EVIDEN

Identity and Access Management

DirX Identity

History of Changes

Version 8.10.10, Edition June 2025

Table of Contents

History of Changes

1. History of DirX Identity Releases

This document contains the history of changes for previous DirX Identity releases as well as the current version.

1.1. DirX Identity 8.10.10

1.1.1. Bug Fixes

- Fixed issue with ParamAD Connector Bug: Validation Source null: delete groups and accounts. (SDX-1196)
- Fixed issue with Critical Vulnerability - Apache Tomcat - remote code execution vulnerability (CVE-2025-24813). (SDX-1146)
- Fixed issue with security issue with the embedded tomcat of DXI. (SDX-1192)
- Fixed issue with Privileges (Roles/Permissions/Groups) correct deletion behavior via regular Process (Consistency Rule / State DELETED). (SDX-1138)
- Fixed issue Default language setting not saved in BUI. (SDX-1109)
- Fixed issue with duplicated user in TS groups. (SDX-489)
- Fixed issue with REST API Get /Worflows returns wrong objects. (SDX-950)
- Fixed issuw with DirX Identity – RQWF and CANCEL Process. (SDX-933)
- Fixed issuw with scriptContext.getObject().getStorage().getRootID() return rootDN upper and lower Case. (SDX-1134)
- Fixed issuw with DXI – REST API call GET /Workflows/{workflowId}/task returns wrong object/results. (SDX-945)
- Fixed issuw with Re-Approval Workflow not found for Persona. (SDX-899)
- Fixed issuw with RestService behavior for invalid roles. (SDX-513)

1.2. DirX Identity 8.10.9.a

1.2.1. Bug Fixes

- Fixed the known issue where validation workflows are broken for some connectors when JoinEngine Log Level is set to FINEST or ALL.

1.3. DirX Identity 8.10.9

1.3.1. Bug Fixes

- Fixed issue with Parameter $now in Rule run by event wf is not recognized. (SDX-1124)
- Fixed warning in JDBC Connector, removed logging for JDBC_PROFILER, as it was only for profiling, but irritated our customers. (SDX-1026)

- Fixed issue to set LDAP control in LDAPConnector. (SDX-947)
- Fixed in Webcenter: Renderer optionList width in "Enter Attributes Activity". (SDX-1056)
- Fixed PasswordPolicies: Minimum password age can be defined. (SDX-1011)
- Fixed Missing Log-MsgID resources will no longer lead to workflows getting stuck. (SDX-882)
- Fixed Obligation handling in onRevocation. (SDX-360)

1.4. DirX Identity 8.10.8

1.4.1. Bug Fixes

- Fixed Inheritance is not case-sensitive. (SDX-368)
- Fixed PrivilegeResolution takes extrem long. (SDX-904)
- Fixed „Member in Group“ not provided under “Group – Overview”. (SDX-924)
- Fixed missing certification attributes in siemens.dxr.service.tags.ObjectTypes. (SDX-964)
- Fixed warning: "Clear text password is not supported in encryption mode". (SDX-1025)

1.5. DirX Identity 8.10.7

1.5.1. Bug Fixes

- Fixed issues with values of role parameters. (SDX-443)
- Fixed issues with schema synchronization over LDAPS. (SDX-646)
- Fixed SoD reapproval starts despite SoD violation. (SDX-893)
- Fixed Permission Match Rules are not evaluated under certain conditions. (SDX-895)
- Fixed ProposalList for attribute values is not reloaded in WebCenter. (SDX 909)
- Fixed REST API change Participants in RQWF - no auditing of the change. (SDX-941)
- Fixed siemens.dxr.service.tagsObjectTypes incomplete. (SDX-964)
- Fixed "Some attributes could not be copied!" error in CreateUser Request Workflow after updating Tomcat 9.0.80 to 9.0.96. (SDX-968)
- Corrected mail templates for user certification. (SDX-970)
- Fixed issues with privilege resolution. (SDX-987)
- Removed duplicated 3rd party libraries. (SDX-1012)
- Fixed NoSuchMethodError after updating from 8.9 to 8.10. (SDX-1020)
- Fixed “Cannot perform initial configuration” error after installation due to a JAVA error in pop-up window. (SDX-1022)
- Implemented change request for password management in REST API. (SDX-890)

1.6. DirX Identity 8.10.6

1.6.1. Bug Fixes

- Fixed that SVCLayerConnector generated a huge number of identical LDAP search operations. (SDX-837)
- Fixed Privilege Resolution with inconsistent Facet Role Heritage. (SDX-650)
- Fixed Privilege Resolution in getMatchingGroups logic. (SDX-407)
- Fixed that O365 returned unexpected objects. (SDX-959)
- Fixed issue in Web Center with labels after loading the IDS-J configuration. (SDX-794)

1.7. DirX Identity 8.10.5

1.7.1. Bug Fixes

- Fixed castor error in Realtime Workflow (KELI-1027)
- Fixed performance issue in DirX Identity Manager (LOC-675) (DDXI-2983, SDX-915)
- Fixed starting Java Workflows failed after updating DirX Identity 8.10 SP1 to SP2 (DDXI-2659, SDX-816)
- Fixed errors when performing self-registration in WebCenter (KELI-867)
- Fixed installation issue with Symlinks in folders on Linux (DDXI-3019, SDX-923)
- Fixed Java workflow failed when storing attributes (LOC-674) (DDXI-2975, SDX-914)
- Fixed cleanup rule does not delete objects (DDXI-2435, SDX-772)
- Fixed issues with WebCenter selenium tests (DDXI-2335)
- Fixed issue in DirX Identity Manager when running reports in HTML/CSV/XML: changed the default save path of reports to user home (KELI-683, KELI-441)
- Fixed issue with the delete button in the Business User Interface when uploading a profile picture on the "My Profile" page (KELI-370)
- Fixed "OK" button on "Profile Picture" pop-up window on "My Profile" page erroneously activates in the Business User Interface (KELI-847)
- Fixed issue when starting Provisioning Service and Rest Service in Tomcat (KELI-1025, KELI-1023)
- Fixed issue when Delete Group from Target System does not set TBA flag (KELI-1024)
- Fixed Workflowstarter xerces error (KELI-1022)
- Fixed Unsupported Java Libary „spring-web.jar“ CVE-2024-38809 / CVE-2024-22262 / CVE-2024-22259 / CVE-2024-22243 (DDXI-3030, SDX-936)
- Fixed minor bugs during installation (KELI-844, KELI-833, KELI-439)

1.8. DirX Identity 8.10.4

1.8.1. Bug Fixes

- Fixed installation issue in DXI V8.10 SP2 (SDX-808, DDXI-2630)
- Fixed issue in WebAdmin - negative values in RequestWorkflowWorkflowEngineListener (SDX-336, DXI-10919, DDXI-887)
- Fixed case sensitive renaming for groups (SDX-421, DXI-10710, DDXI-876)
- Fixed enter attributes for location in WebCenter (SDX-795, DDXI-2510)
- Fixed displaying all users for permission in DXI GUI (SDX-801, DDXI-2617)
- Fixed modify always operation (SDX-833, DDXI-2749)
- Fixed AdsConnector is not working (DDXI-424)

1.9. DirX Identity 8.10.3

1.9.1. Bug Fixes

- Fixed assignment object is removed from TBDEL users upon Deleting a privilege assignment via REST API call (SDX-767,DDXI-2401)
- Fixed Certification notification "Assignment Rejection" sent to all the certified users and ensure only users with revoked privileges receive it. (SDX-649, DXI-10772, DDXI-886) (SDX-809, DDXI-2638)
- Implemented state transition from ENABLED to DELETE when max time to disable an object is set to 0 and the last privilege on the user is revoked which requires an account in a TS (SDX-629, DXI-10978, DDXI-1924)
- Fixed the incorrect evaluation of numbers in the filters which are used by EBR provisioning rules application. (SDX-518, DXI-10991, DDXI-1958)
- Fixed format issue in Salesforce connector (SDX-321, DDXI-2324)
- Fixed connection issue with IBM DB2 Database (SDX-789, DDXI-2473)
- Fixed sending notifications when no rejections during certification campaign (SDX-809, DDXI-2638)
- Fixed incomplete default Object Descriptor TSAccount.xml in Target Systems (SDX-812, DDXI-2641)
- Fixed setting up Java reference when JDK is installed on different drive than C (SDX-814, DDXI-2658)
- Fixed bug with missing resource in the resource bundle (SDX-846, DDXI-2816)
- Additional enhancements of checking whether lock for resolution is required by saving of a User object (DDXI-2615)
- Fixed sending cleartext instead of Unique ID (DDXI-2634)
- Various minor fixes and updates

- Updated Installation Guide (identinstall.pdf, Edition August 2024)

1.10. DirX Identity V8.10 SP2

1.10.1. New Features

1.10.1.1. Synchronous Resolution Handling in Policy and Service Agent

Policy and Service Agent are enhanced with a new parameter called 'Synchronous Resolution':

- Its default value is FALSE and can be configured on the Policy Agent and Service Agent related jobs of the workflows ConsistencyCheck, PolicyExecution, and PrivilegeResolution (see tab 'Policy Agent Parameters' or 'Service Agent Parameters').
- If 'Synchronous Resolution' is set to TRUE: the resolution is synchronously executed by the client which started the process (the Policy Agent or Service Agent) such as it was before V8.10. Compared to the full resolution done in the resolution adapter, it does not check for SoD violations (see asynchronous resolution below).
- If 'Synchronous Resolution' is set to FALSE: The agent only sends a resolution message, analogous to the other clients, namely REST Services and WebCenter. A resolution Adapter in one of the Java servers will process this message as soon as possible.

(Tickets DXI-10695, DXI-10697, DXI-10808).

1.10.1.2. Business User Interface

- Enhanced validation messages for BUI are now available. Replaced default field validation in forms due to current limitation in Formly framework. Now a customer can implement any validators for a field with multiple checks including cross fields validations (Ticket DXI-10681).
- Add support for OAuth2 OICD JWT. Support for OAuth2 was improved at login, after return from OAuth2, BUI token handling was improved (Ticket DXI-10694).
- Changes for OAuth SSO. Same as DXI-10694 (Ticket DXI-10778).
- Added multi-line value support for the user profile description (Tickets DXI-11028, DXI-10361)

1.10.1.3. Identity REST Service

- Add support for OAuth2 OIDC JWT, Support for OAuth2 OIDC JWT inside REST services with support for OAuth2 audiences (can be disabled for setup/configuration/development phase) (Ticket DXI-10693).
- Changes for OAuth SSO. Same as DXI-10693 (Ticket DXI-10778).
- Update to Jackson version 2.13.5 (Ticket DXI-11002).

1.10.1.4. Join Engine

- The behavior when method channelUserHook.epilog() is called was changed: Before, the channelUserHook.epilog() method was called for all channels in the controller.close() along with the globalUserHook.epilog(). That lead to problems when the workflow was interrupted, as the epilog would also be called for channels, that have not been processed. Now, the channelUserHook.epilog() method is called within the loop at the end of handling a channel. Therefore, only processed channels will call their userhook.epilog() (Ticket DXI-10368).

1.10.1.5. Request Workflow Engine

- Request workflow emails cannot be configured to be sent with SSL/TLS (Tickets DXI-10742, DXI-10513, DXI-10422).

1.10.1.6. Identity Domain Connector

- An option 'disableApproveAttributeModifications' was added to the connector that allows disabling the Access Policies when modifying attributes.

1.10.1.7. Support of DirX Directory 8.10 and 9.0

- Identity supports now the DirX Directory versions 8.10 and 9.0.
- Identity also supports indexes for server side sorting in the DirX Directory versions mentioned above.

1.10.1.8. Support of OpenSSL

- Update to OpenSSL 3.1.0 – contains various bug and security fixes (Ticket DXI-10520).

1.10.1.9. Support of Systemd for Red Hat 9

- Identity supports now also the Red Hat 9. See description in the readme documentation.

1.10.1.10. Support of Apache ActiveMQ 5.18.4

- Update to Apache ActiveMQ 5.18.4 – contains various bug and security fixes (Tickets DXI-10882, DXI-10908, DXI-10907, DXI-10875, DXI-10876, DXI-10883, DXI-10871).

1.10.1.11. Support of Apache Embedded Tomcat 9.0.88

- Update to Apache Embedded Tomcat 9.0.88 – contains various bug and security fixes (Ticket SDX-691).

1.10.1.12. Message broker

- Update Tanuki Service wrapper to v3.5.51.

1.10.1.13. Endpoint Identification feature in the SSL configuration

- Installing DirX Identity 8.10 SP2 automatically enables the Endpoint Identification feature in the SSL configuration. To override this setting, the following lines have to be manually commented out:

  ids-j-Domain-S1/bin/idmsvc.ini

  ```
  #28=-Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true
  ```

  messagebroker/bin/service/windows_x86_64/wrapper.conf

  ```
  #28=-Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true
  ```

1.10.2. Bug Fixes

1.10.2.1. Services

- There can cases when Assignment objects (such as a Permission object) exists no more in LDAP, but they still are stored in link related attributes of the users e.g. With this patch the cases by resolution are solved by which DXI stored not assignment related DNs in assignment link related attributes (Tickets DXI-10371, DXI-10550).
- Storage contains unwanted Java statements which write on stdout. This causes indefinitely growing files into which stdout is redirected (Ticket DXI-10517).
- Several items fixed:
  - The event from now on contains the fromApplication in the 'source' tag which is read from the session. If the session does not contain the application, default value 'Java' is used.
    Checking whether there are running state related RQWF instances for a given subject and resource pair.
  - Checking whether Provisioning Rules searchbase is empty; if it is, provisioning rules are not applied.
  - In case of an approval with relevant privilege assignments the user is locked from now on to prevent changes until the related processes (such as request workflow start) e. g. are finished on the user (Tickets DXI-10515, DXI-10991).
- The SvcGroup object's group membership related fields must be updated as well by triggering object descriptions (Ticket DXI-10068).
- In the case of an assignment in approval (with attributes set on it such as StartDate or EndDate), the user cannot change other of his attributes. This change in the code makes a check whether an assignment can be granted by user before making any changes on it (Ticket DXI-10597).
- In case of a non-user-assignable flagged role (dxrUserAssignmentPossible=false) a warning was logged in case of non-direct assignment to point out that the role is not user-assignable. With this solution the warning will be logged only in the case of a direct assignment (Ticket DXI-10637).

- Suppresses now output on stdout. Redirected file stdout.log was growing indefinitely (Ticket DXI-10671).
- In log entries by catching the exceptions, parameters of the log text were defined incorrectly (Ticket DXI-10685).
- The assignment flags were not checked in a correct way, an assignment can have more types of assignment methods (e. g. direct, BOinherited), only one was checked and other ones were ignored (Ticket DXI-10704).
- The check to suppress a warning log in case of naming rule (referenced attribute derives from an SvcUser object) was not implemented correctly (Ticket DXI-10757).
- If an attribute of an account object that is not mastered by a user is changed, no save of account object was done (Ticket DXI-10763).
- Enhancement of logging: When resolution adapter finished processing such information as userDN, dxruid and sending application are logged now. Other already implemented enhancements in logs and corrections such as filling dxrLastResolutionTime attribute of user were done (Ticket DXI-10697).
- In case of a privilege assignment with end date, the de-assignment did not correctly remove the assignment object and the related links on related objects (user, group, account e.g.) (Tickets DXI-10784, DXI-10849, DXI-10829, DXI-10761).
- Unlock the user object as soon as possible after changes saved (Ticket DXI-10812).
- Fixed faulty detection of an attribute change with generalized time by using toString method instead of normalizedString (Ticket DXI-10566).
- Cannot resolve email recipient for order request for a new external user (Ticket DXI-10712).
- In case of REST API calls, no request workflow was started in case of a removal of an assignment whose privilege has a removal request workflow (Tickets DXI-10784, DXI-10836, DXI-10761).
- The filter for searching of groups 'fitting to' matchrules considers a very broad scope of group objects, with this correction the groups of the related privilege are in scope only (Ticket DXI-10867).
- Account is not anymore created and provisioned if assigned privilege is in approval. The reserved account objects are cleared out too (Tickets DXI-10819, DXI-10855).
- In case of disabled User Lock the assignment is still checked for TbDelByResolver flag and these assignments are no more handled as 'active' assignments for further processing in the code (Ticket DXI-10892).
- Fixed NullPointerException in a log entry by handling if assignment object is null (Ticket DXI-10926).- Fixed risk-tracking of inherited assignments for SoD (Ticket DXI-10817).
- Loading of access policies was fixed (Ticket DXI-10864).
- An error has been solved with has prevented the reporting of a lock with the HTTP Code 403 CONFLICT and the scimType "locked" as described in the document "DirX Identity Integration Framework" in chapter "6.7.1 Error Handling" (Ticket DXI-10971).
- Fixed isModified() always returns true issue in the setProperty() method (Ticket DXI-10929).

- Handling the case if group object has its own naming rule of cn's property definition in its object description (Ticket DXI-10961).
- The Identity Manager worked with obsolete display values of a proposal list, because not the most actual RoleParameter object was used. Now the objects are always refreshed from the storage to avoid such issues (Ticket DXI-10811).
- Compound attributes are not replaced anymore during save() if their values are not changed (Ticket DXI-10452, SDX-779).
- Fixed replace operation at multi-valued attribute without change (Ticket DXI-10463).
- Fixed child group references in parent group when child group is deleted (Ticket DXI-10863).
- A collection of changes which handles problem with assignments with approval (Ticket DXI-10958).
- Added handling for renaming user to the same name while changing only uppercase/lowercase characters. (Ticket DXI-10710)
- Fixed evaluation of access policies in applyChange (Ticket SDX-351)
- Rules will now process users in TBDEL state when dxrState is present in a rule filter and a rule filter permits it (Ticket DXI-11012)

1.10.2.2. Event Based Rules

- If the client resolves and there are no resolution related attributes changed, the provisioning rules were not executed in case of the change of a domain permission parameter related attribute (Tickets DXI-10551, DXI-10599).
- The controller can get Add/ModifyRequest and Add/ModifyEvent to process. A missing check of the type of the delivered event caused the ClassCastException (Tickets DXI-10559, DXI-10590).
- The change of the dxrTBA attribute in the event is now checked. If it was changed to true in the modifications of the event, the provisioning rules will be applied (Ticket DXI-10672).

1.10.2.3. Join Engine

- The component regarding an update on the Identity side will use the TS entry from the previous search if the current search result is an empty entry. Therefore, a DELETE in the TS would result in an ADD in DXI, as it would assume the TS entry still exists and must therefore be created in DXI (Ticket DXI-10484).
- LDAP connector throws NoSuchElementException in case of a referral in SearchResponse. Join Engine will now handle the exception by logging a warning and ignoring the referral (Tickets DXI-10495, DXI-10541, DXI-10653).
- Fixed case when message "Entry is currently in use by another event workflow" is written (Tickets DXI-10563, DXI-10593, DXI-10676, DXI-10703, DXI-10718, DXI-10720, DXI-10842, DXI-10839, DXI-10920, DXI-10944, DXI-10951).
- Fixed NullPointerException when creating ModifyRequest (Ticket DXI-10483).
- Error with UserPasswordEventManager: The created modify requests for SetPassword

workflows for accounts contained binary values that caused XML parsing errors. With this fix, only specific identifying attributes [cn, dxruseruid, givenname, sn] are put into the modify request (same as for audit requests) (Ticket DXI-10497).

- Fixed several items: NullPointerException when reading oldIdentifier from search result; NullPointerException when reading empty search result; NullPointerException when logging result entry that is null (Ticket DXI-10653).
- Fixed NullPointerException when reading empty search result (Ticket DXI-10671).
- Realtime workflows have high memory consumption (Ticket DXI-10671).
- SortedValidation stored whole searchresult in a map, which lead to low memory for large amount of data (Tickets DXI-10753, DXI-10833).
- Request type of a mapped entry is NONE instead of ADD after setting request type NONE on previous entry in userhook (Ticket DXI-10773).
- Join Engine throws ClassCastException because LDAP connector returns wrong class; Proper handling of connection errors implemented, e. g. to stop validation workflow (Tickets DXI-10781, DXI-10787, DXI-10789).
- Fixed account entry is currently in use by another event workflow (Ticket DXI-10797).
- Referral error in AD validation workflow fixed (Ticket DXI-10827).
- Adjust log level for messages in userhooks (Ticket DXI-10530).
- Wrong setting of attribute dxrTSState after failed ADD request fixed (Ticket DXI-10881).
- Searching for the TS from an account does recursive searches by parent, until either the TS entry is found, or the top of the tree is reached. While the LDAP connector returns null in case of no entry found, the Identity Domain connector returns an empty searchResult. This was not considered in the Join Engine, therefore Join Engine always assumed the first response, i.e. the direct parent, was the TS. This has now been fixed (Ticket DXI-11023).
- Added operational attribute "searchcontext" to connectivity framework spml search requests (Ticket SDX-193)
- Fixed user creation with delegated administrator – the users were created without base roles. (Ticket DXI-10729)

1.10.2.4. Identity Domain Connector

- Now by default the connector suppresses the sending of change event. The request of the event is sent by the Join Engine as before and only this will be processed by other components such as Event-based workflows (Ticket DXI-10555).
- The connector could not set scramble password for user in ImportWorkflow. Internally encryption was erroneously considered (Ticket DXI-10622).
- Connector tries to rename the channel at the end of a delta workflow leading to error: Entry already exists (Ticket DXI-10638).

1.10.2.5. Provisioning Web Services

- Don’t write sensitive information like passwords to the log files of the Provisioning Web Services (Ticket DXI-10516).

1.10.2.6. Web Center

- Display of old and new values on modification approval form fixed (Ticket DXI-10561).
- Allows the resolution of expressions like “owner@dxrDisableStartDate” in Persona form (Ticket DXI-10646).
- Display of correct editor for workflow parameter attribute “dxmADSGroupType” (Ticket DXI-10859).
- Allows the configuration the sizelimit for role searches by adding the parameter “roles.sizelimit” with the default value 500 to the “webCenter.properties” file (Ticket DXI-10976).
- Handles the display of attribute “parentID” correctly (Ticket DXI-11010).
- Allows the configuration of a default handler for compound attributes (Ticket SDX-692).

1.10.2.7. Business User Interface

- Improved accessibility of user interface (Ticket DXI-10744).
- Personas, user facets and functional user are now visually represented with badges in user search results (Ticket DXI-10617).
- When a User is TBDEL the only thing that is editable on “user-management profile & my-team profile is the “operational”-Area. There you can set the Date to the future, to activate the user again. (Ticket DXI-10815)

1.10.2.8. Request Workflow Engine

- The map attributes activity no longer replaces any characters (like for example +) in attribute values (Ticket DXI-10624).
- Added null check when going through list of e-mail recipients in GenericPlaceholderResolver (Ticket DXI-10925).

1.10.2.9. Identity REST Service

- Search operations were re-implemented (Ticket DXI-10468).
- The service no longer logs cleartext passwords (Tickets DXI-10724, DXI-10556).
- Different syntaxes were used when querying approvals via REST API (Ticket DXI-10721).
- Some data was missing in REST API response (Ticket DXI-10752).
- Renaming of a value in a multi-valued CN attribute fails (Ticket DXI-10642).
- Introduction of three different search strategies for search operations including paged searches DXI-10480).
- Correct handling of “\n” in “postalAddress attributes (DXI-10804).

1.10.2.10. Java-based Server

- NullPointerException in ResultListener or SAXParseException occurred if event from Repository does not contain any XML node (Ticket DXI-10488).

- The issue that an error activity is running in parallel to a join activity in retry has been fixed. The execution of the error activity is now postponed until the join activity has finished all its retries if any (Ticket DXI-10011).
- Mail attribute can be single- or multi-valued – corrected the return value to String or to String[] (Tickets DXI-10540, DXI-10634, DXI-10770, DXI-10823).
- Prevent some XML errors (SAXParseExceptions) when accessing messaging events; XML errors are not print anymore on stderr (Tickets DXI-10488, DXI-10562, DXI-10569, DXI-10600, DXI-10857, DXI-10949, DXI-10977).
- Allow using an agent jar with the Java server: Identity's own system class loader now implements the method appendToClassPathForInstrumentation(String path) (Ticket DXI-10592).
- Do not check if a scheduled Realtime workflow can run on the server where the scheduler is running (Ticket DXI-10633).
- Introduce multiple ResultListener threads to process result entries from realtime workflows (default is 2). Extended the tab Limits for Java server in Identity Manager. Extended Web Admin Overview with JMX Mbean ResultEntries (Ticket DXI-10611).
- This fix reverts changes made with hotfix V8.10-SP1-10. In hotfix 10, the rule has been tightened so that if several workflows match to an event, only one workflow is started. Now several workflows are allowed again. This is still not a recommended case that multiple workflows are matching (One workflow per event) (Ticket DXI-10749).
- TS-specific Listeners: The setting of number of threads was not considered. Message text had missing insert text (Tickets DXI-10783, DXI-10792).
- Missing jar file dxrManager.jar in classpath of Java server (Tickets DXI-10384, DXI-10902).
- Fixed email notification's nationalization issue for default language (Tickets DXI-10795, DXI-10847, DXI-10957).
- Fixed compilation error for complex start conditions for request workflow activities if the import part does not contain any newline between multiple items (Ticket DXI-10903).
- If no error activity exists EventWorkflowRunner produces IndexOutOfBoundsException. This relates to TS-specific realtime workflows (Ticket DXI-11001).

1.10.2.11. Agents / Connectors

- SAPUM Connector: In validation also inherited roles were returned despite checked "directAssignedRoles" flag (Ticket DXI-10483).
- RACF Connector: Problem in paging fixed in synchronization workflow (Ticket DXI-10478).
- RACF Connector: Problem in client-side SSL (SASL bind) to RACF LDAP server fixed (Ticket DXI-10751).
- LDAP Connector: Search constraints are now passed in "search" operation and are not stored at the LDAP connection. This solution doesn't cause any invalid cookies in the LDAP server while processing paged searches (Tickets DXI-10582, DXI-10567, DXI-10679, DXI-10860).
- LDAP Connector: The connector produces ArrayIndexOutOfBoundsException on User

Hook preUpdate Map. This caused a rename with empty DN (Ticket DXI-10671).

- LDAP Connector: Issues with server-side sorting control are fixed (Ticket DXI-10913).
- Policy Agent: Fixed a ClassCastException when iterating through the items found (Ticket DXI-10423).
- ADS Connector: Fixed an ArrayIndexOutOfBoundsException (Ticket DXI-10692).
- JDBC Connector: In the open method a time gap of 30 seconds occurred while reading the database schema on Microsoft SQL databases (Tickets DXI-10658, DXI-10866).
- Office 365 Connector: The AzureAD group filter was not working for attribute groupTypes (Ticket DXI-10774)
- Office 365 Connector: For AzureAD role membership validation: Incorrect prefix was used for roles in memberof attribute (Ticket DXI-10776).
- Metacp: DAP protocol: During processing the input of a string representation of an attribute value with Certificate, Cert-List or Certificate-Pair syntax, BER encoding was used instead of DER encoding. For certificate syntax DER encoding is requested by X.509 standard (DXI-10612).
- Service Agent: Added missing message into resource file (Ticket DXI-11007).

1.10.2.12. C++-based Server

- NullPointer access error occurred when no PSE is available, but encryption is set (Ticket DXI-10719).

1.10.2.13. Messaging

- While trying to send a resolution message the JMS session was in state closed. Now a reconnect is implemented (Tickets DXI-10714, DXI-10722, DXI-10747, DXI-10905).
- Nullify messaging connection, session, and producer after closing to prevent illegal reuse (Ticket DXI-10349).

1.10.2.14. Identity Manager

- An LDIF file with newrdn as BASE64 encoded content was not imported correctly (Ticket DXI-10755).
- The tab "Content (resolved)" is now hidden for the workflow "CheckConsistency" to prevent time consuming generating while opening in the editor (Ticket DXI-10574).
- Read and modify access policies do not display all attributes of selected object type (Tickets DXI-10377, DXI-10384).
- Actions with multi-selection flag are not displayed during multi-selection (Ticket DXI-10893).
- Consistency and provisioning rule items added to the object classes combo box in the policy LDAP search panel (Ticket DXI-10455).
- Fixed a ClassCastException in the target system wizard (Ticket DXI-10910).

1.10.2.15. Miscellaneous

- Linkchecker script: missing log4j jars on the classpath added (Ticket DXI-10481).
- Initial Configuration: The configuration fails because erroneously LDAP controls are tried to add. Now OID names or abbreviation names are checked (Ticket DXI-10748).
- Initial Configuration: Error on Red Hat 7.9 (Ticket DXI-9551).
- The online help for 8.10 was missing a description what means asterisk in the user role name. The documentation has been updated and will be distributed with 8.10 SP2 (Ticket DXI-10807).
- Value of editor in the example of "Editor for Multivalue String" had an incorrect package name, there was an additional “.storage” in the path. Online help in customization guide has been updated (Ticket DXI-10856).
- Adaptations to support Tomcat 9.0.88 (Ticket SDX-700, SDX-756)

1.10.3. Fixes already solved in 8.10 SP1 Release

The following ticket was already solved with 8.10 SP1 release but was not mentioned in the History of Changes document:

- Business User Interface now correctly processes attributes that are marked as read-only in Identity (Ticket DXI-10469).
- No ResourceException is shown anymore in the log when a C++-based server schedule is found (Ticket DXI-10525).

1.10.4. Information About Discontinued Features

DirX Identity V8.10 (SP1/SP2) does no longer support these features:

- Deploy ProvisioningServlet in the Embedded Tomcat of a Java server
- Internet Explorer 11 browser support
- DirX Approvals App for Apple® iOS

DirX Identity V8.10 (SP1/SP2) is the last version that supports the following features:

- Support of Microsoft Lync 2013
- Connectivity package for Imprivata OneSign
- Connectivity package for HiPath 4000
- Connectivity package for SiPass
- Connectivity package for ODBC Agent
- Reapproval Workflows (use Certification campaigns)
- Boston Workstation Connectivity (connector)
- XSLT-based Reports

1.11. DirX Identity V8.10 SP1

1.11.1. New Features

This section lists new features of DirX Identity V8.10 SP1 compared to DirX Identity V8.10.

1.11.1.1. Support of Windows Server 2022

Windows Server 2022 is now supported including Windows Password Listener installation (Tickets DXI-10289, DXI-10330, DXI-10415).

1.11.1.2. Business User Interface

- BUI supports external custom field validation for all Formly forms in *extern/validator.js*. See chapter *Documentation Extensions* in the Readme for a description of the custom validation feature (Ticket DXI-10362).

1.11.1.3. Web Center

- Web Center supports now role assignments with mandatory end dates (Ticket DXI-10009).
- Web Center search filter extension for compound attributes with a blank as delimiter (Ticket DXI-10160).

1.11.1.4. DirX Identity REST service

- A create entry result includes the default attributes of the new entry (Ticket DXI-10148).
- Patch operation remove partly supports value specifications in paths (Ticket DXI-10150).
- Update to Spring version 5 (Ticket DXI-10223). This requires some minor changes to configuration file security.xml.
- Update to Jackson version 2.13.4 (Ticket DXI-10083).

1.11.1.5. TCL Workflows

- An integer attribute search with sort order “descending” presents now the result in correct order (Ticket DXI-10185).

1.11.1.6. Security Settings for Identity SSL Connections

- Set Diffie-Hellman Key Exchange key length to 2048 (Java option “jdk.tls.ephemeralDHKeySize”) (Ticket DXI-10193).

1.11.1.7. Support of Apache ActiveMQ 5.17.2

- Update to Apache ActiveMQ 5.17.2 – contains various bug and security fixes (Tickets DXI-10192, DXI-10443).

1.11.1.8. Support of Apache Embedded Tomcat 9.0.69

- Update to Apache Embedded Tomcat 9.0.69 – contains various bug and security fixes (Tickets DXI-10275, DXI-10352).
- The server version number is not shown any more e.g., on an error page (Tickets DXI-9989, DXI-10205).

1.11.2. Bug Fixes

1.11.2.1. Web Center

- The size limit for listing the direct users of a role in Web Center is now configurable. Web Center displays a message if the size limit has been exceeded (Ticket DXI-9926).
- The Web Center attribute modification approval page correctly displays the old values for an attribute modification with operation replace (Ticket DXI-10061).
- Display a user-friendly error message if an attempt to assign a role to a user fails due to invalid parameter values (Ticket DXI-10046).
- Web Center method Objects.getObjectProperty returns the correct values for virtual properties numSubordinates and numAllSubordinates (Ticket DXI-10118).
- Web Center displays correctly enabled checkboxes on certification form (Ticket DXI-10158).
- Web Center no longer reports an error when saving a user with dxrEndDate (Ticket DXI-10183).
- Fixed sorting search filter proposal list (Ticket DXI-10181).
- Web Center sets and evaluates password status attributes and writes audit logs when checking a user's old password before setting the user's password to a new value (Ticket DXI-10255).
- Evaluation of scoped variables fixed (Ticket DXI-10280).
- Web Center supports expressions for attribute readonlyRow of data properties (Ticket DXI-10402).

1.11.2.2. Services

- It can happen that the dxrRPValues value of the group is not an exact string or a '*' (all), but a partial string such as [cn=*, cn=SomeBO, cn=Custom, cn=BusinessObjects, cn=My-Company]; therefore, check all the matching rules on the current list of groups using the standard algorithm is required in the current logic (Ticket DXI-10062).
- ClassCastException in application Simple Identity Management Service (SIMS) fixed (Ticket DXI-10056).
- The dxrRPValues attribute which is a multi-valued attribute is not defined as multi-valued in its Object description. There were 2 confusing log entries because of missing 'not' (the log entries stated they are multi-valued, but they are not) (Ticket DXI-10013).
- SvcUser methods getAssignedRoles, getAssignedPermissions, and getAssignedGroups initialize the SvcUserCtrl if not yet initialized (Ticket DXI-9730).

- The problem was that roles with roleparameters (RP) cannot be resolved because the handling the value of the RP was invalid. These RP values are dynamical values so not static (expressions), which means their value is determined by an attribute of the user. DXI has read these RPs by the first user and used it as a static list for the next users processed by the consistency check workflow (Tickets DXI-10048, DXI-9773).
- Identity Manager displays 'error(s)' detected by settings user's end date (SvcCode 'SVC_RIGHTS_REMOVED' was not handled properly) (Tickets DXI-10080, DXI-10357, DXI-10302).
- Persona life cycle does not follow User life cycle (Tickets DXI-10080, DXI-10357, DXI-10302).
- Sporadic error in Identity Manager when saving a user object. Resolution adapter and Manager tries to resolution-lock the user object at the same time. If Resolution adapter already has the lock, the Manager shows an error dialog which showed 'null' information (Tickets DXI-10081, DXI-10357).
- The sort index in the proposal lists is fixed so that it works as described in the help (Ticket DXI-9675).
- Evaluation of access policy rules with expression ${resource.dn} fixed (Ticket DXI-10156).
- For the multi-valued attribute dxrOptions in TargetSystemAccount only the first value in the list was stored (Ticket DXI-10090).
- Correction for variable replacement. Timestamps are now shown in a localized format based on email language (Tickets DXI-10153, DXI-10347).
- Corrected starting index in MailServices component for moveSentMails method (Tickets DXI-10153, DXI-10347).
- Fixing NullPointerException when reading the values of an attribute (Ticket DXI-10109).
- In case of an LDAP search with scope baseObject no paging search constraint was correctly provided which caused a NoSuchElementException (Tickets DXI-10182, DXI-10319).
- Performance improvements for HDN role parameters were done (Ticket DXI-10172).
- A date attribute, e. g. dxrStartDate, was set up to now when the date was empty and compared to another date (Ticket DXI-10075).
- If the role parameter cannot be read from the RoleParamsCache of the session, it returns null. This object was not checked by using in logging, which raised a NullPointerException (Ticket DXI-10139).
- If no event-based rule workflow is used, no resolution events are sent by other components of Identity, the accounts of the user are not updated. The solution is to make sure that a save on a user (without resolution) always updated its related accounts (mastered attributes) (Tickets DXI-10126, DXI-10290, DXI-10477).
- Tuning on performance by permissions which have lots of groups (with matchrules):
- using LDAP searches for evaluating permission match rules
- match rules related tuning (Ticket DXI-10171).
- The request reason for an attribute modification is always added to the workflow context attributes (Ticket DXI-10256).

- A paged search resulted in a NoSuchElementException. The real LDAPException behind it was not shown and is now logged (Ticket 10386).
- In case an Identity component like the Identity Manager resolves itself, the dxrTBA flag of the user should be set to false if it was true before (Ticket DXI-10420).
- Create object should not create any object if the new object's name is already assigned to another object (Ticket DXI-10111).

1.11.2.3. Join Engine

- A search to join by a File-based connected directory during export does not make sense and just causes performance issues (Ticket DXI-9762).
- Added dxrTSState handling in Common User Hook for Mail Target System (Tickets DXI-10153, DXI-10347).
- A NullPointerException during mapping process will skip action removeFromDeleteList (Ticket DXI-10115).
- For requestType NONE and without (or erroneous) Identifier mapping, the search for sync TS→Ident is skipped, so that the dxrTSState always resolves to DELETED (Tickets DXI-10218, DXI-10448).
- SyncBase and ValidationController cancellation behavior in case of an error in the channel userhook prolog was inconsistent. While SyncBase would just skip the channel and move on to the next, ValidationController would terminate the whole WF in error state. This has now been harmonized to use the SyncBase-behavior in ValidationController as well (Ticket DXI-10254).
- ValidationController must drop an entry from the internal entryList for deletion when the requestType is NONE (Ticket DXI-10263).
- For synchronization workflows, in case of an ADD request, that is modified to NONE in preUpdate userhook, the return direction (CS→DXI) would set the dxrTSState to DELETED (Ticket DXI-10287).
- Validation workflow produces ArrayIndexOutOfBoundsException in the mapping (Ticket DXI-10287).
- In some cases, validation workflow produces MODIFY requests instead of ADD requests (Ticket DXI-10287).
- After a failed ADD on the JDBC connector, the join engine's search in reverse direction will return the whole table due to a missing identifier (Ticket DXI-10390).
- Join Engine produces log records with empty log level. That leads to a NullPointerException that caused the log record to be written into the Java server warning file (Tickets DXI-10462, DXI-10456).

1.11.2.4. Request Workflows

- Fixed missing Audit Record for request workflow activity "Acknowledge update" (Tickets DXI-9946).
- Suppress unnecessary warning when creating a functional user via workflow (Ticket DXI-9791).

- Handling of the timeout parameter for request workflow activities fixed (Ticket DXI-9940).
- Notifications with Userhooks was missing in standalone activities, e.g., "Notificaton If Rejected" (Ticket DXI-9585).
- Resolution of placeholders in notification email's subject and body removes duplicate email addresses in address fields of the notification (Ticket DXI-9999).
- Expressions in mail subject and mail body are now correctly resolved again if the expressions use dots instead of slashes (Ticket DXI-10260).
- Suppress unnecessary warning "REQWF445 No master attribute available ..." for non-people activities (Tickets DXI-10384, DXI-10328).

1.11.2.5. Manager

- Proposal lists: Fixed a NullPointerException when entering a variable into the LDAP filter in independent DN proposal list; dependent proposal update is not triggered when the property depends on "c" (country) attribute (Ticket DXI-10017).
- The escape sequences in the LDAP search expressions are recognized and kept in the advanced search dialog (Ticket DXI-10093).
- SAXParseException when moving connected directory objects in DirX Identity Manager fixed (Tickets DXI-10305, DXI-10414).
- Enabled editing of password policy attributes in the Data View (e. g. pwdAccountLockedTime) (Ticket DXI-10296).

1.11.2.6. Java-based Server

- The internal framework job pooling configuration was extended to allow up to 400 framework job objects. Up to now the maximum value was 100. This would prevent that exceptions like "CFG514 Exception DxmConnectorException when opening connectors: java.util.NoSuchElementException: Timeout waiting for idle object." do not occur anymore. The maximum value is now also configurable (Ticket DXI-10052).
- Now the LDAP connection pool in the Java server uses a configurable time limit for bind operations to prevent Java server to hang when in rare cases the bind response is not received. Default is 15 seconds (Ticket DXI-10060).
- Set Diffie-Hellman Key Exchange key length to 2048 via a Java option for Java server and message broker (Ticket DXI-10193).
- No ResourceException is shown anymore in the log when a C++-based server schedule is found (Tickets DXI-10176, DXI-10353).
- "Load IDS-J Configuration" method in Identity Manager reloads the nationalized texts in the Java server (Tickets DXI-10271, DXI-10300).
- Fixed problems running Powershell scripts with quotation marks (Ticket DXI-10278).

1.11.2.7. Identity REST Service

- The Identity Rest Service accepts a UID as search base (Ticket DXI-10122).
- Evaluation of Rest Service configuration parameter "auth.userName.userFilter" for basic

authentication fixed (Tickets DXI-10146, DXI-10348).

- The Rest Service returns subject attribute names instead of attribute labels (Ticket DXI-10224).
- The Rest Service supports a new virtual user attribute dxrvPwdState with values "ok", "reset", "expired", and "undefined". This helps clients to recognize if a change password is necessary.
- Compound attribute handling fixed (create, read, and modify operations) (Ticket DXI-10237).
- Task list improvements and fixes (Tickets DXI-10252, DXI-10253, DXI-10256, DXI-10262).
- The Rest Service sets and evaluates login status attributes (Ticket DXI-10266).
- SCIM search filter attributes of type DN accept both, a DN and a UID (Ticket DXI-10210).
- Removing all values of an attribute fixed (Ticket DXI-10382).
- Patching multi-valued DN attributes fixed (Ticket DXI-10419).
- Fixed unauthorized access after Password Reset (Ticket DXI-10245).
- Attribute displayName is no longer read-only (Ticket DXI-10470).
- The Rest Service returns correctly aggregated menu access rights (Ticket DXI-10204).

1.11.2.8. Business User Interface

- Fixed wrong evaluation for read-only fields in profile. Support for custom validators, because Formly custom validator don't work (Ticket DXI-10232).
- dxrSalutation field was displaying the value instead of the label in Create Identity workflows (Ticket DXI-10338).
- Fixed unauthorized access after Password Reset (Ticket DXI-10245).
- Sorting groups is not possible (Ticket DXI-10307).
- A manager without access right for "User Management Menu" can access "User Management Menu" (Ticket DXI-10322).
- The Business User Interface doesn't show a second enter attributes page without pressing F5 (Ticket DXI-10333).
- The Business User Interface doesn't show the changed values for approval properly (Ticket DXI-10334).
- The Business User Interface loses the context of the selected user from "My Team" when you try to create a persona for the user (Ticket DXI-10336).
- BUI supports external custom field validation for all Formly forms in validator.js (Ticket DXI-10338).
- Non-modifiable attributes are editable in Business User Interface. No proper message is displayed (Ticket DXI-10431).

1.11.2.9. Realtime Workflows

- Fixed UnsupportedOperationException due to immutable ArrayList (Ticket DXI-10088).

- For Check Consistency workflow “siemens.dxr.policy” was added to resource manager for logging (Tickets DXI-10153, DXI-10347).
- Check Consistency workflow: With the Mail connector, LDAP entries of objectClass dxrTargetSystemAccount are not necessary represented in service layer as SvcTSAccount, in case of the MailConnector it is SvcEmailAccount. This has led to a ClassCastException in the Check Consistency (Ticket DXI-10194).
- The UserPasswordExpirationNotification workflow ignores subsequent password policies once a policy without password expiration was found (Ticket DXI-10213).

1.11.2.10. C++-based Server

- Fixed multiple execution of activities in TCL workflows (Tickets DXI-9825, DXI-9995, DXI-10162).

1.11.2.11. Identity Domain Connector

- Identity Domain connector must copy operational attributes from request to response, as those are needed in Join Engine on rename (Tickets DXI-9788, DXI-10066).
- Identity Domain Connector must handle parentDN for cases rename and move in case no identifier is provided in request (no id in mapping) (Ticket DXI-9971).
- If an error occurs during the execution of a modify request a temporary exception shall not be thrown, but the error should be returned in the modify response (Tickets DXI-10112, DXI-10380).
- From privilege link related attribute point of view the Identity Domain connector works only on SvcUser objects. Now the connector handles also SvcRole and SvcPermission objects (Ticket DXI-10133).
- If the domain of the connector is not the 'main' Identity Store but another one as a Connected Directory, the storage of the other Identity domain was not found because the URL could not be resolved correctly (Tickets DXI-10231, DXI-10360).

1.11.2.12. CSV Connector

- Fixed usage of parameter “alwaysQuote” (Ticket DXI-10119).

1.11.2.13. Mail Connector

- Changed search behavior to not throw a "Not supported" exception. Instead return an empty result so that an Add request will be sent. Added support for changing encryption algorithm (Ticket DXI-10153).
- The used cypher algorithm in e-mails is not recommended by German BSI (Bundesamt für Sicherheit in der Informationstechnik) (Ticket DXI-10369).

1.11.2.14. RACF Connector

- Client authentication with certificate was not working for a cluster realtime workflow (Ticket DXI-10385).

1.11.2.15. LDAP Connector / ADS Connector

- Delete an entry with child elements was not possible (Ticket DXI-10100).

1.11.2.16. Sharepoint Connector

- Enhanced logging for better diagnostic especially for “org.apache.axis” package (Ticket DXI-10166).

1.11.2.17. SAP ECC UM Connector/Agent

- NullPointerException in agent/connector fixed when setting a password (Ticket DXI-10281).
- SAP ECC UM agent: There were warnings in the processinfo.txt file about missing log4j*core classes (Ticket DXI-10410).

1.11.2.18. JDBC Connector/Agent

- Warning message “JDB1 ... add-argument warning: non-nullable attribute not supplied” changed to debug message (Ticket DXI-10291).

1.11.2.19. Policy/Service/Consistency Agent

- Policy Agent: 'CTX_LIMIT_EXCEEDED' Directory exceptions occurred by some searches in the PolicyExecution workflow. The exception comes always by searches where the filter is very long (about 10.000 characters long). Now the filter length can be configured on the out channel of the job (Ticket DXI-10065).
- Deactivation of audit message “execute operation” of Consistency agent and Policy Execution agent (Ticket DXI-10316).
- There can be cases when between the search by the Service agent and the processing of the (user) object the (user) object is changed. An internal refresh is now done on the locked object to work on the actual (user) object further on (Ticket DXI-10000).

1.11.2.20. Mail Target System

- Configuration of a Mail target system via Global View produces an error message. The Template target system was referencing the wrong Wizard configuration file (Ticket DXI-10120).

1.11.2.21. Configuration Wizard

- Silent installation and configuration now take domain admin password from configuration.ini (Ticket DXI-10304).
- Certain characters for passwords do not work with configuration (e.g. “\”, “>” , “-“) (Ticket DXI-10184).

1.11.2.22. Configuration

- In case of a SvcGroup object the extensions/loadAttributes tag named 'recover' in the

default Group.xml object descriptor is processed by the “save()” method of the SvcGroup object, which causes a full recovery of the object, all done modifications on the StorageObject are reversed (Tickets DXI-10175, DXI-10212).

- The GenericEventController did not have an initial value for its “consruleroot”, which could cause an issue to load all rules from the Policies folder and execute them if criteria matched. This issue is fixed now in the description file of the controller (Tickets DXI-10105, DXI-10331).
- For the objectclass dxrTargetSystem the attributes dxmKeyStorePassword, dxmTrustStorePassword were missing. Also, the fields for these attributes were missing on Workflow Configuration tab for a target system (Ticket DXI-10385).
- For Linux: The setting of the execute bit for shell scripts in delivered tar files was missing. Now in the zip files of utility tools are Windows batch scripts only and on Linux in the tar file just shell scripts with set execute bit only (Ticket DXI-10007).

1.11.2.23. Miscellaneous

- SocketedJob: The updateCacheStrategy was set for a new session to always, which is not needed because the used session by the job is new and start with a newly initialized cache (Ticket DXI-10298).

1.11.3. Information About Discontinued Features

DirX Identity V8.10 SP1 does no longer support these features:

- Deploy ProvisioningServlet in the Embedded Tomcat of a Java server
- Microsoft Internet Explorer 11 browser support
- DirX Approvals App for Apple® iOS

DirX Identity V8.10 (SP1) is the last version that supports the following features:

- Support of Microsoft Lync 2013
- Connectivity package for HiPath 4000
- Connectivity package for Imprivata OneSign

1.12. DirX Identity V8.10

1.12.1. New Features

Main features of this version are:

- DirX Identity Business User Interface:
  - Authentication – Support for authentication with DirX Access PEP method.
  - Authentication – Support for authentication with OAuth2 OIDC PKCE method.
  - Certification Campaign – Support for display, approve and reject tasks for running Certification Campaigns.

- Configuration – Tables definition entry is moved to tables.json file from config.json.
- Configuration – Languages and countries list entry is moved to options.json file from config.json.
- General – Improved search support.
- Login – Displays a dialog box with a message from login-message.json after user login for a specific time period.
- Privileges – Assign multiple privileges with one request for one user (bulk).
- Requests – Support for cancel your own request.
- Requests – Support for change participants list and end date for a request.
- UI – Identities – Displays badges for user types: functional users, personas, and user facets.
- UI – Privileges – Displays notification about current selected privileges in home page and a warning message on logout.
- UI – Requests – Improved requests summary page: request “Reason” is displayed.
- UI – Search in users – Search a user from home page.
- UI – Tasks – Improved tasks summary page.
- User Management – Create users, functional users, personas, and user facets with Create workflows.
- User Management – Displays available identities for authenticated user (My Identities): functional users, personas, and user facets.

- DirX Identity REST Services:
  - New sub-services: User Certification Service, Certification Service, Ticket Service, and Workflow Service.
  - Many extensions to the other services.
  - OpenAPI documents for the REST Service (Ticket DXI-9840).
  - A Swagger-UI based web application to test the REST Service requests.
  - Performance improvements. See the chapter “Configuring the DirX Identity REST Services” in the “Integration Framework Guide” for details.
  - The delivery includes a list of files changed since 8.9, 8.9 SP1, and 8.9 SP2, and a zip file with the old and new versions of the changed files.
  - The request to change another user’s password supports a reset flag (Ticket DXI-9565).
- Support of Unify Office by RingCentral:
  - Supports Unify Office and RingCentral
  - Full and delta import and export of Users per SCIM API with create, update, delete and search operations
  - Based on the standard DirX Identity RESTful SCIM connector
  - Supports automated management and mass provisioning of users and telephone numbers

- Realtime provisioning
- Error reporting and tracing
- Runs on Microsoft Windows and all supported Linux platforms

Detailed features of this version are:

1.12.1.1. LDAP Lock

A user entry needs to be locked when access-relevant changes are performed. The implementation has been drastically changed in this release.

- It locks only, when a privilege assignment is created, updated, or deleted or when a permission parameter is changed
- The lock is only for the minimum time to save the changes at the user and the corresponding assignment entries to guarantee they are consistent.
- To further minimize the lock time and thus the waiting time for end users and clients, only a new component, the resolution adapter resolves the user to calculate the access rights (accounts and groups) in target systems. Therefore, the client applications (such as Web Center, REST and SOAP Services, consistency workflows) send a resolution event after their changes and return. The resolution is then done in realtime, asynchronously in the backend on one of the Java servers.
- Client code, namely custom clients don't need to care about locking any more. It is completely hidden in the SvcUser methods *checkAndSave* and *save*. To simplify migration, the methods on creating and releasing ldap locks, which were explained in the Java Programming Guide of the last release, are still provided but do nothing (no-ops) and are marked as deprecated. Expect that they will be removed in a future release.

Flags like "offline resolution" are not evaluated any more: now resolution is always offline.

Effects on accounts and group memberships might not immediately be visible to end users of the user interfaces (BUI, Web Center) until the resolution has been finished. The only exception is Identity Manager. It saves the changes like the other clients and then tries to resolve the user itself. Only if this is not possible because the user is resolve-locked (a new lock at the user to protect the resolution process), it returns and displays an appropriate information.

Note that the workflows "Event-based user resolution", "User Resolution" (on Java server), and "Privilege Resolution" (Service Agent process) despite their names do not perform resolution anymore but just send the resolution event.

1.12.1.2. Resolution Adapter

To minimize the time when a user is locked, the task to resolve a user has been delegated to the resolution adapter. This adapter listens to requests on the message queue "dxm.request.user.resolve". The message contains the DN of the changed user and the time when the change happened. The resolution adapter locks the user with the so-called resolution lock and performs normal user resolution. That is: calculates new or deleted group assignments and necessary accounts depending on the privilege assignments.

During this time no other process can resolve the user, but other clients can change it, namely assign or remove privileges.

On each Java server, the adapter per default registers 2 listeners at the message broker. The number of listeners can be set at the domain entry: see the corresponding help there. For more information on the adapter and how to monitor it, see the Connectivity Admin Guide, chapter “Managing the Java-based Server” and the User Interface Guide, chapter “Using DirX Identity Web Admin”.

1.12.1.3. Target System Specific Adapter

The features of the target system specific adapter have been extended. It now supports

- Configuration of number of threads per target system. Per default, 2 threads per target systems are started for event-driven provisioning workflows, one for password changes and one for scheduled workflows (such as Validation). The number of threads for event-driven provisioning workflows can now be configured at the connected directory.
- Multiple target systems attached to the same connected directory. This allows to have for example a target system per entry type and run the provisioning workflows in parallel and not affecting other workflows started through the normal provisioning queues.
- Connected directories without any target system attached. This is especially valuable for the DirX Audit HistoryDB, so that its scheduled workflows can run on separate threads and even on selected servers. For such cases the configurable number of threads is applied to the scheduled workflows as no event-driven workflows (for realtime provisioning or password changes) are existing.

1.12.1.4. Personas und Functional Users per User in Identity Manager

- Personas, user facets and functional users linking to a user are shown on the tab “Representations” at the user object in DirX Identity Manager (Ticket DXI-8390).

1.12.1.5. Realtime Connector and Provisioning Workflows for an IBM RACF System

The Java-based RACF connector extends the Java-based LDAP Connector. It provisions the RACF system through the IBM Tivoli Directory Server for z/OS. In previous versions there was only one RACF connector based on TCL and a RACF connector just for password handling written in Java.

The new RACF connector now supports the whole range of event-based provisioning with the following functions:

- Password handling (supported as before)
- ADD (incl. initial password setting), MODIFY, DELETE, and SEARCH of objects and attributes in RACF (Ticket DXI-9361).

1.12.1.6. Extensions for Office 365 Connector and Provisioning Workflows

The connector now supports Microsoft 365 groups (unified groups). Four types including variants can now be created or managed:

- Security group,
- Microsoft 365 group (Public, Private, HiddenMemberShip).

1.12.1.7. Handling of Consistency Rules

- Consistency rules are now handled in alphabetical and not in random order (Ticket DXI-8638).

1.12.1.8. Configuration Changes

- Windows account for ActiveMQ Message broker and Java-based server are now configurable.
- Configurator now creates Notes DLL connector entry for a secondary C++-based server.
- When creating a new Workflow / Activity in Expert View the default value for the C++ based-server DN is now set to the main C++ based server (Ticket DXI-9328).

1.12.1.9. Support of Encrypted E-mails

- Request workflows can send encrypted e-mails (Ticket DXI-8635).

1.12.1.10. Anonymous Access to Connectivity and Provisioning Store

- Anonymous access is no longer necessary for configuration and operation (Tickets DXI-4777, DXI-6051).

1.12.1.11. Mail Target System

- A new target system MAIL contains e-mails which can be created for any occasion using consistency rules. A Realtime workflow sends the e-mail using the Mail connector of the connectivity framework. Those e-mails can be signed and encrypted, when a certificate is added to the mapping at the workflow's TS port channel (Ticket DXI-7581).

1.12.1.12. Delta Mode for Combined Workflows

- Combined Java RT Workflows now can run other RT workflows that are running in Delta mode (Ticket DXI-8510).

1.12.1.13. Identity Manager – Separate Logs per User

- A different destination folder and a different name per logged-in user for the Manager log files are now configurable. So, you can now configure that the log folder is outside of the installation folder (Ticket DXI-8912).

1.12.1.14. Java-based Server – Configuration of Log Folder

- For the Java-based server a destination folder for all the log files of the server is now configurable. So, you can now configure that the log folder is outside of the installation folder.

1.12.1.15. Client-side SSL Support for LDAP, ADS, and RACF Connectors

- For LDAP based RT workflows (e.g. running the LDAP or ADS or RACF connector) an additional authentication mechanism is now supported: client-side SSL (Ticket DXI-9330).

1.12.1.16. Certification Controller

- Certification Campaigns now support sub folder structures (Ticket DXI-8029).

1.12.1.17. Handling of IMPORTED Accounts

- TS accounts are only synchronized to the Connected system, if the “dxrState” attribute holds one of the following values: ENABLED, DISABLED, DELETED or is not yet set (Ticket DXI-9776).

1.12.1.18. Handling of RT Workflows when no Channel Matches

- Real-time account and group events with no matching channels are no longer put into the DeadLetterQueue (Ticket DXI-8915).

1.12.1.19. External Accessible Scrambling Method

- There is now a class available with a static method: Class com.siemens.dirxcommon.crypto.Scrambler with method getInstance() in jar file dxcCrypto.jar.
  Then call method String com.siemens.dirxcommon.crypto.Scrambler.encrypt(String cleartext); (Ticket DXI-9847).

1.12.1.20. Support of Apache ActiveMQ 5.16.3

- Update to Apache ActiveMQ 5.16.3 – contains various bug and security fixes including log4shell issue (Tickets DXI-9582, DXI-9964, DXI-9967, DXI-9968, DXI-9969, DXI-9970, DXI-9972, DXI-9973, DXI-9975, DXI-9977).

1.12.1.21. Support of Apache Embedded Tomcat 9.0.56

- Update to Apache Embedded Tomcat 9.0.56 – contains various bug and security fixes.

1.12.1.22. Web Center

- Web Center component logging has been unified. Web Center classes, JSPs, filters, and DirXweb for JSP classes and filters all write into the same log file and are controlled by the same initialization parameter "com.siemens.webMgr.log.level" in file web.xml.
- New tags <ctrl:LogTag> and <view:LogTag> to log mesages from within JSPs.
- Initialization parameter "logLevel" has been removed from the filters "ExtAuthFilter", "SSOHeaderFilter", and "CSRF Filter" in file web.xml.
- Initialization parameters "CleanUpEnabled", "RequestSyncEnabled", "IgnoreLocale", and "URLRewritingEnabled" have been removed from the filters "RequestFilter" and "BinaryRequestFilter " in file web.xml. Their default values should be fine.

- The DirXweb for JSP tags <dir:connect> and <dir:disconnect> used in JSP controller/tasks/password/changePassword.jsp have been replaced with the new tag <ctrl:checkCredentials>.
- The DirXweb for JSP listeners "siemens.dirxjsp.core.application.Initializer" and "siemens.dirxjsp.core.application.SessionListener" aren’t supported anymore and have been removed from web.xml.
- The File Upload feature supports checking the type of the uploaded files. The check can be customized. For details, see the use case document "Web Center File Upload".
- The self registration feature is deactivated by default for security reasons. See the "Web Center Customization Guide" for how to activate it.
- SoD violations are displayed with localizable texts.
- Web Center supports the new delegation implementation introduced in version 8.9. The old one is also still supported. The domain configuration flag "Delegation Assignment stores Operation" controls which implementation is active.
- Web Center supports the new business object type "Numbering Plans".
- Support for online privilege resolution has been abandoned. The corresponding configuration parameters "offlineResolution" and "offlineResolutionAfterPrivilegeChanges" have been removed from file webCenter.properties.
- Web Center assigns a correlation ID to create workflows.
- The HTTP session is invalidated at the of a request if session attribute "com.siemens.webMgr.loginDN" is empty.
- The delivery includes a zip file with the old and new versions of the files changed since 8.9, 8.9 SP1, and 8.9 SP2.

1.12.2. Bug Fixes

1.12.2.1. Business User Interface

- Fixed issue with Change Password policy that sometimes didn’t display forbidden characters (Ticket DXI-9598).

1.12.2.2. Java-based Server

- The handling of nationalized message strings for request workflows has been improved. A duplicate message key doesn’t result in termination of loading the messages; only that duplicate message cannot be resolved correctly; but all the other messages are available. Logging for such an erroneous situation has been improved (Ticket DXI-9337).
- Settings for remote debugging were adopted for Java 11 (Ticket DXI-9453).
- Server Admin fixed to show status of Java Server in SSL environment (Ticket DXI-9785).
- If an event contains an invalid XML character (non-printable characters e.g. vertical tab) then this event was ignored but the framework controller had no information that an event could not be processed so it switched from event to full synchronization mode. Now this information is returned, and the adaptors eliminate such invalid XML

characters from an event so that the event can be processed (does not apply to the TS-specific adaptor; there you get an error log message). In contrast, events which contain characters which must be escaped in XML data but are not escaped cannot be processed. The event is logged but not put in the Dead Letter Queue (Ticket DXI-9781).

- On startup of the Java-based server non existing request workflows will be removed from the request workflow repository (Tickets DXI-9520, DXI-9620, DXI-9856).
- DeadLetterQueue shows "entry not available"; now response is truncated; also monitor entry (dxmRemark) if a certain limit is reached (Ticket DXI-9541).
- Realtime workflow assignment to a Java-based server is not always consistent (Ticket DXI-9803).
- LDAP error in the TS-specific adapter when there were more than 1000 port definitions in workflows (Ticket DXI-9879).
- In SSL environment the Server Admin displays stopped state for any Java-based server (Ticket DXI-9785).
- If an event contains an invalid XML character (e.g., vertical tab = 0xb) then this event was ignored but the framework controller had no information that an event could not be processed so it switched from event to full synchronization mode. Now this information is returned, and the adaptors eliminate such invalid XML characters from an event so that the event can be processed (does not apply to the TS-specific adaptor; there you get an error log message). In contrast, events which contain characters which must be escaped in XML data but are not escaped cannot be processed. The event is logged but not put in the Dead Letter Queue (Ticket DXI-9781).
- Scheduler: The fact that no valid start time for a schedule could be calculated (because of ranges) was not considered and led to an IllegalArgumentException when a timer was instantiated (Ticket DXI-9832).
- Configuration of allowed TLS protocols for JMX access (Ticket DXI-9715).
- For the adaptors EntryChangeStartWorkflowListener and ProvisioningRequestStartWorkflowListener the counting of requests and responses has been fixed (Ticket DXI-9704).
- For a Request workflow the monitor display name can be defined to include the creation time of the workflow by the following expression:

```
<? JavaFunction
com.siemens.idm.jini.util.GeneralizedTime2ISO8601DateTime
${createTime} ?> ${subject.cn} -> ${resources[0].dxrassignto@cn
```

  If the customer wants to change the format of the timestamp "yyyy-MM-dd'T'HH:mm:ss" then a different version of a suitable Java method must be implemented by the customer.

  The Java method "GeneralizedTime2ISO8601DateTime" is provided (Ticket DXI-9464).

- An error message in a response from a connector is truncated in the Join Engine if greater than 8 KB. This means that a request and its response can normally be inserted

into the Dead Letter Queue (DLQ) database. If a request and its response are still too big for the DLQ database the entry is not inserted at all. Also, a remark in monitor entries is truncated if greater than 8 KB (DXI-9541).

- For Linux: Server start/stop-processes are not handled correct, if more than one java-based server exists (DXI-9993).

1.12.2.3. C++-based Server

- Server is unable to decrypt private keys in <INST_PATH>/ssl/client-key.pem and <INST_PATH>/ssl/server-key.pem. Fixed an error in an internal scramble function that is used for passwords and pinphrases (Tickets DXI-9672, DXI-9819, DXI-9693, DXI-9672).
- Trace files bigger than 2 GB could not be moved to status area (Tickets DXI-9782, DXI-9637).
- When an activity execution ends and the exit code from the agent is neither an error nor a warning code then if the publishing activity status info to the Status Tracker fails this error code is given back to the workflow engine. This interferes the execution of subsequent activities. Therefore, a new flag for the C++-based server in the dxmmssssvr.ini is introduced:
  IgnoreSaveStatusInfoError in the "settings" section
  If set to 1 then errors from sending activity status info are ignored. That means the normal workflow execution continues. Default is 0 (Ticket DXI-9399).
- The disclosure of sensitive information about implemented software and the version number is now prevented (SOAP/JMX port) (Ticket DXI-9989).

1.12.2.4. Agents / Connectors

- Service agent: By mistake sometimes the Service agent sent change events even if configured to suppress change events (Tickets DXI-9663, DXI-9552).
- ConsistencyCheck considered the state TBDEL to be an invalid one (Ticket DXI-9663).
- SAP UM ECC agent/connector: If CUA and no combinedRPS are set then activitygroups where not correctly deleted (Ticket DXI-9593).
- ADS agent: recursive deletion of objects if IADsDeleteOps→DeleteObject() fails with error LDAP_INSUFFICIENT_RIGTHS (Tickets DXI-9900, DXI-9001, DXI-9764).
- SAP Netweaver portal agent: For Java 11 environment some jar files were missing (Ticket DXI-9767).
- JDBC connector: Include date value in ' (apostrophe) to avoid statement errors when special characters are included. Affects just TIMESTAMP values. If there are already apostrophes in the string, then the string is passed as it is (Ticket DXI-9684).
- Office 365 connector: The application secret is now scrambled or encrypted stored in the configuration (Ticket DXI-9277).
- The Notes agent sporadically didn’t create the attribute “Type” when synchronizing groups (Ticket DXI-9544).

1.12.2.5. Request Workflows

- Participant calculation for group members has been extended: If group member is an SvcTSAccount (rather than an SvcUser), then the related SvcUser is returned (identified via "dxrUserLink") (Ticket DXI-9638).
- The participant calculation using group definition now supports groups with SvcTSAccounts as members, too. In that case the user defined by the "dxrUserLink" attribute is returned (Ticket DXI-9461).
- Notifications with Userhooks was missing in standalone activities, e.g., "Notificaton If Rejected" (Ticket DXI-9585).

1.12.2.6. Realtime Workflows

- In case of retry now even after the last retry the event is written to the error channel and therefore the error activity of the workflow is called (Join Engine and Realtime Workflows) (Tickets DXI-9571, DXI-10464).
- New expressions in e-mails of "setPassword"-workflows are supported: "${IDATTR(_originatingusercn)}", "${IDATTR(_originatingusergivenname)}", "${IDATTR(_originatingusermail)}", "${IDATTR(_originatingusersn)}" (Ticket DXI-9595).
- Full Import controller didn’t synchronize correctly in cross membership scenario due to missing information of TS data (Ticket DXI-9727).
- Privilege resolution failed with a NullPointerException when an object was searched and existed before but when processing it that object meanwhile was deleted (Ticket DXI-9747).
- Sporadically a realtime workflow terminated with state "closed.completed.ERROR" (in the monitor view), but no real errors were shown in the logfile (Ticket DXI-9728, DXI-9658).
- Handle now correctly situations in provisioning workflows when the sort attribute has no value (Ticket DXI-9537 and DXI-9568).
- The workflow XML definition contained invalid XML tokens (missing “dsml” prefix in the default value of an export filter definition). For better analysis of such situations a stack trace in the IDS-J logfile will be printed if a workflow could not be loaded successfully (Ticket DXI-9691).
- NullPointerExceptions in Full Synch HistoryDB workflows was fixed (Ticket DXI-9490).

1.12.2.7. Services

- Obligations with naming rules didn’t work for role parameters (Ticket DXI-9801).
- Performance improvements in user resolution while evaluating the matching groups of a permission (Ticket DXI-9647).
- Missing groups in role resolution fixed while evaluating role match rules (Ticket DXI-9698).
- View policies (evaluated in Web Center) and SoD policies resulted in start of a wrong (SoD) approval workflow (Ticket DXI-9034).
- User Resolution failed because permissions were not evaluated correctly when

searching the resolved groups in LDAP. (only when role parameters of type "Group" were used with operator "startsWith", "endsWith") (Tickets DXI-9647, DXI-9628).

- The warning that a user has a privilege that is not flagged "user assignable" is only generated in case the user has that privilege directly assigned (Ticket DXI-9706).
- For compound attributes the same attribute modification was generated in an LDAP MODIFY operation more than once (Ticket DXI-9624).
- Role parameter attributes and other attributes (e.g."netscapemdsuffix") have been dropped from LDAP search requests in case these role parameters are no real LDAP attribute names (Ticket DXI-9718).
- Performance optimizations have been implemented when evaluation the matching groups of a permission (Ticket DXI-9628, DXI-9647, DXI-9695, DXI-9698, DXI-9701, DXI-9711, DXI-9751, DXI-9824).
- DependsOn is now correctly triggered when only the case of an attribute value changes (Ticket DXI-9815).
- dxrOptions attributes are now handled correctly regardless of lower / upper case (Ticket DXI-9802).
- For compound attributes (e.g. dxrOptions) the same LDAP modifications were by mistake generated more than once (Ticket DXI-9624).
- For group assignments with a future start date the property "assign.displayState" is now FUTURE and not the real state like ADD or DELETE as before (Ticket DXI-9679).
- When deleting a user now implicitly the personas and user facets of this user are deleted first (Ticket DXI-9538).
- Separation-of-Duty (SoD) handling now considers also start and end dates in assignments. Approval is requested even when the assignment starts in the future. If the assignment is finished (for example because of end date reached), the SoD exception is removed. If remaining assignments contain an end date with the flag needsReapproval = true, then the end date is removed and needsReapproval set to false (Tickets DXI-9119).
- In some cases, existing lock mechanism caused problems. Components calling createLdapLock were working with outdated User Objects when lock creation made several retries and in the meantime the user to be locked was changed by the other application which had set the lock. The new lock implementation fixes this (Ticket DXI-9266).
- At the point when an approval workflow should be started also a cleartext password is allowed in encryption mode (Ticket DXI-9881).
- Now implicitly personas/user facets are deleted during user deletion (Ticket DXI-9538).

1.12.2.8. Join Engine

- Attributes with "Modify Always" mapping definition were not synchronized if they themselves changed too (Ticket DXI-9468).
- No longer change requestType=NONE to requestType=DELETE if the JoinedEntry doesn’t exist. By mistake this change resulted in setting the dxrTSstate to DELETED when synchronizing the object back to IdentityDomain (Ticket DXI-9908).

- Cross-membership: Due to an internal problem not all the attributes were read which resulted in deletion of the values in "dxrGroupMemberOk" and moving them to "dxrGroupMemberAdd" (Ticket DXI-9835).
- Sporadically a realtime workflow terminated with state "closed.completed.ERROR" (in the monitor view), but no real errors were shown in the logfile (Tickets DXI-9736, DXI-9728).
- No attribute modification on "Modify always" flag (Tickets DXI-9569, DXI-9468, DXI-9665).
- TS accounts are only synchronized either without a value for dxrState or with dxrState is ENABLED or DISABLED or DELETED. By mistake it was not synchronized with state TBDEL (Ticket DXI-9928).
- Fix NullPointerException in Validation controller when filter attribute is null (Ticket DXI-9504, DXI-9944).
- Fixed that no target system info was available for HistoryDB workflow (Ticket DXI-9897).
- A workflow will close in state "closed.completed.OK", even when it was interrupted due to timeout or cancelled. Cancelled or interrupted workflows will now close in state "closed.completed.WARNING" (Ticket DXI-9978).
- Revised parallel handling of multiple provisioning tasks for the same entry, resulting in workflow retry with message "Entry is currently in use by another event workflow." (Tickets DXI-10363, DXI-10089, DXI-10189).

1.12.2.9. Identity Manager

- Removed special entries from the proposal list. These entries are just for internal list processing, not to be displayed to users (Ticket DXI-9519).
- Removed false blank entry from the proposal list (Ticket DXI-9675).
- Fixed component renderer for multi value editor component so it shows display value instead of stored value (Ticket DXI-9713).
- Obsolete action which caused warning has been removed (name: siemens.dxm.actions.ActionShowDefaultMessageServer) (Ticket DXI-9864).

1.12.2.10. Web Center

- Verifying signatures with encoding UTF-8 fixed (Ticket DXI-9661).
- Avoid a ClassCastException when searching in Web Center (Tickets DXI-9589, DXI-9707).
- Web Center optionally takes the attribute labels for workflow activities "enterAttributes" and "approveCreate" from the activity definition. This is controlled by configuration parameter "tasks.useLabelsFromDefinition" in file webCenter.properties (Ticket DXI-9499).
- Do not send duplicate requests on selection of an entry (Ticket DXI-9746).
- Expression evaluation for action parameter defaultFilter fixed (Ticket DXI-9696).
- Configurable search base and search filter for searching the user matching the identification data entered into the Web Center login form. See configuration parameters "loginForm.searchBase" and "loginForm.searchFilter" in file webCenter.properties (Ticket DXI-8874).

- Web Center supports compound attributes like "dxrOptions" for workflow activities "enterAttributes" and "approveCreate" (Ticket DXI-9510).
- A privilege assignment start date must precede its end date (Ticket DXI-9574).
- Previously missing subject attributes are now displayed for all tasks in the task list (Ticket DXI-9912).

1.12.2.11. REST Services

- Take the best-matching object description when creating an object via the REST Services (Tickets DXI-9576, DXI-9587, DXI-9619).
- The REST Services return the correct value for attribute displayName (Ticket DXI-9641).

1.12.2.12. Provisioning Services

- Fix for IndexOutOfBoundsException while trying to find an object descriptor (Tickets DXI-9650, DXI-9707).
- Setting the log level for the provisioning servlet fixed (Ticket DXI-9642).

1.12.2.13. TCL-based Workflows

- Escaping of special characters corrected when calling "meta findentry" (Ticket DXI-9854).
- Notes workflow: LDAP error code LDAP_INSUFFICIENT_ACCESS handled as OK case in search operation (z/OS 2.4) (Ticket DXI-9687).
- When sending the trace file as e-mail fails, the exit code of the “send mail” program is written to stderr and therefore shows up in “ProcessInfo.txt” in the work or status area of the workflow (Ticket DXI-9986).

1.12.2.14. Documentation

- Windows Password Listener (WPL) documentation has been updated regarding the topic that WPL needs an encrypted password in the password.properties file (Ticket DXI-9685).
- A new entry has been added to the Troubleshooting Guide for the case that a web application fails to start with status code 404 – Not Found (Ticket DXI-9498).
- To generate a cert8.db file with the Mozilla command tool certutil on Suse Linux you should use the option
"-d". The given link in the Metacp reference documentation must be updated (Ticket DXI-9309).
- ActiveMQ: In the wrapper.log of Tanuki Software are warnings about missing certificates to verify the signed wrapper executable. In the Troubleshooting Guide a corresponding entry on how to fix it was added (Ticket DXI-9721).
- Nagios: Documentation for using Nagios with Java 11 has been supplemented (Ticket DXI-9911).

1.12.2.15. Password Management

- Remove section "Other Questions" from page “Add Authentication Questions” if the last question in the section has been deleted and the section is configured as not editable (Ticket DXI-9800).

1.12.2.16. APRC

- If the local policy "Interactive Logon: don’t display last signed-in" is active no APRC tile was presented in "Other options" on the logon screen (Ticket DXI-9622).
- APRC was extended so that also monitors with a very high resolution are supported (4K monitors) (Ticket DXI-9717).

1.12.2.17. Miscellaneous

- SPNEGO supports Kerberos authentication via Netscaler (Ticket DXI-9838).
- Bad performance due to missing attribute index for attribute dxrAssignedGroups (Ticket DXI-9683).
- Link Checker: A NullPointerException in paging was fixed (Ticket DXI-9496).
- LDAP SDK for Java: Paging Control is only provided for LDAP searches with paging. Furthermore, if connection is lost a rebind to the LDAP server has been implemented: a configurable number of retries with a waiting timeout before retrying can be defined. That option is provided for all LDAP operations except LDAP searches with paging (Tickets DXI-8811, DXI-9594, DXI-9868).
- Tool MissingUidFixer and workflow UidConsistencyCheckController catch sizelimit exceeded now immediately and write the statistics at the end. In such a case, the tool / workflow should be started again to find the next 1000 (depends on sizelimit) entries without a dxrUid (Ticket DXI-9535).
- Installer: The Installer has been updated to recognize correctly newer Microsoft Visual C++ Redistributable versions and not report an error message (Ticket DXI-9914).
- Replace Apache Log4j version 1.2.8 with Log4j version 2.17.1 because of Log4shell security issue (Tickets DXI-9582, DXI-9964, DXI-9967, DXI-9968, DXI-9969, DXI-9970, DXI-9972, DXI-9973, DXI-9975, DXI-9977).

1.12.3. Information About Discontinued Features

DirX Identity V8.10 does no longer support these features:

- Internet Explorer 11 browser support in Business User Interface
- DirX Approvals App for Apple® iOS

DirX Identity V8.10 is the last version that supports the following features:

- Support of Microsoft Lync 2013
- Connectivity package for HiPath 4000
- Connectivity package for Imprivata OneSign

1.13. Dirx Identity V8.9 SP3

1.13.1. New Features

1.13.1.1. Realtime Connector and Provisioning Workflows for an IBM RACF System

- The Java-based RACF connector extends the Java-based LDAP Connector. It provisions the RACF system through the IBM Tivoli Directory Server for z/OS. In previous versions there was only one RACF connector based on TCL and a RACF connector just for password handling written in Java.

Now the new RACF connector supports the whole range of event-based provisioning with the following functions:

- Password handling (supported as before)
- ADD (incl. initial password setting), MODIFY, DELETE, and SEARCH of objects and attributes in RACF (Ticket DXI-9361).

1.13.1.2. Client-side SSL Support for LDAP, ADS, and RACF Connectors

- For LDAP-based realtime workflows (e.g., running the LDAP or ADS or RACF connector) an additional authentication mechanism is now supported: client-side SSL. Additionally, a migration batch script "MigratePortForClientSSL.bat/sh" is offered to update existing LDAP-based realtime workflows (Ticket DXI-9330).

1.13.1.3. Handling of IMPORTED Accounts

- TS accounts are only synchronized to the Connected system, if the “dxrState” attribute holds one of the following values: ENABLED, DISABLED, DELETED or is not yet set (Ticket DXI-9776).

1.13.1.4. Role Assignments with Mandatory End Dates

- Web Center supports role assignments with mandatory end dates (Ticket DXI-10009).

1.13.1.5. Support of Apache ActiveMQ

- Update to Apache ActiveMQ 5.16.3 – contains enhancements and various bug and security fixes including log4shell issue (Tickets DXI-9582, DXI-9964, DXI-9967, DXI-9968, DXI-9969, DXI-9970, DXI-9972, DXI-9973, DXI-9975, DXI-9977).

1.13.1.6. Support of Apache Embedded Tomcat

- Update to Apache Embedded Tomcat 9.0.62 – contains enhancements and various bug and security fixes (Ticket DXI-10058).

1.13.2. Bug Fixes

1.13.2.1. Request Workflows

- Calculation of participants via a TS-Group has been improved: If the groups hold TS accounts (rather than users) then the related users are identified via the "dxrUserLink" attribute (Ticket DXI-9461).
- Provide now the possibility to have in the Request workflow displayname a creation timestamp (Ticket DXI-9464).
- On startup of the Java-based server non existing request workflows will be removed from the request workflow repository (Ticket DXI-9620).
- Participant calculation for group members has been extended: If group member is an SvcTSAccount (rather than an SvcUser), then the related SvcUser is returned (identified via "dxrUserLink") (Ticket DXI-9461).
- Handling of the timeout parameter for request workflow activities fixed (Ticket DXI-9940).
- Suppress unnecessary warning when creating a functional user via workflow (Ticket DXI-9791).
- Fixed missing Audit Record for request workflow activity "Acknowledge update" (Tickets DXI-9946, DXI-10088).
- Resolution of placeholders in notification e-mail's subject and body: Remove duplicate e-mail addresses in notification e-mail's address fields (Ticket DXI-9999).

1.13.2.2. Join Engine

- NullPointerException in Full HistoryDB Synch workflow was fixed (Ticket DXI-9490).
- Avoid unnecessary modify requests in HistoryDB Sync workflows because of dirxEntryUUID's default mapping (Tickets DXI-9537, DXI-9568).

SP3: Services

- Attributes with flag "M(odify always)" are always modified (Tickets DXI-9569, DXI-9468, DXI-9665).
- New expressions in emails of "setPassword" workflows are supported: "${IDATTR(_originatingusercn)}", "${IDATTR(_originatingusergivenname)}", "${IDATTR(_originatingusermail)}", "${IDATTR(_originatingusersn)}" (Ticket DXI-9595).
- Fixed a NullPointerException during synchronization when a JoinTempException was caught (only in cross membership scenarios) (Ticket DXI-9683).
- Full Import controller didn't synchronize correctly in cross membership scenario due to missing information of TS data (Ticket DXI-9727).
- Realtime workflows terminate with ERROR even if there is none (Tickets DXI-9736, DXI-9728).
- Performance optimizations for a cross membership scenario have been implemented (Ticket DXI-9835).
- New feature "preventMemberUpdate" in "dxrOptions" of TS added to define that the membership for that group is not stored at the account (Ticket DXI-9835).

- By mistake, Join engine misused the request Type from mapping and changed from NONE to DELETE (Ticket DXI-9908).
- TS accounts are only synchronized either without a value for dxrState or with dxrState=ENABLED | DISABLED | DELETED (Ticket DXI-9928).
- No target system info was available for HistoryDB workflow (Ticket DXI-9897).
- Fixed the situation that an error with the processed object cannot be audited as the error message from a connected system contains invalid characters that cannot be marshalled into the XML format necessary for the auditing process (Ticket DXI-9887).
- Fixed NullPointerException when filter attribute is null (Tickets DXI-9944, DXI-9504).
- Update Identifier DN in an add request before it is sent to the Event port, if the DN in the add response is different from the DN in the add request. The add request identifier DN is updated in this case to the DN found in the identifier of the add response (Ticket DXI-9971).
- A search to join by a File-based connected directory during export does not make sense and just causes performance issues (Ticket DXI-9762).

1.13.2.3. Services

- User resolution failed because permissions were not evaluated correctly when searching the resolved groups in LDAP (only when Role parameters of type "Group" were used) (Ticket DXI-9628).
- For compound attributes the same attribute modification was generated in an LDAP MODIFY operation more than once (Ticket DXI-9624).
- - Now implicitly personas/user facets are deleted during user deletion (Ticket DXI-9538).
- Attribute index for dxrRPValues is now set (Ticket DXI-9628).
- Report generation with searches with scope=BASE failed.
- Evaluation of role parameters with "startsWith", "endsWith" corrected. Optimized filter includes the CNs of the relevant groups (Tickets DXI-9628, DXI-9647).
- Wrong display of "assign.displayState": return FUTURE as display state is not a real state like ADD or DELETE (Ticket DXI-9679).
- Missing groups in role resolution while evaluating role match rules (Tickets DXI-9698, DXI-10036).
- Missing groups in role resolution while evaluating role match rules when using attribute name "dn" (Tickets DXI-9697, DXI-9569, DXI-9552, DXI-9628, DXI-9647, DXI-9698, DXI-9695).
- Search constraints are now passed in "search" operation and are not stored at the LDAP connection. This solution doesn’t cause any invalid cookies in the LDAP server while processing paged searches (Ticket DXI-9594).
- Performance problems in role resolution when evaluation the matching groups of a permission (Tickets DXI-9701, DXI-9628, DXI-9647, DXI-9695, DXI-9698, DXI-9701, DXI-9711).
- Bad performance in role resolution (Ticket DXI-9751, DXI-10050, DXI-10051).

- Role parameter attributes (and other attributes e.g., "netscapemdsuffix") have been dropped from LDAP search requests in case these role parameters are no real LDAP attribute names (Ticket DXI-9718).
- Performance optimizations have been implemented when evaluating the matching groups of a permission (Ticket DXI-9824).
- Performance improvements for old delegations (Ticket DXI-9992).
- The warning that a user has a privilege that is not flagged "user assignable" is only generated in case the user has that privilege directly assigned (Ticket DXI-9706).
- CryptSupport was not available in service agent's user storage; Logging in crypting was extended (Ticket DXI-9659).
- New values of a multi-valued attribute with caseIgnoreMatch were not added if old value with different case exists (Ticket DXI-9802).
- SetProperty when just updating the case does not activate the trigger, so that dependsOn won't start e.g., a JavaScript (Ticket DXI-9815).
- Obligations with naming rules didn't work for role parameters (Ticket DXI-9801).
- At the point when an approval workflow should be started by the services also a cleartext password is allowed in encryption mode (Ticket DXI-9881).
- The dxrRPValues attribute which is a multi-valued attribute is not defined as multi-valued in its Object description. There were 2 confusing log entries because of missing 'not' (the log entries stated they are multi-valued, but they are not) (Ticket DXI-10013).
- ClassCastException in application Simple Identity Management Service (SIMS) fixed (Ticket DXI-10056).
- It can happen that the dxrRPValues value of the group is not an exact string or a '*' (all), but a partial string such as [cn=*, cn=SomeBO, cn=Custom, cn=BusinessObjects, cn=My-Company]; therefore, check all the matching rules on the current list of groups using the standard algorithm is required in the current logic (Ticket DXI-10062).

1.13.2.4. Java-based Server

- Dead Letter Queue handling was improved to truncate request responses so that they can displayed in Web Admin instead of showing "entry not available" (Ticket DXI-9541).
- For the adaptors EntryChangeStartWorkflowListener and ProvisioningRequestStartWorkflowListener the counting of requests and responses has been fixed (Ticket DXI-9704).
- Allow to set supported TLS protocols for JMX access (Ticket DXI-9715).
- Target System-specific dispatcher for start workflow requests does now support HistoryDB and File-Import/Export workflows (Ticket DXI-9803).
- Target System-specific adapter now searches with client sizelimit 0 (rather than default 1000) (Ticket DXI-9879).
- Scheduler: No valid schedule start time was found in 1 year ahead. Return code 0 was not considered (Ticket DXI-9832).
- Handling of invalid or not escaped characters in realtime events was implemented (Ticket DXI-9781).

- Server Admin does not show status of Java servers with SSL configuration (Ticket DXI-9785).
- Linux only: Java-based server start/stop-processes are not handled correct, if more than one server exists (Ticket DXI-9993).
- The internal framework job pooling configuration was extended to allow up to 400 active framework job objects per default. Up to now the maximum value was 100. This prevents exceptions from occurring less frequently if a total thread number above 100 is configured across all Resource families (Exceptions like "CFG514 Exception DxmConnectorException when opening connectors: java.util.NoSuchElementException..."). The maximum value is now also configurable via Java system property in idmsvc.ini or in runServer.sh file. Property name is IDM_POOL_MAXACTIVE, default is 400 (Ticket DXI-10052).
- Now the LDAP connection pool in the Java server uses a configurable time limit for bind operations to prevent Java server to hang when in rare cases the bind response is not received. Default is 15 seconds (Ticket DXI-10060).

1.13.2.5. C++-based Server

- Copying files (e.g., trace files) bigger than 2GB from work to status area fails on Windows (Ticket DXI-9637).
- Sporadically an SSL initializing issue in C server (Tickets DXI-9672, DXI-9819, DXI-9693, DXI-10015).
- Disclosure of used gSOAP server name in the C++-based server suppressed (Ticket DXI-9989).

1.13.2.6. Realtime Workflows

- Error activity was not started if a FAILED.TEMPORARY error response was returned. After end of retry the event must be written into error channel (Tickets DXI-9571, DXI-10464).
- Added additional stack trace in log message if parsing of a realtime workflow configuration fails. Default configuration for channels had an XML problem in filter definition due to missing namespace for required tag "<dsml:or>" (Ticket DXI-9691).

1.13.2.7. REST Services

- Take the best-matching object description when creating an object (Tickets DXI-9576, DXI-9587, DXI-9619).
- The REST Services return now the correct value for attribute displayName (Ticket DXI-9641).

1.13.2.8. Web Center

- Avoid a ClassCastException when searching in Web Center (Tickets DXI-9589, DXI-9707).
- Expression evaluation for form field default value fixed (Ticket DXI-9653).
- Web Center supports compound attributes (like dxrOptions) in workflow activities

"enterAttributes" and "approveCreate" (Ticket DXI-9510).

- Subject attributes are now correctly displayed for all tasks in the task list (Ticket DXI-9912).
- The size limit for listing the direct users of a role in Web Center is now configurable. Web Center displays a message if the size limit has been exceeded (Ticket DXI-9926).
- Display a user-friendly error message if an attempt to assign a role to a user fails due to invalid parameter values (Ticket DXI-10046).

1.13.2.9. Provisioning Servlet

- Fixed IndexOutOfBoundsException when trying to find the object descriptor (Tickets DXI-9650, DXI-9707).

1.13.2.10. Manager

- Removed special entries from the proposal list. These entries are just for internal list processing, not to be displayed to users (Ticket DXI-9519).
- Removed false blank entry from the proposal list (Ticket DXI-9675).
- Fixed component renderer for multi value editor component so it shows display value instead of stored value (Ticket DXI-9713).
- Update of online help files LdapHelp.jar and DirXjdiscoverHelp.jar.
- Obsolete configured action which caused warning has been removed (action name: siemens.dxm.actions.ActionShowDefaultMessageServer) (Tickets DXI-9864, DXI-10033).
- Proposal lists: Fixed a NullPointerException when entering a variable into the LDAP filter in independent DN proposal list; dependent proposal update is not triggered when the property depends on "c" (country) attribute (Ticket DXI-10017).

1.13.2.11. Business User Interface

- Fixed issue with Change Password policy that sometimes didn’t display forbidden characters (Ticket DXI-9598).
- Fixed issue that prevented My Profile page to load when the user had Pending Modifications (Ticket DXI-9990).

1.13.2.12. Agents/ Connectors

- SAP UM ECC agent: With settings "CUA" and no "combinedRPS": SAP activitygroups where not correctly deleted (Ticket DXI-9593).
- Service agent: By mistake sometimes the Service agent sent change events even if configured to suppress change events (Tickets DXI-9552, DXI-9665).
- Service agent: Consistency Check considered the state TBDEL to be an invalid one (Ticket DXI-9663).
- JDBC connector: JDBC SQL statement error: Include values in ' (apostrophe) to avoid statement errors when special characters are contained (Ticket DXI-9684).
- SAP UM EP agent: Agent run script was not Java 11 compatible. Missing jars for SOAP

messaging (Ticket DXI-9767).

- ADS agent: Recursive deletion of objects implemented if IADsDeleteOps→DeleteObject() fails with error LDAP_INSUFFICIENT_RIGHTS (Tickets DXI-9764, DXI-9900, DXI-9001).
- Notes agent: The agent sporadically didn't set the attribute "Type" when synchronizing groups (Ticket DXI-9544).
- RACF connector: Add, Remove RACF groups problems: E.g., on assigning groups the "Assignment State" stays on "ADD" and does not change to "ENABLED" (Ticket DXI-9980).
- Identity Domain connector: The connector must copy OperationalAttributes from request to response, as those are needed in join engine on rename (Tickets DXI-9788, DXI-10066).

1.13.2.13. Miscellaneous

- Setting the log level for the Provisioning Servlet and Java-based agents was fixed (Tickets DXI-9642, DXI-9665, DXI-10040, DXI-10032).
- Crypting: Verifying signatures with encoding UTF-8 fixed (Ticket DXI-9661).
- Schema: Attribute index for attribute dxrAssignedAccounts (Ticket DXI-9683).
- RACF TCL Workflows: LDAP error code LDAP_INSUFFICIENT_ACCESS handled as OK case in search operation (z/OS 2.4) (Ticket DXI-9687).
- TCL Workflows: Escaping of special characters corrected when calling "meta findentry" (Ticket DXI-9854).
- TCL Workflows: In case of errors "sendNotification" writes exit code to stderr (found in the file ProcessInfo.txt) (Ticket DXI-9986).
- Schema: Missing attribute index for dxrAssignedGroups was added (Ticket DXI-9683).
- EntryLockManager: The lock mechanism uses new LDAP control NO-MOD-TIME-Upd-CTRL from DirX Directory Server to modify an entry without implicit modifying the "modifyTimeStamp" of that entry (Ticket DXI-9943).
- SPNEGO: Changes for Kerberos authentication via NetScaler (Ticket DXI-9838).
- Security update: Change everywhere to use log4j version 2.17.1 (Tickets DXI-9967, DXI-9969, DXI-9970, DXI-9973, DXI-9975, DXI-9977).
- Tools RunReport, RunWF, Eventing: Set for shell scripts the execute bit. Now on Windows the zip files contain Windows batch scripts only and on Linux the tar files contain shell scripts only (Ticket DXI-10007).
- JmsAuditLogHandler always set option "useInactivityMonitor=false" in the connection URL string for the DirX Auditing ActiveMQ broker. In case failover protocol should be used this is not supported. This setting can now be controlled by a Java system property (Ticket DXI-10077).
- LDAP SDK for Java: Paging Control is only provided for LDAP searches with paging. Furthermore, if connection is lost a rebind to the LDAP server has been implemented: a configurable number of retries with a waiting timeout before retrying can be defined. That option is provided for all LDAP operations except LDAP searches with paging

(Tickets DXI-9594).

1.14. DirX Identity V8.9 SP2

1.14.1. New Features

1.14.1.1. Target System-specific Adaptor Feature

- Target system-specific (TS-specific) adaptor now supports multiple target systems per connected directory (Ticket DXI-9348).
- The number of threads listening to provisioning events (dxm.request.provisiontots.<type.cluster.resource>) is configurable (Ticket DXI-9456). In Identity Manager select the connected directory and in tab "Connected Directory", section "Associate to Server" enter the number into the field "Listeners per Target System". Default is 1. Note that the section might not be visible in custom connected directory types such as DirX Audit History DB or Fusion. In these cases, their object description must be extended the same way as in the out-of-the-box connected directories.
- Web Admin now shows again the number of messages received, failed, etc. for the Dispatchers and the TS-specific adaptors (Ticket DXI-9457). Note that they are displayed when the tree items "Provision Dispatchers" or "Provision TS Listeners" are selected. For TS-specific Listeners the counter for successfully processed messages was added.

These dispatchers and the adaptors for the TS-specific queues follow a different behavior than those for the normal provisioning queues:

They do not store the received messages in their own file repository and therefore need no special handling for high availability. Instead, the adaptors process each message immediately and acknowledge it to the message broker only when processing is finished. In case of breakdown, the not-yet-acknowledged messages are still available in the message broker and are delivered when the adaptor re-connects.

They do not use the workflow engine. Instead, they perform the error handling on their own. They pass the messages directly to the join activity of the workflow. If an error occurs, they send the message again to the broker with a delay according to the configured retry wait time. If that is not possible because the error is not considered temporary or the retry limit is reached, the adaptor runs the error activity and sends the message to the Dead Letter Queue.

Find more details on the adaptors in the Connectivity Administration Guide, chapter "Managing DirX Identity Servers / Managing the Java-based Server".

1.14.1.2. Office 365 Connector

- Filtering possibility and improved pagination was added (Ticket DXI-9264).

Pagination Notes: The paging was revised and needs some adjustments for an already existing TS. In the corresponding Connected Directory, you must activate "Is Active" in the tab "Export" and set "Page Size" to a value equal to 100 for the channels accounts, groups,

members, plans, and roles.
The connector does not support a value greater than 100 in "Page Size" because Microsoft Graph API does not support it.

The service package includes a documentation update for filtering, notes for pagination are not included:

identOffice365.pdf

1.14.1.3. Identity REST Services

- To improve the performance, the REST Services support LDAP connection pools

for user identification and authentication and for request processing (Ticket DXI-9485):

The REST Services include a new authentication provider with name "dxiLdapUserNameAuthenticationProvider" for checking HTTP basic credentials via user name and password (as an alternative to the Spring-based provider).

The name of the user details service has changed from "ldapUserDetailsService" to "dxiLdapUserDetailsService".

The configuration parameter keys of the user details service in file security.properties have been changed from "auth.<subName>" to "auth.userDetails.<subName>".

The configuration files "security.xml" and "security.properties" have been updated.

- The authentication samples have been updated.
- The log configuration files haven been revised and renamed.

For details, see the documentation update "identintegration.pdf" included in this service package in folder "INST_PATH/patches/SP2/Man/Documentations". Chapter 6 "DirX Identity REST Services" includes a new section on "Configuring LDAP Connection Pools", and updated sections on "Configuring User Authentication" and "Configuring Application Logging".

1.14.1.4. Support of Apache ActiveMQ 5.16.1

- Update to Apache ActiveMQ 5.16.1 – contains various bug and security fixes (Tickets DXI-9438, DXI-9518).

1.14.1.5. Support of Apache Embedded Tomcat 9.0.43

- Update to Apache Embedded Tomcat 9.0.43 – contains various bug and security fixes (Tickets DXI-9249, DXI-9438).

1.14.1.6. Supported Browser Microsoft Edge Chromium

- The Identity Web applications Web Center, Web Admin, Server Admin, Business User Interface, and the Approvals App now support Microsoft Edge Chromium.

1.14.2. Bug Fixes

1.14.2.1. Services

- Using "is present" for binary attributes like jpegPhoto in Consistency rule filters are now handled correctly in event-based maintenance workflows. In older versions this could lead to ClassCastExceptions (Ticket DXI-9151).
- Multithreading problems in Java-based server in the area of event policies. Event policies were ignored sometimes. Deadlocks could occur (Tickets DXI-9156, DXI-9232, DXI-9300, DXI-9138).
- Performance improvements in privilege resolution have been implemented: When evaluating the matching groups of a permission (and role parameters apply) now a single LDAP search is executed (Ticket DXI-8976).
- Filter conditions like owner=<ownerdn> could lead to NullPointerExceptions in older versions. It occurred when a multi-valued ObjectReference property was used. If this property (owner in the sample) contained a broken link a NullPointerException was thrown. Now such cases are treated as "not equal" (Ticket DXI-8567).
- Too many modifications were generated for "dxrOptions" of an account even if there were no changes in the attribute values (Ticket DXI-9256).
- Renaming of an object resulted in a wrong entry change event message (listing the old RDN) (Ticket DXI-9262).
- Avoid NullPointerExceptions in master mechanism. Problem occurred when you have a multi-valued master and the mastered property is a multi-valued StorageObject. If one of the StorageObject references (at the master) were broken the exception occurred. Now in such cases an info message is logged. Example:

  INF(SVC103): Fri Nov 6 09:21:07.153 2020: Broken link: object: cn=TestUser,dc=Test,cn=Users,cn=My-Company master: cn=xx,cn=Custom,cn=BusinessObjects,cn=My-Company index: 0 Attname(master): dxrCategoryLink Attname: dxrproject

(Ticket DXI-9432).

- CopyPrivileges method of SvcUser now also checks the Access Policies for Role Parameter values. Checking is strict. If not all parameter values of one assignment are allowed the complete assignment is not copied. This also affects the Web Center "copy Privileges" functionality (Ticket DXI-9431).

1.14.2.2. Join Engine

- Synchronization in a cross-membership scenario didn’t work properly (Ticket DXI-9228).
- The Validation workflow sometimes terminated if there was a problem when synchronizing an object without trying to synchronize at least all the other objects (Ticket DXI-9251).
- If a NONE operation had been generated and the object doesn’t exist in the TS then no search for that object is done when synchronizing back to the Identity Store. Furthermore, the PostMapping for a Notes synchronizing was corrected so there is no

NullPointerException while logging the Identifier of the mapped entry (Tickets DXI-9286, DXI-9386).

1.14.2.3. Web Center

- Don’t display attribute values from modification requests that haven’t yet been approved in the user list (Ticket DXI-9258).
- Assigning or de-assigning groups occasionally failed since assignment properties were set at the group instead of at the assignment (Ticket DXI-9246).
- Form fields of type Date are no longer initialized with the current date (Ticket DXI-9353).
- Display correct proposal lists for input fields on enter attributes forms of create workflows (Ticket DXI-9368).
- The list of finished activities on a workflow details page shows the approval results and, optionally, the cancelled activities (Ticket DXI-9381).
- Refresh the proposal list for a role parameter value each time an assignment operation is started (Ticket DXI-9311).
- Web Center supports filtering by attribute dxrOptions (Ticket DXI-9434).
- Values of order attributes with operation type "replace" are correctly displayed on modification approval pages (Ticket DXI-9463).

1.14.2.4. Java-based Server

- A schedule for a Java workflow started too early if schedules were synchronized shortly before the workflow should have started (Tickets DXI-9051, DXI-9209).
- Dead Letter Queue entries with error code 3 and WF STATE=SUCCEDDED: Now a differently annotation is given - especially the workflow name/ID is given and if available the dn of a monitor entry (Tickets DXI-8825, DXI-9129, DXI-9358).
- Component workflow status writer now can do a re-connect to the connectivity or provisioning store (Tickets DXI-9289, DXI-9356, DXI-9355).
- WhenApplicable definition for workflows accepts now also <present .../> sub-elements without leading "dsml:" namespace prefix (Ticket DXI-9322).
- Sporadically the monitor entries of a realtime workflow were missing (Ticket DXI-9227).
- TS-specific adaptor sends finally failed requests to Dead Letter Queue, handles failures on activity start as temporary and detects more temporary failures of connectors (Ticket DXI-9247).
- TS-specific adaptor didn’t retry when connector could not bind; 2nd and further retries were redelivered immediately. Now they are delayed according the configured retry wait time of the activity (Ticket DXI-9247).
- The synchronization handling of active workflow definition lists was improved regarding "Load IdS-J Configuration" (Tickets DXI-9321, DXI-9297).
- Internally, there was an unexpected error related to operations on an audit channel that resulted in an infinite wait for accessing an object. Now the waiting time is set to a maximum of 5 minutes (Ticket DXI-9366).

- In batch files runServer.bat/.sh to start a Java-based server, SSL parameters were separated to individual options (Ticket DXI-9359).
- The internal component ResultListener was hanging indefinitely because it could not write events to the Dead Letter Queue (DLQ). Now this is limited to wait just for a certain time. In that case, the event is probably not written to the DLQ. Warning IDSJ177 is written to indicate this issue (Ticket DXI-9383).

1.14.2.5. C++-based Server

- The PIDs of a running agent are written as informal message into the server log file; if at the end of a workflow a file cannot be copied from work to status area a Windows batch script (DXIRunCommand.bat) is called that can be used to execute any tools to analyze the error situation more deeply (Ticket DXI-9233).
- In some cases, the watchdog executable of the C++-based server did not correctly encrypted a given cleartext password in the dxmmsssvr.ini file (Ticket DXI-9362).

1.14.2.6. Realtime Workflows

- Check consistency: LogHandlers were not removed from the root logger at the end of the workflow and caused an out-of-memory issue (Ticket DXI-9141).
- Event-based rules workflows: Userhooks did not work – a ClassNotFoundException was thrown (Tickets DXI-8981, DXI-9371).

1.14.2.7. Request Workflows

- In the ParticipantContext now a SvcSession is available (Ticket DXI-9320).
- The default locale for replacing a nationalized message string is "en" in case a user has no "preferredLanguage" set (Ticket DXI-9159).
- Usage of class BasicJob for customer implementations of request workflow activities resulted in "ClassNotFoundException" (Ticket DXI-8875).
- In Web Center the next "people" activity didn’t show up in time for complex request workflow with combinations of "people" , "join" and "automatic" activities (Ticket DXI-9442).

1.14.2.8. Identity Manager

- Provisioning search panel. If you change the "Search Base" to a non-existing value and start the search the error occurred. Due to an internal NullPointerException the "Search" button was unusable afterwards . Now an error box with "invalid search base!" pops up. You can correct the search base and search again (Ticket DXI-9224).
- Refresh did not refresh (parse again the xml content) of request workflow activities, escalations. For example, the timeout for an escalation changed by another application was not visible after a refresh. Now the XML content attribute is parsed again after the refresh and the changes are now visible after refresh (Ticket DXI-9416).
- If you create an Object Description at the "object descriptions" folder of a Target System (via right click and selecting New → "XML description") older Identity versions produced an object with dxrType=XML which was wrong. Now the correct value ODML is created

(Ticket DXI-8681).

- Moving Connected Directories or Java/TCL Workflow in Identity Manager(Connectivity View) could result in broken links in CDIcons and WFLines in a scenario. Now the links are adjusted correctly (Ticket DXI-9334).
- Creating realtime channel objects in Identity Manger via "new Channel" created channels with a not hidden "Content (resolved)" property page which causes parsing and resolving of the xml content even if design mode is switched off. Now as default resolvevar is hidden via dxmmgrlayout property, this avoids xml parsing if design mode is off (Ticket DXI-9259).

1.14.2.9. Business User Interface

- Fixed task name (truncate it) when task name is very long. Fixed phone number format when format number is not in "standard" format (Ticket DXI-9377).

1.14.2.10. REST Services

- Don't read member accounts of a group unless explicitly requested (Tickets DXI-9332, DXI-9484).
- Search operations use the default search base from the resource configuration (Ticket DXI-9437).
- Access to the REST Services failed after server reboot (Ticket DXI-9548).

1.14.2.11. Office 365 Connector

- Userhook "postUpdate" - Error message now returns more details (Ticket DXI-9255).
- Error in mapping of userPrincipalName: A hyphen is removed from the e-mail address, e.g. from
  JOIN137 userPrincipalName: aaron.schmid1@stud.bms-zuerich.ch. to
  JOIN137 userPrincipalName: aaron.schmid1@stud.bmszuerich.ch
  (Ticket DXI-9278).
- Validation of accounts does not start or takes a long time - since no filtering was supported at that time the log messages were extended to show progress (Ticket DXI-9257).

1.14.2.12. Identity Domain Connector

- The connector now retries to gain the user lock, if the first attempt failed (Tickets DXI-9303, DXI-9307, DXI-9308).
- The connector is now deployed to IdS-J server's confdb/common/lib folder rather than to confdb/job/framework/lib folder (Ticket DXI-9352).

1.14.2.13. Connector

- LDAP Connector now supports case sensitive renaming. To activate the feature, you must provide the operational attribute caseExactRDNComparison.

Here a sample request (ou=RedFlag → ou=Redflag):

```
    <spml:modifyRequest requestID="mod-2">
    <spml:identifier
        type = "urn:oasis:names:tc:SPML:1:0#DN">
        <spml:id>ou=Redflag,cn=Custom,cn=BusinessObjects,cn=My-
Company</spml:id>
    </spml:identifier>
    <spml:operationalAttributes>
        <spml:attr name="dxrPrimaryKeyOld">
            <dsml:value type="string"
>ou=RedFlag,cn=Custom,cn=BusinessObjects,cn=My-Company</dsml:value>
        </spml:attr>
        <spml:attr name="caseExactRDNComparison">
            <dsml:value type="string">true</dsml:value>
        </spml:attr>
    </spml:operationalAttributes>
    <spml:modifications>
        <spml:modification name="description" operation="replace">
               <dsml:value>erster modify</dsml:value>
            </spml:modification>
    </spml:modifications>
   </spml:modifyRequest>
```

To get this into the workflow you can use the "Op. Mapping" tab of your channel.

Specify here:

```
<?xml version="1.0" encoding="UTF-8"?>
<mappingDefinition>
    <operationalAttrMapping mappingType="constant"
name="caseExactRDNComparison">
        <value>true</value>
    </operationalAttrMapping>
</mappingDefinition>
```

(Ticket DXI-9241).

1.14.2.14. JDBC Connector

- Now the connector accepts numerical column names (Ticket DXI-9318).

1.14.2.15. JMS Audit Listener

- Prevent ActiveMQ inactivityMonitor thread for each connection attempt.
- Duplicate XML-Headers were written in audit messages (Ticket DXI-9282).

1.14.2.16. Agents

- Service agent: Consistency Check Workflow sometimes ended with ERROR due to some NullPointerException (NPE) when SequentialReadPage function got NoSuchElementException. The NPE is avoided now in SequentialReadPaged(nextElement) and NoSuchElementException is handled in callers (continue with next element) (Ticket DXI-9230).
- Metacp stand-alone environment: The keystore password in the file INST_PATH\ssl\password.properties was in cleartext, that was not expected. Now it will be encrypted. In this case only the keystore password is relevant other passwords are not encrypted (Ticket DXI-9146).

1.14.2.17. Certification Campaign

- Certification campaign controller: Apply Changes actions are not executed when all certifications are certified, but campaign end date is not reached.
- Certification campaign service: Each thread (for create or apply changes) uses an individual session.
- Certification campaign service: Extended logger output for saving changes actions.
- Certification campaign service: Session used for saving changes is always in interactive mode set to false.

1.14.2.18. Miscellaneous

- Java Mapping compiling was restricted up to Java version level 7 (Ticket DXI-9243).
- Patch tool (Windows only): The HOMEDIR and CD variables (in patch.bat) are compared case insensitive; otherwise patch installation terminates with error (Ticket DXI-9347).
- Patch tool: The "Directory administrator" fields are now editable (which is useful in case the data in "configuration.ini" is not correct) (Ticket DXI-9275).
- Configuration Wizard: Fixed issue with initial configuration of the ActiveMQ message broker after the 8.9-SP1 installation (Tickets DXI-9346, DXI-9397, DXI-9404).
- 3rd party software: Update of Apache commons-codec to newest version 1.15 (Ticket DXI-9426).
- Service Management sample Web server: Delete role assignment without parameters failed because the given uid was passed to order factory. This results in an order that contains the uid as identifier which was not working. Now, if there are no parameters/start/EndDates in the SPML request, the role-dn is used as identifier for the order (Ticket DXI-9049).
- Updates in Salesforce workflow and ODs required.
- When generating a report based on Jasper technology, following exceptions might

occur, for example if sizelimit is exceeded for a list of associated entries like affected users of a permission: ServiceException cannot be cast to class java.util.List (Ticket DXI-9522).

1.14.2.19. Fixes already solved in 8.9 SP1

The following tickets were already solved with 8.9 SP1:

- Hanging threads in Java server were solved through classloading changes (Ticket DXI-9293).
- Fixed showing some negative values in Web Admin overview. This was fixed internally (Ticket DXI-9263).
- The Request Workflow Timeout Check checks only RUNNING workflow instances on startup. It ignores workflow instances that already have expired (Tickets DXI-8770, DXI-8793, DXI-8794, DXI-9111, DXI-9125, DXI-9126, DXI-9127).

1.14.2.20. Fixes already solved in 8.9 Release

The following ticket was already solved with 8.9 release:

- Sometimes the task list in Web Center's home page was empty or incomplete whereas the task list was ok when explicitly requesting it (Ticket DXI-8589).

1.15. DirX Identity V8.9 SP1

1.15.1. New Features

1.15.1.1. Business User Interface

The Business User Interface was extended by the following points:

- Supports single sign-on Kerberos authentication (Tickets DXI-8797, DXI-8747, DXI-8700).

The configuration file contains a new section for Kerberos authentication: "kerberosAuthServer" and a new entry in "authentication" section: "KERBEROS".

1.15.1.2. Identity REST Services

The Identity REST services were extended by the following points:

- Supports single sign-on Kerberos authentication (Tickets DXI-8797, DXI-8700).

The service package includes a documentation update for the REST API:

identintegration.pdf (extended chapter 6)

- The CORS-Filter (Cross-origin resource sharing) of the REST services has been activated. It rejects now by default cross-origin requests. This will for example be case if the Business User Interface is loaded from a different origin than the REST services (an origin includes protocol, host and port: <protocol>://<host>:<port>.) It is usually also the

case if the REST services are accessed via a proxy. You can configure accepted cross-origins in file WEB-INF/security.properties. To get detailed logging set the log level for package com.dirxcloud.dxi.rest.filter to FINE:

com.dirxcloud.dxi.rest.filter.level=FINE.

1.15.1.3. Support of Apache ActiveMQ 5.15.12

- Update to Apache ActiveMQ 5.15.12 – contains various bug fixes.

1.15.1.4. Office 365 Connector

The connector and the associated workflows were extended by the following points:

- The connector now uses the newer Microsoft Graph API.
- The Patch operation for REST API calls in the connector was fixed, the connected directory and workflow configuration was updated and adopted to the Graph API changes (Ticket DXI-8890).

The service package includes a documentation update for the Office 365 connector:

identOffice365.pdf

- The pagination has been implemented. The problem of only 100 objects that were synchronized was fixed (Tickets DXI-9105, DXI-8481).

Note that the Office 365 connector currently just accepts one filter expression with an equality match. No combinations with AND, OR, and NOT. So, you can either use a filter as part of the join definition in the Join tab of the account/member channel or a filter expression in the Export tab of the account/member channel.

1.15.1.5. Sending mail in the Java-based server

- The SendMail workflow now explicitly sets the "Sent Date" in the mail header (Ticket DXI-8660).

1.15.1.6. Link checker

- Link Checker: The 2 log records

  a. ERR(LNC406): Role | link attribute | broken link (check)

  b. ERR(LNC410): 0 unreferenced map items detected: 0 unreferenced map items removed.

  are now logged as INFO logs. Both messages are logged independent from given log level like the start message

```
"INF(LNC201): Program 'Link Checker', Version
                    '2.0.0.0' of '2013-02-01' started ***."
```

New messages:

```
LNC211 is a header line for following broken links.
```

```
LNC212 is the information that map items were checked without
unreferenced items (Ticket DXI-9020).
```

1.15.2. Bug Fixes

1.15.2.1. Web Center

- Filter resolver supports LDAP attribute names containing underscores (Ticket DXI-8701).
- Web Center optionally resolves privileges after privilege changes (Ticket DXI-8791).
- Support for search base and filter for assigned roles fixed (Ticket DXI-8863).
- Expression evaluation for action parameter defaultFilter and for form field default value fixed (Ticket DXI-8973, DXI-8979).
- Allow usage of a customized date format (Tickets DXI-9009, DXI-9071).
- Web Center no longer displays an additional HDN role parameter value "0" (Ticket DXI-8699).
- Web Center correctly encodes username and password when binding to the Request Workflow service (Ticket DXI-8742).
- Filter for assigning privileges to business objects fixed (Ticket DXI-9110).

1.15.2.2. Services

- Attribute "dxrHistory" is no longer written in an additional LDAP modify operation (Ticket DXI-8617, DXI-8682).
- Attribute "dxrOptions(lock)" is no longer written in an additional LDAP modify operation (where possible) (Ticket DXI-8617).
- A ConcurrentModificationException in the Services was fixed (Ticket DXI-8731).
- Variable substitution in Request workflows e-mails didn't work properly for expressions with role parameter values. The old parameter value was not shown correctly (Ticket DXI-8895).

Please note that the old parameter value of course can only be shown correctly if the ApplyChanges activity of the workflow has not run yet.

- SoD check: Avoid ConcurrentModificationException during analyzing SoDs. Internal bug in Java map handling was fixed (Ticket DXI-8924).
- Extend lock component to check that object in memory is up to date (Tickets DXI-8887, DXI-8988, DXI-9017).
- In BO Inheritance pending SoD workflows were not checked correctly which led to

recurring start of SoD workflows. In older versions it was just checked for CREATE assignment workflows not for SoD assignment workflows (Ticket DXI-8955).

- When doing a SoD check it is checked if there are already running workflows for a potential SoD Violation. This check was extended. In older Identity versions running workflows that had just the SoD flag set in the WhenApplicable section were not included which led to multiple starts of SoD workflows (Ticket DXI-8955).
- When a "save" script catches an error, a stack trace is now shown in the logfile (Ticket DXI-8867).
- If the role structure is evaluated in the services the privilege DNs are logged if recursion level is greater than 16. (Support for analysis of loops in the role structure definition) (Ticket DXI-9029).
- Problems with SoD-Exceptions for Personas and Functional Users. NamingRule for cn extended for Personas and Functional Users (Ticket DXI-9058).
- Performance for reading the assignment parameters of a role with HDN parameters improved (Ticket DXI-9040).
- Access policy evaluation for assigning privileges to business objects fixed (Ticket DXI-9110).
- There were some performance problems when searching users in Web Center (Ticket DXI-9130).

1.15.2.3. Java-based Server

- The DeadLetterQueue adaptor stopped working when an event should be stored that is bigger than 32KB (message: IDSJADP004 Adaptor 'DeadLetterQueue' stopped unexpectedly). This caused the component ResultListener to hang which indirectly leaded to the fact that the counters for the adaptor queues were not updated. Also, If the DeadLetterQueue adaptor cannot process an event (e.g., SQL constraint violation) then the adaptor should not go into suspended mode. The size limit was increased to 64KB (Tickets DXI-8625, DXI-8251, DXI-8930, DXI-9006, DXI-8777).
- If an event contains an invalid character regarding the XML content then this event was still stored in the file repository and put to the DeadLetterQueue which caused to stop the DeadLetterQueue adaptor. Subsequently the counting of the adaptors was not done anymore. This resulted in a hanging Java server. Now the event is deleted from the file repository and not put to the DeadLetterQueue (Ticket DXI-8969)
- The Request Workflow Timeout Check checks only RUNNING workflow instances on startup. It ignores workflow instances that already have expired (Tickets DXI-8770, DXI-8793, DXI-8794, DXI-9111, DXI-9126, DXI-9127).
- Messages can now be excluded also in the StatisticsHandler (server.xml) not just for handlers regarding server*.txt and warnings*.txt log files (Ticket DXI-8908).
- Migration of the PSE key to a new one: Java server does not use strong encryption if there a 3 PSE keys and one fails (with the 2 provided PINs). Now it looks for the 2 highest serial numbers of the private keys and checks only these 2 (Ticket DXI-9000).
- Provisioning Message Dispatcher was unable to extract type, cluster and resource from a message topic after reloading workflows (Load IdS-J configuration) or when upper/lower case of the topic was different (Tickets DXI-9083, DXI-9002, DXI-9133).

- The scheduler ID of a schedule must be unique. If is not unique a warning is shown in the logfile, but still the last definition for that scheduler ID will be the only one that is executed (Ticket DXI-9101).
- The classloading in the server has been fixed (Tickets DXI-9124, DXI-9134).

1.15.2.4. C++-based Server

- The C++-based server crashed because the path length was greater than 255 characters. Now this is checked. Limit is MAX_PATH which is 260 (Ticket DXI-8624).
- The C++-based server fails during startup, logging this diagnostic error in log files and/or Event log:

  ```
  MSS2384: Encrypt/Decrypt error: Service not started. Reason:
  Function: dxc_start_encr_session, error: DXC_CERT_EXPIRED (at
  pwd).
  ```

  This has been fixed (Tickets DXI-9173, DXI-9175, DXI-9176, DXI-9177, DXI-9182, DXI-9189, DXI-9205).

1.15.2.5. Default Applications

- Sample references in "control.tcl" are no longer evaluated (as they might not work if new activities have been integrated in the workflow) (Ticket DXI-8714).

1.15.2.6. Identity Manager

- Function "LdapDN" didn’t escape a DN according to the rules of LDAP specification (Ticket DXI-8266).
- Setting the userPassword in the Dataview was not possible if the Connectivity Database was configured with SSL (Ticket DXI-9041).
- Typo in profile dxrViewGroup.xml. Therefore, the value of dxrIsInconsistent was not shown correctly in "Icons" column (Ticket DXI-9091).
- To avoid re-reading of User attributes (performance) when clicking on an "O" or "OU" tree node the loadAttributes was extended in the corresponding Object Descriptions (Ticket DXI-9092).

1.15.2.7. Identity REST Services

- Correctly handle date attribute values in filter when searching for users (Ticket DXI-9072).
- Display correct privilege assignment state (Ticket DXI-8692).
- Return an empty password policy if no policy is assigned to a user and no default policy is defined (Ticket DXI-8897).
- File password.properties is encrypted on application start-up (Ticket DXI-8939).

1.15.2.8. Provisioning Web Service

- SPMLv2 connector sends wrong Filter in search request (Tickets DXI-9090, DXI-9148).

1.15.2.9. Request Workflows

- The "WhenApplicable" section was not correctly evaluated for equality matching without attribute values being present (Ticket DXI-8594).
- Activity "ApplyChanges" terminated with state WAITINERROR, if ActiveMQ was not available and JMS messages could not be sent (to trigger Realtime workflows) by the service component. This was already fixed in 8.9, but two log messages were missing (Ticket DXI-8268).
- Activity "ApplyChanges" terminated with stated FAILED (instead of RETRY), if the LDAP lock for the user couldn’t be set (Ticket DXI-8814).
- Request workflows are only executed by IdS-J servers with active Request Workflow adaptors (Ticket DXI-8704).
- The coding was extended to ensure that the correct workflow name is in the thread context for the logging in the monitor area (Ticket DXI-8543).
- The Source provisioning workflows sporadically failed due to an EntryLockedException while reading the request workflow (Ticket DXI-8841).
- There was a NullPointerException while reading a request workflow from LDAP: Please note that this issue was fixed with DirX Identity 8.9 but was not documented in the release notes (Ticket DXI-8727).

1.15.2.10. Connectors / Agents

- History Agent: History values with invalid characters (e.g., control characters) were never deleted from LDAP due to an XML unmarshalling exception (Ticket DXI-8705).
- SPMLv2 Connector sends wrong filter in search request (Ticket DXI-8849).
- Identity Domain Connector: Several Fixes for session handling, binary attributes, move, delete, and assignments. Also, for direct password change and noSuchIdentifier in add; no superior node was created (Tickets DXI-8932, DXI-9069, DXI-8813); detailed logging of requests (Ticket DXI-9155).
- Identity Domain Connector: delete of single binary value failed (Ticket DXI-9084).
- Policy Agent: Improve logging of custom extensions for e.g., for consistency rules. Log is now done in one line and allows debug messages (Tickets DXI-8823, DXI-8862).
- SharePoint Connector: The userhook "preupdate" didn’t escape "(" and ")" in the LDAP filter; the userhook simply returned even in case of serious error; now it returns false and therefore the synchronization in the Join Engine stops for that object (Ticket DXI-8906).
- Notes Connector: The default behavior of the Notes connector (FullName is internally set by the Notes-API) can be changed by providing an operation attribute processFullName. If set to "true", the FullName is set by using the value from the SPML ADD or MODIFY request (Ticket DXI-8898).
- Notes Agent: The agent provided the "DBQuotaSizeLimit" in GB (rather than in MB) (Ticket DXI-8511).

- Policy Agent / Ruleprocessing: Logging was improved. If an error occurs during initialization of a rule, then additional to message RPC721 the stack trace is also logged (Ticket DXI-9012).
- SAP ECC UM Connector: Better support for SAP S/4HANA; internally in the connector each modify operation has its own retry due to SAP asynchronous processing. The retry is configurable (number and time interval) (Ticket DXI-8343).
- Service Agent: Deleting of outdated role assignment which caused SoD Exception(s). Remove the SoD Exception object also if privilegeLink is the only one that is stored at SoD Exception object in removeException. Problem occurred if SoD policy is based not on the role but on groups or permissions. In such cases the Service Agent could not remove the SoD Exception object from LDAP (Ticket DXI-8953).
- Office 365 Connector: The attributes accountEnabled and skuID are now correctly synchronized from the workflow.
  If in case an account is created but the membership group does not exist in Azure then the back synchronization of the account failed. The connector has been extended to accept one filter expression. Additionally, for fixing that you must manually define a second join definition in the account channel of an Office 365 target system. The default join definition should now be written as follows:

```
<joins xmlns:dsml="urn:oasis:names:tc:DSML:2:0:core"
xmlns:spml="urn:oasis:names:tc:SPML:1:0" >
    <join>
        <searchBase
type="urn:oasis:names:tc:SPML:1:0#GenericString">
            <spml:id>${source.dxrPrimaryKey}</spml:id>
        </searchBase>
    </join>
    <join>
        <filterExtension>
            <dsml:equalityMatch name="userPrincipalName">
                <dsml:value>
${source.dxmADsUserPrincipalName}</dsml:value>
            </dsml:equalityMatch>
        </filterExtension>
    </join>
</joins>
```

The Office 365 connector was extended to just accept one filter expression with an equality match. No AND, OR, and NOT is accepted. Therefore, you cannot combine that with a filter expression in the Export tab of the account channel (Tickets DXI-9011, DXI-9020, DXI-9105).

- JDBC Connector: Bugfix in JDBCMVFilter implementation. When no grace period is

defined an account is deleted immediately. In this case a delete request is sent to the connector. The Filter must handle to delete the memberships first. Therefore, the filter searches for remaining memberships and deletes all these memberships via the identifier from the search result. If there was no identifier in search result the following deletes were failing. This situation may occur if the membership table has no explicitly defined primary key (via Configuration or if it is an auto-generated key). To avoid such situation the Filter now builds the identifier on its own and puts this generated identifier (like: groupid=3+accid=H8753,table=member) to the delete membership request (Ticket DXI-9137).

1.15.2.11. Realtime Workflows

- Consistency Rules with filters on binary attributes like (objectClass= "dxrTargetSystemAccount" and dxrUserLink=* and jpegphoto=*) were not evaluated correctly inside event-based Maintenance workflows (Ticket DXI-8921).
- Sporadically a realtime workflow terminated with state "closed.completed.ERROR" (in the monitor view), but no real errors were shown in the logfile (Tickets DXI-8771, DXI-9085, DXI-9161, DXI-9229).

1.15.2.12. Join Engine

- The sort order DESCENDING was not correctly evaluated by the Join Engine (Ticket DXI-8748, DXI-9254).
- Join filter didn’t handle the "present" and "substrings" filter component (causing a NullPointerException in the connector or no matching channel was found when evaluating the channel’s Export filter) (Tickets DXI-8856, DXI-9129).
- The operational direct mappings for JOIN operations were only executed for the first incoming event (Ticket DXI-8914).
- The Monitor entry for a Cluster workflow shows now a message when switching to another TS (Ticket DXI-8936).
- For Realtime workflows the "Join" definition can be missing if not needed (e.g., when synchronization is only done in one direction no "Join" definition is needed in the source channel) (Ticket DXI-9028).
- Fixed a NullPointerException while generating an audit record (Ticket DXI-9065).
- In Cross-Membership scenario, a DELETE operation in the Connected System resulted in no updates on the way back to Identity Store (Ticket DXI-9132).

1.15.2.13. Certification Campaign

- The certification date now is always a date in the future (Tickets DXI-8726, DXI-8792).
- For old certification campaigns: The LDAP lock for the user could not be set due to wrong UID in the resource order of the request workflow (Ticket DXI-8800).

1.15.2.14. Metacp

- Sending of e-mails in metacp jobs requires new jar file "javax.activation.jar" instead of "activation.jar" in the classpath (Ticket DXI-9089).

1.15.2.15. Online Help

- Search in the online help jars was fixed. Regarding content the delivered help jars are the same as the ones from the 8.9 release. Note that an updated Integration Framework guide (identintegration.pdf) is delivered with this SP but the corresponding online help jar refers to 8.9 release (Tickets DXI-9014, DXI-9024).

1.15.2.16. Windows Password Listener

This service package includes an updated installation package for the Windows Password Listener.

- Windows Password Listener installer does not correctly create the service (Tickets DXI-8918, DXI-8965, DXI-9135).

The package is in "INST_PATH/patches/SP1/Man/WPL".

1.15.2.17. JMS Audit Log Handler

- DirX Identity JMS audit log handler sends audit records with duplicated xml prefix. The handler contains several changes:
- doesn’t send audit records with duplicated xml prefix any more
- doesn’t wait endlessly, if the broker is not willing to accept messages.
  Please note that this issue was fixed with DirX Identity 8.9 but was not documented in the release notes (Ticket DXI-8940).

1.15.2.18. Miscellaneous

- Configuration: Schema version "V8.6_3" must be handled during update installation (Ticket DXI-8704).
- Target System wizard: The Salesforce target system wizard component either hangs or crashes (Ticket DXI-8891).
- Suppress illegal reflective access warnings for GUI tools (Ticket DXI-9067).
- Password digest tool for ActiveMQ: The classpath in the scripts dximqdigest.bat/dximqdigest.sh were corrected (Ticket DXI-9075).
- Configurator: Silent Configuration: delete domainadmin.password=.. in IdS-J template file (.tpl) if deletePasswordsAfterSilentConfiguration=1 is set (Ticket DXI-9116).

1.16. DirX Identity V8.9

1.16.1. New Features

Main features of this version are:

- DirX Identity Business User Interface
  - Delegations. The Business User Interface allows creating, editing and modifying delegations.

    - Requests. User can now edit participants list and cancel their own requests. Request types supported: roles, permissions, groups and profile changes.
    - Change Password. A team manager can reset the password for team members, and users can change their own password.
    - Improved performance in home page.
    - Change password on next login. The Business User Interface can enforce change password on next login for users
    - Improved Access Policy handling.
- DirX Identity REST Services: New requests to manage delegations, change passwords, listing and reading details of pending approval workflows and tickets, cancelling workflows and changing a workflow participant.
- Support of a new type of delegations in Business User Interface.
- Provisioning workflows for selected target systems can be assigned to dedicated Java-based servers; they run only on these servers. This helps to separate for example target systems with a slow API or with lot of traffic so that they do not block or slow down the provisioning of other systems. As a side effect, all the logs for one such system can be on one server and are not distributed any more. For this purpose, new JMS listeners (aka adapters) have been introduced. They are created and started automatically for each target system with separate provisioning. These adapters do not require an extra adapter repository: they process an event or run a scheduled workflow immediately and handle the next only when the previous one is finished. Scheduled workflows and real-time event handling are processed in parallel (Tickets SYQN7M, DXI-6662).
- SoD checks are now available for running requests (Ticket DXI-8616, PTVKC5).
- Salesforce extensions: Support of additional Salesforce objects: accounts, contacts, permission sets. Salesforce permission sets and profiles are synchronized to Identity Store only, but Salesforce accounts, contacts and users are synchronized in both directions. The new approach allows administration of Salesforce Community users.
- The dxrSecCostunitLink (“more CostUnits” in “Organization” tab of User) is now also evaluated for BO inheritance.So the privileges defined at the CostUnits referenced by”more CostUnits” are inherited to the user via BO inheritance (Ticket R8UJF1).
- Multi Selection was not implemented. But now you can configure the JnbReference Editor to remember the last selection. So, you do not need to browse again to the last selection wenn adding a new item. For more information see the documentation” Editor for Object References”: JnbReference: Parameter lastselection=true in the Customization Guide (Ticket DXI-8081).
- In Request Workflow and Request Activities, an expression can now be used in the following LDAP attributes: description” and “title”. The last attribute applies only for Request Activity (Ticket ROPPUB).
- Support of Windows Server 2019 (with Desktop Experience).
- Removal of the prefetch cache for agent-based Policy Execution/Privilege Resolution: The prefetch cache had to be disabled because the users could not be locked during resolution. This reduces overall performance.
  It can be compensated by running several of these workflows in parallel. By applying appropriate search filters, these workflows can process distinct user and privilege sets.

Of course, this requires appropriate hardware: 1 CPU per workflow.
We recommend using the workflows running in the Java-based server (User Resolution, Consistency Check, MarkAffectedUsers) instead of agent-based Policy Execution and Privilege Resolution.

- Web Admin: On the Dead Letter Queue detail page the action buttons “Process” and “Remove” have been added. So, these action buttons are now not only on the overview page available.
- Reports can now be generated using TIBCO Jaspersoft® technology, the same technology that is used in DirX Audit. This allows output formats such as PDF and Excel. The reports can be generated in the same way as the classic XSLT-based ones: from Web Center, Identity Manager and scheduled with the *ReportGeneration* workflow. For the development and design of these reports you can use the graphical tool Jaspersoft® Studio. The installation provides report samples out-of-the-box for users and certification campaigns. Note: this feature is currently experimental, a use case document is provided with this release and additional templates will be provided soon!

Detailed features of this version are:

1.16.1.1. DirX Identity Business User Interface

BUI has been extended:

- Integrated access policies

  Extended support access policies for all pages. The BUI administrator can handle rights to view pages, rights to create/modify/delete entries and rights to execute actions.

- Show actor / approver

  The BUI now presents details about running requests for current user and requests where the user is involved (e.g. as approver). The user can replace the participants for his own requests and can cancel his own requests.

- Requests

  New request types extended with support for profile changes requests.

- Customize user attributes

  Improved support for user attributes and custom attributes in profile attributes and all other pages (e.g. taks, access rights).

- Delegation

  The user can see the current delegations: “assigned to” and “assigned from”. With BUI is possible to create and modify delegations. Currently are supported two types of delegations: approve and grant. The BUI allows deleting you our delegations “assigned to”.

1.16.1.2. DirX Identity REST Services

REST Services have been extended:

- Create, read, update and delete delegations.
- List delegated delegations and assigned delegations.
- Read password policy and change password.
- Read another user's password policy and reset his password.
- Read details of a pending privilege.
- List pending profile changes and read details of a pending profile change.
- List pending initiated requests and read details of a pending initiated request.
- Count methods for various lists returning just the number of list items.
- Cancel request workflows and change a participant of request workflows.
- Managed team includes delegated teams.
- Localization of requests workflow data.

1.16.1.3. Delegations

- As of version V8.9, DirX Identity supports a new type of delegations which are easier to understand and to use than the old delegations. You can either continue to use the old delegations, or switch to the new ones, but you cannot use them both in parallel.
  The new delegations support only operation types grant and approve. They cannot be restricted to specific subsets of resources.
  The new delegations are supported by the Identity REST Services and can be managed in the Business User Interface, but not in Web Center.

1.16.1.4. Support of Java 11

- This version is running with Java SE 11. Note that the Identity installation does not offer any more to use an embedded Java JRE runtime. The Java environment has to be externally provided.

1.16.1.5. Support of Apache ActiveMQ 5.15.9

- Update to Apache ActiveMQ 5.15.9 – contains various bug fixes and security updates.

1.16.1.6. Support of openSSL v1.0.2r

- Metacp and the C++-based server now support openSSL v1.0.2r.

1.16.2. Bug Fixes

1.16.2.1. Java-based Server

- A deadlock situation in the server classloading was fixed (Ticket DXI-8606).
- An erroneously message (IDSJ060) was written. Now the message comes only on the

Java server, where the Request Activity Task Listener is running and which determines that the desired Resource Family is not activated (Ticket DXI-8372).

- Debug-Logging of User Lock has been improved so that the stack trace is no longer shown as a kind of exception (Tickets DXI-7950, DXI-8219).
- The Java scheduler sporadically didn't start workflows.Creating a JMX-enabled object caused an AccessControlException with results in a recursion to log this (Ticket DXI-8026).
- A memory leak was fixed: Publisher event connections were not all closed (Ticket DXI-8196).
- A call to abort a workflow via Web Admin resulted in a deadlock situation which affected also other worker threads (Ticket DXI-8069).
- Topic for scheduled CombinedWorkflows has changed so that the workflow no longer requires an active EntryChangeListener, but an active ProvisioningRequestListener (Ticket DXI-8179).
- Java workflows were not running via scheduler if the domain flag "Include domain into topic" is not set (Ticket 35141).
- Embedded Tomcat has been update to version 9.0.13 (Ticket DXI-8462).
- Setting log levels via Web Admin fixed (Ticket DXI-8360).
- The following error message should no longer appear when running a Process Internal Tickets workflow in the ids-j log:
  STG103 Detected problems while reading XML-formatted Object Descriptors (cause: Cannot connect to storage://DirXmetaRole/cn=Config.xml,cn=Object Descriptions,cn=Configuration,cn=HDW?content=dxrObjDesc&uid=uid-a43f445-62528c06-169b131735d-16e0) (Ticket DXI-8513).

1.16.2.2. Documentation

- Certification campaign. Documentation for Certification campaign user hooks was improved and extended. Certification campaign user hooks Java Doc API and samples are delivered with the installation DVD (Ticket DXI-8479).
- Certification campaign documentation was updated to present current limitations. Current implementation does not allow sub containers in Certification Campaigns container (Ticket DXI-8386).
- Documentation of "Approval on deassign" flag at Domain - RequestWorkflows tab was corrected (Ticket DXI-8427)

1.16.2.3. C++-based Server

- A crash caused by a schedule with Time interval null and ranges was fixed (Ticket DXI-8523).
- A crash caused by an erroneous configuration file entry that was tried to log was fixed (DXI-8586).

1.16.2.4. Request Workflows

- In HTML notification e-Mails a multi line reason for accepting/rejecting a privilege was shown in a single line. Now multiple lines are used (Ticket DXI-7893).
- ApplyChanges locks by mistake an organization object if that object is a subordinate object in the user tree (Ticket DXI-8563).
- Salutation in e-mail bodies of request workflow e-mails sporadically was wrong due to wrong evaluation of "if" statement (Ticket DXI-8150).
- Workflow context attributes can now be used in e-mail notifications, e. g. "${workflow.contextAttributes.requestreason}" (Ticket DXI-8146).
- After restart of IDS-J, the activities in RETRY mode are scheduled correctly (before they were started immediately) Furthermore "waitBeforeRetry" was internally handled as INTEGER value which resulted in a maximum value of 24,85 days (MAX_INT was reached). Now it's handled as LONG value without limitations (Ticket 35274).
- When no Uid is available in an order, the user object is not locked in ApplyChanges activity (Ticket DXI-8587).
- When starting of an attribute approval workflow failed with "no matching workflow found" internally the changeInfo was not cleared.In this error case it fails because the workflow that should match has a condition using the attribute value of the attribute to be approved.Once you run in this error all attemps afterwards also failed even you typed in a matching attribute value. With this fix the changeInfo is cleared correctly and the following attempts will use the actually changed attribute values for finding the matching workflow (Ticket DXI-8068).
- "ApplyChanges" terminated with state WAITINERROR, if ActiveMQ was not available and JMS messages could not be sent (to trigger Realtime workflows) by the service component (Ticket DXI-8268).
- Subject and Resource Orders were not correctly processed due to problems with conversion from internal JSON format (Ticket DXI-8367)

1.16.2.5. Realtime Workflows

- For combined workflows the following warning occured sometimes in ids-j log: *com.siemens.idm.server.resource.ldap.Resolve.getResolvedValue() can't find resVar DOMAIN.* Now this warning should no longer be shown for combined workflows (Ticket DXI-8447).
- Workflow Consistency CheckConsistency now evaluates the ConsistencyRule filter correctly (Ticket DXI-8539).
- A sync workflow in cross membership scenario doesn't update the membership if an attribute (e.g. "cn") is used as "Source for Referenced Property" (at the TargetSystem) (Ticket DXI-8281).
- AccountPasswordManager and RestartAccountPasswords workflows could not be activated via scheduler due to a missing resolution variable "topicSet" in their XML workflow definition (Ticket DXI-8538).
- Old certification campaign with roles with role parameters resulted in "Attribute or value already exists" because "dxrResourceLink" contains the same user DN several

times (Ticket DXI-8165).

- The channels were not processed in the correct sequence if there are several channels with same Export search base and filter (Ticket DXI-8077).
- Validation workflow (in a cross-membership scenario) failed because TS specific data was not read correctly (Ticket SMTN71).
- Additional attributes of the user are forwarded to the "SetPassword" workflow as identifier attributes, but new names are used: "_usercn", "_usergivenname", "_usermail" and "_usersn" (instead of "cn", "givenname", "mail" and "sn"). This should avoid collisions with account attributes with same attribute name, but different attribute value (Ticket DXI-8067).
- UserPasswordEventManager controller uses a configurable attribute (samAccountNameAttribute) to retrieve the account (default is still "dxrName"). Extension required in XML section of controller: <property name="samAccountNameAttribute" value="<your attribute name>"/> (Ticket DXI-8200).
- EventBased Maintenance Workflows: Fixed clear rule provider in open method to ensure it is re-instantiated with potentially changed rules root. Changed handling of provisionRulesRoot so that several workflows (persona or user) may have different values configured (Tickets DXI-8597, QNEIPO).
- Workflow Process Internal Ticket sometimes ended with errors caused by internal session handling. In logfile messages like “STG103 Detected problems while reading XML-formatted Object Descriptors (cause: Cannot connect to storage://DirXmetaRole/cn=Config.xml,cn=Object Descriptions,cn=Configuration,cn=<domain>?content=dxrObjDesc&uid=uid-a43f445-62528c06-169b131735d-16e0)” occurred. Session handling was fixed (Tickets DXI- 8513).
- Monitor entries for combined real time workflows were missing if the same sub-workflow is defined several times in the sequence definition (DXI-8425).

1.16.2.6. Web Center

- Role parameter properties DN, uid and dxrOptions are made available via the DirX Identity API (Ticket RV0OS3).
- Security issue due to improper expression language evaluation fixed (Ticket RWOII5).
- Web Center displays an error message if revoking a role with HDN parameters fails due to insufficient access rights (Ticket RXBJPB).
- Security issues due to improper expression language evaluation and missing request parameter validation fixed (Ticket SNPKM3).
- Web Center sets the correct re-approval dates when assigning users to a privilege (Ticket S0NKWT).
- Web Center supports more than one parent base node when creating entries (Tickets SC3LKG and DXI-8593).
- Web Center correctly evaluates the flag "Content read only" for approval activities within self registration workflows (Ticket DXI-8039).
- Web Center displays the role parameter default value when assigning users to a role

(Ticket DXI-8062).

- Access to the request workflow service works now after the authenticated user changed his password (Ticket DXI-8105).
- Web Center skips submit checks when a search button is pressed (Ticket DXI-8125).
- Web Center correctly displays the subscription status for users with special LDAP characters in their names (Ticket DXI-8135).
- The navigation history displays the property configured in the language resource file instead of just property $displayName (Ticket DXI-8136).
- A new application context parameter let's you define a different log4j.properties file per Web Center application. This allows to configure per-application log files for Log4j's RollingFileAppender (Ticket DXI-8152).
- After creation of a request workflow instance, Web Center waits until the first people activity is running (Ticket DXI-8180).
- Web Center displays the correct proposal list for employee types when cresting personas via request workflows (Ticket DXI-8202).
- Web Center suppresses a misleading error message when adding a user to a role while the user has role assignments awaiting re-approval which the authenticated user doesn't have the grant access right for (Ticket DXI-8240).
- Web Center displays the tooltip for checkboxes if a tooltip is defined for the corresponding form property (Ticket DXI-8254).
- Web Center takes a more flexible approach to find a matching object description for the form configuration for enter attributes activities of create workflows (Ticket DXI-8280).
- The context menu for the task list now includes the additional items changeParticipant, complete and acquire for the active item (Ticket DXI-8341).
- The Javascript code for navigation history no longer includes user passwords (Ticket DXI-8362).
- Web Center validates all user input to avoid JSP expression injection (Ticket DXI-8403).
- Expression evaluation for combobox options fixed (Ticket DXI-8404).
- Unexpected error message after searching for tasks is no longer displayed (Tickets DXI-8414 and DXI-8421).
- A security issue related to authentication questions has been fixed (Ticket DXI-8544).
- The evaluation of expressions including session-scoped variables for form property attributes has been fixed (Ticket DXI-8572).
- The customization of HTML and JSP text files for languages other than German and English has been simplified (Ticket DXI-8586).
- Web Center respects the list sizes defined in tiles definitions (Ticket DXI-8592).
- The confirmation button in the password expiration warning message box triggers the expected action (Ticket DXI-8601).
- Unassigning Privilege to User in webCenter. Is unassignable is now checked and accessibility to given role parameter values are checked. If no Roleparameter value is

provided and Role Assignment is not unassignable it is counted as error. In the Tomcat log you see traces like: 2019-03-25 13:41:03,088 ERROR [http-bio-8080-exec-6] util.PrivilegeToUsers - Unassigning user cn=HDNUser,o=HDNTest,cn=Users,cn=My-Company from privilege cn=OU AdminDN,cn=IAM,cn=Functional Roles,cn=RoleCatalogue,cn=My-Company failed java.lang.SecurityException: Not unassignable for user cn=DomainAdmin,cn=My-Company, remove privilege failed! If Roleparameter values are provided, as much as possible roleParameter Values are removed from the assignments. If assignments do not have the provided values or you have no access rights for these vaulues these values are ignored for the assignment (Ticket DXI-8323).

- When searching with objectcollections and requesting dynamiyc attributes like numSubordinates the used storage method getPartialObject does no longer take the object out of the cache. So now the numSubOrdinates value is always up to date. In former versions you might had trouble while creating groups recursively via WebCenter (new group beneath the formerly created group) (Ticket DXI-8571).
- Performance. When assigning or un-assigning privileges, Web Center does not check any more view policies; they are already checked before the privileges are presented to the user.User-group relations are resolved only once after the last assignment to a user (Ticket DXI-8231).

1.16.2.7. Services

- Campaigngenerator puts now the value of dxrUid attribute to the generated subject order. This enables the repair mechanism to search for the given subject uid if DN of subject has changed (Ticket DXI-8164).
- When using ObjectCollection for LDAP searches, the attributes numSubordinates, numAllSubordinates are no longer requested by default. Identity Manager appends these attributes to the list of requested attribtues. Requesting these attributes prevents LDAP caching (Tickets DXI-8476, DXI-8502, DXI-8545).
- Provisioning rule filters are stored escaped in LDAP except the time constructs. Asterisks * in conditions are stored as *. This means it is used as wildcard. If you want to check for an asterisk use \2a (use the LDAP filter window) (Ticket RJYNS3).
- PolicyRules filter is stored escaped in LDAP except "time expression" is unescaped. So now you cna define in the fileter editor something like a(b)c as value for a condition ant it is internally stored as a\28b\29c (Tickets DXI-8198, TB 35180).
- There was a wrong operation link in consistency rule "ResolveInconsistentGroupMembership" (Ticket DXI-8361).
- When evaluating access policies, then the old attribute values (before modifying the subject) need to be evaluated when applying the access policy match rules (Ticket DXI-8095).
- A search for OUs resulted in a SIZE-LIMIT-EXCEEDED error even if there are other OUs that should be returned (where Access Policies don’t apply). Now search is done with paging (Ticket DXI-8085).
- There was a Nullpointer exception when storing a user object and that object is locked (Ticket SBTQ8L).

- 'Process Internal Tickets' workflow is now able to set/change the userpassword. The cryptographic support from GlobalContext is now passed to order context. In older versions "SVO543 Changing the password failed for DN=: com.siemens.dxm.password.PwdException: Error code 15; Illegal object state (com.siemens.dxm.password.PwdLDAPManager) " was reported (Ticket 35423).
- When scrambling passwords, by mistake the base-64 value contained CR/LF in its value (Ticket DXI-8548).
- If the propetry dxrRPValues() is not defined explicitly at the group, the corresponding Property description at t the User is used (with the name). After copying/cloning property descriptors for permission parameters to the group remove existing triggers in copy as we do not want to get them executed at the group. In older versions this could lead to problems if the dependent attribute isn't available at group (Ticket DXI-7922).
- Access policies could not be deleted (Ticket DXI-8540).
- Group assignments in Web Center didn't work if offlineResolution is set (Ticket 35308).
- When PolicyExecution leads to a user state change then the corresponding personas were resolved if no Change Event Policies are configured. This occured also if PolicyAgent was started with Provisioning.mode=AssignOnly. In some cases when also Prefetch Cache was used (userStorage.useUserCache=TRUE) an additional account was created. Now in such cases the offlineResolution flag is propagated to the affected personas. They are not resolved, just flagged with TBA. Subseqently privilegResolution runs will resolve user and Persona (Ticket DXI-8490).
- The audit records didn't hold correct "whyDetails" when a provisiong rule is evaluated and applied. The "whyDetails" simply didn't hold the rule that has been applied. The reason for this erroneous behavior was that attributes that hold a value for "subsetdelimiter" in the Object Description were not evaluated correctly (Ticket RXOKLY)
- No history record (dxrHistory) was written, if a new object is created and the "cn" is set using a Java script (as default value) (Ticket DXI-8449).
- The services no longer request the attributes "numSubordinates" and "numAllSubordinates" and therefore usage of the (DirX-)LDAP-Cache is optimized as these attributes are no longer updated all the time. But keep in mind, that these attributes are still used when running the DirX-Identity-Manager or Web Center (Ticket DXI-8457).

1.16.2.8. Business User Interface

- Access Policies for My Team pages was fixed and improved (Ticket DXI-8610).
- Updated custom style for latest version of Microsoft Edge (Ticket DXI-8509).

1.16.2.9. REST Services

- The Spring LDAP authentication provider configuration has been fixed in order to support domain names with spaces (Ticket DXI-8565).

1.16.2.10. Messaging

- Apache ActiveMQ was updated to version 5.15.9 (security reason) (Ticket DXI-8580).
- There as a NullPointerException in the Services when sending JMS messages (to start workflows) and ActiveMQ was not available (Ticket DXI-8423, DXI-8428).

1.16.2.11. Join Engine

- The Operational Attribute Mapping didn't handle "direct" mappings properly (Ticket DXI-8618).
- Simple expressions didn't work in the IdentifierAttributes section of an EXPORT search base or a JOIN search base (Ticket DXI-8053).
- The validation workflow by mistake deleted an entry at the very end (or marked as deleted) even if that entry could successfully be updated before. But after successful update the userhook "postUpdate" failed with an exception afterwards (Ticket 35290).
- There was a NullPointerException while generating the active participant of an audit record (Ticket DXI-7998).
- The "UserPasswwordEventManager" workflow evaluates a new configuration option at the domain "Ignore Missing User Link" that prevents password events from being processed for accounts in state IMPORTED (and therefore still have not been associated to a user). Therefore, such password events no longer end up in the (dead letter queue (Ticket DXI-8614).
- The automatic creation of superior nodes (in Validation Workflows) failed, if the same RDN value of missing superior node existed in another RDN, too (Ticket DXI-8669).

1.16.2.12. Provisioning Web Service

- Support custom object types for creation of users, roles, permission, locations, organizations, organizational units, contexts and cost units (Tickets DXI-8113 and DXI-8120).
- Skip access right check for user modification if a request to modify a user affects privilege assignments only (Ticket DXI-8272).
- Reference types (like dxrRoleLink) are considered case-insensitive (Ticket DXI-8272).
- Some performance improvements (Ticket DXI-8637).

1.16.2.13. Windows Password Listener

- UserPasswordEventManager controller uses a configurable attribute (samAccountNameAttribute) to retrieve the account (default is still "dxrName"). Extension required in XML section of controller: <property name="samAccountNameAttribute" value="<your attribute name>"/> (Ticket DXI-8200).

1.16.2.14. Identity Manager

- Links to Resource Families are now relocated if you move a Resource Family in the Identity Manager expert view (Ticket DXI-8412).

- Attribute changes generated in a "save" script are lost, if the naming attribute changes, too and an LDAP-Rename operation is executed first. This happens only when executed by the DirX-Identity Manager (Ticket DXI-8224).
- The following warnings in system.000.log should no longer appear: DBG(STG100): log4j:WARN No appenders could be found for logger (org.castor.core.util.AbstractProperties). DBG(STG100): log4j:WARN Please initialize the log4j system properly (Ticket DXI-8384).

1.16.2.15. Request Workflow Service

- There was a NullPointerException if the modifications were sent to the wrong activity using the RequestWorkflow-Service interface. (Modifications for an activity of type "Enter Attributes" need to be sent to the subactivity named "...-0", "...-1" etc.) (Ticket DXI-8211).
- APIs for reading/replacing Request workflows could be called with a Transaction Identifier but without Session. Then the session was created implicitly but returned to the session pool before the replace operation was executed in the commit operation. The result was missing attributes in the request workflow (Ticket DXI-8000).
- Abort of a request workflow in Web Center failed due to an internal problem in the request workflow services (Tickets DXI-8410, DXI-8420).
- When canceling a "people" activity, sometimes that activity is displayed in Web Center again. Now both the activity and the workflow terminate with state FAILED.ABORTED (Ticket DXI-7723).
- When reading the truststore for single sign-on from Web Center, ignore certificates with wrong key usage (Ticket DXI-8529).

1.16.2.16. Connectors

- SAP UM connector: With activated logging the connector writes now the trace files response.<thr-name>.xml and conn.<thr-name>.properties in the folder logs of the Java server. When running as agent then in the temporary folder of the user under which the process is running (Ticket DXI-8630).
- SAP UM connector: Validation was blocking with java.util.NoSuchElementException. If for domain is no correct DN given this error occurred (Ticket DXI-8186).
- LDAP connector: The LDAP connector now handles customer-specific binary attributes correctly as these ones are now configured in its XML definition (Ticket DXI-8206).
- JDBC connector: Performance issue with PostgreSQLOverJdbcOdbcDriver. PostgreSQLOverJdbcOdbcDriver now uses a “select * from <table> where false” in createSQLForMetadata. Old version without this where condition had poor performance for large tables (Ticket SOHOR7).
- SPML Connector: SPML v1 strict handling was fixed (Ticket DXI-8319).
- Notes Connector: The handling of Deny Groups (as part of a Notes server document) can be disabled by setting the new operational attribute “ignoreDenyGroups” to “true” (Ticket DXI-8351).

1.16.2.17. Default Workflows

- All options of the SAP UM connector are now visible in the port section of the default SAP UM workflows (Ticket SCNJOD).
- In TCL workflows you can now send e-mails using SSL (Ticket DXI-8550).
- The TCL script "common.tcl" used "jaxp.jar" in the class path when sending emails. That jar file is no longer installed and therefore has been dropped from the TCL script (Ticket DXI-8346).

1.16.2.18. Agents

- The Service Agent now behaves like in older versions when resolving the users matching the subject filter. The user in not locked for user resolution. No users are ignored for resolution because of their timestamp (Ticket DXI-8376, DXI-8433).
- When Service Agent wants to delete a user with direct group assignments in approval a ClassCastException occured:java.lang.ClassCastException: siemens.dxr.service.nodes.SvcOrderDisplayAss cannot be cast to siemens.dxr.service.nodes.SvcGroup Now this is handled correctly (Ticket SC1P9P).
- In sample files for the Remote AD agent a dummy password is now not given (Ticket DXI-8031).
- Policy Agent: "dxrTBA" was set only once by Policy Agent. This resulted in problems if several rules for the same user have to be applied and PrivilegeResolution running in parallel resets the "dxrTBA" flag in between. Now "dxrTBA" is set correctly (Ticket DXI-8329).
- Policy Agent writes "log.info(...)" as a WARNING message (instead of a LOG message) if that call is provided in a customer-specific jar file (e.g. in a Java Action implementation of a Consistency rule) (Ticket 35342).
- Policy Agent: When executing customer specific consistency rules INFO messages were by mistake shown as WARNING (Ticket DXI-8234).
- ADS Agent: Ads Agent needs to establish a connection using SSL when "use Encryption" is set in order to search objects in the "Deleted Objects" subtree (Ticket DXI-8493).
- ADS Agent needs to establish a connection using SSL when "use Encryption" is set in order to search objects in the "Deleted Objects" subtree (DXI-8659).

1.16.2.19. Installation and Configuration

- OpenSSL libraries were not installed if just base package and Notes / SAP HR agents are selected. Customer just wanted to use metacp (which is always installed) (Ticket DXI-8104).
- Upgrade installation for huge databases failed. The attribute indexing took a long time and caused a timeout on client side so that additional schema changes were not done and/or other attributes were not indexed (Ticket DXI-8159).
- Configuration: Strong name checking during Java Server step can be disabled by setting the following property in configuration.ini: IdS-J.relaxed_name_check=1 (Ticket DXI-7976).

1.16.2.20. Meta Controller

- Metacp is now able to send e-mails (notifications) to mail servers that need authentication with user name and password. Metacp can send e-mails now via SSL (Tickets P1BLNV, DXI-8650)
- Metacp crashed if an LDAP attribute name is longer than 64 bytes (Ticket DXI-7941.
- Metacp now supports TLS 1.3 (Ticket DXI-8549).
- Metacp crashed in "ats send" if the message broker could not be reached (Ticket DXI-8495).
- TCL workflows running in MERGE mode terminated unexpectedly (after an ADD operation) if releasing an internal handle failed (Ticket DXI-7980).
- Metacp crashed with access violation due to memory allocation problems (Ticket 35580).
- A new version of the NSS (Network Security Services) libraries (3.42) has been integrated. In the Mozilla LDAP component. SSL3.0 is no longer supported. As a new feature the mozilla ldap libraries support the version 1.3 of the TLS protocol. The accepted range of the TLS version versions is by default set to TLS1.0 up to TLS1.3. This range can be restricted by means of the environment variables DIRX_SET_TLS_LEVEL_MIN and DIRX_SET_TLS_LEVEL_MAX. The valid values for these are "1.0", "1.1", "1.2" and "1.3". The support of extended signature schemes - like RSA_PSS_RSAE_SHA384 - is disabled by default. It can be enabled by setting the environment variable DIRX_EXTENDED_SIG_SCHEME (which should be set before starting metacp). There are three cases:
  a) DIRX_EXTENDED_SIG_SCHEME is not set: The interface "SSL_SignatureSchemePrefSet()" is not called. This results in the same behavior of metacp prior to DirX-Identity V8.9.
  b) DIRX_EXTENDED_SIG_SCHEME=all (case sensitiv!): The interface "SSL_SignatureSchemePrefSet()" is called. All Signature Schemes supported by NSS 3.42 are supported. This includes ssl_sig_rsa_pkcs1_sha1 ssl_sig_rsa_pkcs1_sha256 ssl_sig_rsa_pkcs1_sha384 ssl_sig_rsa_pkcs1_sha512 ssl_sig_ecdsa_secp256r1_sha256 ssl_sig_ecdsa_secp384r1_sha384 ssl_sig_ecdsa_secp521r1_sha512 ssl_sig_rsa_pss_rsae_sha256; ssl_sig_rsa_pss_rsae_sha384; ssl_sig_rsa_pss_rsae_sha512 ssl_sig_ed25519 ssl_sig_ed448 ssl_sig_rsa_pss_pss_sha256 ssl_sig_rsa_pss_pss_sha384 ssl_sig_rsa_pss_pss_sha512 ssl_sig_dsa_sha1 ssl_sig_dsa_sha256 ssl_sig_dsa_sha384 ssl_sig_dsa_sha512 ssl_sig_ecdsa_sha1
  c) DIRX_EXTENDED_SIG_SCHEME=1: The interface "SSL_SignatureSchemePrefSet()" is called. But only the following Signature Scheme is supported: ssl_sig_rsa_pss_pss_sha384. You must set the environment variable to "all", if "metacp" needs to connect to different ldap servers that use different types of Keys (Ticket DXI-8189*)*.
- TCL entry handle is released before join handle is released (error in case of an ADD Operation) (Ticket DXI-8374).

1.16.2.21. APRC

- The APRC was changed so that also after a reboot the domain\username from the last login is shown in the corresponding input field (Ticket DXI-8123).

1.16.2.22. Certification Campaign

- Certification Workflow Problem: Fixed session handling: proper disposal and session load threshold (Ticket DXI-8649).
- A user can finish his certification campaign tasks even if one of the assignments to be certified has been removed since the campaign started (SBCPWY).

1.16.2.23. Miscellaneous

- Auditing: Invalid XML characters don’t result in an Exception when audit records need to be created (Ticket DXI-8375).
- The DirX Identity administrative points must hold the value CP (Context Prefix) in the LDAPattribute "dseType". Otherwise, the whole subtree will not be visible (Ticket DXI-8331).
- AuditJMSLogHandler: Component was fixed to suppress now consecutive warning logs after first one until it could successfully send a message to the broker (Ticket DXI-8330).
- In the setup of the Default Domain all entries now have a unique value for attribute “dxrUid” (Ticket DXI-8461).

1.16.3. Information About Discontinued Features

DirX Identity V8.9 does no longer support these features:

- Windows NT agent
- Dashboard Agent and Tcl-Workflows
- Soarian Clinicals Workflows
- SAP GRC in Request Workflows
- UNIX-PAM TCL Workflows

DirX Identity V8.9 is the last version that supports the following features:

- Internet Explorer 11 browser support in Business User Interface

1.17. DirX Identity V8.7 SP4

1.17.1. New Features

1.17.1.1. Business User Interface

- The Business User Interface supports now single sign-on via Kerberos – the Kerberos authentication is available in Business User Interface configuration file

There is a new value for “authentication” section in file config.json. To enable Kerberos authentication method, move value “KERBEROS” to first position in “authentication” section:

E.g.:

```
"KERBEROS",
            "BASIC",
            "X509"
        ]
```

Each authentication method has an individual server setting:

“BASIC” – “basicAuthServer” section

“X509” – “x509AuthServer” section

“KERBEROS” – “kerberosAuthServer” section

(Ticket DXI-8700).

- Extended support for customization with JavaScript hooks is now available.

1.17.1.2. Identity REST Services

- The REST Services support single sign-on via SPNEGO / Kerberos. The description to use SPNEGO / Kerberos is available on request (Ticket DXI-8700).

1.17.1.3. Support of Apache ActiveMQ 5.15.10

- Upgrade to Apache ActiveMQ 5.15.10 – contains various bug fixes.

1.17.1.4. Upgrade of embedded Tomcat

- Upgrade of embedded Tomcat in Java server to 8.5.46.

1.17.1.5. Java-based Server

- The "sendMail" workflow now explicitly sets the "Sent Date" in the mail header (Ticket DXI-8660)

1.17.2. Bug Fixes

1.17.2.1. Web Center

- Performance issue: When assigning or un-assigning privileges Web Center does not check any more view policies; they are already checked before the privileges are presented to the user. User-group relations are resolved only once after the last assignment to a user (Ticket DXI-8231).
- Security issue fixed: Javascript code for navigation history does no longer include user passwords (Ticket DXI-8362).
- Expression evaluation for combo box options fixed (Ticket DXI-8404).
- Unexpected error message after searching for tasks is no longer displayed (Tickets DXI-8414, DXI-8421).

- Javascript code for navigation history does no longer include user passwords. Validate input in order to avoid JSP expression injection (Tickets DXI-8362, DXI-8403).
- Security issue related to authentication questions fixed (Ticket DXI-8544).
- Web Center respects list size defined in tiles definition (Ticket DXI-8592).
- Web Center no longer displays an additional HDN role parameter value "0" (Ticket DXI-8699).
- Confirmation button in password expiration warning message box triggers expected action (Ticket DXI-8601).
- Filter resolver supports LDAP attribute names containing underscores (Ticket DXI-8701).
- Web Center correctly encodes user name and password when binding to the Request Workflow service (Ticket DXI-8742).
- Evaluation of expressions including session-scoped variables for form property attributes fixed (Ticket DXI-8572).
- Web Center optionally resolves privileges after privilege changes; see configuration parameter "offlineResolutionAfterPrivilegeChanges" in file webCenter.properties (Ticket DXI-8791).
- A user can finish his certification campaign tasks even if one of the assignments to be certified has been removed since the campaign started (Ticket DXI-7935).

1.17.2.2. Services

- The services no longer request the attributes "numSubordinates" and "numAllSubordinates" and therefore usage of the (DirX-)LDAP cache is optimized as these attributes are no longer updated all the time. But keep in mind, that these attributes are still used when running the DirX-Identity-Manager or Web Center (Tickets DXI-8476, DXI-8457, DXI-8502).
- When PolicyExecution leads to a user state change then the corresponding personas were resolved if no Change event policies are configured. This occurred also if Policy agent was started with Provisioning.mode=AssignOnly. In some cases when also Prefetch Cache was used (userStorage.useUserCache=TRUE) an additional account was created. Now in such cases the offlineResolution flag is propagated to the affected personas. They are not resolved, just flagged with TBA. Subsequent privilegResolution runs will resolve user and Persona (Ticket DXI-8490).
- "dxrHistory" is missing for new objects if "cn" is set to a default value (e.g., by Javascript) (Ticket DXI-8449).
- Access policies were not deleted as DELETE operation was not implemented (Ticket DXI-8540).
- ApplyChanges locks by mistake an organization object if that object is a subordinate object in the user tree (Ticket DXI-8563).
- When no Uid is available in an order the user object was not locked in ApplyChanges activity. In such situations now the attribute “dxrUid” of the user object is evaluated for setting the LDAP user lock (Ticket DXI-8587).
- "dxrHistory" is no longer written in an additional LDAP modify operation (Tickets DXI-

8617, DXI-8682, DXI-8683).

- Attribute "dxrOptions(lock)" is no longer written in an additional LDAP modify operation (where possible) (Ticket DXI-8617).
- Fixed a ConcurrentModificationException in the Services (Ticket DXI-8731).

1.17.2.3. Business User Interface

- Fixed and improved Access Policy handling for MyTeam pages (Ticket DXI-8610).
- Fix for login page for Microsoft Edge browser (Ticket DXI-8509).
- Fixed search issue when different privilege types are not displayed (Ticket DXI-8685).
- Assignment state is displayed correctly for account state (Ticket DXI-8692).
- Authorization header is no longer send when SSO is used (Ticket DXI-8747).
- Fixed typo in hook.js function name. Improved hook function calls (Ticket DXI-8735).

1.17.2.4. Request Workflows

- Subject and Resource Orders were not correctly processed due to problems with conversion from internal JSON format (Ticket DXI-8367).
- Salutation in e-mail bodies of request workflow e-mails sporadically was wrong due to wrong evaluation of "if" statement. Furthermore the "To" address was not evaluated correctly, too (Ticket DXI-8150).
- Cancel-, Suspend-, and Resume-Operation for a request workflow failed in Web Center due to a NullPointerException while reading the request workflow (Tickets DXI-8410, DXI-8694, DXI-8696, DXI-8770).
- Process Internal Tickets. If you assign privileges that require approval with a due date, tickets are created that refer to the corresponding request workflow. If the Approval Workflow just has an ApplyChange and no Approval step, due to timing condition, this results sometimes in inconstant tickets (the apply change could not find the corresponding ticket because ApplyChange started before ticket was saved to LDAP) (Ticket DXI-8535).
- Request workflows are only executed by Java servers with active Request Workflow adaptors (Ticket DXI-8704).
- Reading of a request workflow failed due to a NullPointerException (Ticket DXI-8727).
- Recertification fails when role DN changes. The campaign generator puts now the value of dxrUid attribute to the generated subject order. This enables the repair mechanism to search for the given subject uid if DN of subject has changed (Ticket DXI-8164).
- The "WhenApplicable" section was not correctly evaluated for equality matching without attribute values being present (Ticket DXI-8594).

1.17.2.5. Join Engine

- The Join Engine didn’t evaluate operational attribute mappings (for JOIN) correctly: "direct" mapping was not resolved as source attributes were not provided to the mappings (Ticket DXI-8618).

- Password events for accounts without "dxrUserLink" attribute (e.g., if account is still in state IMPORTED) are not stored in the DLQ and are ignored (Ticket DXI-8614).
- The automatic creation of superior nodes (in validation workflows) failed if the same RDN value of superior node existed in another RDN, too (Tickets DXI-8669, DXI-8729).

1.17.2.6. Java-based Server

- An erroneously message (IDSJ060) was written. Now the message comes only on the Java-based server, where the Request Activity Task Listener is running and which determines that the desired Resource Family is not activated (Ticket DXI-8372).
- For combined workflows the following warning occurred sometimes in the server log: 16.02.2019 10:11:17.685 [Main-S2] [ ] *** WARNING *** Called from com.siemens.idm.server.resource.ldap.Resolve.getResolvedValue() can’t find resVar DOMAIN.
  Now this warning should no longer be shown for combined workflows (Ticket DXI-8447).
- A deadlock situation in the server classloading was fixed (parallel loader capability) (Ticket DXI-8606).
- Hotfix prevents that the DLQ adaptor stops working (message: IDSJADP004 Adaptor 'DeadLetterQueue' stopped unexpectedly). This caused the internal ResultListener thread to hang which indirectly leaded to the fact that the outstanding responses counters were not updated (Ticket DXI-8625, DXI-8251).
- The Request Workflow Timeout Check checks only RUNNING workflow instances on startup. It ignores workflow instances that already have expired (Ticket DXI-8770, DXI-8793, DXI-8794).
- Workflow definition names are now internally handled with lower case names (Ticket DXI-8470).
- If the DeadLetterQueue adaptor cannot process an event (e.g., constraint violation) then the adaptor should not go into suspended mode to ensure that other events are processed furthermore (Ticket DXI-8777).
- The scheduler component has more logging to see the queue name the scheduler is using (Ticket DXI-8259).
- The outstanding responses counters in Web Admin overview for the ProvisioningRequestStartWorkflowListener and EntryChangeStartWorkflowListener have been fixed to show now correct values (Ticket DXI-8839).

1.17.2.7. C++-based Server

- Fixed crashing of server caused by a schedule with time interval null and ranges (Ticket DXI-8523).
- Server crashed while scanning an incomplete workflow definition – it tried to log a TCL code string with over 20.000 characters (Ticket DXI-8586).
- Server crashed because the path length was greater than 255 characters. Now this is checked. Limit is MAX_PATH which is 259 characters (Ticket DXI-8624).

1.17.2.8. Messaging

- "ApplyChanges" terminated with state WAITINERROR, if ActiveMQ was not available and JMS messages could not be sent (to trigger realtime workflows) by the service component (Ticket DXI-8268).
- There was a NullPointerException when sending messages and ActiveMQ was not available (Tickets DXI-8423, DXI-8542).

1.17.2.9. Configuration Data

- There was a wrong operation link in consistency rule "ResolveInconsistentGroupMembership" (Ticket DXI-8361).

1.17.2.10. Connectors

- Audit Connector: Invalid XML characters don’t result in an Exception anymore when audit records need to be created (Ticket DXI-8375).
- Notes Connector supports operational attribute "ignoreDenyGroups" to avoid access to the server document (for attribute "DenyAccess"). Furthermore, the connector is more stable and doesn’t terminate if an exception in one of the operations occurs (Ticket DXI-8351).
- SPML Connector: Fixed SPML v1 strict handling (Ticket DXI-8319).
- SAP UM ECC Connector/agent: With activated logging some trace files couldn’t be written due to parallel running threads (Ticket DXI-8630).

1.17.2.11. Agents

- Service Agent: The Service Agent now behaves like in older versions when resolving the users matching the subject filter. The user is not locked for user resolution. No users are ignored for resolution because of their timestamp (Tickets DXI-8376, DXI-8433).
- Policy Agent: "dxrTBA" is set only once. This results in problems if several rules for the same user must be applied and a Privilege Resolution is running in parallel which resets the "dxrTBA" flag in between (Ticket DXI-8329).
- Metacp: Support of a new Security library (NSS 3.40) has been integrated in order to support various signature schemes (Ticket DXI-8189).
- Metacp: "ats send" command crashes or return an error "Invalid bin-ID ..." if a message could not be sent to the message broker (when broker is unreachable) (Ticket DXI-8495).
- ADS Agent: Agent needs to establish a secure connection using SSL when "use Encryption" is set in order to search objects in the "Deleted Objects" subtree (Tickets DXI-8493, DXI-8659).
- History Agent: delete as many "dxrHistory" values as possible (with 1 modify operation - up to a PDU size of approximately 16MB) (Tickets DXI-8617, DXI-8617, DXI-8683).
- History Agent: History values with invalid characters (e.g., control characters) were never deleted from LDAP due to an XML unmarshalling exception (Ticket DXI-8705).

1.17.2.12. Realtime Workflows

- Monitor entries of scheduled Java-based workflows "Process Internal Tickets" and "CertificationCampaignController" now contain the correct value "scheduled" in the field "Initiator" (Tickets DXI-8513, DXI-8763).
- Monitor entries for combined realtime workflows were missing if the same sub-workflow is defined several times in the sequence definition (Ticket DXI-8425).
- If the UserResolutionController detects modified attributes that are mastered in Personas, UserFacets or Functional Users it does a resolution and propagates these attributes to affected Personas, UserFacets or Functional Users.

  If com.siemens.idm.jobs.ebr logging is set to all in such cases the following message appears in the Java-based server log:

  EBRDBG100 Mastered properties of Facet, Persona or Functional Users are affected do a resolution (Ticket DXI-8652).

- Default AD realtime provisioning workflows now create accounts with UserAccessControl value 512 for security reasons. This means a password is required. Ensure that a valid password is provided or adapt the UserAccessControl mapping (Ticket DXI-8745).
- A NullPointerException in the ConsistencyCheck workflow was fixed (Ticket DXI-8656).

1.17.2.13. Identity Manager

- When scrambling passwords, by mistake, the base-64 value contained CR/LF in its value (Ticket DXI-8548).

1.17.2.14. Identity REST service

- Display correct privilege assignment state (Ticket DXI-8692).

1.17.2.15. Default Applications

- TCL entry handle is released before join handle is released (error in case of an ADD Operation) (Ticket DXI-8374).
- There was an undefined TCL variable ‘errorCode’ that caused termination of the synchronization script. Exchange of common.tcl was missing in 8.7-SP3 for Linux only (Ticket DXI-8647).
- Sample references in "control.tcl" are no longer evaluated (as they might not work if new activities have been integrated in the workflow) (Ticket DXI-8714).

1.17.2.16. Documentation

- Approval on de-assign flag at Domain updated. An updated online help for Provisioning Administration is delivered (Ticket DXI-8427).
- The online help for the new ImportToIdentity workflow was missing. An updated online help for Application Development is delivered.

1.17.2.17. Miscellaneous

- The class SocketedJob has been extended to set for all root loggers setUseParentHandlers with true. That prevents that logging for all components is suddenly activated (Ticket DXI-8415).
- Web Admin: Setting log levels via Web Admin fixed (Ticket DXI-8360).
- SendMail in TCL workflow environment now supports mail connections via SSL using STARTTLS (Tickets P1BLNV, DXI-8550, DXI-8650).
- SPNEGO jars for Tomcat 8.5 and Tomcat 9 are delivered (Tickets SM4OY7, DXI-8574).
- Certification campaign workflow: Fixed session handling: proper disposal and session load threshold (Ticket DXI-8649).
- Old Certification campaign: The certification date now is always a date in the future (Tickets DXI-8726, DXI-8792).
- Old Certification campaign: For old certification campaigns the LDAP lock for the user could not be set due to wrong uid in the resource order of the request workflow (Ticket DXI-8800).
- Old Certification campaign: Recertification fails on multiple assignments with different role parameters (Ticket DXI-8165).

1.18. DirX Identity V8.7 SP3

1.18.1. New Features

1.18.1.1. Business User Interface

The Business User Interface was extended by the following points:

- Support for Access Polices for widgets (menus), entries and attributes.
- Support for dynamic forms in My Profile and Manage User Profile.
- Support for custom columns in all tables.
- Support for custom search in all tables.
- Support for custom sort in all tables.
- Support for color theme change and store in LDAP user object.
- Improved internationalization and localization support.
- Support for privileges filter.
- Updated to Angular 6.1.7 and Angular Material 6.4.1

The service package includes an update of the relevant manuals: DXI_BusinessUserInterfaceConfiguration.pdf and DXI_BusinessUserInterfaceGUI.pdf.

1.18.1.2. Identity REST Services

The Identity REST services were extended by the following points:

- Evaluation of attribute access rights.
- Support to create, read, update and delete domain objects.
- Support for compound attributes.
- Main configuration moved to JSON file resources.json.

The service package includes an update of the relevant manual: identintegration.pdf (chapter 6 is extended).

1.18.1.3. Support of Apache ActiveMQ 5.15.6

- Update to Apache ActiveMQ 5.15.6 – contains various bug fixes.

1.18.1.4. Support of openSSL v1.0.2p

- Metacp and the C++-based server now support openSSL v1.0.2p.

1.18.1.5. Support of VMware ESXi 6.5

- As a virtual machine infrastructure VMware ESXi 6.5 is now supported.

1.18.1.6. Realtime Workflows

- 2 new realtime workflows for importing users from an external LDAP to the Identity Store are provided.

a. Full Import of external LDAP Users

   The workflow is started from the DirX Identity Manager (either manually or by schedule) and performs either the initial load of users from an external LDAP directory or the complete resynchronization of the external LDAP directory. In the latter case, users may be deleted or marked as to-be-deleted in the Identity Store.

b. Import Users from external LDAP

   The workflow is normally started by event and imports a user (or updates a user or deletes a user or marks a user as to-be-deleted) depending on the incoming event and the existence of that user in the Identity Store.

   If the workflow is started by the DirX Identity Manager manually or triggered by the scheduler, then it performs a resynchronization of the external LDAP users (without deleting users or marking users as deleted).

The service package includes an update of the relevant manual: See chapter 5.1.8 of the identappldevgd.pdf (Application Development Guide).

1.18.1.7. Services

- A new Flag at the domain (Domain Object - Property Page RequestWorkflows) controls the behavior of starting Rule assigned privileges that must be approved. You can define if an Approval Workflow should be started or not. **Start Approval for Rule Assignments**

controls the behavior for assigning privileges by Rule; for example via the Policy Execution Workflow. If the privilege is subject of an approval, setting this flag to false suppresses the Approval Workflow (Ticket DXI-8151).

- The flag **Start Approval for BO inherited Assignments** is now visible at the domain (Domain Object - Property Page RequestWorkflows). For further information please use the context sensitive help.
- A new flag at the domain (Policies - Property Page) enables read/modify Access Polies where you can define access rights on attribute level for the BUI. **Enable attribute policies** - whether (checked) or not (unchecked) previously defined Business User Interface attribute policies (Access Policy - Attributes Read and Access Policy - Attributes Modify) are enabled. If enabled the Business User Interface just presents the readable attributes that the Access Policy - Attributes Read defines. Attributes that the Access Policy - Attributes Modify defines can be changed via the Business User Interface.

1.18.2. Bug Fixes

1.18.2.1. Services

- When evaluating access policies, then the old attribute values (before modifying the subject) need to be evaluated when applying the access policy match rules (Ticket DXI-8095).
- No stack trace is logged in "createLdapLock" and "releaseLdapLock" (Ticket DXI-8219).
- Attribute changes generated in a "save" script are lost, if the naming attribute changes, too and an LDAP rename operation is executed first. This happens only when executed by the DirX-Identity Manager (Ticket DXI-8224).

1.18.2.2. Web Center

- Skip form field validation in Web Center when a search button is pressed (Ticket DXI-8125).
- Show subscription status fails for users with special LDAP characters in their names (Ticket DXI-8135).
- Navigation history displays the property configured in the language resource file instead of just property “$displayName” (Ticket DXI-8136).
- Access to the request workflow service works now after the authenticated user changed his password (Ticket DXI-8105).
- After creation of a request workflow instance wait until a people activity is running (Ticket DXI-8180).
- Web Center suppresses a misleading error message when adding a user to a role while the user has role assignments awaiting re-approval which the authenticated user doesn’t have the grant access right for (Ticket DXI-8240).

1.18.2.3. Java-based Server

- Scheduler sporadically didn’t start workflows (Ticket SPFRH0).

- Creating a JMX-enabled object caused an AccessControlException with results in a recursion to log this (Ticket SPFRH0).
- In the Java server worker threads were hanging because a call to channel.addEOF() was hanging indefinitely - now there is a wait of maximum 5 minutes (Ticket DXI-8069).
- Problem with scheduling combined java workflow - version 8.7 SP1. Topic for scheduled CombinedWorkflows has changed so that the workflow no longer requires an active EntryChangeListener, but an active ProvisioningRequestListener (Ticket DXI-8179).

1.18.2.4. Join Engine

- UserPasswordEventManager workflow uses a configurable property (in his XML definition) to search the relevant account. Up so far it used "dxrName" (which is still the default, if the new property "samAccountNameAttribute" is not set.) (Ticket DXI-8200).
- Sync-Workflow in cross membership scenario doesn't update the membership if an attribute "cn" is used as "Source For Referenced Property" (Ticket DXI-8281).

1.18.2.5. Request Workflows

- There was a NullPointerException if the modifications were sent to the wrong activity using the Request Workflow service interface. (Modifications for an activity of type "Enter Attributes" need to be sent to the sub-activity named "...-0", "...-1" etc.) (Ticket DXI-8211).
- APIs for reading/replacing Request Workflows could be called with a Transaction Identifier but without Session. Then the session was created implicitly but returned to the Session pool before the replace operation was executed in the Commit operation. The result was missing attributes in the request workflow (Ticket SCWJWM).
- Workflow context attributes can now be used in e-mail notifications, e.g. "${workflow.contextAttributes.requestreason}" (Ticket DXI-8146).

1.18.2.6. Provisioning Web Services

- The provisioning web service no longer requires the modify access right when assigning privileges to a user (Ticket DXI-8272).
- The provisioning web service supports custom object types when creating users, roles, permission, locations, organizations, organizational units, contexts and cost units (Ticket DXI-8120).
- Reference types (like dxrRoleLink) are case-insensitive (Ticket DXI-8272).

1.18.2.7. Configuration Wizard

- Configuration of more than one Java Server: Sn (n>1) fails with weak checking (Ticket SCCMDQ).

1.18.2.8. Schema

- Setting of attribute index fails due to time out problem (Ticket DXI-8159).
- The DirX Identity administrative points must hold the value CP (Context Prefix) in the

LDAPattribute "dseType". Otherwise the whole subtree will not be visible (Ticket DXI-8331).

1.18.2.9. Default Applications

- TCL workflow terminates unexpectedly due to unknown global variable "errorCode" in procedure "handleSourceEntry" (Tickets DXI-8129, DXI-8321)

1.18.2.10. Metacp

- Using command "ats initialize -bindid ... -server ..." no longer causes the meta controller to crash.

1.18.2.11. LDAP connector

- The LDAP connector now handles customer specific binary attributes correctly as these ones are now configured in its XML definition (Ticket DXI-8206).

In the “Connection” section of the XML connector definition, the following property can be set:

binaryattributes - (optional); using this property a customer specific list of LDAP attribute types can be defined

Put that element after the definition of single valued properties. A sample definition looks as follows:

```
<connector className="siemens.dxm.connector.ldap.LdapConnector"
name="IdentityDomain"
role="connector">
<connection password="{SCRAMBLED}aG5WPw=="
port="389"
server="localhost"
ssl="FALSE"
type="LDAP"
user="cn=DomainAdmin,cn=My-Company">
    <mvproperty name=”binartyattributes>
        <value>AttributeType-1</value>
        <value>AttributeType-2</value>
        …
        <value>AttributeType-n</value>
    </mvproperty>
</connection>
</connector>
```

1.19. DirX Identity V8.7 SP2

1.19.1. New Features

None.

1.19.2. Bug Fixes

1.19.2.1. Java-based Server

- The realtime workflow monitor logging caused a memory leak in the Java-based server.
- There was a NullPointerException in Full Check when reading of a workflow failed (when activating the workflow with state RESOLVED at startup of Java server).

1.19.2.2. Services

- Editing permission parameters at a group failed sometimes. If the property dxrRPValues(<permissionparameter>) is not defined explicitly at the group, the corresponding Property description at the User is used (with the name <permissionparameter>). In older versions also the defined dependencies for this attribute were used implicitly (definition from user OD).This could lead to problems if the dependent attribute isn't available at group. Now such dependencies are ignored (Ticket SAZOID).
- When starting of an attribute approval workflow failed with "no matching workflow found" internally the changeInfo was not cleared. In this error case it fails because the workflow that should match has a condition using the attribute value of the attribute to be approved. Once you run in this error all attempts afterwards also failed even you typed in a matching attribute value. With this fix the changeInfo is cleared correctly and the following attempts will use the actually changed attribute values for finding the matching workflow (Ticket DXI-8068).
- Search for OUs resulted in a SIZE-LIMIT-EXCEEDED error even if there were other OUs that should be returned (where Access Policies don't apply)(Ticket DXI-8085).

1.19.2.3. Installation/ Configuration

- There was a TCL error while removing a user policy with spaces in the DN (Ticket DXI-8073).
- Strong name checking during Java Server step can be disabled by setting the following property in configuration.ini:

  IdS-J.relaxed_name_check=1

  (Ticket SCCMDQ).

- Same jar files coming from different versions were released in the INST_PATH\lib\java\ext folder (Ticket DXI-8075).

1.19.2.4. Join Engine

- The channels were not processed in the correct sequence, if there are more channels with same Export search base and filter (Ticket DXI-8077).
- Simple expressions didn't work in the IdentifierAttributes section of an EXPORT search base or a JOIN search base (Ticket DXI-8053).

1.19.2.5. Web Center

- Display role parameter default value when assigning users to a role (Ticket DXI-8062).
- Display certification tasks for custom user types (Ticket DXI-8144).

1.19.2.6. Business User Interface

- Name sorting is missing when requesting a new privilege.
- Invalid field assignment to endDate for read only assigned privileges. Change to correct assignment: startDate.

1.19.2.7. Password Workflows

- Avoid collisions between account attributes and user attributes: "_usercn", "_usergivenname", "_usermail" and "_usersn" (instead of "cn", "givenname", "mail" and "sn") (Ticket DXI-8067).

1.19.2.8. Request Workflows

- A signed audit record now complies with the correct format and contains a section <activeParticipant> representing the subject of the action (Ticket DXI-8051).

1.19.2.9. Message Broker

- Using the dximqdigest batch script failed because a wrong jar file was on the classpath (Ticket DXI-8115).

1.19.2.10. JMS Audit Handler

- The new plugin contains fixes so that an encrypted password for the Audit message broker can be used. In case a record could temporarily not been sent to the Audit message broker the record was stored in a wrong format. This has also been fixed.

1.20. DirX Identity V8.7 SP1

1.20.1. New Features

1.20.1.1. SP1: Business User Interface

The Business User Interface was extended by the following points:

- Widget "My Team" to manage the members of a team. It is possible now to edit

assignments and the profile of the team members and to request new privileges for the team members.

- Handling of access rights and requests now include permissions and groups not just roles.
- Support of type hierarchical DN for role parameters.
- Logon authentication with PKI card.
- Support of Internet Explorer 11.

The service package includes an update of the relevant manuals: DXI_BusinessUserInterfaceConfiguration.pdf and DXI_BusinessUserInterfaceGUI.pdf.

1.20.1.2. Identity REST Services

- New REST service interfaces to read, search and modify users, assign privileges to users, and get the users managed by the authenticated user.
- Log configuration revised.
- The service package includes an update of the relevant manual: identintegration.pdf (chapter 6 is new).

1.20.1.3. Support of Apache ActiveMQ 5.15.3

- Update to Apache ActiveMQ 5.15.3 – contains various bug fixes.

1.20.1.4. Support of openSSL v1.0.2n

- Metacp and the C++-based server now support openSSL v1.0.2n.

1.20.1.5. C++-based Server

- All JMS messages are now be sent with a defined JMSExpiration time.

1.20.2. Bug Fixes

1.20.2.1. Web Center

- Security issue due to improper expression language evaluation fixed (Ticket RWOII5).
- Security issues due to improper expression language evaluation and missing request parameter validation fixed (Ticket SNPKM3).
- Display an error message if revoking a role with HDN parameters fails due to insufficient access rights (Ticket RXBJPB).
- Set correct re-approval dates when assigning users to a privilege (Ticket S0NKWT).

1.20.2.2. Web Center API

- Role parameter properties DN, uid and dxrOptions made available via Web Center API (Ticket RV0OS3).

1.20.2.3. Services

- When Web Center is running with service layer in offline mode (file: <inst_path>/web/webCenter-<domain>/WEB-INF/webCenter.properties; property: offlineResolution = false) then group assignments can no longer be done. Groups can't be selected and moved down to the "Assigned groups" field (Ticket RXIK4L).
- The workflow "Process Internal Tickets" cannot set any password (Error code 15; Illegal object state) (Ticket SYWIYK).
- The debug logging of the User Lock feature has been improved so that the stack trace is no longer shown as a kind of exception (Ticket SBPLCU).

1.20.2.4. Java-based Server

- Workflowengine thread: In the cleanup procedure of the Workflow engine that is called at the end of a workflow run, an infinitely long waiting call happened sporadically. This is now limited to 10 minutes. In this case, a warning with message number IDSJ698 is logged. The engine does not hang infinitely anymore (Ticket SBQKOE).
- Java workflows were not running via scheduler if the domain flag "Include domain into topic" is not set (Ticket RJGORJ).

1.20.2.5. Provisioning Web Services

- ClassNotFoundError occurred in the Provisioning servlet in password requests. With updated XML security and serializer jar files this does not happen anymore.

1.20.2.6. Request Workflows

- The value of "waitBeforeRetry" is now evaluated correctly as LONG value. Before this fix the maximum value was reached after 25 days (Ticket RWXLY0).
- CalculateRisk Request Activity is now also aware of SoD violations. In older versions SoD violations were not counted for calculation the new risk score.
- When canceling a "people" activity, sometimes that activity is displayed in Web Center again. Now both the activity and the workflow terminate with state FAILED.ABORTED (Ticket RHWIXD).
- In HTML notification emails a multiline reason for accepting/rejecting a privilege was shown in a single line. Now multiple lines are used (Ticket SYIQKR).
- NullPointerException happened in FullCheck.activateResolvedWorkflow if a lock for a request workflow could not be set (as "dxrUID" and "cn" are different in former versions). Now the request workflow is never read by its dxrUID. This was already fixed with hotfix 2 of 8.7.
- The Validation workflow in a cross-membership scenario failed because Target System (TS) specific data was not read correctly. This was already fixed with hotfix 2 of 8.7 (Ticket SMTN71).
- Parallel approval with definition "only-one-may-decide" resulted in approval activities with state=RUNNING. The workflow was not proceeding as it seemed as if the approval has not been done (Ticket SNJOPM).

- Activities with dxrState=RETRY were started immediately after IdS-J server restart without taking care of the parameter "waitBeforeRetry" (Ticket S0WOAX).

1.20.2.7. Connectors / Agents

- Policy Agent: The agent writes log messages using the method "log.info(...)" as a WARNING message if that call is provided in a customer-specific jar file (e.g. in a Java Action implementation of a Consistency rule) (Ticket RXUJ22).
- Metacp: Metacp crashed with access violation due to memory allocation problems (Ticket SB1KBD).
- Metacp: Metacp crashed with signal 11 if an LDAP attribute name is longer than 64 bytes (Ticket SBIJV5).

1.20.2.8. Realtime Workflows

- Salesforce workflows: Due to a missing role in the "TS"-connector definition ("role="connector") the Salesforce workflows cannot be loaded at run time.

1.20.2.9. Join Engine

- In case of errors in an update operation the Validation workflow deleted (marked as deleted) the entry. This was already fixed with hotfix 2 of 8.7 (Ticket R84MK1).
- Join engine produces now monitor log entries for password workflows.

1.20.2.10. General

- SPNEGO jar is delivered for Tomcat versions 8.5 and 9 (Ticket SM4OY7).
- Default applications: A TCL workflow running in MERGE mode terminated unexpectedly in case of an ADD operation because a non-existing join result handle is released (Ticket SCFPGK).

1.21. DirX Identity V8.7

1.21.1. New Features

Main features of this version are:

- DirX Identity Business User Interface - The features provided by this new web application focus on the most common use cases of business users.
- DirX Identity REST Services – the new services are used to integrate DirX Identity into application environments which want to use the standard HTTP protocol and the performance and scalability advantages of REST-based services.
- DirX Identity Domain connector - A specialized real-time connector supports the provisioning of a DirX Identity domain.
- Combined workflows: Realtime Java-based workflows can now be started in sequence.
- Java-based workflows are now startable by a batch script.

- All Java-based workflows write now by default monitor entries in the Status Area.
- Support of Windows Server 2016 (Long-Term Service Channel – LTSC)
  For non-productive use (demos or POCs) you can also install DirX Identity on Windows 10.

Detailed features of this version are:

1.21.1.1. General

- In a “Combined Workflow” you can combine a set of Java-based workflows. You define in which sequence the workflows (sub workflows) should be executed. Compared to several schedules starting each sub workflow with a given start time it is guaranteed with a Combined Workflow that the sub workflows are started in a sequence one after another. There are no overlays or gaps between the workflows.

  There is additionally a new script (“runJavaWf.bat” on Window, “runJavaWf.sh” on Linux) for starting any Java-based workflow available (Tickets Q6OPGE, NJKLAZ, NXFMIN, QKLQIE).

- If in request workflow notifications the flag “Separate mails” is set, then e-mails are sent to each recipient separately. Now every recipient sees all the CC- and BCC-recipients, if available (Ticket Q94LIM).
- Java Actions on all selected entries (Ticket PLBJZE).
  The action "siemens.dxr.manager.actions.ActionRunJavaScriptByURL" now supports multiple selection. Set the multiselection="true" in the object description. With this feature it’s now possible to run an action implemented in a customized java script for multiple entries. Here the configuration for the “RunJavaScript restartWF” action of an Request Workflow Instance:

  ```
  <action
  class="siemens.dxr.manager.actions.ActionRunJavaScriptByURL"
  multiselection="true"
  parameter="restartWF@storage://DirXmetaRole/cn=restartReqWF.js,cn=
  RequestWorkflows,cn=JavaScripts,cn=Configuration,$(rootDN)?content
  =dxrObjDesc" />
  ```

- New approach for monitoring Java workflows in V8.7:
  - New flag “Monitor Java Workflows” in the domain configuration, so it is no longer dependent on setting the "Write Audit Log" parameter in the controller Tab of the realtime workflow.
  - Generates now correct Start and End Time.
  - In the "Remark" field only errors will be shown by the realtime workflows. Other Java-based workflows may additionally show some informal messages about the steps/tasks they executed.

    The "Remarks" (if any) are always shown in the Workflow Status entry. If there are

    - more than 300 remarks, then subordinate Activity Status entries (with up to 300 remarks) are generated.
    - There is no statistics information at the Activity Status entries.

  (Tickets QCKPT1 QLTJPY, QCKPNO, RR1I2E, R31IVT, R31JB6, QOCNQY, QOJMZ2, QOXQAJ)

- APRC is now fully available for Windows 10 (Ticket P9DJB6).
- Windows Password Listener is now available for Windows Server 2016 (Tickets RR4JCI, RCRJ5G).
- A variant of the Web Center calender renderer supports time fields (hours, minutes and seconds) (Ticket PPIPCO).
- Web Center supports attributes for assignments of groups to permissions, and of permissions and junior roles to roles (Ticket Q6WOQK).
- By defining an event policy with the values

    - SvcUserToRole
    - ObjectClass: dxrUserToRole
    - ObjectClass 2: dxrAssignment
    - Send: true

  events are fired for parameterized role assignment. ADD, MODIFY and DELETE events are now correctly supported (Ticket R5QJ1G).

- In Exchange 2013/2016 now different – than user - mailbox types can be created or shared by assigning the new DirX Identity AD target system shared-, room- and equipment-enabing groups (Ticket Q7TOFO).

1.21.1.2. Provisioning workflows for a target system can run on a dedicated server

You can dedicate the provisioning workflows of a target system to one or more Java-based servers. Reasons for this might be:

- Separate target systems with many events from others
- Separate slow target systems from others
- Run workflows for a specific target system behind the firewall
- Better support file-based workflows
- Workflows for one target system always on the same server for easier problem analysis

In order to assign a target system or a cluster of target systems to a Java-based server, assign the corresponding connected directory (a cluster has only one connected directory) to the server. You can also run the workflows for a target system on more than one server.

In that case the servers dynamically create target system specific queues. The queue names contain a target system identifier, which is built using the attributes type, cluster and domain of the target system: <type>.<cluster>.<domain>. For an Active Directory with a forest name “Europe” and domain “Germany” the identifier would be

“ads.europe.germany”.

Please avoid special characters in cluster and domain names of target systems. Especially avoid using the following characters: ‘.’, ‘*’, ‘>’, ‘?’, ‘\’, ‘/’.

For more information see the chapter *Managing DirX Identity Servers / Distributed Deployments and Scalability / Distributing Java-based Servers / Running workflows for a target system on a dedicated server* in the *Connectivity Administration* guide.

1.21.1.3. Support of Apache ActiveMQ

- Update to Apache ActiveMQ 5.15.0 (Tickets R5CLM4, RVFO4J).

1.21.1.4. Support of openSSL

- OpenSSL libraries were updated to openSSL version 1.0.2l.

1.21.1.5. New Consistency Rules / Workflows

A new consistency rule **ResolveInconsistentGroupMembership** is provided that could be run using the new workflow **ResolveInconsistentGroupMembership** (which runs the PolicyAgent executing that consistency rule).The rule resolves situations when you have many realtime workflows running in parallel and working on same users or groups. In such a scenario (e.g. when the group membership is stored at the user), it could happen that the user holds the attributes “dxrGroupMemberImported” and “dxrGroupMemberOK” with same values. That situation is normally of no harm as next time when a user resolution (or the realtime workflow) runs the attributes values are updated consistently. But in order to avoid confusion, the workflow **ResolveInconsistentGroupMembership** will make the values consistent, too. We recommend scheduling that worklow once a day/week.

1.21.2. Bug Fixes

1.21.2.1. Documentation

- For warnings during start-up of the Java server regarding workflow definitions a solution was added in the Troubleshooting Guide (Ticket Q2MMNN).
- The documentation in the Application Development Guide was extended by describing more clearly the delete behavior of the RestoreTS controller in contrast to the SyncOneWay2TS controller (Ticket R4GI9U).
- The Certification Campaign Use Case document was updated with information about setup, usage, available templates and the path for user hook deployments was corrected. The Certification Campaign tutorial document was updated to describe all Notification objects used in the tutorial (Ticket QWQRU0, Q8QQFE).
- Handling of displayname property in Identity Manager was described. The Troubleshooting Guide was extended for “How to show LDAP displayname” (Ticket R1SP6X).
- Attributes in DirX Identity for which the new DirX Directory feature “Improved search operation processing“ applies are described in the Migration Guide (Ticket RKYKA2).

1.21.2.2. Java-based Server

- Integration of Castor 1.4.1 in order to solve performance problems with XML unmarshalling of request workflow orders (Ticket QEZNRD).
- A schedule was started by mistake, if for one day no ranges were defined but ranges for other days existed (Ticket QWYLSW).
- The XML parsing mechanism has been changed to not using "defer node expansion" which is the default (Ticket REPJQ6).
- Password for JMS AuditHandler is now contained in a bind profile where the password stored in LDAP is either scrambled or encrypted (Ticket RRUI4Z).

1.21.2.3. C++-based Server

- The Mozilla LDAP C SDK used by the C++-based server now supports "Netscape Portable Runtime (NSPR) 5.15" and "Network Security Services (NSS) 3.31" with latest updates for SSL (Tickets RHBNNK, RHYPMO).
- Termination issue of the scheduler component in the in the C++-based server was fixed (Ticket QESLAB).
- C++-based server now supports TLSv1.1 and TLSv1.2 (Ticket RMFRPZ).

1.21.2.4. Certification Campaign

- The Certification Campaign notification engine now supports direct language values in email notification templates (Ticket RG2NLE).

1.21.2.5. Request Workflows

- The request workflow instances now hold new values in "dxmSpecificAttributes" that allow to filter them, e.g. searching for creation, modification, deletion workflows etc. Supported values are: ctx.iscreateassignmentworkflow true ctx.iscreateworkflow true ctx.ismodifyassignmentworkflow true ctx.ismodifyworkflow true ctx.isdeleteassignmentworkflow true ctx.isdeleteworkflow true ctx.issodassignmentworkflow true ctx.isreapprovalworkflow true ctx.iscertificationworkflow true ctx.iscreateprivilegeassignmentworkflow true ctx.isdeleteprivilegeassignmentworkflow true (Ticket OKUPPX).
- Complex expressions in the "To" field of an email notification were not handled properly (Ticket QKPQ5R).
- When calculating the participants of an approval activity, all delegations of an initially listed participant are evaluated (and not just the very first one) resulting in a "1:n"-list of substitutes (Ticket QLPMIT).
- In e-mail notifications complex expressions are supported in the "To" address field and internally the "To" variable (representing a SvcUser object) is set which then can be used in other expressions too (Ticket Q9XQAQ).
- The Request Workflow service applies workflow filters and/or activity filters in the correct sequence. Preferred solution is to apply workflow filter first (as many attributes to be used in the filter are stored at the LDAP workflow instance.) This fix applies to interfaces like "GetWorklist" or "ListInstances" (Ticket RZPOV1).

- An activity in state WAITINERROR first goes to RETRY before it (finally) ends up in state FAILED (rather than FAILED.EXPIRED). So an administrator has the chance to correct the problem that causes the WAITINERROR situation before resuming the activity (Ticket RQJPXF).
- Display Name in Request workflows was not resolved properly if expressions like "${startTime} ${subject.cn}" were used. "${startTime}" always resolved to the value "0". Furthermore expressions like "${subject.cn}+ ${subject.cn}" simply resolved to "+" (Ticket R5DLQ0).
- The SendMail workflows now runs in RETRY mode and processes mails once again, if sending e-mails fails (Ticket RIVPU1).
- There was a NullPointerException in ApplyChanges if a role with role parameter (using "Reference Expression") was used because the "user" object was not set internally (Ticket RTXIRG).

1.21.2.6. Request Workflow Service

- Sporadically occurring connection issues fixed (Tickets RIFL8W, RHVLFI, R31P60, QFQK2T).

1.21.2.7. Web Center

- Privilege resolution or WebCenter hangs/loops, if variable substitution (e.g. in Object Descriptions) couldn't find the suffix in an expression (Tickets R6FSUN, R6OJ45).
- CSRF filter was too strict for complex pages with tabs and custom buttons on forms (Ticket R71JOV).
- Web Center access policies evaluation fixed (Ticket R7GLAF).
- Configuration extensions for assigning privileges to locations and cost units (Ticket R55I91).
- Reading the subscription status for users with @ in their DNs fixed (Ticket R6IPEL).
- Assign pages with request reason will again extend to the full page width (Ticket R6IN8S).
- Disabling loadAll icon on load on demand tabs fixed (Ticket RVXMCN).
- Display of member account name fixed (Ticket R61Q6K).
- MarshalException when reading a workflow task fixed (Ticket R0QMNR).
- Attribute dxrCostUnitLink added to configuration of some user pages (Ticket R3NJ6E).
- German translation for a user's Windows display name changed to Anzeigename (Ticket RERKA5).
- Access to the request workflow service works if Web Center is used with external authentication against an ADS or LDAP directory and the connection between Web Center and the request workflow service has been set up as in the case of single sign-on (Tickets R7MPKP, RWXL4Y).
- Searching for workflow tasks via subject or initiator fixed (Ticket R8UOCR).
- Evaluation of expression in form property attribute readonly fixed (Ticket R7NJ8L).

1.21.2.8. Services

- Handling of SoD violations / SoD exceptions for ReApproval has been corrected (Ticket QFQJPF).
- BO Inheritance is now also available for Cost Units (Ticket Q6IMB7).
- Former versions of copyPrivileges just copied parameterized role assignments if no assignment for this role exists in the target. Now parameterized role assignments are copied if the target does not have an assignment with the given parameter value. The once-only assignment flag is respected (Ticket Q7ONV5).
- When unassigning roles containing Role Parameters of type HDN with "Apply Policy for selection" checked or type DN with "Object Type for Access Control"=dxrRoleParam the actual role parameter values are checked. If no grant Access Policy allows it you cannot unassign the role (same check as when you create such an assignment) (Ticket QWJJ8P).
- If there are broken links (e.g. a permission referenced in a role with role parameters doesn't exist) then no updates are done in LDAP (neither the user object is updated nor the assignment objects are created). That situation may also be present, if the updates normally should be done in an "ApplyChanges" activity of a request workflow (Ticket RZWJRM).
- When the processing of SoD policies referencing permissions InitializeReapproval and StartReapproval started approval workflows because of SoD violations the SoD exceptions regarding permissions were not shown during approval in WebCenter. Now the SoD exceptions are shown correctly for SoD policies referencing permissions, too (Ticket RZWQZD).
- Remove script was just called when the remove method was called. Some objects were deleted using the removeLeaf instead of remove. Now the remove script is also called in removeLeaf. So it now should be processed for every object when it is deleted (Ticket R04O5V).
- When the end date of a delegation is changed then the delete date is computed again (Ticket RQEPFC).
- Privilege resolution or Web Center hangs/loops if variable substitution (e.g. in Object Descriptions) couldn't find the suffix in an expression (Ticket R6FSUN).
- When running "Entry Change Workflows" (Event-based maintenance workflows) the Domain flag "Inheritance from Business Objects" for "User Facets" was not handled correctly. So the BO inheritance was sometimes not working here. Now this flag is handled correctly (Ticket R6SOEO).
- Due to incompatible time stamp handling in DirX and DirX-Identity, too many updates were done in LDAP where no updates are necessary. (The difference in the time stamp values was only the suffix ".000Z" showing the milliseconds. Now time stamps with suffix ".000Z" and without suffix (for milliseconds) are considered to be equal and thus no changes are done in LDAP (Tickets R5WP7F, RTHP0V)
- Modifications for accounts some times were not stored in LDAP (Ticket RHXIMH).
- There was an endless loop while checking the uniqueness of attribute values as defined in the ObjectDescription. The problem came up when the definition for "uniqueIn" was set but the value was calculated by a Naming Rule that always returned the same value

(Ticket RTVIQ7).

1.21.2.9. Join Engine

- By mistake the Validation workflow deleted entries in IdentityStore, if LDAP server was temporarily unavailable and joining of entries of the Connected System failed before. Now the Join engine terminates the Validation workflow if LDAP server is temporarily unavailable (Ticket QWWOVW).
- For Cluster workflows, the connection to the Connected System was setup using wrong parameter values (Ticket RASKY2).

1.21.2.10. Password Management

- The situation when an account has no value for the attribute "dxrUserLink" (which is a valid scenario for privileged accounts) will no longer be logged as error. Now only an info logging is generated (Ticket Q2KPOZ).

1.21.2.11. Provisioning Web Service

- The service supports now all role parameter match rule operator types (Ticket RVKNGH).
- The service returns an error if a modification fails due to an invalid LDAP attribute name (Ticket PLJP3Z).
- The service supports now single sign-on with DirX Access (Ticket R54KFU).

1.21.2.12. Default Applications

1.21.2.13. Changes in the Default Applications (common.tcl): On Linux a TCL-based workflow sporadically failed due to a TCL-"puts" command to "stdout" (Tickets RF2MII, R6MK5H, PKDMLJ).Identity Manager

- The field "System Default" for nationalized message texts is no longer shown in the DirX Identity Manager (Ticket R7GOZU).
- “Show References...” for C++-based workflows and Java-based workflows shows also references from Schedules. In former versions these references were not shown (Ticket RAXM7K).

1.21.2.14. Connectors

- SharePoint connector: The SharePoint connector now continues reading members and roles of further groups if reading the members or roles of a specific group failed (Ticket Q5DJEK).
- LDAP connector: For non-paged searches the LDAP connector throws an exception now in case getNextEntry returns SIZE LIMIT or TIME LIMIT exceeded. This prevents join engine from unintended object deletions due to a reduced search result (note: paged searches are handled correctly already) (Ticket RYZKYU).
- SAP ECC UM connector: Now the agent/connector deletes the affected whole row in the table PARAMETER1 (Ticket RY5IFG).
- SAP ECC UM connector: Now adding to the table PARAMETER1 works again (Ticket

RNRPVO).

- SAP ECC UM connector: Adding and deleting SAP roles with active CUA does not work. Previous hotfix did contain a new routine which checks if a role that is to be added is already assigned. This lead to an error in the CUA branch (Ticket R0YLLH).
- SAP ECC UM connector: So far the agent/connector did not allow in CUA mode to provision other attributes than "dxrRole.NAME" for SAP roles. Note that this is a pseudo attribute. Now the agent/connector also allows to manipulate "dxrRole." e.g. TO_DAT, FROM_DAT. Note also that in CUA mode the attributes for SAP roles start with "dxrRole" not with "ACTIVITYGROUPS" (like in non-CUA mode). Also you have to add a configuration parameter "useAdditionalRoleParameters" in the connection section of the connector: This parameter is only relevant for CUA if you use dxrRole.NAME and other dxrRole fields (Tickets RQMMDP, RDSOSJ).
- SAP ECC UM connector: A delete SAP role operation in CUA case was not handled correctly (Ticket RIOMXJ).
- SpmlV1ToV2Connector: the connector handles functional users now correctly (Tickets RZPNUO, RELOW7).
- Salesforce connector: There was a ClassCastException in ADD operation while evaluating the attributes for a password update request (Ticket R5HJ33).

1.21.2.15. Agents

- Metacp: metacp now creates superior nodes implicitly when a MODIFY or MODIFY-DN operation failed before due to missing superior node (Ticket RFGJE1).
- Metacp: metacp didn’t create superior nodes implicitly (Ticket RR4NDZ).
- Metacp: The Mozilla LDAP C SDK used by metacp now supports "Netscape Portable Runtime (NSPR) 5.15" and "Network Security Services (NSS) 3.31" with latest updates for SSL (Tickets RHBNNK, RHYPMO, R5ZKV0).
- Metacp now supports TLSv1.1 and TLSv1.2 (Ticket RMFRPZ).
- Policy Execution agent: ruleprovider.base for Policy Execution workflow: Umlauts are now handled correctly (UTF-8). Property ruleprovider.base in .ini file for Policy Execution workflow: Umlauts are now handled correctly (UTF-8 used for reading .ini file) (Ticket PLEQ10).
- ADS agent: Agent failed creating or modifying mailbox-enabled users when running on Windows 2012 (Tickets RTQJ3Y, R71INT).
- ADS agent: AD synchronisation with a negative uSNChanged value:
  In delta exports the highestUSN was converted incorrectly to a negative string representation taken as LDAP search filter part for values above 2,147,483,648 (Ticket RVNPOD).
- Service agent: The agent uses internally a PrefetchCache. For target system with assignmentStates=False the fetching of groups did not work correctly in some cases (Ticket Q7HOQ4).
- Service agent: the agent of V8.6 used the SvcPrefetchCache just for exactly one User at a time. With this fix it will again use it for the configured amount of users (object prefetch size). This will increase the performance for many user which are members of

large (lot of members) groups (Ticket R3JPYU).

- Lotus Notes agent: Notes agent has been corrected so that it is able to delete the last member of a group (Ticket RO1POG).
- The History Agent generates a temporary XML file (filename starts with "tmp-") which is renamed to its final filename at the very end thus allowing applications to pick the XML files that are completely processed (Ticket QLCLZ4).

1.21.2.16. Installation and Configuration

- Fixed a bug in the custom code that tries to print some additional information to log and that crashes with null pointer exception (Ticket RA0OBA).
- The installation of a service pack doesn’t show passwords in clear text in the log file (Ticket R6SPF5).

1.21.2.17. Miscellaneous

- Several 3rd party jar files have been updated. A detailed list is now available in the Readme documentation (Ticket QEZORU).
- Export Collection now supports paging for the internal one level searches. Via page size="n" now the page size can be specified. 0 is default which means no paging. In the workflow configuration in the perform activity you can specify the value in the export tab in the "Page Size" field. For usage with export Collection action via the Identity Manager specify in the dxi.cfg: collection.pagesize=100. When using the batch script exportConfig specify -pageSize 100 (Ticket QI3PAR).
- The report engine now supports binary attributes (Ticket QWHRKQ).
- Transport workflows: Handling of binary attributes like jpegPhoto in transport import workflows fixed. Octet String attributes like jpegPhoto are now passed as jpegphoto;raw to LDAP Connector. Other binary attributes like userCertificate are passed, as before, as userCertificate;binary to LDAPConnector (Ticket R04OD5).
- APRC: In case of smart card option and if GetPolicy request fails (no policy found) APRC should use the policy from the registry (Ticket RFXKIY).
- Tool Link Checker now supports SSL. Specify ssl=true in the connection section of the configuration file (Ticket RSMOSH).

1.21.3. Information About Discontinued Features

DirX Identity V8.7 does no longer support these features:

- Platform support for Oracle Solaris 11 and Solaris Zones
- Repository support for DirX Directory V8.4

DirX Identity V8.7 is the last version that supports the following features:

- Windows NT agent
- Dashboard Agent and Tcl-Workflows
- Soarian Clinicals Workflows

- SAP GRC in Request Workflows
- UNIX-PAM TCL Workflows
- Former certification: Campaign Generation workflow

DirX Product Suite

The DirX product suite provides the basis for fully integrated identity and access management; it includes the following products, which can be ordered separately.

DirX Identity

DirX Identity provides a comprehensive, process-driven, customizable, cloud-enabled, scalable, and highly available identity management solution for businesses and organizations. It provides overarching, risk-based identity and access governance functionality seamlessly integrated with automated provisioning. Functionality includes lifecycle management for users and roles, cross-platform and rule-based real-time provisioning, web-based self-service functions for users, delegated administration, request workflows, access certification, password management, metadirectory as well as auditing and reporting functionality.

DirX Directory

DirX Directory provides a standards-compliant, high-performance, highly available, highly reliable, highly scalable, and secure LDAP and X.500 Directory Server and LDAP Proxy with very high linear scalability. DirX Directory can serve as an identity store for employees, customers, partners, subscribers, and other IoT entities. It can also serve as a provisioning, access management and metadirectory repository, to provide a single point of access to the information within disparate and heterogeneous directories available in an enterprise network or cloud environment for user management and provisioning.

DirX Access

DirX Access is a comprehensive, cloud-ready, scalable, and highly available access management solution providing policy- and risk-based authentication, authorization based on XACML and federation for Web applications and services. DirX Access delivers single sign-on, versatile authentication including FIDO, identity federation based on SAML, OAuth and OpenID Connect, just-in-time provisioning, entitlement management and policy enforcement for applications and services in the cloud or on-premises.

DirX Audit

DirX Audit provides auditors, security compliance officers and audit administrators with analytical insight and transparency for identity and access. Based on historical identity data and recorded events from the identity and access management processes, DirX Audit allows answering the “what, when, where, who and why” questions of user access and entitlements. DirX Audit features historical views and reports on identity data, a graphical dashboard with drill-down into individual events, an analysis view for filtering, evaluating, correlating, and reviewing of identity-related events and job management for report generation.

For more information: support.dirx.solutions/about

Legal remarks

On the account of certain regional limitations of sales rights and service availability, we cannot guarantee that all products included in this document are available through the Eviden sales organization worldwide. Availability and packaging may vary by country and is subject to change without prior notice. Some/All of the features and products described herein may not be available locally. The information in this document contains general technical descriptions of specifications and options as well as standard and optional features which do not always have to be present in individual cases. Eviden reserves the right to modify the design, packaging, specifications and options described herein without prior notice. Please contact your local Eviden sales representative for the most current information. Note: Any technical data contained in this document may vary within defined tolerances. Original images always lose a certain amount of detail when reproduced.