI Customization, Chapter 7. Generating Unsolicited SAML Response from SSO UI
- SSO-542: New parameters for SessionRelayService: isPassive, forceAuthn and oneTimeUse
  See:Login UI Customization, Chapter 7. Generating Unsolicited SAML Response from SSO UI
- SSO-545: Ubisecure favicon
- SSO-565: Template API
  See: SSO Management document, Chapter 10. Template API
- SSO-566: Discovery API
  See: SSO Management document, Chapter 9. Discovery API

Corrections

- SSO-496: Misleading "user is not authenticated" error message logged
- SSO-518: Stack trace on third-party IDP logout after access denied
- SSO-519: Exception is thrown when SSO receives AuthnRequest whose AssertionConsumerServiceURL is set to be something else than Location of the first AssersionConsumerService in SP Metadata
- SSO-530: Required attribute condition is not checked when no attributes are formed in an Authorization Policy
- SSO-533: SSO admin userface removes name format and friendly name specifications by itself
- SSO-534: Pressing Exit on the consent screen returns exception
- SSO-559: SMS OTP authentication method breaks in AD when method user amount exceeds 1500
- SSO-561: OTP login prompts for "Password sequence number: 1" when there are none left
- SSO-564: External Discovery always interrupts with error message EXTERNAL_DISCOVERY_INVALID_AUTHENTICATION_METHOD

Ubisecure SSO 6.x.x

Ubisecure SSO 6.8.0.34260 (4 October 2013)

Improvements

- SSO-118: Java EL expressions may be used in auhtorization policy rules and expressions
- SSO-112: NameID content in Assertions can be controlled in authorization policies
- SSO-511: Attribute-values can be concatenated in authorization policies
- SSO-515: Upgrade to Java 7 64bit
- SSO-516: Upgrade to OpenLDAP 2.4.35 64-bit
- SSO-517: Upgrade to Apache Tomcat 7.0.42
- SSO-520: Timelife of WS-Federation tokens can be changed

Corrections

- SSO-395: JSVC requires /usr/lib/libcap.so which may not exist

Ubisecure SSO 6.7.1.33229 (20 June 2013)

New Features

- SSO-501: ETSIMSS: Possibility to disable Schema validation

Improvements

- SSO-493: OTP Server with Ubilogin Directory user support
- SSO-506: macro.jar support for cmd.exe special characters

Corrections

- SSO-494: Text of close button in OTP List Print dialog cannot be localized
- SSO-498: Server does unwanted http queries to www.w3.org
- SSO-504: Disabled OTP list works if otp is the only method configured

Ubisecure SSO 6.7.0.32899 (17 May 2013)

New Features

- SSO-470: WS-Federation IdP support for SharePoint integrations

Improvements

- SSO-492: Add support for SHA256 digest
- SSO-483: Support for SAML metadata key-rollover when validating messages

Corrections

- SSO-476: Metadata Updater: If the SAML Metadata feed contains unexpected elements import fails.

Ubisecure SSO 6.6.2.32839 (6 May 2013)

Improvements

- SSO-340: Remove Ubilogin Managementin reset secret function
- SSO-472: Robots.txt search engine hiding
- SSO-477: OTP Print Screen to show printable OTP list top down
- SSO-488: Use Ubilogin management to set compatibility flags

Corrections

- SSO-475: Session status request refresh parameter counts timeout incorrectly

Ubisecure SSO 6.6.1.32263 (19 March 2013)

Improvements

- SSO-462: More specific UI customization for unregistered MPKI users
- SSO-454: Login form autocomplete works better in some browsers (Internet Explorer)
- DIRECTORY-46: Change DirectoryServices to return singleton LDAP and SQL connections

Corrections

- SSO-467: Javascript error during logout with IE8
- SSO-465: No audit log entry when user logs out.
- SSO-463: OpenID method NPE during login in SSO 6.6.0
- SSO-460: Management: Agent list on Method screen overflows
- SSO-459: Managed by rights for sites are not propagated through group memberships
- SSO-449: "Authentication method selected" entry missing from the audit log

Ubisecure SSO 6.6.0.30674 (28 Dec 2012)

New Features

- SSO-423: Cert AP configuration improvement
- SSO-440: Support for custom Tomcat server.xml configuration

Improvements

- SSO-59: Simplify Custom SSL certificate installation
- SSO-60: Tomcat Hardening
- SSO-293: During IDP initiated logout display warning if no SP sessions were terminated
- SSO-361: Set default template title tag to Ubisecure SSO
- SSO-450: Move keystore.pfx to custom folder
- SSO-452: Tomcat 7.0.34
- SSO-453: Java 1.6.37

Corrections

- SSO-172: Tomcat Log Rollover
- SSO-448: Two assertion received entries in audit log per one Tupas sign-in

Ubisecure SSO 6.5.0.29603 (9 Nov 2012)

New Features

- SSO-425: Print new OTP list during logon

Improvements

- SSO-400: Change etsimss to use etsimss-jaxb implementation
- SSO-417: SSO session management
- SSO-426: OTP Server with Katso SQL support
- SSO-428: Use 2048 bit key length for self-signed certificate
- SSO-438: Network address tracker disabled by default

Corrections

- SSO-419: Extraneous trailing commas in JSON conversation variables

Ubisecure SSO 6.4.0.28078

New Features

- SSO-408: Navigation to external applications from SSO UI

Improvements

- SSO-381: Authentication of REST services
- SSO-412: SSO UI javascript API

Corrections

- SSO-411: LDAP/SSL Performance degradation in JDK 1.6.0_29/30

Ubisecure SSO 6.3.2.27688

Corrections

- SSO-360: Method name (not Title) shown after PROXY_LOGIN_TEXT
- SSO-402: REST User Mapping service corrected
- SSO-405: install_initd failed on RedHat Linux 6.1

Ubisecure SSO 6.3.1.27499

Improvements

- SSO-394: Include selected attributes in audit logging
- SSO-396: On linux use lsb scripts for installing/removing service

Corrections

- SSO-368: AuthPolicy editor add attribute not working with IE8/IE9
- SSO-392: Mobile PKI with registered user should not ask for spam-code
- SSO-393: Internet Explorer 9 compatibility improvements (Ubilogin management)
- SSO-395: Linux: missing /usr/lib/libcap.so may prevent service ubilogin-server start
- SSO-397: Landing Page does not support locales nor templates

Ubisecure SSO 6.3.0.27241 (30 Apr 2012)

New Features

- SSO-110: Mobile PKI (Ficom Mobiilivarmenne) with Directory SPI support
- SSO-351: Session status request - REST interface to check server session status
- SSO-357: Ubisecure OTP List Server- REST interface for OTP list management

Improvements

- SSO-274: Multi-master replication with OpenLDAP on Linux
- SSO-374: OpenLDAP disk I/O performance, clustering improvements
- SSO-376: Java™ SE 6 Update 31
- SSO-377: Apache Tomcat Version 7.0.26
- SSO-378: OpenLDAP 2.4.30

Corrections

- SSO-347: Minor UI improvements in Management application
- SSO-352: SessionNotOnOrAfter was not set in assertion issued by SSO
- SSO-356: IDPProxy ForceAuthn=true caused isPassive=true
- SSO-359: Value of font-family in template-created CSS is always unicode-encoded
- SSO-360: Method name (not Title) shown after PROXY_LOGIN_TEXT
- SSO-366: Session object housekeeping improvements during logout
- SSO-368: AuthPolicy editor add attribute not working with IE8/IE9
- SSO-372: Locale attribute transfer fixed in IDP Proxy cases
- SSO-385: SSO Server assertExists error corrected

Ubisecure SSO 6.2.0.23692 (28 Oct 2011)

New Features

- SSO-292: OpenID Relying Party method with SAML IDP Proxy support
- SSO-332: Support for Common Domain Cookie discovery (CDC)

Improvements

- SSO-77: Password application improvements to detect password method automatically
- SSO-79: Configurable return link on successful/failed password change
- SSO-334: Password reset app can be used with more than one authentication method
- SSO-147: LDAP paging performance improvements
- SSO-215: Group Dynamic Member configuration directory selection drop down
- SSO-297: Management tool UI improvements for directory management
- SSO-275: OpenLDAP recompiled with SSL/TLS support for Linux
- SSO-314: Tomcat version upgraded to 7.0.20

Corrections

- SSO-235: OTP list cant be printed
- SSO-306: Services do not start automatically, even though Startup Type is Automatic
- SSO-318: Space character in method name caused error
- SSO-331: IDP-proxy and up-link IDP initiated front-channel logout corrected
- SSO-335: Custom template's color definitions now used on error page

Ubilogin SSO Server 6.1.1.21804 (1 Aug 2011)

New Features

- SSO-299: Support for External Discovery (aka WAYF)
- SSO-269: Support for Tupas v2.3
- SSO-183: Support for requiring user consent before permitting access

Improvements

- SSO-300: Java Web Agent does SP initiated logout by default

Corrections

- SSO-301: User defined css is not used on error page
- SSO-287: Directory SPI does not decrypt ldap connection credentials
- SSO-289 & SSO-290: Linux install issues

Ubilogin SSO Server 6.1.0.21057 (10 May 2011)

New Features

- SSO-185: Ability to add and remove Directory SPI repositories and authentication methods from management UI
- SSO-229: Add user interface to obtain user consent, before assertion is sent to application.
- SSO-217: Support for CDC discovery

Improvements

- SSO-176: Add feature to metadata-update tool to check revocation of installed IDP metadata
- SSO-213: Upgrade Tomcat to version 7
- SSO-216: Allow specifying SP specific Compatibility settings
- SSO-221: In SSO server discovery menu, display image links for methods
- SSO-222: Implement feature to present discovery menu methods in logical UI groups
- SSO-223: Create more rules for method visibility in discovery menu
- SSO-225, SSO-226, SSO-198, SSO-203 & SSO-224: Various cosmetic improvements in Management UI

Corrections

- SSO-211: Tomcat Installation script doesn't set write access to application server temp-directory for Local Service-account
- SSO-228: OTP authentication method help text shows "NIL" text for undefined lists as a list identifier.
- SSO-244: StepUp Login UI doesn't always show correct authentication methods, when there are many methods to select from
- SSO-262: Logout doesn't remove the SSO cookie
- SSO-263: SSO Server produces ticket or saml response after logout when navigating back in history with back button

Ubilogin SSO Server 6.0.1.19314 (12 January 2011)

Improvements

- SSO-193: Search application default wider view
- SSO-99: Resizeable LogViewer screen
- SSO-94: Logviewer more tolerant on bad end of line characters
- SSO-97: Improved UI button texts to add context to actions
- SSO-130: Simultaneous IPv6 and IPv4 support in SAML and Ticket protocol configuration
- SSO-69: Version information now shown on /uas/info page
- SSO-186: /uas/trace is enabled by default. Disable for production servers.
- SSO-190: Template-specific UI texts

Corrections

- SSO-84: Accessing disabled context menus causes server error
- SSO-164: Incorrect ubiloginAuthMethodType used in uas.ldif and methods.ldif
- SSO-169: Activating OTP list before enabling causes exception
- SSO-189: SSO Server fails with NPE after upgrade from 5.0.7
- SSO-191: InstantiationException from /uas/error
- SSO-192: Exit causes stack trace on timed out session
- SSO-196: "Update" button only partly visible on the home screen of management UI with IE7
- SSO-197: Form double submit happens in success screen if user succeeds in pressing Continue button before autosubmit

Ubilogin SSO Server 6.0.0.18955 (23 December 2010)

New Features

- SSO-117: SSO Server end-user UI redesigned
- SSO-50: javascript loggedin/loggedout function using status.js, success.png and pixel.gif
- SSO-158: Support for multiple SAML signing certificates
- SSO-161: Hashed TUPAS support
- SSO-27: Localized graphic resources
- SSO-31: Alternative order in login sequence: username + password, then method selection
- SSO-33: Save logout returnurl upon login
- SSO-65: Select authentication method in UAS and/or UWA
- SSO-128: Decide authentication method and user repository based on user name

Improvements

- SSO-92: HTML page validation
- SSO-146: Store session objects in ldap as dynamicObject types
- SSO-165: Attribute FriendlyName and Name Format support in updated Authorization Policy editor

- SSO-170: Mark session and other cookies HttpOnly
- SSO-187: Resizable Ubilogin Management UI
- SSO-12: Template and locale remembered during logout

Corrections

- SSO-13: Fatal error after Ticket validation error / attachTicketRequest
- SSO-17: IdP Proxy with multiple agents causes loop on logout
- SSO-19: Fix the functionality of UAS cancel and back buttons when only one method is configured
- SSO-58: Disable ADAMDisablePasswordPolicies during win32 install
- SSO-122: Default ADAM tombstone settings
- SSO-163: SPI Password does not display passwordLastSet
- SSO-181: Attribute name format setting for SAML messages