Identity Server 2019.1 Release Notes

Release highlights

This release focuses on introduction of the following new features:

Accounting Service which is used to gather statistics of authenticated users in your system. You are able to access three different reports from this service:

- Monthly active unique user counts per authentication method
- Daily active unique users per authentication method
- Daily successful authentication events

With the addition of this feature there have been some changes related to installation and upgrade documentations which we highly recommend going through before starting any installation/upgrade. For the purpose of data storage of the pseudonymised usage records, the Accounting service **requires** that you have a PostgreSQL database available even if you are utilising only the SSO features within Identity Server. If you are unsure about pseudonymisation, please see: https://tietosuoja.fi/en/pseudonymised-and-anonymised-data

Per user authentication matching is a UI extension that delivers smoother user experience for your end-users. The JavaScript permits Administrators to configure groups of users or whole organizations towards a specific authentication method or methods. This limits the authentication options presented to specific users and makes sure that organizations that require higher level of assurance are given those options.

Typical use case

If a website offers multiple authentication methods to sign in, automatically selecting the preferred method based on the email address entered by the user streamlines the user experience and reduces training and support costs.

For example, the software could be configured so that:

- Users from email domain @example.IDP.com will be redirected to their standard SAML IDP login
- Users from email domain @SMS.customer.com will be require an SMS code for login, their login will move directly to the IDS SSO screen where they need to fill in their authorisation SMS.
- Users from email domain @gmail.com will be redirected to Google OAuth2 login
- All other users will revert to basic password method

How does it work?

For this example use case, when you utilise Per user authentication matching in your IDS environment, the login screen will show only a field requesting the users email address as the initial login screen. Based on email address domain entered, the user is redirected to their appropriate authentication provider. The login password field will only be shown for users from organizations without an external authentication provider or two-factor authentication method activated.

With the Finnish Trust Network coming into active use and replacing TUPAS, we have been focused on ensuring functionality for all of our customers. You can read more about FTN here at our public blog https://www.ubisecure.com/authentication/finnish-trust-network-ftn/

With each minor release, we aim to ensure that observed defects (bugs) and known issues are being removed from the software while no regression (reintroduction) of defects occurs. So behind the scenes we are increasing our levels of automated testing including load testing. In this release you will find two key annotations in our release notes, Improvements and Corrections. Improvements are adjustments to existing features based on our reviews and your feedback. Corrections are the removal of known defects found within existing features. For your ease of review, within CustomerID we have grouped several items into functional areas.

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

We have also updated utilised 3rd party components and libraries in both applications to ensure that you have the most up-to-date security patches possible. For details on the packages used, please see 3rd party licenses - SSO and 3rd party licenses - CustomerID.

Reminder: Please note that since IDS 2018.1 release Java Runtime Environment (JRE) is no longer included in the distribution package. Both CustomerID and SSO can utilise the same Java installation See Documentation

What does this mean for our customers?

- Excluding Java from the installation media reduces the size and allows use of existing installations
- Faster customer environment Java upgrades independent of the Ubisecure release cycle

Change log

SSO 8.4.2

Improvements

- IDS-2728 - ubixmlsec library has been updated to version 1.5.8.50495 to support http://www.w3.org/2009/xmlenc11#aes128-gcm encryption algorithm that will be taken into use by Suomi.fi service

SSO 8.4.1

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)

CustomerID 5.4.1

Improvements

- IDS-2255 - Query User REST calls in API 2.0 and 2.1 has been updated to also include organizationEntityName and organizationId in the response. More information about what values are returned can be found from REST API 2.0 - CustomerID and REST API 2.1 - CustomerID

Corrections

- IDS-1467 - There was an ability to alter Organisational structure during the Approval of pending users. This feature was implemented erroneously and has been removed from the Pending User approval tab. Utilising this feature, in CustomerID 5.4.0 and previous versions will result in a synchronisation error to occur between LDAP and SQL records for all pending users in the modified Organization
- IDS-81 - Fix for User Defined Federation logout when locale is included in URL
- IDS-2167 - Fix for NullPointerException in REST API 1.0 REQ004b "*Query Organizations*" when querying an organization in a non-case sensitive manner
- IDS-2203 - Fix for Query requests in REST API 2.0 and 2.1 where additional parameters (i.e. exactMatch) are used. In CustomerID 5.4.0 the additional parameters are not considered in the requests. More information about the additional parameters and usage can be found from REST API 2.0 - CustomerID and REST API 2.1 - CustomerID
- IDS-1704 - Fix for updating user attributes returned by CustomerID backend call during registration process. See documentation on how to use Backend query configuration - CustomerID
- IDS-2300 - Fix for sending API requests through proxy using X-Forwarded-For with multiple IPs. This previously resulted in UnknownHostException and incorrect client IP was logged
- IDS-1415 - Fix for Application error if user has pressed Enter key during email confirmation in registration. This fix only resolves error condition, Enter key can still not be used to confirm the email address in registration
- IDS-1521 - Fix for Administrators to be able to change pending user's organization in approval stage. There are still a few identified issues related to changing organization for pending users, IDS-2311 (changing main organization fails to create new sub-organization) and IDS-2312 (changing technical name of organization to name with Scandinavian letters)
- IDS-2301 - Fix for encrypted organization custom attributes if there is an empty value in the field or one of the organizations. Previously this would return Internal Error when querying organization with REST API 2.1

SSO 8.4.0

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

CustomerID 5.4.0

Improvements

- IDS-80 - CustomerID now supports locale (language setting) URL parameter in registration
- IDS-209 - Search field and "Filter results"-button is hidden if there are no mandates present
- IDS-949 - CustomerID now supports configuration for locale parameter in returnURL (General properties - CustomerID)
- IDS-1079 - Updated CustomerID external library (3rd party) dependencies (3rd party licenses - CustomerID)
- IDS-1110 - Documented the following : CustomerID database migration from 5.x.x to 5.4 (Single node upgrade - CustomerID)
- IDS-1168 - REST POST log entries are configurable for testing purposes (General properties - CustomerID)
- IDS-1314 - Removed unnecessary "Are you sure you want to leave this page?" window in mandate role delegation screen
- IDS-1568 - Enabled apostrophe ' as valid character in email address, i.e. john.o’reilly@ubisecure.com

Corrections

Approvals

- IDS-1028 - Fix for cancelling rejection of role approval. If an approver cancels the rejection of role approval, the role does not get removed anymore
- IDS-1081 - Approval tab button now updates the number of pending approvals if users that have pending approvals get deleted
- IDS-1126 - Fix for expiration of pending users if approval is required
- IDS-1198 - Fix for deletion of pending user if a role was added to the user through approval tab
- IDS-1388 - Fix for unnecessary "Are you sure you want to leave this page?" window in approval rejection
- IDS-1408 - Fix for deletion of pending user. Previously there might have been references left in the organization where there pending user was created

Configuration

- IDS-611 - Fix for locales parameter in the eidm2.properties file
- IDS-1099 - Fix for /eidm2/error/authnCancelled redirection
- IDS-1187 - Fix for system user privileges related to role removal

Installation

- IDS-1003 - Documentation correction for CREATE COLLATION on PostgreSQL 10.5 and newer versions (PostgreSQL preparation on Windows - CustomerID, PostgreSQL preparation on Linux - CustomerID)
- IDS-1313 - Fix for import.cmd if filename contains space character on windows

Logging

- IDS-1072 - Removed invalid error in server.log when user is redirected from registration to CustomerID UI
- IDS-1367 - Organization changes are now written to diag and audit logs

Mandates

- IDS-1075 - Fix for re-notification email for pending ORGTOORG mandate
- IDS-1076 - Fix for expiration email for pending ORGTOORG mandate
- IDS-1078 - Fix for filtering pending mandates
- IDS-1362 - Email is now sent to mandatee when their mandate is removed
- IDS-1363 - Fix for mandates allowed if user has OrganizationOwner role
- IDS-1420 - Fix for PERTOORG mandate tab UI
- IDS-1434 - Fix for mandate permission in organization title
- IDS-1512 - Enforce mandate name in organization creation

Miscellaneous

- IDS-1114 - Fix to ensure that Administrators can not unlink strongly authenticated accounts which use UDF linking
- IDS-1300 - Fix for moving user to another organization in order not to save extra custom attribute to SQL anymore
- IDS-1331 - Fix for invalid error message after successful mobile phone verification
- IDS-1366 - Fix for removing sub-organization so that it no longer redirects the user to the frontpage
- IDS-1371 - Error messages fixed to highlight which input fields do not meet requirements
- IDS-1378 - Fix for importing users with uniqueID that is not 36 characters
- IDS-1384 - Fix for when changing organization branch or organization identifier a unnecessary pop up "do you want to leave" does not appear anymore
- IDS-1386 - Fix for when changing to a new password that is longer than 64 digits, the password is no longer shown in the error message
- IDS-1414 - Updated documentation related to Organization Technical Name validator (Data model - CustomerID)
- IDS-1470 - Fixed check/uncheck all check box

Permissions

- IDS-1012 - Search box is no longer displayed if the user does not have permissions to list users
- IDS-1443 - Fix for redirection after deleting sub organization if the user doesn't have permissions to parent organization

Registration

- IDS-687 - Fix for duplicate user check in registration, blocked waiting for registration users
- IDS-735 - Fixed unnecessary email sent when changing password for pending user
- IDS-1205 - Fix for notification about user registration is sent to the inviter
- IDS-1369 - If user gives too long password in registration, the default validation message does not show the password anymore
- IDS-1581 - Fixed email / mobile phone validation check when user tries to register with invalid information

REST API

- IDS-661 - Permit listing all organization attributes from a single REST call (REST API 2.0 - CustomerID, REST API 2.1 - CustomerID)
- IDS-816 - Removed stack trace from CustomerID diag log file for many REST calls
- IDS-1005 - Removed internal server error when using REST API v2.1: POST /organizations. Error is now correctly shown as a HTTP 201 client side error
- IDS-1125 - Fix for REST: MOD014: Create mandate approval to permit administrator to set to true to false (always approved or always requested)
- IDS-1240 - Fix for UI error when role invite is sent to user whose account was originally created via REST
- IDS-1317 - Fix for REST API PUT103 operation to update a users password and make an audit log entry.
- IDS-1422 - Removed URL pluralisation in MOD026 Create Pending user (REST 1.2) where URL path should be singular (“pendinguser” not “pendingusers”). REST: Create Registration/Pending user returns invalid url

- IDS-1423 - Fix for REST MOD014 : Create duplicate mandate to return 409 conflict instead of 400 Bad Request
- IDS-1435 - Fix in search behaviour for all REST calls where the user data contains potential wildcard characters (i.e. underscore, hyphen or period in a user email address)
- IDS-1471 - Fix for REST operation MOD026 Create Pending User to set a default password rather than creating the user with no password (uncorrected behaviour required Admin to set an initial password for each new user manually)

Roles

- IDS-1295 - Fixed role search to ensure duplicate entries are not shown
- IDS-1077 - Removed an error message shown to administrator when they send a reminder or re-invitation to a pending user
- IDS-1189 - Resized the Add Role popup window layout for ease of viewing
- IDS-1197 - Fix for logged error message when role invite is sent via UI to new user who is waiting for registration
- IDS-1364 - Removed visibility of Add Role button from users who do not have administration permission
- IDS-1403 - Fixed error which permitted a user Role invitation when an organization is not set
- IDS-1447 - Fix for error when an existing user requests access to a pre-selected role
- IDS-1570 - Fixed pending user registration via REST MOD026 to assign additional roles (new users created within existing organisation should received pre-assigned roles)

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-1182	If SSO is configured with Redis to use password but no password is provided the user is presented with a stacktrace instead of a user-friendly error message.
IDS-1469	There is a known issue where a stack trace will returned to the browser in response to a SAML AuthnRequest sent incorrectly to the AssertionConsumerService endpoint. SAML AuthnRequest messages should be sent to SingleSignOnService endpoints. This error occurs only when the system is misconfigured.
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 with invalid credentials are present.
IDS-1511	There is a known issue where an existing SSO token can remain to be valid, but not refreshed, even though the user has performed a password reset.
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-2032	There is a known issue for SSO where changing/setting the debug levels in SSO management interface does not take effect without a server restart. There is no work around for this issue - a server restart is required.
IDS-2058	There is a know issue that an old feature called ubiloginAuthMapping, if enabled, might exhaust LDAP connections and cause waiting threads.
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-2158	There is a known issue that the version visible in the footer of SSO admin view is not the version installed

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 work around.
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. Work around: 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. Work around: 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. Work around: 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. Work around: 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. Work around: 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 with 3 or more characters of their first or last name. Password verification does not permit this, and an error is raised.
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. Work around 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 when a 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 work around for this issue.
IDS-2170	There is a known issue in CustomerID if debug mode is turned on and any invalid credentials are used, then a stack trace will be added to the debug log. There is no work around for this item.
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-2207	There is a known issue in CustomerID where interrupting the creation of a pending user will reset localisation of the browser session.
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.

Considerations and limitations

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

```
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.