EVIDEN

Identity and Access Management

DirX Identity

History of Changes

Version 8.10.17, Edition November 2026



All product names quoted are trademarks or registered trademarks of the manufacturers concerned.

© 2026 Atos Group

All Rights Reserved

Distribution and reproduction not permitted without the consent of Atos Group.

Table of Contents

Copyright ii
History of Changes 1
1. History of DirX Identity Releases 2
1.1. DirX Identity 8.10.17 2
1.2. DirX Identity 8.10.16 32
1.3. DirX Identity 8.10.16 33
1.3.1. Other Improvements and Fixes 52
1.4. DirX Identity 8.10.15 52
1.5. DirX Identity 8.10.14 60
1.6. DirX Identity 8.10.13 76
1.6.1. Bug Fixes 76
1.7. DirX Identity 8.10.12 77
1.7.1. Bug Fixes 77
1.8. DirX Identity 8.10.11 77
1.8.1. Bug Fixes 77
1.9. DirX Identity 8.10.10 78
1.9.1. Bug Fixes 78
1.10. DirX Identity 8.10.9.a 78
1.10.1. Bug Fixes 78
1.11. DirX Identity 8.10.9 78
1.11.1. Bug Fixes 78
1.12. DirX Identity 8.10.8 79
1.12.1. Bug Fixes 79
1.13. DirX Identity 8.10.7 79
1.13.1. Bug Fixes 79
1.14. DirX Identity 8.10.6 80
1.14.1. Bug Fixes 80
1.15. DirX Identity 8.10.5 80
1.15.1. Bug Fixes 80
1.16. DirX Identity 8.10.4 81
1.16.1. Bug Fixes 81
1.17. DirX Identity 8.10.3 81
1.17.1. Bug Fixes 81
1.18. DirX Identity V8.10 SP2 82
1.18.1. New Features 82
1.18.1.1. Synchronous Resolution Handling in Policy and Service Agent 82
1.18.1.2. Business User Interface 82
1.18.1.3. Identity REST Service 82
1.18.1.4. Join Engine 83

1.18.1.5. Request Workflow Engine . . . 83
1.18.1.6. Identity Domain Connector . . . 83
1.18.1.7. Support of DirX Directory 8.10 and 9.0 . . . 83
1.18.1.8. Support of OpenSSL . . . 83
1.18.1.9. Support of Systemd for Red Hat 9 . . . 83
1.18.1.10. Support of Apache ActiveMQ 5.18.4 . . . 83
1.18.1.11. Support of Apache Embedded Tomcat 9.0.88 . . . 83
1.18.1.12. Message broker . . . 83
1.18.1.13. Endpoint Identification feature in the SSL configuration . . . 84
1.18.2. Bug Fixes . . . 84
1.18.2.1. Services . . . 84
1.18.2.2. Event Based Rules . . . 86
1.18.2.3. Join Engine . . . 86
1.18.2.4. Identity Domain Connector . . . 87
1.18.2.5. Provisioning Web Services . . . 87
1.18.2.6. Web Center . . . 88
1.18.2.7. Business User Interface . . . 88
1.18.2.8. Request Workflow Engine . . . 88
1.18.2.9. Identity REST Service . . . 88
1.18.2.10. Java-based Server . . . 88
1.18.2.11. Agents / Connectors . . . 89
1.18.2.12. C++-based Server . . . 90
1.18.2.13. Messaging . . . 90
1.18.2.14. Identity Manager . . . 90
1.18.2.15. Miscellaneous . . . 91
1.18.3. Fixes already solved in 8.10 SP1 Release . . . 91
1.18.4. Information About Discontinued Features . . . 91
1.19. DirX Identity V8.10 SP1 . . . 92
1.19.1. New Features . . . 92
1.19.1.1. Support of Windows Server 2022 . . . 92
1.19.1.2. Business User Interface . . . 92
1.19.1.3. Web Center . . . 92
1.19.1.4. DirX Identity REST service . . . 92
1.19.1.5. TCL Workflows . . . 92
1.19.1.6. Security Settings for Identity SSL Connections . . . 92
1.19.1.7. Support of Apache ActiveMQ 5.17.2 . . . 92
1.19.1.8. Support of Apache Embedded Tomcat 9.0.69 . . . 93
1.19.2. Bug Fixes . . . 93
1.19.2.1. Web Center . . . 93
1.19.2.2. Services . . . 93
1.19.2.3. Join Engine . . . 95
1.19.2.4. Request Workflows . . . 95

1.19.2.5. Manager . . . 96
1.19.2.6. Java-based Server . . . 96
1.19.2.7. Identity REST Service . . . 96
1.19.2.8. Business User Interface . . . 97
1.19.2.9. Realtime Workflows . . . 97
1.19.2.10. C++-based Server . . . 98
1.19.2.11. Identity Domain Connector . . . 98
1.19.2.12. CSV Connector . . . 98
1.19.2.13. Mail Connector . . . 98
1.19.2.14. RACF Connector . . . 98
1.19.2.15. LDAP Connector / ADS Connector . . . 99
1.19.2.16. Sharepoint Connector . . . 99
1.19.2.17. SAP ECC UM Connector/Agent . . . 99
1.19.2.18. JDBC Connector/Agent . . . 99
1.19.2.19. Policy/Service/Consistency Agent . . . 99
1.19.2.20. Mail Target System . . . 99
1.19.2.21. Configuration Wizard . . . 99
1.19.2.22. Configuration . . . 99
1.19.2.23. Miscellaneous . . . 100
1.19.3. Information About Discontinued Features . . . 100
1.20. DirX Identity V8.10 . . . 100
1.20.1. New Features . . . 100
1.20.1.1. LDAP Lock . . . 102
1.20.1.2. Resolution Adapter . . . 102
1.20.1.3. Target System Specific Adapter . . . 103
1.20.1.4. Personas und Functional Users per User in Identity Manager . . . 103
1.20.1.5. Realtime Connector and Provisioning Workflows for an IBM RACF System . . . 103
1.20.1.6. Extensions for Office 365 Connector and Provisioning Workflows . . . 103
1.20.1.7. Handling of Consistency Rules . . . 104
1.20.1.8. Configuration Changes . . . 104
1.20.1.9. Support of Encrypted E-mails . . . 104
1.20.1.10. Anonymous Access to Connectivity and Provisioning Store . . . 104
1.20.1.11. Mail Target System . . . 104
1.20.1.12. Delta Mode for Combined Workflows . . . 104
1.20.1.13. Identity Manager – Separate Logs per User . . . 104
1.20.1.14. Java-based Server – Configuration of Log Folder . . . 104
1.20.1.15. Client-side SSL Support for LDAP, ADS, and RACF Connectors . . . 105
1.20.1.16. Certification Controller . . . 105
1.20.1.17. Handling of IMPORTED Accounts . . . 105
1.20.1.18. Handling of RT Workflows when no Channel Matches . . . 105
1.20.1.19. External Accessible Scrambling Method . . . 105

1.20.1.20. Support of Apache ActiveMQ 5.16.3 . . . 105
1.20.1.21. Support of Apache Embedded Tomcat 9.0.56 . . . 105
1.20.1.22. Web Center . . . 105
1.20.2. Bug Fixes . . . 106
1.20.2.1. Business User Interface . . . 106
1.20.2.2. Java-based Server . . . 106
1.20.2.3. C++-based Server . . . 108
1.20.2.4. Agents / Connectors . . . 108
1.20.2.5. Request Workflows . . . 109
1.20.2.6. Realtime Workflows . . . 109
1.20.2.7. Services . . . 109
1.20.2.8. Join Engine . . . 110
1.20.2.9. Identity Manager . . . 111
1.20.2.10. Web Center . . . 111
1.20.2.11. REST Services . . . 112
1.20.2.12. Provisioning Services . . . 112
1.20.2.13. TCL-based Workflows . . . 112
1.20.2.14. Documentation . . . 112
1.20.2.15. Password Management . . . 113
1.20.2.16. APRC . . . 113
1.20.2.17. Miscellaneous . . . 113
1.20.3. Information About Discontinued Features . . . 113
1.21. Dirx Identity V8.9 SP3 . . . 114
1.21.1. New Features . . . 114
1.21.1.1. Realtime Connector and Provisioning Workflows for an IBM RACF System . . . 114
1.21.1.2. Client-side SSL Support for LDAP, ADS, and RACF Connectors . . . 114
1.21.1.3. Handling of IMPORTED Accounts . . . 114
1.21.1.4. Role Assignments with Mandatory End Dates . . . 114
1.21.1.5. Support of Apache ActiveMQ . . . 114
1.21.1.6. Support of Apache Embedded Tomcat . . . 114
1.21.2. Bug Fixes . . . 114
1.21.2.1. Request Workflows . . . 115
1.21.2.2. Join Engine . . . 115
1.21.2.3. Services . . . 116
1.21.2.4. Java-based Server . . . 117
1.21.2.5. C++-based Server . . . 118
1.21.2.6. Realtime Workflows . . . 118
1.21.2.7. REST Services . . . 118
1.21.2.8. Web Center . . . 118
1.21.2.9. Provisioning Servlet . . . 119
1.21.2.10. Manager . . . 119

1.21.2.11. Business User Interface . . . 119
1.21.2.12. Agents/ Connectors . . . 119
1.21.2.13. Miscellaneous . . . 120
1.22. DirX Identity V8.9 SP2 . . . 121
1.22.1. New Features . . . 121
1.22.1.1. Target System-specific Adaptor Feature . . . 121
1.22.1.2. Office 365 Connector . . . 121
1.22.1.3. Identity REST Services . . . 122
1.22.1.4. Support of Apache ActiveMQ 5.16.1 . . . 122
1.22.1.5. Support of Apache Embedded Tomcat 9.0.43 . . . 122
1.22.1.6. Supported Browser Microsoft Edge Chromium . . . 122
1.22.2. Bug Fixes . . . 123
1.22.2.1. Services . . . 123
1.22.2.2. Join Engine . . . 123
1.22.2.3. Web Center . . . 124
1.22.2.4. Java-based Server . . . 124
1.22.2.5. C++-based Server . . . 125
1.22.2.6. Realtime Workflows . . . 125
1.22.2.7. Request Workflows . . . 125
1.22.2.8. Identity Manager . . . 125
1.22.2.9. Business User Interface . . . 126
1.22.2.10. REST Services . . . 126
1.22.2.11. Office 365 Connector . . . 126
1.22.2.12. Identity Domain Connector . . . 126
1.22.2.13. Connector . . . 126
1.22.2.14. JDBC Connector . . . 127
1.22.2.15. JMS Audit Listener . . . 128
1.22.2.16. Agents . . . 128
1.22.2.17. Certification Campaign . . . 128
1.22.2.18. Miscellaneous . . . 128
1.22.2.19. Fixes already solved in 8.9 SP1 . . . 129
1.22.2.20. Fixes already solved in 8.9 Release . . . 129
1.23. DirX Identity V8.9 SP1 . . . 129
1.23.1. New Features . . . 129
1.23.1.1. Business User Interface . . . 129
1.23.1.2. Identity REST Services . . . 129
1.23.1.3. Support of Apache ActiveMQ 5.15.12 . . . 130
1.23.1.4. Office 365 Connector . . . 130
1.23.1.5. Sending mail in the Java-based server . . . 130
1.23.1.6. Link checker . . . 130
1.23.2. Bug Fixes . . . 131
1.23.2.1. Web Center . . . 131

1.23.2.2. Services . . . 131
1.23.2.3. Java-based Server . . . 132
1.23.2.4. C++-based Server . . . 133
1.23.2.5. Default Applications . . . 133
1.23.2.6. Identity Manager . . . 133
1.23.2.7. Identity REST Services . . . 133
1.23.2.8. Provisioning Web Service . . . 134
1.23.2.9. Request Workflows . . . 134
1.23.2.10. Connectors / Agents . . . 134
1.23.2.11. Realtime Workflows . . . 136
1.23.2.12. Join Engine . . . 136
1.23.2.13. Certification Campaign . . . 136
1.23.2.14. Metacp . . . 136
1.23.2.15. Online Help . . . 137
1.23.2.16. Windows Password Listener . . . 137
1.23.2.17. JMS Audit Log Handler . . . 137
1.23.2.18. Miscellaneous . . . 137
1.24. DirX Identity V8.9 . . . 137
1.24.1. New Features . . . 137
1.24.1.1. DirX Identity Business User Interface . . . 139
1.24.1.2. DirX Identity REST Services . . . 140
1.24.1.3. Delegations . . . 140
1.24.1.4. Support of Java 11 . . . 140
1.24.1.5. Support of Apache ActiveMQ 5.15.9 . . . 140
1.24.1.6. Support of openSSL v1.0.2r . . . 140
1.24.2. Bug Fixes . . . 140
1.24.2.1. Java-based Server . . . 140
1.24.2.2. Documentation . . . 141
1.24.2.3. C++-based Server . . . 141
1.24.2.4. Request Workflows . . . 142
1.24.2.5. Realtime Workflows . . . 142
1.24.2.6. Web Center . . . 143
1.24.2.7. Services . . . 145
1.24.2.8. Business User Interface . . . 146
1.24.2.9. REST Services . . . 146
1.24.2.10. Messaging . . . 147
1.24.2.11. Join Engine . . . 147
1.24.2.12. Provisioning Web Service . . . 147
1.24.2.13. Windows Password Listener . . . 147
1.24.2.14. Identity Manager . . . 147
1.24.2.15. Request Workflow Service . . . 148
1.24.2.16. Connectors . . . 148

1.24.2.17. Default Workflows . . . 149
1.24.2.18. Agents . . . 149
1.24.2.19. Installation and Configuration . . . 149
1.24.2.20. Meta Controller . . . 150
1.24.2.21. APRC . . . 150
1.24.2.22. Certification Campaign . . . 151
1.24.2.23. Miscellaneous . . . 151
1.24.3. Information About Discontinued Features . . . 151
1.25. DirX Identity V8.7 SP4 . . . 151
1.25.1. New Features . . . 151
1.25.1.1. Business User Interface . . . 151
1.25.1.2. Identity REST Services . . . 152
1.25.1.3. Support of Apache ActiveMQ 5.15.10 . . . 152
1.25.1.4. Upgrade of embedded Tomcat . . . 152
1.25.1.5. Java-based Server . . . 152
1.25.2. Bug Fixes . . . 152
1.25.2.1. Web Center . . . 152
1.25.2.2. Services . . . 153
1.25.2.3. Business User Interface . . . 154
1.25.2.4. Request Workflows . . . 154
1.25.2.5. Join Engine . . . 154
1.25.2.6. Java-based Server . . . 155
1.25.2.7. C++-based Server . . . 155
1.25.2.8. Messaging . . . 156
1.25.2.9. Configuration Data . . . 156
1.25.2.10. Connectors . . . 156
1.25.2.11. Agents . . . 156
1.25.2.12. Realtime Workflows . . . 157
1.25.2.13. Identity Manager . . . 157
1.25.2.14. Identity REST service . . . 157
1.25.2.15. Default Applications . . . 157
1.25.2.16. Documentation . . . 157
1.25.2.17. Miscellaneous . . . 158
1.26. DirX Identity V8.7 SP3 . . . 158
1.26.1. New Features . . . 158
1.26.1.1. Business User Interface . . . 158
1.26.1.2. Identity REST Services . . . 158
1.26.1.3. Support of Apache ActiveMQ 5.15.6 . . . 159
1.26.1.4. Support of openSSL v1.0.2p . . . 159
1.26.1.5. Support of VMware ESXi 6.5 . . . 159
1.26.1.6. Realtime Workflows . . . 159
1.26.1.7. Services . . . 159

1.26.2. Bug Fixes . . . 160
1.26.2.1. Services . . . 160
1.26.2.2. Web Center . . . 160
1.26.2.3. Java-based Server . . . 160
1.26.2.4. Join Engine . . . 161
1.26.2.5. Request Workflows . . . 161
1.26.2.6. Provisioning Web Services . . . 161
1.26.2.7. Configuration Wizard . . . 161
1.26.2.8. Schema . . . 161
1.26.2.9. Default Applications . . . 162
1.26.2.10. Metacp . . . 162
1.26.2.11. LDAP connector . . . 162
1.27. DirX Identity V8.7 SP2 . . . 163
1.27.1. New Features . . . 163
1.27.2. Bug Fixes . . . 163
1.27.2.1. Java-based Server . . . 163
1.27.2.2. Services . . . 163
1.27.2.3. Installation/ Configuration . . . 163
1.27.2.4. Join Engine . . . 164
1.27.2.5. Web Center . . . 164
1.27.2.6. Business User Interface . . . 164
1.27.2.7. Password Workflows . . . 164
1.27.2.8. Request Workflows . . . 164
1.27.2.9. Message Broker . . . 164
1.27.2.10. JMS Audit Handler . . . 164
1.28. DirX Identity V8.7 SP1 . . . 164
1.28.1. New Features . . . 164
1.28.1.1. SP1: Business User Interface . . . 164
1.28.1.2. Identity REST Services . . . 165
1.28.1.3. Support of Apache ActiveMQ 5.15.3 . . . 165
1.28.1.4. Support of openSSL v1.0.2n . . . 165
1.28.1.5. C++-based Server . . . 165
1.28.2. Bug Fixes . . . 165
1.28.2.1. Web Center . . . 165
1.28.2.2. Web Center API . . . 165
1.28.2.3. Services . . . 166
1.28.2.4. Java-based Server . . . 166
1.28.2.5. Provisioning Web Services . . . 166
1.28.2.6. Request Workflows . . . 166
1.28.2.7. Connectors / Agents . . . 167
1.28.2.8. Realtime Workflows . . . 167
1.28.2.9. Join Engine . . . 167

1.28.2.10. General . . . 167
1.29. DirX Identity V8.7 . . . 167
1.29.1. New Features . . . 167
1.29.1.1. General . . . 168
1.29.1.2. Provisioning workflows for a target system can run on a dedicated server . . . 169
1.29.1.3. Support of Apache ActiveMQ . . . 170
1.29.1.4. Support of openSSL . . . 170
1.29.1.5. New Consistency Rules / Workflows . . . 170
1.29.2. Bug Fixes . . . 170
1.29.2.1. Documentation . . . 170
1.29.2.2. Java-based Server . . . 171
1.29.2.3. C++-based Server . . . 171
1.29.2.4. Certification Campaign . . . 171
1.29.2.5. Request Workflows . . . 171
1.29.2.6. Request Workflow Service . . . 172
1.29.2.7. Web Center . . . 172
1.29.2.8. Services . . . 173
1.29.2.9. Join Engine . . . 174
1.29.2.10. Password Management . . . 174
1.29.2.11. Provisioning Web Service . . . 174
1.29.2.12. Default Applications . . . 174
1.29.2.13. 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 . . . 174
1.29.2.14. Connectors . . . 174
1.29.2.15. Agents . . . 175
1.29.2.16. Installation and Configuration . . . 176
1.29.2.17. Miscellaneous . . . 176
1.29.3. Information About Discontinued Features . . . 176
Legal Remarks . . . 179

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 8.10.17

Ticket ID	Affected Version	Domain	Summary
SDX-1426	V8.10	Identity, WebCenter	Action-based access control prevents unauthorized WebCenter page access.
SDX-1514	8.10.12	Provisioning, LDAP	Optimized policy processing performance by reducing large-group LDAP overhead.
SDX-1544	8.10.13	Provisioning, Connectivity	Support for TOTP authentication when accessing target system configurations.
SDX-1555	8.10.13	Installer	Improved installer prevents deletion of custom files during upgrades.
SDX-1575	8.10.12	Entitlement, Permissions	Fix for data inconsistencies during concurrent permission assignments.
SDX-1625	8.10.13	Provisioning, GraalJS	Fix GraalJS Polyglot Exception when setting properties with JS-Arrays.
SDX-1637	8.10.12	Provisioning, LDAP	Optimized LDAP reads for groups with large member lists.
SDX-1645	8.10.12	Provisioning, Active Directory	Fix for Infinite Log Growth and Concurrent Class-Loading Race
SDX-1652	V8.9 SP3	Installer, Email encryption	SSL/TLS Email Encryption Support for DirX Identity V8.9 SP3
SDX-1735	8.10.14	Audit Manager	Fix role name resolution in Audit Manager event data logs.
SDX-1756	8.10.14	Entitlement, Facets	Ensure Facet objects are marked as faulty for invalid dates.
SDX-1761	8.10.15	Platform, Security	Log4j Security Vulnerability CVE-2026-34477 Resolved via ActiveMQ Upgrade
SDX-1786	8.10.15	Provisioning, HCL Notes Connector	HCL Notes Connector password change and ID Vault synchronization fix.
SDX-1802	8.10.14	Entitlement, Workflows	Fix for incorrect workflow triggering during role assignment replacement.
SDX-1826	V8.9 SP3	Platform, Security	Fix for Security issue: concurrent attribute modifications bypass approval workflows.

Ticket ID	Affected Version	Domain	Summary
SDX-1827	8.10.10	Provisioning, Xerces XML Parser	Resolved fatal Xerces XML parsing error during Java Server startup.
SDX-1832	8.10.15	Provisioning, SAP JCo Connector	Fix SAP Realtime Userhook failure caused by duplicate connector JARs.
SDX-1834	8.10.15	Entitlement, Workflows	Fix race condition in Create RQWF privilege assignments.
SDX-1844	8.10.14	Provisioning, LDAP	Performance fix for redundant LDAP searches when no policies exist.
SDX-1856	V8.9 SP3	Provisioning, LDAP	Fix for LDAP filters with special characters in Policy Execution.
SDX-1874	8.10.15	Entitlement, Workflows	Fix for misleading ADS workflow durations caused by logging defect.
SDX-1886	8.10.15	Provisioning, ConsistencyCheck	Optimize ConsistencyCheck workflow by reducing redundant LDAP lock/unlock operations.
SDX-1887	8.10.15	Entitlement, Workflows	Optimized workflow locking to resolve 30-second portal timeouts.
SDX-1898	9.0.1	Identity, WebCenter	Fix for unnecessary table columns impacting Web Center form layouts.
SDX-1901	8.10.14	Identity Manager, Permissions	Fix stale user identity links during permission deletion process.
SDX-1909	8.10.15	Provisioning, C-Server	Fix for C-Server workflow failure caused by thread storage exhaustion.
SDX-1911	8.10.16	Provisioning, GraalJS	Automatic conversion of GraalJS script return values to Java types.
SDX-1914	8.10.15	Provisioning, LDAP	Enhanced UidConsistencyCheck workflow logging for detailed LDAP error diagnostics.
SDX-1916	8.10.15	Provisioning, Custom Java Connector	Custom Java Connector connection drops after search in 8.10.15.
SDX-1918	8.10.14	Provisioning, Performance	Performance-optimized refresh mechanism for concurrent identity resolution.
SDX-1919	8.10.15	Provisioning, Java Server	Configure resolution listener threads per individual J-Server instance.
SDX-1926	8.10.16	Identity, Provisioning	Fixed Group Provisioning Rules tab display error in DirX Identity.

Ticket ID	Affected Version	Domain	Summary
SDX-1934	8.10.15	Entitlement, Workflows	Fix for domain-specific message queue routing in UidConsistencyCheck-Workflow.
SDX-1944	8.10.14	Identity, Provisioning	Fixed handling of empty tag values in string-tag properties.
SDX-1947	8.10.16	Identity, Provisioning	Fix for missing workflows in Identity Manager Provisioning view.
SDX-1951	8.10.16	Identity, Provisioning	Include dxmSpecificAttributes(name) in default workflow instance object descriptor.
SDX-1954	8.10.15	Provisioning	Improved error reporting for HCL Notes ID Vault password resets.
SDX-1958	8.10.16+2130	Platform, Logging	Fix for infinite log loop during LDAP size limit errors.
SDX-1962	8.10.16+2130	Installation, Upgrade	Preserve truststore password entries during patch installations and upgrades.
SDX-1968	8.10.16+2130	Provisioning	Fix for postponed error emails in SAP password sync workflows.
SDX-1996	8.10.16+2130	Provisioning	Fix for Provisioning Rule tab visibility for group objects.
SDX-1997	8.10.16+2130	Identity Manager	Prevent Identity Manager GUI from automatically setting dxrStartDate.
SDX-2020	V8.9 SP2	Provisioning, SAP JCo Connector	SAP JCo 3.1.14 update fix for SNC username/password authentication.
SDX-2021	8.10.16+2130	Platform, Security	Update log4j to version 2.26.1 to meet security requirements.
SDX-2024	8.10.16+2130	Platform, Messaging	ActiveMQ connection exhaustion during mass provisioning due to resource leaks.
SDX-2035	8.10.16+2130	Identity Manager	Fix for SVC904 error during nested group obligation resolution.
SDX-2036	8.10.16+2130	Identity Manager	Patch request fails when including unchanged naming attribute 'cn'
SDX-2043	8.10.16+2130	Installer, Upgrade	Fix InitialConfig wizard resetting User-Policy SearchLimit to default values.
SDX-2059	8.10.16+2130	Entitlement, Workflows	CheckConsistency workflow deletes dxrOptions due to stale data processing.
SDX-2067	8.10.13	Provisioning	Fix JDBC-Agent failing to export DATE values from MS-SQL databases.
SDX-2081	8.10.16+2130	Platform, Security	Feasibility of independent log4j updates for DirX Identity.

Ticket ID	Affected Version	Domain	Summary
SDX-2083	8.10.10	Platform, Security	Guidance on manual Log4j library updates for DirX Identity
SDX-2091	8.10.16+2130	Identity, REST API	Fix URISyntaxException for DomainObject DNs containing spaces in REST responses.
SDX-2094	8.10.16	Entitlement, Workflows	Fix JavaScriptActionRunner storage caching issue in ConsistencyRuleProvider.
SDX-2100	8.10.10	Platform, Security	Impact assessment of Windows Authenticode vulnerability CVE-2013-3900 on DirX products.

▾ *details SDX-1426*

This update introduces a new security feature that allows administrators to restrict access to specific WebCenter actions using proposal lists and access policies tailored to the access rights of users and user groups. These enhancements prevent unauthorized page access via request manipulation, ensuring a more secure environment for delegated administration.

Problem	Solution
A penetration test revealed a vulnerability in WebCenter where users could bypass menu-based access controls. By intercepting and modifying POST requests (e.g., changing a legitimate Struts action to an unauthorized one), users could access pages and data they were not permitted to see. This occurred because the system previously relied on access checks only during menu generation rather than validating every incoming request.	The solution implements a robust action-based access control mechanism. The `MetaActionServlet` and `ACL Manager` were enhanced to verify every incoming request against new "Allowed Action" proposal lists and access policies. Administrators can now explicitly define which Struts actions are permitted for specific user roles, ensuring that even manipulated requests are rejected if they violate the defined security policies.

▾ *details SDX-1514*

This update significantly improves policy processing performance by eliminating unnecessary large-group attribute reads during privilege resolution. Additionally, a more efficient inline resolution method has been implemented to reduce system overhead and event processing delays.

Problem	Solution
The customer experienced critical performance degradation during policy processing, with throughput dropping to approximately 20 records per minute. Investigation revealed that the system was incorrectly loading all members of large LDAP groups (up to 250,000 members) during privilege resolution, causing significant "dead time" and JVM blocking. Furthermore, the existing customization used an inefficient event-based resolution chain that created unnecessary system load.	The resolution involves a two-pronged approach: first, applying a fix to restrict LDAP group reads to only necessary attributes, bypassing the loading of massive member lists. Second, the processing logic was optimized by switching to the `checkAndResolve()` method, which performs inline resolution without triggering the resource-intensive ChangeEvent and ResolutionAdapter queue. These changes restore acceptable processing speeds for large-scale data initializations.

▾ *details SDX-1544*

A new authentication dialog has been implemented to support Time-based One-Time Passwords (TOTP) when accessing target system configurations in the Identity GUI. This ensures that users with multi-factor authentication enabled can securely bind to the connectivity domain and manage target systems without session failures.

Problem	Solution
In DirX Identity, users with the `dirxTOTPUser` object class enabled were unable to load target system (TS) configurations within the Identity GUI. The system previously attempted to reuse the initial provisioning session credentials to bind to the connectivity domain; however, because TOTP tokens are single-use and time-limited, these background bind attempts failed. This effectively prevented administrators from using multi-factor authentication while managing target system environments.	The solution introduces a dedicated login dialog that triggers when a user first accesses a target system container. This dialog prompts for both the password and a fresh TOTP token, allowing a valid authentication bind to the connectivity domain. The fix has been integrated into the `siemens.dxr.manager.Session` component to ensure full multi-factor authentication support across both provisioning and connectivity operations.

▾ *details SDX-1555*

The DirX Identity installer now automatically backs up and restores custom configurations, SSL certificates, and libraries during version upgrades. These enhancements, along with updated documentation on protected directories, ensure that user-specific modifications are preserved throughout the update process.

Problem	Solution
During upgrade installations (e.g., from 8.10 SP2 to 8.10.13), the installer was deleting custom files and folders—such as modified scripts in `tools/utilities` and configuration files in `client/conf`—without creating backups, logging the deletions, or providing clear warnings. This lack of transparency and protection for customizations forced users to manually restore files from their own backups and created uncertainty regarding which directories were safe for custom content.	Starting with version 8.10.15, the installer has been enhanced to automatically back up and restore "configurable content" before proceeding with the upgrade. A defined list of protected directories (including `/conf/`, `/ssl/`, and `/lib/java/custom/`) has been established, and a new environment variable (`DIRXIDENTITY_CUSTOMLIB_PATH`) allows users to store custom libraries in external locations. Additionally, the product documentation has been updated to clearly outline best practices for placing custom files to ensure they remain unaffected by future updates.

▾ *details SDX-1575*

When two permissions with group obligations updating the same user attribute were assigned or approved at the same time, only one group's value was written, leading to data inconsistencies in ATTRIBUTE1. The resolution corrects the multi-value handling in the service layer so that concurrent permission assignments now reliably merge all obligation values into the user attribute.

Problem	Solution
Concurrent assignment or approval of two permissions whose groups both had obligations updating the same user attribute (ATTRIBUTE1) resulted in only one group's value being written, causing repeated data inconsistencies in ATTRIBUTE1 in production.	The service layer logic for handling multi-valued user attributes was corrected (in `SvcNode.handleMultiValuesExtOpt` / `setVolatileProperty`) so that concurrent resolution of multiple permissions now reliably merges all obligation values into the target user attribute

▾ *details SDX-1625*

Users migrating scripts to GraalJS will no longer encounter PolyglotList type conversion errors when using standard JavaScript array methods. The system now correctly handles combined arrays, ensuring seamless compatibility between JavaScript objects and internal property setters.

Problem	Solution
During script migration to GraalJS, using the `concat()` method to combine results from `getStringValues()` with standard JavaScript arrays causes a `PolyglotException`. When the resulting object is passed to `setProperty()`, the engine identifies it as a `com.oracle.truffle.polyglot.PolyglotList` instead of the required Java type, leading to a "Invalid value type" warning and script failure.	The integration layer between GraalJS and the core application will be updated to automatically map Polyglot types to compatible Java types during property assignment. This ensures that intuitive JavaScript operations like array concatenation work natively without requiring manual conversion to Java-specific collections, maintaining script stability and reducing migration effort.

▾ *details SDX-1637*

The system now improves performance when evaluating groups with many members by limiting the attributes requested, preventing long-running LDAP operations.

Problem	Solution
In DirX Identity, the Privilege Resolution Workflow and ConsistencyAgent were experiencing severe performance degradation when interacting with LDAP groups containing a high volume of members (e.g., 250,000+). The root cause was a code path that performed full LDAP base-level searches requesting all attributes (*), resulting in massive 15MB+ data transfers per operation. This led to 13–17 second latencies per read, high LDAP server CPU utilization, and extreme delays in mass-assignment scenarios (e.g., 16 hours for 20,000 assignments).	The solution involves modifying the `SvcPermission` and `GroupDao` components to use a restricted attribute set during group evaluation. Instead of loading all attributes, the system now only requests the specific structural and state attributes required for match-rule evaluation and membership resolution, explicitly excluding large member lists like `uniqueMember` when they are not needed.

▾ *details SDX-1645*

This update resolves a critical issue where the Active Directory Real-Time workflow entered an infinite loop, causing log files to grow excessively up to 5GB. The fix prevents a NullPointerException within the LDAP connector’s sequential read process, ensuring stable workflow execution and disk space management.

Problem	Solution
Customers utilizing Active Directory Real-Time (RT) workflows experienced a severe system instability where a `java.lang.NullPointerException` in the `siemens.dxm.connector.ldap.enums.SequentialRead` class triggered an infinite logging loop. This behavior led to rapid disk space consumption—with log files reaching sizes of 5GB for a single thread—and required a manual Java Server restart to terminate the hanging process and clear the error state.	The software has been patched to improve the robustness of the LDAP connector's sequential read operations. By implementing proper null-value handling and terminating the iteration loop upon encountering unrecoverable exceptions, the system now prevents the "endless message" cycle. This ensures that workflows fail gracefully or skip problematic entries without impacting server performance or exhausting storage resources through excessive logging.

▾ *details SDX-1652*

DirX Identity now supports SSL/TLS encryption and user authentication for SMTP email services in version 8.9 SP3. This update enables secure communication with modern mail relays and includes fixes for SMTP object creation and icon display issues.

Problem	Solution
The customer's transition to a mandatory secure mail relay required SSL/TLS encryption and user authentication for all outgoing emails. While these features were available in newer versions (V8.10+), they were missing in the customer's current V8.9 SP3 environment, preventing secure email notifications within request workflows. Additionally, the initial hotfix introduced a NullPointerException during SMTP object creation and caused the SMTP service icon to disappear from the context menu.	The required SSL/TLS and authentication features were backported to DirX Identity V8.9 SP3 via a dedicated hotfix (8.9-SP3-71). The solution includes a robust fix for the `onEdit` script to prevent NullPointerExceptions during object initialization and restores the SMTP service icon by correcting the resource path extension. These improvements ensure full compatibility with modern secure mail relays while maintaining system stability.

▾ *details SDX-1735*

This update resolves an issue where role names were displayed as internal Java class identifiers instead of readable names within the Audit Manager. The fix ensures that privilege assignments are correctly serialized, allowing administrators to clearly identify assigned roles in audit logs.

Problem	Solution
In DirX Identity 8.10.14, users found that role names were not being correctly resolved in the Audit Manager's "Event Data" tab. Instead of a readable role name, the system displayed a technical Java class identifier (e.g., `siemens.dxm.history.PrivilegeAssignment@7c407d6b`). This occurred because the `PrivilegeAssignment` class lacked a `toString()` override, causing the audit serialization layer to default to a meaningless JVM runtime hash code that could not be recovered or mapped back to the original role.	The development team implemented a `toString()` override in the `PrivilegeAssignment` class to ensure that the role's Distinguished Name (DN) and the type of change (ADD/DELETE/MODIFY) are explicitly captured during audit record creation.

▾ *details SDX-1756*

This update ensures that Facet objects are correctly marked as faulty when their start date is later than their end date. The fix aligns Facet validation behavior with Identity objects, preventing inconsistent states during data imports and manual updates.

Problem	Solution
In DirX Identity, objects with a lifetime (start and end dates) must have a start date that precedes the end date. While Identity objects correctly trigger an error state when these dates are invalid, Facet objects were failing to do so. Specifically, when invalid dates were imported via the ServiceLayer or updated via the REST API, the Facet was not marked with the `dxrError` attribute, leading to incorrect state calculations and data inconsistency.	The issue was traced to the `SvcUserFacet.java` class, which lacked the necessary date validation calls found in its parent class. The fix involves adding explicit `checkDates()` calls within the `resolveUserGroupRelations()` and `checkAndResolve()` methods. This ensures that any date validation exceptions are properly caught and reflected in the object's status, maintaining consistency across all object types and interfaces.

▾ *details SDX-1761*

This update addresses the CVE-2026-34477 security vulnerability by upgrading Log4j dependencies to version **2.26.0**. The fix includes an update to ActiveMQ 5.19.10 to ensure all components, including the Message Broker, are protected.

Problem	Solution
DirX Identity version 8.10.15 was identified as vulnerable to CVE-2026-34477 due to its use of Log4j version 2.25.3. While most components could be updated easily, the Message Broker remained vulnerable because the then-current ActiveMQ version (5.19.7) still bundled the affected Log4j library.	The development team updated Log4j dependencies to version **2.26.0** across the platform. To fully resolve the issue within the Message Broker, the system was upgraded to ActiveMQ 5.19.10, ensuring a comprehensive fix for the vulnerability in the DirX Identity 8.10.17 release.

▾ *details SDX-1786*

The HCL Notes Connector has been updated to ensure reliable password changes and ID Vault synchronization by resolving a code defect that previously bypassed these operations. Additionally, the update removes the requirement for an undocumented system environment variable, simplifying the configuration for remote C Server deployments.

Problem	Solution
The HCL Notes Connector failed to perform password resets in the ID Vault when running on a remote C Server. Investigation revealed a code defect where a critical function (`ProcessLockbox`) contained an unconditional return statement that bypassed the actual synchronization logic. Furthermore, the system required an undocumented environment variable (`DXM_ENABLE_NOTES_PASSWORD_RESET`) to function, leading to configuration complexity and silent failures.	The code was corrected to remove the premature return and properly implement the ID Vault lockbox update logic within the `NotesAgent`. The requirement for the undocumented environment variable was removed to streamline deployment. These changes ensure that password updates are correctly propagated to the ID Vault and that the connector operates reliably without hidden configuration flags.

▾ *details SDX-1802*

Replacing a parameterized role assignment in a single transaction now correctly triggers separate removal and assignment workflows instead of a single modification workflow. This ensures that all required approval processes are properly initiated when role parameters change.

Problem	Solution
When a user removes a role assignment with a specific parameter and adds the same role with a different parameter in the same transaction, the system incorrectly identifies this as a single modification. Consequently, only one "Modification" approval workflow is triggered, rather than the expected "Removal" workflow for the old parameter and "Assignment" workflow for the new one. This behavior prevents proper oversight and auditing of role changes where parameters define distinct access levels.	The logic in `AttributedAssignmentComparatorImpl` was updated to specifically detect when only role parameters have changed during a direct assignment update. The system now intercepts these instances and splits the operation into two distinct orders: a deletion of the existing assignment and a new assignment for the updated parameters. This fix ensures that the correct independent workflows (Removal and Assignment) are started, and the assignment states (DELETE and ADD) are accurately reflected before the final approval activity.

▾ *details SDX-1826*

A security issue was identified where modifying a user attribute while an approval workflow is already active for that user causes the second change to be saved directly to the directory without authorization. To ensure all changes are properly governed, users should consolidate all attribute updates into a single save operation until a permanent fix is applied.

Problem	Solution
In DirX Identity, the system currently prevents multiple concurrent attribute-modify approval workflows for the same subject. When a user attempts to save a second attribute change while a previous approval workflow is still running, the duplicate-workflow prevention logic silently skips the new workflow trigger. Critically, because the attribute change is committed to the LDAP directory before the workflow start is attempted, the second modification is persisted without any administrative oversight or approval, creating a policy bypass.	The root cause is a hardcoded check in the `WorkflowStarterImpl` component that blocks new workflows if any "modify" instance is active for the subject. The recommended solution involves refining this logic to allow parallel workflows for independent attribute policies or implementing a queuing mechanism. Until a code fix is deployed, the Service Desk must be instructed to perform all necessary attribute changes in a single transaction (one "Save" click), which correctly triggers a single workflow encompassing all modifications.

▾ *details SDX-1827*

This update resolves a fatal Xerces parsing error that occurred during the startup of the Java Server and IdS-J Server reloads. The fix implements a defensive mechanism to strip invalid characters, such as Byte Order Marks (BOM) or leading whitespace, from XML configuration content before parsing.

Problem	Solution
During the migration from SLES-12 to SLES-15 and upgrading DirX Identity from version 8.9 to 8.10, customers encountered a fatal XML parsing error (`IDSJUTL043: Content is not allowed in prolog`) when starting the Java Server. This issue was caused by the XML parser encountering unexpected characters—specifically UTF-8 Byte Order Marks (BOM) or leading whitespace—in the `dxmContent` attributes of workflow fragments or referenced channel entries stored in LDAP. While these characters were invisible in many editors, they caused the Xerces parser to fail during runtime assembly of the workflow XML.	A code fix was applied to the `XmlConfigurationImpl.load(String content)` method within the `dirx-dxi-util` library. This defensive update automatically sanitizes XML content by stripping any leading BOM or whitespace before it reaches the parser. Additionally, the system now provides clearer diagnostic logging to identify empty or malformed content, preventing cryptic "prolog" errors and ensuring a more robust server startup process across different OS environments and LDAP configurations.

▾ *details SDX-1832*

This update resolves an issue where SAP Realtime Userhooks failed due to duplicate connector JAR files in the system classpath. By consolidating these files into a shared directory, the system now correctly initializes the SAP connection without registration conflicts.

Problem	Solution
Following an update to version 8.10.15, users encountered a `java.lang.IllegalStateException: DestinationDataProvider already registered` error when executing SAP Realtime Userhooks. This occurred because the `SapUM4Role.jar` was being deployed to both the shared library folder and the specific job framework folder. Since SAP JCo allows only one registration per JVM, the presence of duplicate JARs across different classloaders caused a conflict that prevented the establishment of SAP connections.	The build process was modified to ensure that connector JARs, specifically `SapUM4Role.jar`, are only deployed to the shared `confdb/common/lib` directory and are no longer copied into the `confdb/jobs/framework/lib` folder. This deduplication ensures a single, consistent class instance is loaded by the parent-first delegating classloader, satisfying SAP JCo's singleton requirements.

▾ *details SDX-1834*

A race condition in the Create Request Workflow caused SEVERE errors (rc: 20) and lost obligation attributes when assigning privileges with groups, because the resolution event fired prematurely on the temporary DN (`cn=SvcTemporary-uid-...`) while the Apply Change step still held the entry lock. From now on in case of an SvcTemporary object no resolve message will be sent.

As an improvement based on the use-case of this ticket a new "Batch processing of resources" checkbox on some Apply Change activity now consolidates all privilege assignments into a single modify-event, reducing the number of sent change-events.

Problem	Solution
During a Create RQWF, the Apply Change activity saved the object under a temporary DN and immediately triggered a resolution event via JMS. The Resolution Adapter on ActiveMQ attempted to write obligation attributes back to the same temporary DN, but the workflow still held the entry lock (~600 s). This race condition produced `EntryLockManager` warnings, SEVERE `OrderException` errors (rc: 20), and **lost obligation attributes** — group assignments were not retried after failure. Affected: DirX Identity 8.10.15, customer BWI, on customer side always reproducible with multiple privileges in one RQWF step.	Adding additional check to prevent sending resolve message in case of SvcTemporary objects. As an improvement based on the use-case of this ticket a new "Batch processing of resources" flag on the Apply Change activity consolidates all privilege assignments into a single modify-event (instead of one per privilege).

▾ *details SDX-1844*

A performance issue has been resolved where the system performed multiple redundant LDAP searches during user save operations if no attribute policies were defined. The policy cache now correctly handles empty results, significantly reducing server load and improving response times for attribute updates.

Problem	Solution
In DirX Identity, the `PolicyCacheImpl` component failed to correctly cache results when an LDAP search for attribute policies returned zero entries. Because the cache remained in an uninitialized state, every subsequent request to check for policies—which occurs for every modified attribute during a `StorageObject.save()` operation—triggered a new, redundant LDAP query. In environments with no active attribute policies, this resulted in dozens of unnecessary network calls per save, leading to measurable performance degradation and increased LDAP server load.	The fix involves updating the `fillCache()` method in `PolicyCacheImpl` to explicitly initialize the internal policy table to an empty map when no policies are found in the directory. This ensures the cache is marked as "loaded," preventing further LDAP lookups until the next scheduled refresh. This optimization has been implemented, ensuring stable performance even when attribute-based approval workflows are disabled or not configured.

▾ *details SDX-1856*

The Policy Agent has been updated to correctly handle LDAP filters containing special characters and hex escape sequences in INI configuration files. This fix ensures that characters like parentheses and spaces are no longer incorrectly replaced, allowing for

accurate rule processing and search results.

Problem	Solution
The Policy Agent was unable to find provision rules when the search filter in the INI configuration file contained LDAP hex escape sequences (e.g., `\29` for `)` or `\20` for a space). This occurred because the system unconditionally replaced all backslashes with forward slashes to handle Windows file paths, which corrupted valid LDAP filters and resulted in zero rules being processed.	The fix involved replacing the blanket backslash substitution with a more sophisticated `AgentIniReader` that correctly handles INI file parsing. By improving how the configuration is loaded, the system now preserves backslash characters required for LDAP hex escapes, allowing complex filters to function as expected across DirX Identity versions 8.9, 8.10, and 9.0.

▾ *details SDX-1874*

This update resolves a logging defect where ADS realtime workflows incorrectly appeared to have long runtimes due to reused worker threads retaining previous activity contexts. By ensuring the logging context is initialized before starting new activities, the system now provides accurate duration statistics and eliminates misleading performance reports.

Problem	Solution
Users reported that individual tasks in the Java logs for the `ident_ads_realtime_bw` workflow appeared to have extremely long runtimes, sometimes exceeding 60 to 90 minutes, compared to the expected 1–2 seconds. This led to concerns that ADS worker threads were being exhausted, potentially delaying event-based processing. However, detailed log analysis revealed that the workflows were actually completing in less than 6 seconds, and the inflated durations were a result of a logging and statistics attribution defect in the `logANT` tool and the `ActivityTask` class.	The investigation identified that `ActivityTask.run` logged a new activity's start before replacing the worker thread's previous logging context. Consequently, the `logANT` tool associated the new activity's start time with the previous (already completed) workflow ID, artificially extending its reported duration by the gap between tasks. The solution involves reordering the code to initialize the activity's logging context *before* emitting the `INF_ACTIVITY_START` message. This ensures that statistics accurately reflect actual execution times and prevents the false appearance of thread occupancy.

▾ *details SDX-1886*

The ConsistencyCheck workflow has been optimized to eliminate unnecessary LDAP lock and unlock operations for users without privilege changes. This improvement significantly reduces directory load by performing only essential attribute updates when no modifications are required.

Problem	Solution
The `ConsistencyCheck` workflow currently performs a high volume of redundant LDAP operations, including multiple lock/unlock cycles and attribute modifications (setting and resetting `dxrTBA`), even when no actual privilege changes are necessary. Analysis revealed that for a single unchanged user, up to 13 LDAP operations were being executed, with only one being meaningful (`dxrlastresolutionstarttime`). This inefficiency creates significant unnecessary load on the directory, especially in large environments, where it can result in over a million wasted operations per run.	The solution implements a "short-circuit" logic within the `ConsistencyCheck` workflow to handle unchanged users more efficiently. Key optimizations include: • **Conditional Locking**: Modifying `checkSingleObject()` and `checkAndResolve()` to only initiate a lock when a tangible change (e.g., removing an expired assignment) is detected. • **Redundancy Reduction**: Eliminating the redundant cycle of setting `dxrTBA=TRUE` only to immediately reset it to FALSE for users requiring no updates. • **Single-Operation Updates**: For users with no privilege changes, the workflow now performs a single LDAP update to set the `dxrlastresolutionstarttime` and reset the `dxrTBA` flag, bypassing the entire pessimistic lock/unlock sequence. These changes reduce the number of LDAP operations for unchanged users by approximately 88%, drastically improving overall system performance.

▾ *details SDX-1887*

This update resolves a performance issue where object creation workflows in the portal would time out due to excessive exclusive locking by the REST service. The fix introduces a lock-free polling mechanism and optimized retry intervals, significantly reducing typical processing times from over 30 seconds to under 6 seconds.

Problem	Solution
When creating new objects in the portal, the REST service repeatedly requested exclusive locks on the workflow engine. This caused a resource contention where the engine could not obtain the necessary lock, leading to multiple 10-second retries and frequent 30-second portal timeouts for users.	The REST service was updated to perform initial status checks without taking an exclusive lock, and the polling frequency was increased from 3000ms to 750ms. These changes eliminate the lock-race condition, ensuring the engine can process tasks immediately and reducing overall transaction times to approximately 4–6 seconds.

▾ *details SDX-1898*

We have resolved an issue where Web Center forms incorrectly generated empty table

columns that disrupted page alignment. This fix ensures consistent layout rendering across all forms using standard renderers.

Problem	Solution
Following an upgrade to DirX Identity 9.0.1, customers observed inconsistent HTML rendering in Web Center forms. Specifically, when using the "empty" label renderer, the system failed to generate the corresponding table cell (`<td>`) because the template was stripped of whitespace during processing. This caused the remaining content to shift and misalign, creating unnecessary columns that disrupted the overall page layout across the application.	The `emptyField.htm` template was updated to include a non-breaking space ( ) that survives the trimming process, ensuring the label cell is always rendered and the table structure remains intact. This fix stabilizes the UI layout and prevents content shifting, with the resolution included in versions 8.10.17 and 9.0.3.

▾ *details SDX-1901*

This update addresses an issue where deleting a permission could leave broken references on user identities, leading to resolution errors. No fix delivered, issue should have been solved on customer side.

Problem	Solution
When a permission is deleted using the `removeIncomingAssignments()` API method, the system correctly removes assignment objects and facet-level links but fails to clean up Level 2 derived attributes (such as `dxrInheritedUserFacetPrivilegeLink` and `dxrPrivilegesGrantedLink`) on the user identity. These stale links cause privilege resolution to fail with errors (SVC844/SVC819) because the system attempts to load a permission object that no longer exists in the repository.	There is no bug in the code of the product. Customer was advised to change his custom code by not deleting the permission object immediately and let time the asynchronous resolution to remove it from the concerned objects.

▾ *details SDX-1909*

A fix has been implemented to resolve an issue where the secondary C-Server would stop processing workflows due to a "Thread Local storage limit reached" error caused by repeated ActiveMQ reconnection attempts. The update ensures that thread handles are properly released during reconnection cycles, preventing resource exhaustion and maintaining stable workflow execution even after network interruptions.

Problem	Solution
In environments with a secondary DirX Identity C-Server, network interruptions or connectivity issues with the main server's message broker can lead to a complete halt of workflow processing. The secondary C-Server repeatedly attempts to reconnect to the ActiveMQ broker, but due to a resource leak in the reconnection logic, it fails to release internal thread handles. Over time, this exhausts the operating system's "Thread Local Storage" (TLS) limit, resulting in the error message `cms::CMSException: Thread Local storage limit reached`. Once this limit is hit, the C-Server process can no longer initiate any new tasks, including scheduled or manually started workflows, requiring a full service restart to restore functionality.	A fix has been implemented in the DirX Identity C-Server (`dxmmsssvr.exe`) to ensure proper resource management during network reconnection cycles. The ActiveMQ subscriber logic was updated to explicitly release thread handles (`CContext::releaseAMQThreadHandle()`) on all exit paths during reconnection attempts. This prevents the accumulation of stale thread-local storage registrations, ensuring that the system remains stable and continues to process workflows even after experiencing transient network failures. Until these updates are applied, periodically restarting the secondary C-Server remains the recommended workaround to reset the resource pool.

▾ *details SDX-1911*

This update ensures that virtual attributes calculated via GraalJS scripts are correctly rendered as string arrays in the Web Center interface. Users no longer need to manually convert script return values to Java string arrays to avoid rendering errors.

Problem	Solution
When using GraalJS scripts to define virtual attributes (e.g., filtered group lists) in DirX Identity, the Web Center fails to render the results correctly. While the DXI Manager handles the GraalJS `Object[]` return type, the Web Center requires an explicit `String[]` type, leading to "Renderer missing" errors or incorrect data display (e.g., `L[java.lang.Object…`) unless manual conversion is performed within the script.	The solution involves enhancing the storage layer (`StorageObject.convertPolyglotValue`) to automatically convert polyglot return values from GraalVM into the expected Java types defined in the property description. This ensures consistency between DXI Manager and Web Center, allowing standard renderers to process script outputs without requiring developers to add explicit Java conversion logic in their JavaScript code.

▾ *details SDX-1914*

The UidConsistencyCheck workflow has been enhanced to provide detailed diagnostic information when it fails to save newly generated UIDs in DirX Identity. This update ensures that the exact LDAP error codes and server messages are captured in the logs, allowing for faster identification of underlying permission or schema issues.

Problem	Solution
The `UidConsistencyCheck` Java workflow in DirX Identity fails to save newly generated `dxrUid `values for entries where they are missing. While the workflow correctly identifies entries with missing UIDs and generates new ones, the subsequent LDAP modification fails with a generic "error result" message in the logs. This lack of diagnostic detail prevents administrators from identifying the root cause—such as insufficient LDAP write permissions for the bind profile or schema restrictions—making it impossible to resolve the underlying data inconsistency.	To resolve this diagnostic gap, the `UidConsistencyCheckController` has been enhanced to provide detailed error reporting. The code was updated to specifically catch `LDAPException` during the modification process and log the exact LDAP result code and server error message. This improvement, released in versions **8.10.17** and **9.0.3**, allows for immediate identification of the failure reason (e.g., ACL restrictions). Additionally, a new configuration property `additionalTypes2Exclude `is proposed to allow customers to exclude specific structural containers from the check, preventing false positives for entries that are not intended to carry a `dxrUid`.

▾ *details SDX-1916*

Following the upgrade to version 8.10.15, an issue was identified where custom Java connectors could drop connections or fail to execute modify requests due to duplicate JAR files being deployed across different library folders. This regression has been resolved by ensuring proper classloader handling and removing redundant library copies, with fixes included in versions 8.10.17 and 9.0.3.

Problem	Solution
Following an upgrade to DirX Identity version 8.10.15, custom Java connectors (specifically the GCMS connector) experience connection failures during real-time provisioning. While the initial search request completes successfully, the subsequent modify request fails with a `java.net.ConnectException: Connection refused`. This issue is caused by a regression in the 8.10.15 build process that results in duplicate connector JAR files being deployed across different library folders (`confdb/common/lib` and `confdb/jobs/framework/lib`). This duplication leads to classloader conflicts where shared singleton states or connection managers become inaccessible or misconfigured between operations, rendering the connector unusable for updates.	The issue is resolved by ensuring that connector JAR files and their dependencies are not duplicated across the server's library directories. To restore functionality, customers should manually remove any duplicate connector JARs from the `confdb/jobs/framework/lib` directory, keeping only the version in `confdb/common/lib`, and then restart the IDS-J server. This alignment of the deployment structure prevents classloader conflicts and allows the connector to maintain a stable connection between search and modify operations. Permanent fixes have been integrated into versions 8.10.17 and 9.0.3 to prevent this dual-deployment pattern in future builds.

▾ *details SDX-1918*

A race condition during concurrent processing could cause master-derived attributes to be transiently cleared on target accounts due to stale identity data. This update introduces a performance-optimized refresh mechanism that ensures account updates always use the most recent identity information from storage.

Problem	Solution
In high-concurrency environments, target system accounts experienced an "add-remove-add" oscillation for master-derived attributes. This occurred because the multi-threaded `ResolutionAdapter` could operate on an obsolete in-memory snapshot of an Identity while a parallel workflow was committing changes to the same master attributes. Because these processes used different locking scopes (LDAP-locking vs. Resolution-locking), the stale data from the resolution pass would transiently overwrite or clear the correctly committed values on the account.	The solution implements a gated, performance-conscious refresh mechanism in the `SvcUser` resolution logic. Before analyzing changes for groups and accounts, the system now performs a lightweight `modifyTimestamp` check to detect if the Identity has been modified in LDAP since it was first read for resolution. If a concurrent modification is detected, the Identity object is refreshed from storage to ensure the latest master attributes are propagated to the accounts, while sequential executions remain unaffected by additional LDAP read overhead.

▾ *details SDX-1919*

Administrators can now configure the number of resolution listener threads directly on individual J-Server instances, rather than only at the domain level. This enhancement

significantly reduces infrastructure overhead by allowing high-performance servers to handle more concurrent resolution tasks without requiring multiple service deployments

Problem	Solution
Previously, the "Number of resolution listener per Server" setting was globally defined at the domain level. In high-scale environments, increasing the number of resolution threads on a specific remote server required deploying multiple J-Server instances (e.g., eight J-Servers to achieve 64 threads if the domain was set to eight). This created a massive administrative burden for installation, maintenance, and operational monitoring, as well as inefficient resource utilization.	A new "Resolution Adapter" tab has been introduced in both the Domain and J-Server instance configurations, allowing for instance-specific overrides. The system now follows a clear precedence logic: J-Server settings take priority over Domain settings, which in turn override hard-coded defaults. This allows a single J-Server to be configured with a high thread count (e.g., 64 threads), reducing the required number of managed instances by up to 87.5% in the described use case and simplifying overall system architecture.

▾ *details SDX-1926*

Resolved an issue where the Group Provisioning Rules tab incorrectly displayed a file path instead of the intended configuration content. This fix ensures that provisioning rules are correctly loaded and visible within the user interface.

Problem	Solution
In DirX Identity 8.10.16, users encountered an "Error while processing BML file" when accessing the Provisioning Rules tab for groups. The root cause was a syntax error (an extra space) in the factory-data LDIF file, which caused the system to store the literal file path string instead of importing the actual BML content.	The syntax error in the `TS_Default.ldif` template has been corrected to ensure proper file indirection during provisioning. For existing environments, a data repair LDIF file has been provided to update the affected directory entries with the correct BML content, restoring full functionality to the Provisioning Rules tab.

▾ *details SDX-1934*

The UidConsistencyCheck-Workflow now correctly identifies and uses domain-specific message queues for notifications instead of defaulting to a single global queue. This ensures that email notifications are properly processed and delivered in multi-domain environments where the "Include domain into Topic" flag is active.

Problem	Solution
In multi-domain environments where the "Include domain into Topic" flag was active, the UidConsistencyCheck-Workflow defaulted to a single global message queue. This caused failures in identifying the correct domain-specific queues, leading to potential processing delays or delivery failures for email notifications.	The workflow logic was modified to correctly identify and route notifications to the appropriate domain-specific message queues. This change ensures full compatibility with multi-domain configurations and guarantees that notifications are handled by the intended messaging infrastructure.

▾ *details SDX-1944*

Selecting the "(None)" option in a tagged property now correctly clears the attribute instead of storing the literal string. The fix ensures that the empty-value marker is recognized regardless of casing or surrounding whitespace, aligning the behavior with product documentation.

Problem	Solution
A bug in the backend string comparison logic caused the special tag value `(None)` to be handled incorrectly. While the documentation specifies `(None)` (capital 'N') as the marker to clear an attribute, the code performed a case-sensitive comparison against a lowercase hardcoded string `(none)`. As a result, the system failed to recognize the "empty" selection, treating it as a standard string value and persisting the text "(None)" into the database/LDAP attribute instead of deleting it.	The resolution involves updating `AttributeConfigMapper.java` to use case-insensitive string comparison (`equalsIgnoreCase`) and trimming whitespace when evaluating tag values. This ensures that `(None)`, `(none)`, or variations are correctly identified as the "no value" selection. When this selection is made, the backend now properly triggers the deletion of the attribute as intended. The fix is implemented in versions **8.10.17** and **9.0.4**. Note that existing data containing the literal string "(None)" must be cleaned up manually, as the fix is not retroactive.

▾ *details SDX-1947*

The Identity Manager has been updated to ensure that workflows are correctly displayed and accessible in the Provisioning view for all target systems. This fix improves the robustness of connectivity actions and provides clearer error messaging to help resolve configuration issues related to workflow lines.

Problem	Solution
Following an update to version 8.10.16, users encountered an issue where workflows were no longer appearing in the Provisioning View when attempting to start them manually for a target system. This was particularly critical for clustered workflows, which can only be initiated through this view. Investigation revealed that the UI failed to build the workflow submenu if it could not identify exactly one workflow line associated with a connected directory, resulting in "ambiguous" or "missing" workflow line errors in the logs.	The developer implemented a fix in the `dxrManager.jar` (specifically within the `ActionConnectivityWrapper` class) to make the Manager's connectivity actions more robust and fault-tolerant. This update ensures that workflows are correctly resolved even in complex configurations and provides clearer, more actionable error messages in the UI to help administrators identify and resolve underlying data or configuration issues.

▾ *details SDX-1951*

The default object descriptor for workflow instances has been updated to include the `dxmSpecificAttributes(name)` property. This ensures that custom storage configurations for workflow names are preserved during patch installations and no longer require manual restoration.

Problem	Solution
In DirX Identity, the system persists the workflow definition name in the LDAP attribute `dxmSpecificAttributes(name)`. However, the default object descriptor (`WorkflowInstance.xml`) shipped with the product did not explicitly declare this property. As a result, customers who manually added this descriptor to enable specific search or display functionality found their changes overwritten and reverted every time a product patch or update was applied.	The solution involves updating the standard `dxrRequestWorkflowInstance` object descriptor in the product's factory data to include a `StoragePropertyDescriptor` for `dxmSpecificAttributes(name)`. By incorporating this as a default product property, the configuration remains stable across updates, eliminating the need for manual customer workarounds.

▾ *details SDX-1954*

The HCL Notes password change process has been improved to provide detailed diagnostic information when a failure occurs during the ID Vault reset. Instead of a generic error message, the system now propagates the specific Domino status code and error text to facilitate faster troubleshooting and resolution.

Problem	Solution
Following recent updates to the HCL Notes password-change workflow, failures during the `SECidvResetUserPassword()` process were being reported with a generic "JOIN536" error or a vague "'ProcessLockbox()' failed" message. This lack of detail masked the underlying Domino-side cause, such as permission gaps or vault configuration issues, making it difficult for support teams and customers to diagnose and resolve environment-specific failures.	The solution involves modifying the `ProcessLockbox()` function in both the C connector server and the NotesAgent to capture and propagate detailed Domino status codes and error text. By adding an error detail out-parameter to the internal API calls, the system now surfaces the exact failure reason in the exception messages and logs.

▾ *details SDX-1958*

This update resolves a critical issue where paged LDAP searches could enter an infinite loop and flood system logs when encountering a size limit error. The system now correctly terminates the search process after a fatal error, preventing excessive memory and disk space consumption.

Problem	Solution
When a paged LDAP search in DirX Identity encounters a fatal error, such as `SIZE_LIMIT_EXCEEDED`, the system fails to clear the error state. This causes the search iterator to incorrectly report that more elements are available, leading to an infinite loop of `NoSuchElementException` errors. This loop floods system logs, consumes significant CPU and memory, and can eventually fill up the server's disk space.	The error handling logic in the `PartialBase` and `EnumBase` classes has been refactored to ensure that fatal exceptions are surfaced exactly once before terminating the enumeration. The fix includes clearing the stored exception after it is reported, replacing direct stack trace printing with controlled logging, and ensuring that LDAP referrals are handled as skippable events rather than fatal errors. These changes stabilize the system's behavior during large-scale directory searches and prevent resource exhaustion.

▾ *details SDX-1962*

A fix has been implemented to ensure that truststore password entries in configuration files are preserved during patch installations and upgrades. This prevents service disruptions for WebCenter SSO and Kerberos authentication that previously occurred when these entries were inadvertently removed.

Problem	Solution
During DirX Identity patch installations or upgrades, the configuration process was overwriting or deleting the `truststore` entry in `ssl/password.properties` and `private/password.properties`. This occurred because the installer's cleanup logic was designed to perform a full refresh of files, but it failed to account for existing truststore configurations. The removal of these entries caused critical failures in WebCenter Single Sign-On (SSO) and Kerberos authentication, as the system could no longer validate secure connections to the Request Workflow Server (idsJ).	The configuration logic in the `[PRV] IdS-J Server` component has been updated to check for existing `truststore` passwords before applying updates. The system now explicitly preserves these entries if they are present in the property files, ensuring that custom security configurations remain intact across versions.

▾ *details SDX-1968*

A boundary condition error in the workflow engine was corrected to ensure that administrator notification emails are sent immediately after a password synchronization failure. Previously, the system incorrectly postponed these notifications when the maximum number of retry attempts was reached.

Problem	Solution
When a password change fails in the SAP UM SetPassword-Java-Workflow due to SAP rule violations (e.g., invalid characters like ? or !), the system was failing to send the expected error notification email to administrators. h4	The root cause was identified as an "off-by-one" boundary check in the `WorkflowTask.calculateState()` method within the `dirx-dxi-idsj-server-core` library. The logic used `if (retryCount ⇐ retryLimit)` to decide whether to postpone the error activity, which remained true even when the counts were equal (i.e., retries exhausted).

▾ *details SDX-1996*

An issue was resolved where the Provisioning Rule tab for group objects failed to display correctly due to a configuration error. This fix ensures that provisioning rules for groups are now visible and accessible in the user interface as expected.

Problem	Solution
Following a version update, users were unable to view provisioning rules for group objects, although rules for permissions and roles remained visible. This was caused by an error while processing a specific BML file (`GroupProvisioningRules.bml`), which contained an incorrect reference, leading to a failure in rendering the Provisioning Rule tab.	The development team identified a typo in the LDIF configuration that caused the BML processing error. The configuration has been corrected to ensure the group provisioning rules are properly loaded and displayed, eliminating the need for manual workarounds.

▾ *details SDX-1997*

A fix has been implemented to prevent the Identity Manager GUI from automatically setting the `dxrStartDate` attribute to the current date when saving user objects. This ensures that existing user records, particularly those marked for deletion, can be edited without triggering date-validation errors.

Problem	Solution
In DirX Identity (starting with version 8.10.15/16), the Identity Manager GUI was automatically populating the `dxrStartDate` attribute with the current system date whenever a user object was saved, even if the field was previously empty. This behavior caused critical validation failures for user objects with a state of `TBDEL` (To Be Deleted) and an existing `dxrEndDate` in the past. In these cases, the GUI would throw an error stating that the start date was greater than the end date, effectively preventing administrators from editing or managing these records.	The logic within the Identity Manager GUI component has been corrected to ensure it no longer unilaterally assigns values to the `dxrStartDate` attribute during save operations. The system now preserves the empty state of the attribute if no value is explicitly provided by the user, restoring the original functionality and allowing records with historical end dates to be processed correctly.

▾ *details SDX-2020*

Updating to SAP JCo version 3.1.14 or higher requires an explicit configuration to maintain username and password authentication when SNC is enabled. A new property, `snc_sso=false`, has been introduced to ensure the connector correctly transmits login credentials to the SAP backend.

Problem	Solution
After updating the SAP Java Connector (JCo) to version 3.1.14, the SAPUMAgent failed to log in to SAP systems when Secure Network Communications (SNC) was active. This occurred because newer JCo versions default to Single Sign-On (SSO) via certificates when SNC is enabled, preventing the transmission of provided username and password credentials.	The `SapUM4Role.jar` was updated to support the `snc_sso` property, allowing users to explicitly disable SSO and force username/password authentication over SNC. Additionally, workflow templates were updated via .ldif files to include this new configuration option, enabling successful connections with the latest SAP JCo versions.

▾ *details SDX-2021*

The log4j library has been updated to version 2.26.1 to meet enhanced security requirements and address vulnerabilities identified in previous versions. This update is included in DirX Identity version 8.10.17, ensuring all components, including the Message Broker, utilize the latest compliant logging framework.

Problem	Solution
* The log4j components (versions 2.25.3 and 2.26.0) included in DirX Identity version 8.10.16.2130 do not meet the security requirements of the customer (Volkswagen Financial Services AG). Their vulnerability reports require log4j to be at version 2.25.5 or 2.26.1 at a minimum to address potential security risks.	* The log4j libraries have been updated to version 2.26.1 across the product. This includes updating the integrated ActiveMQ component to version 5.19.10 (which bundles log4j 2.26.1) and upgrading all other standalone log4j instances to 2.26.1. These security improvements are officially delivered with DirX Identity version 8.10.17 (Build 2379).

▾ *details SDX-2024*

Resolved an issue where mass provisioning caused ActiveMQ to exceed its maximum client connection limit, leading to failed data synchronization. The fix addresses resource leaks in the messaging layer to ensure connections are properly closed during error recovery.

Problem	Solution
During large-scale data imports (300,000+ records), the system exhausts the available ActiveMQ connection pool (limit 1,000). This results in `JMSD114` errors, preventing the creation of message publishers and causing significant data inconsistencies, with approximately 80,000 records failing to provision.	The solution involves patching the Identity Java Server to fix resource leaks in the JMS publisher and listener retry logic. By ensuring that connections are strictly terminated and cleaned up during transport failures, the system maintains stable connection counts within configured limits even under heavy provisioning loads.

▾ *details SDX-2035*

This update resolves a recurring SVC904 error that occurred when processing obligations for nested group assignments without a valid account context. The system now correctly identifies and handles these scenarios, preventing unnecessary resolution failures and identity inconsistencies.

Problem	Solution
Users assigned to nested groups in Active Directory were triggering recurring SEVERE SVC904 errors during synchronization. This occurred because the DirX resolution engine attempted to apply obligations requiring a `SvcTSAccount` context to nested assignments which, by design, do not have associated account objects. This resulted in identities being flagged as inconsistent and blocked further automated resolution.	The obligation handling logic was enhanced to tolerate missing account contexts specifically for nested assignments. A new internal check, `isMissingAccountTolerated()`, was implemented to allow the system to skip account-based properties for nested groups while maintaining standard error reporting for primary assignments. This ensures smooth synchronization for complex group hierarchies without compromising data integrity.

▾ *details SDX-2036*

A regression in DirX version 8.10.16+2130 causes SCIM PATCH operations to fail with a 400 Bad Request if the naming attribute 'cn' is included without changes. This update ensures that unchanged naming attributes are ignored during multi-attribute updates to maintain compatibility with existing client applications.

Problem	Solution
Following the update to DirX version 8.10.16+2130 (post-8.10.SP1), the SCIM REST API incorrectly rejects PATCH requests that include the `cn` attribute if its value has not changed. The system returns a `400 Bad Request` error with the detail: *"Naming attribute 'cn' can only be changed in a stand-alone operation."*	The REST API logic will be adjusted to validate whether the provided `cn` value differs from the existing value in the directory. If the value is identical, the operation will proceed by ignoring the redundant `cn` update rather than throwing an error. This restoration of legacy behavior allows applications to perform multi-attribute PATCH operations without requiring immediate code changes to strip unchanged naming attributes from their requests.

▾ *details SDX-2043*

The InitialConfig wizard now preserves existing User-Policy SearchLimit settings instead of resetting them to default values during configuration. This update ensures that custom search limits, such as those required for large group queries, remain intact after running the wizard.

Problem	Solution
When running the InitialConfig wizard (e.g., to switch from non-secure to secure LDAP), the tool automatically resets the User-Policy (USP) SearchLimit to its default value. This overwrites critical custom configurations, such as the 32768 size limit required for `DXMC=DirXmetahub/DXMC=Groups/CN=Read`, leading to potential query failures or performance issues for DomainAdmin operations.	The configuration logic has been updated to check for existing User-Policy and SearchLimit settings before applying changes. The wizard will now only set these values if they do not already exist, ensuring that pre-configured search limits and subtree definitions are preserved during the initial configuration or update process.

▾ *details SDX-2059*

The CheckConsistency workflow has been updated to ensure it uses real-time data when recalculating account attributes, preventing accidental deletion of user rights. This fix addresses an issue where long-running maintenance tasks could overwrite recent permission changes with outdated information.

Problem	Solution
The `CheckConsistency` workflow, designed to ensure data integrity, is causing data loss in Extranet target system accounts. Specifically, the `dxrOptions` attribute (which stores user rights like `IAMxnetBw-Nutzergruppe-1`) is being deleted from account objects. This occurs because the workflow, which can run for several days, appears to use a "snapshot" or stale search result from its start time. If a user is granted a right *after* the workflow starts but *before* it processes that specific user, the workflow recalculates the attribute based on the old data (where the right was missing) and performs a `MODIFY/delete` operation, effectively reverting the recent update.	To prevent this inconsistency, the workflow's data retrieval mechanism must be modified to fetch the most current state of the object and its linked attributes (specifically `$varBwPrivilegesGrantedLink` mastered by `dxrUserLink.dxrPrivilegesGrantedLink`) immediately before the recalculation script `calcDxrOPxnetRollenIAMBwverwaltet` executes. • **Technical Fix:** Implement a "fresh read" policy within the `CheckConsistency` workflow to bypass any cached search results for the target objects. • **Mitigation:** Until the fix is deployed in version 8.10.17, avoid running the `CheckConsistency` workflow during periods of high administrative activity or reduce the scope of the workflow to smaller batches to minimize the window for stale data conflicts.

▾ *details SDX-2067*

The JDBC-Agent now correctly exports attributes of type DATE when synchronizing with Microsoft SQL Server databases. This fix ensures that date fields, such as hire or birth

dates, are no longer skipped during the data export process.

Problem	Solution
When using the JDBC-Agent with the Microsoft SQL JDBC driver (v13.6.0) to synchronize a MS-SQL database, fields specifically of the type `DATE` (e.g., `HIRE_DATE`, `FIRE_DATE`) were not being exported to the target system. Investigation revealed that while the agent could read the values, the internal conversion logic returned a null value for the `DATE` type, causing these attributes to be omitted from the final search response.	The conversion logic within the JDBC-Agent was updated to properly handle `DATE` types by implementing a DATE-to-DSML string conversion. The agent now uses the configured date format or a default serialization to ensure these values are correctly processed and included in the export, maintaining parity with the behavior of other database drivers like Oracle.

▾ *details SDX-2081*

Updating log4j independently of the product version is not recommended due to numerous internal dependencies and potential stability risks. Customers should instead update to DirX Identity 8.10.17, which includes the verified log4j 2.26.1 update.

Problem	Solution
A customer requested a short-term update of the log4j library to a newer version without performing a full DirX Identity product update.	The development team analyzed the feasibility and concluded that a manual update is too risky due to at least 50 hardcoded version references in JAR manifests and scripts. The official solution is the release of DirX Identity 8.10.17 (planned for late November 2026), which integrates log4j 2.26.1.

▾ *details SDX-2083*

Manual updates to the Log4j library are not recommended due to complex internal dependencies and potential stability risks. Customers should instead perform a standard product update to ensure all components and references are correctly verified.

Problem	Solution
A vulnerability was identified in the `log4j-api-2.17.1` library within DirX Identity version 8.10.10. The customer inquired whether it is possible to manually update only the Log4j library to a newer version without applying a full product patch or update.	While technically possible to replace JAR files, the library is referenced in over 50 locations across manifest files, scripts, and text files, making manual replacement high-risk and difficult to verify. The recommended solution is to apply the standard product update, which includes the verified library upgrade alongside other product improvements, ensuring system stability and full vulnerability remediation.

▾ *details SDX-2091*

Resolved an issue where modifying objects with spaces in their Distinguished Name (DN) caused internal server errors during URI generation. The REST service now correctly encodes special characters in the resource location attribute to ensure compatibility with web standards.

Problem	Solution
Following the update to DirX Identity 8.10.16+2130, the REST API fails to process certain requests for objects whose Distinguished Names (DN) contain spaces (e.g., "cn=VCD Accounts"). While the underlying operation (such as a PATCH or POST) succeeds in the database, the `ResponseHandler` attempts to construct a `meta.location` URI using the unencoded DN. This triggers a `java.net.URISyntaxException: Illegal character in path`, preventing the client from receiving a clean response and cluttering server logs with severe errors.	The fix involves updating the class `com.dirxcloud.dxi.rest.scim.attributes.RefHandler` to properly escape special characters and spaces. By applying URL encoding to the path segments derived from the object's DN or container name, the service ensures that the generated "location" attribute is a valid URI. This change restores full functionality for REST operations on entries within containers that use non-alphanumeric characters in their naming convention.

▾ *details SDX-2094*

A fix has been implemented to ensure that the JavaScriptActionRunner correctly updates its storage context when reused with different sessions. This prevents errors where scripts would attempt to use a disposed session when executing consistency rules.

Problem	Solution
When using `ConsistencyRuleProvider` to execute rules in custom code, the `JavaScriptActionRunner` fails to update its internal `UserStorage` and `RuleStorage` references when a new session is provided. It incorrectly caches the storage from the first session; if that session is disposed and a second session is used, the runner attempts to access the disposed session, resulting in a `StorageException` (STG616) and "StorageLDAPConnection is null" warnings, even if the target object exists.	The `JavaScriptActionRunner` was modified to refresh its context from the `RuleContext` on every execution. A new internal method, `refreshContextFromRuleContext()`, was introduced to synchronize the simulation state and storage references (User and Rule storage) before the script runs. This ensures that the runner always uses the active session's storage, even when the provider is reused.

▾ *details SDX-2100*

An assessment was conducted to determine the impact of the Windows Authenticode signature verification vulnerability (CVE-2013-3900) on DirX products. It was confirmed that DirX Directory is not affected as it utilizes independent signature files rather than the Windows Authenticode format.

Problem	Solution
The customer requested a verification of whether DirX Identity (DXI) and DirX Directory (DXD) are impacted by the mitigation of vulnerability CVE-2013-3900. This vulnerability involves changes to how Windows Authenticode verifies signatures for executable files (.exe) and dynamic link libraries (.dll).	Technical analysis confirmed that DirX Directory (DXD) is not affected by this change. The product uses OpenSSL to generate separate `.sig` signature files for its binaries and does not rely on the Windows Authenticode signature verification mechanism (WinVerifyTrust) targeted by this vulnerability.

1.2. DirX Identity 8.10.16

Customers benefit from the following fixes of the 8.10.16+2130 patch:

Ticket ID	Affected Version	Domain	Summary
SDX-1907	8.10.16	Provisioning, JavaServer	Fix for JavaServer thread leak in DirX Identity 8.10.16+2130.

▾ *details SDX-1907*

This update resolves a critical issue where JavaServer threads would accumulate indefinitely following a service restart or connection hiccup. The fix ensures proper cleanup of JMS sessions, restoring system stability and preventing potential service crashes due to resource exhaustion.

Problem	Solution
After upgrading to DirX Identity version 8.10.16, customers observed an unbounded growth in Java threads within the JavaServer processes (increasing from ~3,000 to over 42,000 threads in 12 hours). This was caused by a regression in the ResolutionAdapterManager where a transition to a shared JMS connection model failed to explicitly close individual listener sessions during reconnect cycles. Consequently, each reconnection attempt leaked ActiveMQ dispatch threads, leading to high resource consumption and eventual system instability or crashes.	The following corrective actions have been implemented: • **Explicit Session Management**: The ResolutionAdapterManager has been updated to iterate through all active jmsSessions and explicitly close each session prior to terminating the shared connection. • **Enhanced Error Logging**: The error handling logic was revised to log JMSException occurrences during the close sequence instead of suppressing them, providing better visibility into potential transport failures. • **Automated Verification**: A new test suite (TestResolutionAdapterManagerSessionCleanup) was added to verify that all sessions are successfully closed even in scenarios where the shared connection termination fails. The fix is scheduled for release in versions 8.10.16+2130 and 9.0.1HF1.

1.3. DirX Identity 8.10.16

Customers benefit from the following fixes of the 8.10.16+2127 patch:

Ticket ID	Affected Version	Domain	Summary
SDX-1575	8.10.12	Resolution Service	Fix data inconsistency when concurrently assigning permissions with group obligations.
SDX-1645	8.10.12	Provisioning	Fix for Infinite Log Growth and NullPointerException in SequentialRead.
SDX-1697	8.10.13	Provisioning	Fix LDAP Bind Authentication Issues When Using Java Keystores.
SDX-1628	8.10.12	Privilege Resolution, REST API	Optimizing REST API Performance by Improving LDAP Group Membership Queries
SDX-1622	8.10.13	Identity Management	Suppress invalid group errors when dxrNoWarningIfNoMatch flag is TRUE

Ticket ID	Affected Version	Domain	Summary
SDX-1759	8.10.15	Provisioning	Fix SAP account creation error with CombinedRoleProfileSubsystem validity dates.
SDX-1673	8.10.14	Provisioning	Resolved redundant approval notifications triggered after user activity completion.
SDX-1662	8.10.14	Platform Security	DirX Identity Security Vulnerability: Hardcoded Passwords and Scrambler Keys Exposed in JAR Files
SDX-1569	V8.9 SP3	Provisioning, ADSAgent	Fix ADSAgent 32-bit overflow for high HighestCommittedUSN values.
SDX-1850, SDX-1761	8.10.15	Platform Security	Security update: Log4j and ActiveMQ upgraded to resolve vulnerabilities.
SDX-1806	8.10.13	Entitlement Management, EventProcessor	Fix for missing event source and originating user in IEventProcessor
SDX-1797	8.10.15	Resolution Service, Consistency Rules	Fix LDAP size limit error in consistency rule processing.
SDX-1743	8.10.15	Provisioning, LDIF Connector	Enable LDIF change record support in the LDIF Connector.
SDX-1760	9.0.0	Identity Management, Paging on search results	Implementation of full paging support for DirX Identity REST services.
SDX-1686	9.0.0	Storage	Fix InvocationTargetException with null Values in GeneralizedTime Attributes
SDX-1671	V8.9 SP3	Provisioning, C Server	Fix for C Server for secure string handling to ensure system stability
SDX-1660	8.10.14	Provisioning, IdsJ	Added sender's name to email FROM parameter
SDX-1625	8.10.13	Provisioning	Fix GraalJS Polyglot Exception when setting properties with JS-Arrays
SDX-1592	8.10.13	Entitlement Management, GraalVM JavaScript	Improved GraalVM JavaScript support for reading assigned account groups.
SDX-1333	8.10.10	Resolution Services	Downgrade spurious lock deletion WARNING logs to INFO level.

Ticket ID	Affected Version	Domain	Summary
SDX-1624	8.10.13	WebCenter Services	Expression language failure with compound attributes in Web Center forms.
SDX-853	V8.10 SP1	Provisioning, TCL CSV Import	Fix TCL CSV imports failure with "Data decryption failed" after upgrade due to missing LDAP permission.
SDX-408	V8.10	Provisioning	Fix for 'meta encryptvalue' failure after DXI 8.10 upgrade.
SDX-1380	8.10.12	Entitlement Management, Policy Agent	Policy Agent performance optimization and privilege prefetching implementation.
SDX-1750	8.10.14	Platform, Vulnerability	Remove default property (password) value in Report generation
SDX-1722	8.10.14	Entity Management, Request Workflow	Fix for thread-safety issues causing data corruption in parallel workflows.
SDX-1617	9.0.0	Entity Management, Obligations	Fix for obligations linked to target system groups not executing.
SDX-1827	8.10.10	Provisioning, IdS-J Server reloads	Fix fatal Xerces XML parsing error during server startup.
SDX-1698	V8.9 SP3	Resolution Service, Workflow	Standardize assignment UID inclusion in reapproval workflow objects.
SDX-1785	8.10.13	Identity Management, REST Services	Fix for REST HTTP 500 Error During Identity Object Modifications
SDX-572	V8.10	Entity Management, Provisioning	New Provisioning Rules tab for Roles, Permissions, and Groups.
SDX-1832	8.10.15	Provisioning	Fix SAP Realtime Userhook failure due to duplicate connector JARs.
SDX-1755	8.10.15	Manager - Connectivity	Deleting mapping items in Connectivity view now automatically removes them from LDAP, not only from the UI.
SDX-1707	9.0.0	WebCenter, Libraries	Update WebCenter Apache Tika library to version 3.3.0.
SDX-1884	8.10.15	Resolution Service, Workflows	Fix lock release failure for renamed user entries in workflows.

▾ *details SDX-1575*

When two permissions with group obligations updating the same user attribute were assigned or approved at the same time, only one group's value was written, leading to data inconsistencies in ATTRIBUTE1. The resolution corrects the multi-value handling in the service layer so that concurrent permission assignments now reliably merge all obligation values into the user attribute.

Problem	Solution
Concurrent assignment or approval of two permissions whose groups both had obligations updating the same user attribute (ATTRIBUTE1) resulted in only one group's value being written, causing repeated data inconsistencies in ATTRIBUTE1 in production.	The service layer logic for handling multi-valued user attributes was corrected (in SvcNode.handleMultiValuesExtOpt / setVolatileProperty) so that concurrent resolution of multiple permissions now reliably merges all obligation values into the target user attribute

▾ *details SDX-1645*

This update resolves a critical issue where the Active Directory Real-Time workflow entered an infinite loop, causing log files to grow excessively up to 5GB. The fix prevents a NullPointerException within the LDAP connector's sequential read process, ensuring stable workflow execution and disk space management.

Problem	Solution
Customers utilizing Active Directory Real-Time (RT) workflows experienced a severe system instability where a `java.lang.NullPointerException` in the `siemens.dxm.connector.ldap.enums.SequentialRead` class triggered an infinite logging loop. This behavior led to rapid disk space consumption—with log files reaching sizes of 5GB for a single thread—and required a manual Java Server restart to terminate the hanging process and clear the error state.	The software has been patched to improve the robustness of the LDAP connector's sequential read operations. By implementing proper null-value handling and terminating the iteration loop upon encountering unrecoverable exceptions, the system now prevents the "endless message" cycle. This ensures that workflows fail gracefully or skip problematic entries without impacting server performance or exhausting storage resources through excessive logging.

▾ *details SDX-1697*

Fix an issue where LDAP username and password authentication failed when a Java keystore was present. The system now correctly prioritizes credential-based login by suppressing unintended client certificate responses during the handshake process.

Problem	Solution
When the DirX Identity (IDS-J) component has an active keystore, it defaults to Java's standard behavior of attempting a certificate-based handshake if an LDAP directory (such as RedHat Directory Server) requests MutualTLS "WANT." Because the keystore often lacks a specific valid client certificate for that directory, the authentication fails, even when the system is configured to use username and password credentials.	The product has been updated to explicitly suppress the default Java behavior that forces certificate-based responses when a keystore exists. This ensures that credential-based authentication remains functional regardless of the presence of a keystore or the directory's optional certificate requests, eliminating the need to manually comment out keystore configurations in the `idmsvc.ini` file.

▾ *details SDX-1759*

Resolved a critical issue where creating new SAP user accounts failed when using combined role and profile subsystems with specific validity dates. The fix ensures that role attributes like start and end dates are now correctly processed during the initial account creation phase.

Problem	Solution
When using the SAP-UM-Cluster-Workflow with CombinedRoleProfileSubsystem and useAdditionalRoleParameters enabled, the system throws a "SEVERE" error stating that the dxrRole.FROM_DAT attribute is not supported. This failure only occurs during the creation (ADD) of a new user account, whereas modification (MODIFY) of existing accounts functions correctly. This asymmetry prevented the provisioning of new SAP accounts whenever specific role validity dates were required.	The root cause was identified as a missing code path in the connector's `createUser()` method that failed to mirror the attribute handling logic present in the `modifyUser()` method. The solution involves updating the SAP-UM connector to explicitly allow and process FROM_DAT and TO_DAT attributes during the user creation process. This alignment between ADD and MODIFY paths restores full provisioning functionality for customers using combined role and profile subsystems.

▾ *details SDX-1673*

Fix an issue where notification emails were being sent a second time immediately after a user completed an approval activity. This fix ensures that warning emails are only sent once as intended, preventing unnecessary inbox volume and outdated information.

Problem	Solution
The `notifyBefore` workflow notifications were incorrectly re-triggering after a user performed an activity (such as an approval). This behavior was especially prevalent when the activity was completed on the same day it was assigned, leading to duplicate or incorrect emails being sent to all assigned users and creating confusion.	The notification logic has been updated to ensure that handled activities do not trigger the `notifyBefore` process a second time. This stabilization ensures that users receive timely warnings without redundant follow-up emails once an action has already been taken.

▾ *details SDX-1662*

DirX Identity Security Vulnerability: Hardcoded Passwords and Scrambler Keys Exposed in JAR Files

Problem	Solution
In DirX Identity 8.10.14, default LDAP connection passwords and secrets used for password scrambling were present in application binaries and visible in code, exposing sensitive information and weakening the protection of administrative credentials.	Default LDAP connection passwords were removed from Web Admin and Provisioning Reports, and password-related secrets were secured so that all credentials and scrambling data are now provided via configuration rather than embedded in the code, restoring expected functionality while improving security.

▾ *details SDX-1569*

The ADSAgent has been updated to correctly handle 64-bit Active Directory USN values exceeding the previous 32-bit limit. This fix ensures that delta synchronizations continue to function correctly in environments with very high update sequence numbers.

Problem	Solution
The Active Directory highestCommittedUSN attribute is a 64-bit integer. In large production environments, this value can exceed the 32-bit unsigned integer limit (4,294,967,295). Because the ADSAgent was using 32-bit data types to process this value, an integer overflow occurred, causing the USN to be truncated (e.g., 4,304,148,812 became 9,181,516). This discrepancy prevented the agent from performing successful delta synchronizations, effectively halting incremental updates.	The ADSAgent C component was modified to support 64-bit integers for USN tracking without requiring a full 64-bit binary port. Key internal variables were updated from ULONG to ULONGLONG, and 32-bit API calls (like GetPrivateProfileInt) were replaced with 64-bit compatible alternatives (_strtoui64). These changes allow the agent to natively handle the full range of Active Directory USN values. A hotfix (V8.9-SP3-72) has been delivered to the customer, and permanent fixes are integrated into versions 8.10.16 and 9.0.1.

▾ *details SDX-1850, SDX-1761*

This update addresses security vulnerabilities CVE-2026-34478 and CVE-2026-34480 by upgrading Log4j dependencies to version 2.26.0. The fix also includes an upgrade to ActiveMQ 5.19.8 to ensure the Message Broker and all platform components are fully protected.

Problem	Solution
DirX Identity version 8.10.15 was identified as vulnerable to security risks (CVE-2026-34477, CVE-2026-34478, and CVE-2026-34480) due to the use of outdated Log4j version 2.25.3. While most components could be updated independently, the Message Broker remained at risk because the bundled ActiveMQ version (5.19.7) still utilized the affected Log4j library.	The development team updated Log4j dependencies to version 2.26.0 across the platform. To fully resolve the issue within the Message Broker, the system was upgraded to ActiveMQ 5.19.8, ensuring a comprehensive fix for the vulnerability in the DirX Identity 8.10.16 release.

▾ *details SDX-1806*

The IEventProcessor now correctly receives the event source and originating user information during modify and add operations. This fix ensures that custom event processors can accurately identify the initiator of a change, aligning behavior with other policy types

Problem	Solution
Customer using the IEventProcessor interface reported that ModifyEvent.getSource() returned null, even when the source was present in the underlying request. Additionally, the Source object lacked the originatingUser information, making it impossible for stakeholders to identify which user or session initiated a specific change. This gap prevented the implementation of use cases requiring audit-level visibility into event triggers within the DirX Identity environment.	The resolution involved updating the AbstractEventController to ensure that the Source object is explicitly propagated from incoming requests to the userhook event objects. Furthermore, the system was enhanced to automatically enrich the Source with the originatingUser by retrieving the effective user from the active session.

▾ *details SDX-1797*

A bug was resolved where consistency rules failed when processing more than 100,000 elements due to an incorrect internal property key. This fix ensures that configured LDAP page sizes are correctly applied, allowing large-scale consistency checks to complete successfully.

Problem	Solution
When running a Java Consistency Resolution Activity against a large dataset (e.g., 216,900 elements), the process fails with an LDAPException: Sizelimit exceeded error after 100,000 entries. This occurs because a property key mismatch in the ConsistencyCheckController.java code prevents the configured LDAP page size from being recognized, defaulting it to 50 entries and causing the operation to hit server-side search limits.	The solution involves a code fix to align the property key name in ConsistencyCheckController.java with the configuration (changing userStorage.ldap.page.size to userStorage.ldap.pagesize). Additionally, customers are advised to verify that their DirX Directory server's search and paging policies (usp and pagp) are configured to accommodate the total number of entries in their environment.

▾ *details SDX-1743*

The LDIF Connector now supports reading and writing LDIF change files, including add, modify, and delete operations. This enhancement allows for seamless delta exports and automated Java-based workflows within the Identity environment.

Problem	Solution
The existing LDIF Connector was limited to handling standard LDIF content files and lacked support for LDIF change records (delta exports). This created a gap in modernizing legacy processes that rely on exporting change and content files to file shares, as the connector could not perform the necessary modify or delete operations required for delta synchronization.	The LDIF Connector has been enhanced to support the LDIF-CHANGE content type, enabling full processing of add, modify, and delete records. Key implementation details include a refactored writer initialization, new utility methods for change record conversion, and updated logging to ensure robust handling of delta exports within Java workflows.

▾ *details SDX-1760*

This update introduces comprehensive paging support across REST services, including the implementation of startIndex and totalResults for accurate search navigation. Users can now effectively browse through large result sets in both domain searches and approval task lists.

Problem	Solution
The existing REST API implementation lacked functional paging, with the documentation noting that itemsPerPage and startIndex were reserved for future use. Specifically, the rest-domain service ignored the startIndex parameter in responses, and the rest-approval service lacked an offset parameter entirely, preventing users from navigating beyond the first page of results. Additionally, totalResults incorrectly reflected only the current page size rather than the total number of available records.	The solution involves a full-stack implementation of paging logic across rest-domain and rest-approval services. Key changes include updating StorageUtils and EntityManagerImpl to respect LDAP offsets, correcting ResultList to return accurate SCIM-compliant metadata, and adding $skip parameter support to approval resources. This ensures that clients can request specific result offsets and receive correct information regarding the total number of items available.

▾ *details SDX-1686*

Fix an issue where scripts returning null values for GeneralizedTime attributes caused `InvocationTargetException` errors, preventing successful saving of objects.

Problem	Solution
When using scripts on attributes of type GeneralizedTime (e.g., `` `dxrStartDate ``, `dxrEndDate`, `iamStartDate`), an `InvocationTargetException` error occurred when the script returned the value `null`. This prevented successful saving of objects.	The type conversion in the Storage layer has been improved to consistently handle null values and empty strings. Scripts can now return null without issues to indicate that an attribute should have no value.

▾ *details SDX-1671*

This update resolves an issue where the C Server could terminate unexpectedly when processing workflows with exceptionally long parameter values. The fix implements secure string handling to ensure system stability and prevent service interruptions during complex workflow executions.

Problem	Solution
The DirX Identity C Server was experiencing abnormal terminations and reaching its restart limit, requiring manual intervention to restore service. Investigation revealed that the crash was caused by a stack buffer overflow in the dxmfrontend.cpp component. Specifically, when a workflow was executed with a long parameter (e.g., 256 characters), the resulting activity Distinguished Name (DN) exceeded the fixed 256-byte buffer, leading to a memory corruption (SIGSEGV) and process failure.	The development team replaced unsafe, unbounded string formatting calls with bounded formatting (`snprintf`) to ensure all data writes respect defined buffer size limits. This fix was validated through a dedicated verification test that successfully reproduced the overflow before the patch and confirmed safe data truncation and service stability after the patch. A hotfix has been prepared for version 8.9 SP3, with permanent fixes also integrated into versions 8.10.16 and 9.0.1.

▾ *details SDX-1660*

Resolved an issue where email notifications sent by DirX Identity lacked a proper sender name in the "FROM" field, which could lead to confusion for recipients and potential filtering by email clients.

Problem	Solution
The email notifications generated by DirX Identity were being sent the email address specified in the configuration without an associated sender name. This resulted in emails appearing as coming from an address like "mail@domain.net <mail@domain.net>" rather than a more user-friendly format such as "DirX Identity <mail@domain.net>".	The email from parameter can now be configured to include a sender name in addition to the email address. The system will format the "FROM" field of outgoing emails to display the sender name followed by the email address in angle brackets, improving clarity for recipients and reducing the likelihood of emails being marked as spam or ignored.

▾ *details SDX-1625*

Users migrating scripts to GraalJS will no longer encounter PolyglotList type conversion errors when using standard JavaScript array methods. The system now correctly handles combined arrays, ensuring seamless compatibility between JavaScript objects and internal property setters.

Problem	Solution
During script migration to GraalJS, using the concat() method to combine results from getStringValues() with standard JavaScript arrays causes a PolyglotException. When the resulting object is passed to setProperty(), the engine identifies it as a com.oracle.truffle.polyglot.PolyglotList instead of the required Java type, leading to a "Invalid value type" warning and script failure.	The integration layer between GraalJS and the core application will be updated to automatically map Polyglot types to compatible Java types during property assignment. This ensures that intuitive JavaScript operations like array concatenation work natively without requiring manual conversion to Java-specific collections, maintaining script stability and reducing migration effort.

▾ *details SDX-1592*

The GraalVM script executor has been enhanced to automatically convert array object types to Java Object[] types, simplifying group assignment retrieval. This update ensures that JavaScript filters in TSAccounts.xml can correctly process assigned groups without requiring manual type conversion.

Problem	Solution
In DirX Identity version 8.10.13, users encountered issues when attempting to read assigned groups (e.g., Groups.Assigned) within GraalVM JavaScript filters in TSAccounts.xml. The script would return null or throw exceptions during UI updates because the returned polyglot values were not automatically converted to the expected Java array types, forcing users to implement complex manual type conversions.	The script executor class was updated to handle automatic conversion of array objects to the Java Object[] type, ensuring compatibility with the platform's service layer. This fix allows scripts to retrieve and iterate through assigned groups using standard JavaScript syntax, and it has been verified as downward compatible with existing manual conversion workarounds.

▾ *details SDX-1333*

The system has been updated to correctly identify when entry locks have already been removed during automated processing. This change ensures that redundant cleanup attempts are logged as informational events rather than warning messages, preventing unnecessary log noise.

Problem	Solution
During nightly user resolution processes, the `EntryLockManager` frequently generates false-positive "WARNING" logs when attempting to release locks that were already deleted by a preceding operation. These logs occur because the system incorrectly interprets a "no such attribute" response from the LDAP server as a warning-level exception, even though the desired outcome—the removal of the lock—has been successfully achieved.	The `EntryLockManager` logic has been modified to recognize the `noSuchAttribute` (code 16) result as a benign, expected condition during lock release. This specific response is now handled at the "INFO" logging level, matching the behavior for existing "constraint violation" checks and ensuring that log files remain clear of misleading warnings while maintaining accurate audit trails.

▾ *details SDX-1624*

A limitation was identified where compound attributes using the '#' character cannot be evaluated within Apache Common Expression Language expression in Web Center form property attributes like "readonly." To resolve visibility or editability issues based on these compound attributes, a workaround using session variables within the JSP is recommended.

Problem	Solution
Web Center users are unable to control the visibility or "readonly" state of form properties when the condition depends on a compound attribute. The system uses the '#' character to identify compound attributes (e.g., `dxr0ptions#myTrigger`), but this character is reserved and cannot be escaped in the Apache Common Expression Language (CEL). Consequently, using these attributes in expressions causes the form to either fail to load or ignore the intended logic.	Since the '#' character is fundamentally incompatible with the current expression evaluator, the recommended solution is to bypass direct CEL evaluation for these attributes. Instead, the compound attribute should be retrieved via the JSP that loads the form and stored in a session variable. This session variable, which does not contain the protected character, can then be successfully used within the `readonly` or `visible` attributes of the form property.

▾ *details SDX-853*

This update resolves an issue where TCL CSV imports failed with a "Data decryption failed" error following a system upgrade. The fix restores necessary LDAP permissions for certificate retrieval, ensuring that encrypted passwords can be correctly processed during import operations.

Problem	Solution
After upgrading to DXI 8.10, customers encountered a METACP 6147: Data decryption failed error during TCL CSV import workflows. Investigation revealed that the upgrade process removed the AccessControl-Subentry-Anonymous-KOW ACI as part of security hardening. However, the lStringEncrypt function still relied on an anonymous LDAP bind to read encryption certificates from cn=server_admin,dxmC=DirXmetahub. Without this permission, the system could not decrypt stored passwords, causing the entire import process to fail.	The resolution involves reinstating the critical KOW ACI in the upgrade schema to allow the system to read the necessary encryption keys. This fix is shared with SDX-408, which addressed a similar failure in the meta encryptvalue command. Additionally, the lStringEncrypt function was made more fault-tolerant by implementing a fallback to the existing active LDAP bind if the secondary bind fails.

▾ *details SDX-408*

This update resolves an issue where the 'meta encryptvalue' command failed due to the removal of anonymous access during system upgrades. The system now uses authenticated LDAP binds for encryption operations, ensuring secure and reliable certificate retrieval.

Problem	Solution
Following an upgrade from DXI 8.9 to 8.10, the meta encryptvalue command (and lStringEncrypt) stopped functioning, returning a "No such object" error. This occurred because the Configuration Wizard deleted the AccessControl-Subentry-Anonymous-KOW ACI as part of security hardening. However, the underlying C-Server code still relied on an anonymous LDAP bind to read encryption certificates from cn=server_admin,dxmC=DirXmetahub, which was no longer permitted without that ACI.	The resolution involved a two-part strategy: first, the critical ACI was reinstated in the upgrade logic to provide immediate relief and prevent regressions in future upgrades. Second, the system was hardened by updating the C-Server code to replace the anonymous LDAP bind with an authenticated bind using configured credentials from dxmmsssvr.ini. Comprehensive validation confirmed that the system now correctly rejects unauthenticated access while maintaining full encryption functionality with valid credentials.

▾ *details SDX-1617*

In earlier 8.10.x builds at customer, obligations linked to target system groups via an Obligation Link were not executed when the group assignment was performed, even though the same logic worked when configured directly under OnAssignment/OnRevocation on the groups. With DirX Identity 8.10.14 (build 1858), this behavior could not be reproduced in integration and regression tests, and the issue is considered fixed; customers are advised to upgrade to 8.10.14 to ensure obligations assigned via Obligation Link are applied correctly during group assignments.

Problem	Solution
At customer, obligations attached to target system groups via an Obligation Link were not executed when users were added to those groups, even though the same obligation logic worked correctly when configured directly on the target system groups under OnAssignment and OnRevocation. This led to inconsistent behavior: from the customer's perspective, identical business rules behaved differently depending on whether they were configured via an Obligation Link or directly on the group.	**Root Cause:** The wasApplied flag in SvcObligation.processOnAssignments() was implemented as a single boolean per Obligation instance, acting as a global singleton across all TargetSystems. When a user already had a group from TargetSystem A referencing a shared ObligationLink, the system incorrectly treated the obligation as "already applied" for groups from TargetSystem B — skipping execution of both onAssignment and onRevocation. **Fix:** Replaced the single boolean wasApplied with a Set<AccountDN> that tracks per-Account (i.e. per-TargetSystem) whether the obligation was already applied. Additionally, corrected the related counters in SvcObligation to be handled per TargetSystem rather than globally. For user-based group memberships (no account), the fix remains compatible since the TargetSystem is null and the SvcUser object is consistent, so the correct values are retrieved from the Sets and Maps.

▾ *details SDX-1380*

The Policy Agent now supports prefetching privileges into cache, significantly improving performance during rule processing and group assignments. Additional optimizations include batched LDAP reads and cross-request caching to reduce processing time for large-scale user updates.

Problem	Solution
Following an upgrade to DirX Identity 8.10, the Policy Agent experienced a significant performance degradation, running nearly three times slower than version 8.9. This was primarily due to the lack of privilege prefetching and a high volume of sequential LDAP round-trips required for privilege resolution, which caused severe bottlenecks when processing rules for large numbers of users.	The "Enabling prefetching privileges into cache" feature was implemented for the Policy Agent to align its performance with the Service Agent. Furthermore, the resolution pipeline was optimized through batched LDAP searches, redundant attribute read elimination, and the introduction of a short-lived cross-request cache for role and permission definitions, resulting in a more efficient and scalable processing model.

▾ *details SDX-1785*

Resolved an issue where certain REST API requests failed with an HTTP 500 error due to

keystore configuration conflicts. The system now correctly filters keystore entries to ensure stable authentication during identity object modifications, even if multiple certificates are present.

Problem	Solution
Users encountered an HTTP 500 "Cannot recover key" error when performing specific identity modifications (e.g., ADD or AssignGroup) via the REST API. This occurred because the Java KeyManagerFactory attempted to recover all private key entries in the keystore using a single password; if an unrelated entry (such as a server certificate) had a different password, the entire initialization failed, even if the correct client key was present.	The solution involved a code improvement in the KeyStoreClient to filter the keystore for the specific target alias before initialization. By loading only the required key entry, the system prevents unrelated entries with different passwords from causing recovery failures, providing greater robustness against keystore configuration errors and certificate rotation issues.

▾ *details SDX-1750*

This update removes a hardcoded default password from the report generation process to improve system security. Reports now utilize externalized credentials, ensuring the connection remains functional without relying on embedded sensitive data.

Problem	Solution
A security vulnerability was identified where a default scrambler key and password were hardcoded within the report generation library. This practice posed a critical security risk and did not meet penetration testing standards, as sensitive credentials were stored directly inside the application environment.	The hardcoded property value was removed from the Main.java class within the report generation component. The system now verifies that report generation remains functional through a smoke test of the report configuration, ensuring secure connectivity without the presence of default passwords in the source code.

▾ *details SDX-1722*

This update resolves a critical issue where parallel real-time workflows could inadvertently share data, leading to incorrect directory operations under heavy load. By implementing a thread-safe connector registry, the system now ensures complete data isolation for all provisioning activities.

Problem	Solution
The DirX Identity framework contained a systemic architectural flaw where multiple workflow threads shared a single connector instance stored in a global context. Under heavy load or when using multiple listeners, this lack of thread-safety caused race conditions, resulting in data corruption such as "ModifyDN" operations being applied to the wrong accounts or groups.	A framework-level ThreadLocal Connector Registry was implemented to ensure each workflow thread maintains its own isolated connector instance. This architectural fix secures all connector types (LDAP, JDBC, SharePoint, etc.) against concurrent data mangling without requiring changes to individual connector code, providing a future-proof and backward-compatible resolution.

▾ *details SDX-1827*

This update resolves a fatal Xerces parsing error that occurred during the startup of the Java Server and IdS-J Server reloads. The fix implements a defensive mechanism to strip invalid characters, such as Byte Order Marks (BOM) or leading whitespace, from XML configuration content before parsing.

Problem	Solution
During the migration from SLES-12 to SLES-15 and upgrading DirX Identity from version 8.9 to 8.10, customers encountered a fatal XML parsing error (IDSJUTL043: Content is not allowed in prolog) when starting the Java Server. This issue was caused by the XML parser encountering unexpected characters—specifically UTF-8 Byte Order Marks (BOM) or leading whitespace—in the dxmContent attributes of workflow fragments or referenced channel entries stored in LDAP. While these characters were invisible in many editors, they caused the Xerces parser to fail during runtime assembly of the workflow XML.	A code fix was applied to the XmlConfigurationImpl.load(String content) method within the dirx-dxi-util library. This defensive update automatically sanitizes XML content by stripping any leading BOM or whitespace before it reaches the parser. Additionally, the system now provides clearer diagnostic logging to identify empty or malformed content, preventing cryptic "prolog" errors and ensuring a more robust server startup process across different OS environments and LDAP configurations.

▾ *details SDX-1698*

Reapproval workflow objects now consistently include the unique identifier (UID) for all processed assignments, regardless of whether the roles are parametrized. This update improves traceability and simplifies the identification of specific user assignments during the reapproval process.

Problem	Solution
Currently, DirX Identity reapproval workflows do not consistently reference the specific assignment being processed. While parametrized roles include the assignment UID, non-parametrized roles only provide the distinguished name (DN) of the role. This inconsistency forces support teams to perform manual, ambiguous lookups to identify the actual affected assignment, leading to increased troubleshooting time and delayed error resolution when workflows fail.	The system has been updated to ensure that the assignment UID (CN) is consistently populated in the dxmResourceState attribute for all reapproval scenarios. By providing an unambiguous reference to the assignment being processed, this change enables faster identification and correction of failed reapprovals, reduces operational burden on downstream data consumers, and maintains full backwards compatibility.

▾ *details SDX-1832*

This update resolves an issue where SAP Realtime Userhooks failed due to duplicate connector JAR files in the system classpath. By consolidating these files into a shared directory, the system now correctly initializes the SAP connection without registration conflicts.

Problem	Solution
Following an update to version 8.10.15, users encountered a java.lang.IllegalStateException: DestinationDataProvider already registered error when executing SAP Realtime Userhooks. This occurred because the SapUM4Role.jar was being deployed to both the shared library folder (confdb/common/lib) and the specific job framework folder (confdb/jobs/framework/lib). Since SAP JCo allows only one registration per JVM, the presence of duplicate JARs across different classloaders caused a conflict that prevented the establishment of SAP connections.	The build process was modified to ensure that connector JARs, specifically SapUM4Role.jar, are only deployed to the shared confdb/common/lib directory and are no longer copied into the confdb/jobs/framework/lib folder. This deduplication ensures a single, consistent class instance is loaded by the parent-first delegating classloader, satisfying SAP JCo's singleton requirements and restoring stable connectivity for SAP Realtime Userhooks.

▾ *details SDX-1755*

Deleting mapping items in Connectivity view now automatically removes them from LDAP, not only from the UI.

Problem	Solution
Deleting mapping items in Connectivity would only remove the from the UI, but they were still in the LDAP, requiring manual deletion. Therefore they would be visible in the Data View.	Deleting mapping items in Connectivity now deletes them from LDAP too. Since this deletion is part of a transaction, the deletion is only performed on 'Save'. Pressing 'Cancel' does not perform any deletion.

▾ *details SDX-1707*

The Apache Tika library in WebCenter has been updated to version 3.3.0 to address security vulnerability CVE-2025-54988. This update ensures secure file processing and can be applied manually by replacing the existing JAR file in the library directory.

Problem	Solution
The current version of tika-core-2.1.0.jar used in the DirX Identity WebCenter is identified as a security risk due to CVE-2025-54988. Stakeholders require a resolution that mitigates this vulnerability without necessitating a full system update.	The tika-core library will be officially updated to version 3.3.0 in the upcoming 8.10 and 9.0 releases. For immediate mitigation, the library can be manually updated by replacing the outdated JAR file in the \webCenter\WEB-INF\lib directory, maintaining full functionality for features such as user photo and certificate uploads.

▾ *details SDX-1628*

We have optimized the REST API performance for retrieving user-specific data by improving how LDAP group memberships are verified. This change eliminates delays caused by loading large group datasets, ensuring a fast and consistent portal experience for all users.

Problem	Solution
The portal experiences significant performance lag (up to 8 seconds) when users with specific administrative assignments attempt to load pages. This delay is caused by a REST API call that triggers an inefficient LDAP operation in the AclManager, which attempts to read entire group objects containing over 250,000 members rather than simply verifying the individual user's membership.	The solution involves restricting the attributes loaded during group cache building to only structural metadata (objectClass, cn) instead of fetching all attributes like uniqueMember. By preventing the exhaustive loading of large member lists, the API response times are normalized to sub-second levels across all user profiles without affecting the accuracy of access policy evaluations.

▾ *details SDX-1622*

Suppress invalid group errors when dxrNoWarningIfNoMatch flag is TRUE

Problem	Solution
When a dxrPermission object is created without assigned groups, the system generates a "SEVERE" error log during every permission check, even if the dxrNoWarningIfNoMatch flag is set to TRUE. This occurs because the flag was only being evaluated during runtime privilege resolution and ignored during structural consistency validations, leading to excessive and misleading error logs for administrators.	The consistency validation logic has been updated to evaluate the dxrNoWarningIfNoMatch attribute. When this flag is enabled, the system will no longer log "Permission is invalid" errors for permissions without assigned groups, aligning the validation behavior with the intended configuration and existing runtime logic.

▾ *details SDX-572*

A new "Provisioning Rules" tab has been added to the management interface for Roles, Permissions, and Groups. This allows administrators to easily identify which provisioning rules are linked to specific entitlement objects, improving visibility and support.

Problem	Solution
Administrators currently lack a direct way to see which Provisioning Rules are associated with a specific entitlement object (Role, Permission, or Group) within the DirX Identity Manager UI. This makes it difficult to maintain a complete overview of the role and rights structure, leading to increased effort during support and system audits.	The DirX Identity Manager UI has been enhanced with a dedicated "Provisioning Rules" tab for Roles, Permissions, and Groups. This tab displays a table of all provisioning rules that reference the object, mirroring the existing pattern used for users and personas to ensure a consistent and efficient administrative experience.

▾ *details SDX-1884*

Resolved an issue where user entries renamed during the "Create User" workflow remained locked for the full lease duration. The system now correctly identifies renamed entries and releases their locks immediately, preventing 10-minute processing stalls.

Problem	Solution
During the "Create User" Request Workflow, a temporary user object is created and locked. When the object is renamed (MODRDN) via a SaveScript, the EntryLockManager fails to release the lock because it still attempts to use the old Distinguished Name (DN). Since the releaseLockNew() method does not correctly handle the NO_SUCH_OBJECT error as a "not found" signal, the UID-based fallback mechanism is never triggered, leaving the entry locked until the 10-minute lockleasetime expires and blocking subsequent processes.	The releaseLockNew() method was updated to explicitly handle the LDAPException.NO_SUCH_OBJECT result code by throwing a LockException(true). This change ensures that when a lock release fails due to a renamed DN, the system correctly triggers the UID-based fallback to locate and unlock the entry at its new DN. Comprehensive unit tests have verified that locks are now released immediately after a rename, eliminating processing delays while maintaining backward compatibility for non-renamed entries.

1.3.1. Other Improvements and Fixes

Affected Version	Domain	Summary
8.10.16, 9.0.1	Rest Services	The Approval REST service now includes unique identifiers (UIDs) alongside Distinguished Names (DNs) in its JSON responses to improve client-side processing and security. A new configuration flag `worklist.participantsListWithUid` in the “approval.properties” file allows administrators to optionally enable these enhanced participant lists for approval workflows. When enabled, this flag transforms the participant list from a simple DN array into a detailed object array containing both DNs and UIDs, ensuring backward compatibility while providing the requested identifier flexibility.

1.4. DirX Identity 8.10.15

Ticket ID	Affected Version	Domain	Summary
SDX-1608	8.10.13	Platform	Fix for Log4j vulnerability, release Log4j 2.25.3
SDX-1334	8.9 SP3	Provisioning	Fix for SAP Password Rule Violations in SAP UM SetPassword Workflow
SDX-1674	8.10.14	Provisioning	DXD crash and size-limit issues during paged SAP import search after DXI 8.10.14 upgrade.
SDX-1630	8.10.9	Platform	CVE-2025-15467 – OpenSSL CMS AEAD Stack Overflow Risk in DirX Identity

Ticket ID	Affected Version	Domain	Summary
SDX-1326	8.10.10	Platform	DXI Schema Synchronization Now Supports LDAPS (Port 636) with Correct SSL Handling and Secure Logging
SDX-1317	8.10.11	Identity Manager	Fix for GUI: DirX Identity Ensures Read-only Attributes Remain Non-Toggleable with Empty Values
SDX-1666	8.10.11	REST Services	Fix for REST endpoint `/approvals/+{workflowUID}+`: Resource UID (dxruid) Now
SDX-1616	8.10.13	Provisioning	Fix for SAP-UM-Java Workflow: DxrRole Attributes Missing in Account Channel's Joined-Entry Search Results, Regardless of checkModification Flag
SDX-1594	8.10.12	Resolution Services	Fix for RQWF Approval Workflows Log Frequent
SDX-1590	8.10.12	Identity Manager	Malformed XML Detection in Dead Letter Queue (DLQ)
SDX-1392	8.10.11	Resolution Services	Enhancement for RQWF on the domain configuration, with which allows to avoid/suppress resolve messages
SDX-1291	8.10.10	Identity Manager and WebCenter	Standardized ComboBox rendering and character encoding in WebCenter and Identity Manager.

▾ *details SDX-1608*

Fix for Log4j versions (2.17.x / 2.24.x / 2.25.1 / 2.25.2), which triggered vulnerability findings such as CVE-2025-68161 for customers. All Log4j usages have been consolidated and upgraded so that DirX Identity 8.10.15 and 9.0.0 now ship only Log4j 2.25.3, including through updated transitive dependencies (e.g. ActiveMQ)

Problem	Solution
A vulnerability scan reported that DirX Identity still contained multiple outdated Log4j versions (2.17.x / 2.24.x / 2.25.1 / 2.25.2) across different components and dependencies, triggering findings for CVE -2025-68161 and raising the customer's question: "With which DXI patch will Log4j v2.25.3 be delivered?".	All Log4j usages in DirX Identity 8.10 and 9.0 were consolidated and upgraded to Log4j 2.25.3, including updates/overrides of transitive dependencies (e.g. Spring Boot logging, axis-jakarta) and the bundled ActiveMQ version, and the result was verified via automated DependencyCheck reports. The vulnerability is now resolved in DXI 8.10.15 and DXI 9.0 (and later), which are the releases that deliver only Log4j 2.25.3.

▾ *details SDX-1334*

In the SAP UM SetPassword workflow at customer instance, certain SAP password rule violations (e.g. invalid first character) caused the SAP call to fail, but due to faulty connector logic the overall task still returned “User successfully modified” and no error email was sent to the administrator. The SAP UM connector was corrected so that if both the productive password change and the fallback “set as initial password” attempt fail, the workflow now returns a proper failure response (FAILED) instead of success, ensuring password sync errors are reported correctly and can trigger admin notification.

Problem	Solution
The SAP UM SetPassword workflow in DirX Identity reported “User successfully modified” and tracked a successful password change even when the underlying SAP password change failed due to SAP password rule violations (e.g. “Choose the first character of the password to be different from ? and different from !.”). The SAP UM connector logic tried a fallback (setNewPasswordAsInitial) after a failed changePassword call and returned SUCCESS if the overall modify task completed, so cases where both the productive password change and the initial-password attempt failed were still reported as successful, and no error mail was sent to the administrator.	The SAP UM connector was corrected so that the SPML response is now set to FAILURE whenever the changePassword call fails and the subsequent setNewPasswordAsInitial attempt also fails, instead of masking these situations as success. With this fix (delivered for V8.9 SP3, 8.10.15, and 9.0), the SetPassword workflow correctly returns a FAILED result for SAP password rule violations, password-sync errors are visible in monitoring, and admin error notifications can be triggered as intended.

▾ *details SDX-1674*

DXD crash and size-limit issues during paged SAP import search after DXI 8.10.14 upgrade.

Problem	Solution
A DirX Directory (DXD) crash occurred during a paged search after upgrading DirX Identity, due to an unhandled error during audit log rotation when the log file was locked. Additionally, a size limit was exceeded for the paged search, causing the Identity workflow to wait indefinitely.	Documentation can be found in Manual Migration

▾ *details SDX-1630*

CVE-2025-15467 – OpenSSL CMS AEAD Stack Overflow Risk in DirX Identity

Problem	Solution
This incident addresses an inquiry regarding CVE-2025-15467, which concerns an OpenSSL CMS AEAD Stack Overflow Risk. The problem was that DirX Identity was not yet updated to OpenSSL 3.6.1, which resolves this CVE, and there was uncertainty about whether DirX products were affected.	The solution involved upgrading OpenSSL within DirX Identity. Binaries for OpenSSL 3.5.5 for both Windows and Linux were built, and Jenkins scripts were updated to use these new binaries for metacp, dirxutil, and dirxcrypto. The fix versions are 8.10.15 and 9.0.0.

▾ *details SDX-1326*

Enabled DXI schema synchronization to work correctly over LDAPS (port 636) in environments where only SSL connections are permitted. The schema read logic was fixed to honor the configured SSL settings and secure port of the connected directory service, aligning synchronization behavior with LDAPS configurations.

Problem	Solution
DXI schema synchronization from DirX Directory to DirX Identity failed when only LDAPS (port 636) was allowed, because the schema read logic did not correctly use the configured SSL setting and secure port of the connected directory service.	The schema synchronization implementation in `LdapCDObject#readSchema` and the related service/bind profile handling was corrected so that the SSL configuration is now honored consistently. When the Service has the SSL flag set, the implementation looks up a bind profile with a matching SSL setting and uses it for the schema read; this results in an LDAPS connection to the secure port (typically 636) with the appropriate JSSE socket factory and without falling back silently to plain LDAP. If no matching SSL bind profile is found, the code now explicitly falls back to an anonymous, non-SSL LDAP connection over the data port (389 by default), making the behavior predictable and correctly aligned with the configuration. In addition, logging was cleaned up so that bind passwords are no longer printed in clear text.

▾ *details SDX-1317*

If an attribute on the object description was mastered and marked readonly=true, an empty value could cause the attribute to lose its readonly state and become toggleable in the GUI. Impact: attributes intended to be read-only could be edited or toggled by users under specific conditions. Resolution: the readonly status now persists for mastered attributes regardless of whether the value is empty; the GUI correctly prevents toggling. No data migration required.

Problem	Solution
At customer, a mastered Boolean compound attribute in DirX Identity Manager was defined as readonly="true" in the object description but still appeared as a toggleable checkbox in the GUI whenever its value was empty. This visual/editability bug meant that attributes which should be strictly read-only (because they are mastered from another object, e.g. via dxrUserLink.myVirtualAttributes(syncsdm)) could be clicked and “changed” by users, and scripts depending on the attribute (dependsOn) saw an inconsistent situation where the UI state did not match the mastered directory value.	The Identity Manager GUI logic for mastered attributes was corrected so that the readonly flag is now evaluated reliably even when the current value is empty, and such fields remain non-interactive in all cases. With this fix (delivered in 8.10.15), mastered attributes that are marked readonly="true" in the object description consistently stay read-only and cannot be toggled by users, while scripts and dependent properties continue to operate on the authoritative mastered value from the directory.

▾ *details SDX-1666*

The REST endpoint `/approvals/+{workflowUID}+` returned approval tasks with "resource": { "dxruid": null }, so clients could not reliably obtain the resource UID and had to fall back to DNs/folders. The implementation was corrected so that the resource UID (dxruid) is now always populated in the response, and the fix is delivered in DirX Identity 8.9 SP2 HF 204, 8.10.15, and 9.0.1.

Problem	Solution
At customer, the DirX Identity REST endpoint `/approvals/+{workflowUID}+` returned approval tasks with `"resource": { "dxruid": null }`, so the client could not obtain the UID of the target resource and had to fall back to DNs/folders, which they explicitly want to avoid.	The REST service implementation was corrected so that the resource UID (dxruid) is now populated in the approval task response, and the fix is delivered for DirX Identity V8.9 SP2 (HF 8.9 SP2 204), 8.10.15, and 9.0.1.

▾ *details SDX-1616*

Join search requests previously returned only attributes from channel mappings that had checkModification = true, which unintentionally excluded other mapped attributes from the search result. This could lead to incomplete data being available to the join engine.

With this change, join search requests now include all attributes defined in the channel mappings, regardless of the checkModification flag. The flag continues to control whether a value is added to a ModifyRequest, but it no longer limits which attributes are requested during join searches.

Impact / Risk: The additional attributes returned in join search responses do not affect the standard behavior of the join engine. However, customers should review any custom logic that relied on attribute filtering based on the checkModification flag, as this filtering is no longer applied at search time.

Problem	Solution
Context: Channel mappings offer a flag called "checkModification". When this is set, the join engine compares the values of the joined entry with the mapped values and only adds changes to the ModifyRequest if the value has actually changed. For join search requests, the requested attributes include only those defined in the channel mappings, filtered by the "checkModification" flag... only attributes with checkModification == true were returned in this query.	For join search requests, no longer filter via "checkModification" flag, instead including both flagged and not flagged attributes in the search result. **Risk**: While additional attributes in the search response do not interfere with the general behavior of the join engine, customers need to be aware of this change, in case their customizations rely on the filtering of requested attributes via the "checkModification" flag

▾ *details SDX-1594*

In DirX Identity 8.10.12, RQWF approval workflows could intermittently fail with EntryLockManager.lockEntry failed ... entry still locked for 60000 msec, especially after Java server restarts or when multiple approval workflows were started in succession. With the changes included up to build 8.10.14, this locking problem could no longer be reproduced in the affected approval workflows.

Problem	Solution
In DirX Identity 8.10.12, many RQWF approval workflows (“4-Eye Approval”) frequently logged EntryLockManager.lockEntry failed ... entry still locked for 60000 msec, especially after Java server restarts and when multiple approvals were started in succession. This resulted in a high number of lock warnings (around 50% of running approval workflows and ~85% of succeeded approvals showing the warning in dxrError), raising concerns about workflow stability.	Cumulative workflow/repository changes delivered in DirX Identity 8.10.14 removed the locking problem; therefore, upgrading to at least 8.10.14 is the recommended resolution.

▾ *details SDX-1590*

Malformed XML Detection in Dead Letter Queue (DLQ)

Problem	Solution
Previously, Malformed XML Detection in Dead Letter Queue (DLQ), associated events failed silently or showed empty values, making troubleshooting difficult for administrators.	Implemented detection and clear reporting of malformed XML in the Web Admin DLQ interface: Detection: Regex pattern identifies common malformed patterns (square brackets instead of angle brackets) Logging: SEVERE log entry written when malformed XML is detected GUI Indication: Fields display "ERROR" instead of empty values Transparency: Original malformed XML is always shown in the event details

▾ *details SDX-1392*

By changing a privilege in any DXI client (DXI Manager, WebCenter, REST) asynchronous resolution resolves the affected users, by sending as many resolve messages as users count. It can cause performance problem if the resolve queue (of the resolution adapter) is overloaded with messages.

With this enhancement a new flag is delivered on the domain configuration, with which the resolve messages can be avoided/suppressed, and the resolution of the affected users is done immediately or the TBA flag of the changed privilege is set.

Problem	Solution
After upgrading from 8.9 to 8.10.11, user group memberships in DirX Identity were often not recalculated immediately after changes (e.g. role assignments) in WebCenter/Manager/REST. Instead, the system frequently logged “No need to resolve user … as last resolution was after last save time” and deferred the actual privilege resolution until the next nightly Privilege Resolution run, leaving critical permissions (e.g. for physicians) missing for many hours. Parallel it was seen in delivered logs that thousands of resolve messages were sent to users in a few seconds.	On one side the customer was supported by some reconfiguration of his privilege resolution workflows avoiding unnecessary resolutions. On the other side a new, configurable flag was introduced on the domain configuration (“Avoiding sending resolve message of users by privilege related changes”). When enabled, resolve messages are suppressed • DXI Manager, REST: affected users are resolved immediately/synchronously • WebCenter: the TBA flag of the changed privilege is set, the resolution of affected users can be done by executing a on customer side configured PrivilegeResolution or CheckConsistency workflow in synchronous resolution mode to avoid sending resolve messages there too So given the option in DXI to eliminate the overloaded resolution queue as a bottleneck and ensuring better performance in environments where the overloaded queue can cause issues.

▾ *details SDX-1291*

Improved consistency of attribute displays by resolving encoding issues and standardizing ComboBox behavior across the WebCenter and Identity Manager. Users will now see German umlauts correctly rendered, and tag-based formatting in selection lists will appear without unintended characters.

Problem	Solution
Customers experienced inconsistent rendering of the same attribute between the DirX Identity Manager and WebCenter. Specifically, German umlauts (e.g., "ä") were not displaying correctly in the Manager due to XML encoding mismatches, and ComboBox elements in the WebCenter were showing unintended curly brackets when using specific tag syntax in the object description.	The solution involves two primary fixes: updating the object description XML headers to use **UTF-8** encoding to ensure proper character rendering on Linux-based systems, and standardizing the attribute tag processing. The rendering logic was adjusted to handle display values and storage values correctly, removing the visible brackets. These changes ensure a unified user experience across both management interfaces and provide clearer configuration guidance for custom object descriptions.

1.5. DirX Identity 8.10.14

Ticket ID	Affected Version	Domain	Summary
SDX-1511	8.10.12	Request Workflow	assignDirect access policies for administrative roles
SDX-1466	8.10.12	Provisioning, Connectivity	NullPointerException in the IdS-J Server
SDX-1432	8.10.12	Installation & deployment	configuration and custom content stored under <IDENTITY_INSTALL>/conf is deleted during upgrades
SDX-1430	8.10.11	Privileged Resolution	“Remove privileges from TBDEL user” policy on users in TBDEL state does not remove all dxrAssignment child objects
SDX-1581	8.10.11	Provisioning, HistDB Workflows	DirX Audit HistDB workflows triggers error JOIN926 (“No target system node found") during execution
SDX-1559	8.10.13	Provisioning, Notification Workflow	SMTP mapMailAddress option overrides the recipient (TO) address of workflow notification emails
SDX-1545	V8.10	Provisioning, Log-Level Handling	ConsistencyCheckController could leave the global log level permanently set to DEBUG
SDX-1326	8.10.10	Provisioning, Schema Synchronization	LDAPS schema synchronization and logging
SDX-1536	8.10.13	Provisioning, Workflow Correlation	Align DirX Identity and Directory workflow SIDs

Ticket ID	Affected Version	Domain	Summary
SDX-1491	8.10.13	Identity Management, REST Services	Return all certificate attributes as JSON objects
SDX-1523	8.10.12	Identity Management, Web Center	Fix Web Center multi-value renderer comma handling
SDX-1524	8.10.12	Identity Management, Web Center	Fix Web Center group member date rendering
SDX-1416	V8.9 SP3, 8.10x	Identity Management, REST Services	Fix pre-1970 date conversion in REST/SCIM queries
SDX-1527	8.10.11	Resolution Service, Request Workflow	Restore NoApprovalAdmin assignDirect no -approval behavior
SDX-1561	8.10.12	Request Workflow	Store correct REST initiator DN on assignments
SDX-1517	8.10 SP1, 8.10.13	Installation & deployment	Clarify installer start method for upgrade
SDX-1440	8.10.10	Installation & deployment	Avoid logging service account passwords in Windows
SDX-1444	8.10.x	Connectivity, Mail Connector	Enable Mail Connector STARTTLS TLS -secured SMTP connections
SDX-1488	8.10.6	Provisioning, Status Tracker	Fix Status Tracker activity name truncation logic
SDX-362	V8.9, 8.10x	Request Workflow, Approval Workflow	Report group-deleted cause in RACF approval workflows
SDX-1486	8.10.13	Provisioning, HCL Notes Extension Groups	Fix HCL Notes extension group creation and handling
SDX-1520	8.10.13	Installation & deployment	Handle pre-stopped IDS-J services without installation errors
SDX-568	8.10x	Request Workflow, Approval Workflow	Trigger approvals for high-trust assignments during object creation

Ticket ID	Affected Version	Domain	Summary
SDX-1479	8.10.12	Request Workflow	Allow REST approval to update assignment end date
SDX-1617	8.10SP2	Request Workflow, Obligation Handling	Obligation Link–attached group obligations not executed
SDX-1190	8.10SP2	Provisioning, Connector	ADS agent configurable UTF-8 handling for AD
SDX-1656	8.10SP2	Provisioning, MetaCP	MetaCP UTF-8 handling for DirX Directory writes

▾ *details SDX-1511*

- In DirX Identity 8.10.12, *assignDirect* access policies for administrative roles were not evaluated correctly, causing permission assignments to always trigger an approval workflow instead of allowing direct assignment as intended. This was fixed by correcting the logic in the permission assignment service (SvcObjAss.class), restoring the expected behavior.

Problem	Solution
In DirX Identity 8.10.12/8.10.14 and 9.0, the access policy with operation *assignDirect* for administrative roles no longer worked as in earlier versions (e.g. 8.9 SP2/SP3). Even when an administrator had an Access Control Policy (ACP) that should allow direct assignment of a permission without starting an approval workflow, DirX Identity always started the approval workflow for the permission assignment. This affected a productive customer process where certain admin users must be able to assign permissions directly (e.g. via WebCenter) based on *assignDirect* access policies.	The root cause was identified in the service logic handling permission assignments (SvcObjAss.class in dxrServices.jar). A condition in this class did not correctly evaluate the *assignDirect* access policy in versions 8.10.12/8.10.14 and 9.0, so the system always triggered the approval workflow. The implementation was corrected in SvcObjAss.class This fix restores the original and expected behavior of *assignDirect*-based access policies in DirX Identity.

▾ *details SDX-1466*

Fixed a NullPointerException in the IdS-J Server that prevented startup after upgrading to DXI 8.10.12 and migrating to new hardware when unfinished workflows from an older installation were present.

Problem	Solution
• The customer used a DB Backup from DXI 8.9 as a basis for a new DXI 8.10.12 installation. • After initial configuration, the java server didn't start due to a NullPointerException in ResourceManager • The NullPointerException was caused by the Java Server trying to run unfinished workflows, that were not present on the new host system.	• Robustness fix (already done via hotfix and included in 8.10.14 / 9.0): ◦ Prevent NullPointerException and fail gracefully when workflow resources or LDAP base DNs are missing. • Documentation update for: ◦ Migration to new hosts/OS with DB restore. ◦ Requirement to close workflows before backup/migration.

▾ *details SDX-1432*

Fixe for DirX Identity to preserves customer-specific configuration and custom content stored under <IDENTITY_INSTALL>/conf during upgrades (including 8.10.14 and 9.0). This prevents loss of unpacked tools such as runwf that previously could be deleted when upgrading from 8.10.12+1634.

Problem	Solution
• After upgrading DirX Identity 8.10.12 (Build 1634), the customer's manually unpacked and customized runwf directory under the DXI installation root was deleted by the installer, causing runwf.bat to stop working. • Restoring runwf still failed with LDAP errors (Authenticated bind failed, No such object: dxmc=dirxmetahub) because hard-coded parameters in runwf.bat and the truststore/configuration no longer matched the actual environment. • There was no clear, upgrade-safe location for customer-specific tools/configuration, and the documentation did not warn against placing runwf directly in the DXI install folder.	• Introduced and documented <IDENTITY_INSTALL>/conf as a dedicated, upgrade-safe folder for customer-specific configuration and custom content that must be preserved during upgrades. • Adjusted upgrade behavior (8.10.14, 9.0 / Build 28684) so that files in <IDENTITY_INSTALL>/conf remain untouched; this is verified by acceptance tests that keep a custom test file across upgrades. • Updated guidance to instruct customers to unpack tools like runwf.zip outside the DXI root or into <IDENTITY_INSTALL>/conf, and to re -adapt runwf configuration (host/port/SSL/rootDN/user/truststore) when relocating it.

▾ *details SDX-1430*

Clarification for Remaining assignment objects (**dxrTbDelByResolver=TRUE**). Behavior when cleaning up **TBDEL** users with role assignments was analyzed and confirmed to work as designed in versions 8.10.14 and 9.0. Assignments flagged with **dxrTbDelByResolver=TRUE** do not cause unintended reassignment and are removed

later by the resolver or when the user and its child objects are finally cleaned up.

Problem	Solution
In DirX Identity 8.10.11 / DirX Directory 9.0, running the “Remove privileges from **TBDEL** user” policy on users in **TBDEL** state does not remove all dxrAssignment child objects. Some assignment objects remain and are only flagged with **dxrTbDelByResolver=TRUE**. These flagged assignments are never deleted, and there was concern that they could later lead to renewed, unintended role assignments. The questions were why these assignments are not removed and how to ensure they are ultimately cleared.	Reported issue is fixed by: • iterating children in reverse to safely remove leaf objects without skipping entries • using a backward loop prevents index shifting caused by *removeLeaf()*. Previously, *removeLeaf()* modified the underlying collection, shifting elements left and causing the forward loop to skip some children, resulting in undeleted assignments. • added additional logging to capture the assignment ID during deleting.

▾ *details SDX-1581*

Fixed an issue in the DirX Audit HistDB workflows where error JOIN926 (“No target system node found for DN 'cn=TargetSystems,CN=IAMBw'”) occurred during execution. The HistDB workflows Ident_HistDB_Sync_TargetSystems_Full and Ident_HistDB_Sync_Groups_Full now run without triggering this error.

Problem	Solution
In the customer production environment (DirX Identity 8.10.12, DirX Directory 9.0), the DirX Audit HistDB workflows Ident_HistDB_Sync_TargetSystems_Full and Ident_HistDB_Sync_Groups_Full consistently failed during execution with error JOIN926: “No target system node found for DN 'cn=TargetSystems,CN=My-Company' in the channel …” The issue occurred every time the DXT History workflow ran and persisted even with a newer DXI version.	The HistDB-related export configuration is not limited to a specific target system, therefore looking up the target system information logged a fatal error. However, in case of HistDB workflows, the target system information is not needed and the workflow proceeds correctly without it. It’s just that the log message suggests otherwise. After applying the fix, HistDB workflows execute successfully without triggering the JOIN926 error message, leaving the logging of that message to error handling.

▾ *details SDX-1559*

Fixed the SMTP *mapMailAddress* option so that it only overrides the recipient (**TO**) address of workflow notification emails, as documented, and no longer changes the sender (**FROM**) address.
This ensures mail forwarding for testing and demos works correctly even when only the configured service account is allowed to send emails.

Problem	Solution
The SMTP *mapMailAddress* option in DirX Identity behaved differently from the documentation and replaced both the **TO** (recipient) and **FROM** (sender) addresses with the mapped address, causing workflow notification emails to fail in environments where only the configured service account is allowed to send mails.	The implementation was corrected so that *mapMailAddress* now only overrides the **TO** address for workflow notification emails as documented, leaving the **FROM** address unchanged, thereby restoring the ability to safely test and demo email workflows via mail forwarding.

▾ *details SDX-1545*

Fixed an issue in **ConsistencyCheckController** where exceptions in **ruleProcessingEnd** could leave the global log level permanently set to DEBUG, causing unintended verbose logging. The log-level manipulation was removed from **ConsistencyCheckController**, ensuring the global log level now remains stable and unaffected by consistency check processing errors.

Problem	Solution
Exceptions thrown in *ConsistencyCheckController.ruleProcessingEnd* could interrupt the restoration of the original global log level after temporarily switching to DEBUG, leaving the system in DEBUG mode and generating unintended, excessive logging.	The logic that changed the global log level in **ConsistencyCheckController** was removed so that consistency check processing no longer manipulates the global log level, ensuring logging configuration remains stable even if errors occur.

▾ *details SDX-1326*

Enabled DXI schema synchronization to work correctly over LDAPS (port 636) in environments where only SSL connections are permitted. The schema read logic was fixed to honor the configured SSL settings and secure port of the connected directory service, aligning synchronization behavior with LDAPS configurations.

Problem	Solution
DXI schema synchronization from DirX Directory to DirX Identity failed when only LDAPS (port 636) was allowed, because the schema read logic did not correctly use the configured SSL setting and secure port of the connected directory service.	The schema synchronization implementation was fixed so that, when SSL is configured, it now connects over LDAPS using the secure port 636 and the proper SSL settings of the connected directory, enabling successful schema synchronization in SSL-only environments.

▾ *details SDX-1536*

Fixed an issue where the initiator session ID (SID) in the DirX Identity Java server log did not match the SID recorded in the DirX Directory LDAP audit log for clustered synchronization workflows. The SID handling for clustered workflows was corrected so that the same workflow ID is consistently used in both Java and LDAP audit logs, enabling reliable cross-correlation of events (e.g. in Splunk).

Problem	Solution
In clustered DirX Identity environments, the initiator session ID (SID) written to the Java server log did not match the SID stored in the DirX Directory LDAP audit log for synchronization workflows, making it difficult to reliably correlate workflow executions and audit events across systems (e.g. in Splunk).	The SID handling for clustered synchronization workflows was corrected so that the same workflow ID is now consistently used in both the Java server log and the LDAP audit log, restoring end -to-end traceability of workflow-related events.

▾ *details SDX-1491*

Certificate-type custom attributes in DirX Identity REST responses were returned only as raw byte arrays, while the standard **userCertificate** attribute was returned as a detailed JSON certificate object, leading to inconsistent output for clients. The REST service was changed to use the certificate editor configuration (e.g. *siemens.DirXjdiscover.api.ldap.beans.JnbLdapCertificate)* so that all certificate attributes are now returned consistently as JSON certificate objects like **userCertificate**.

Problem	Solution
DirX Identity REST responses returned the standard **userCertificate** attribute as a detailed JSON certificate object, but other certificate-type custom attributes (e.g. **iamUserCertificateAuth**) were returned only as raw byte arrays, causing inconsistent output and confusion for clients expecting the same structure.	The REST service logic was changed to use the certificate editor configuration (*siemens.DirXjdiscover.api.ldap.beans.JnbLdapCertificate* and the attribute's data type [B] instead of the hard-coded attribute name, so that all certificate-type attributes are now returned consistently as JSON certificate objects like userCertificate.

▾ *details SDX-1523*

In Web Center multi-value fields using string list snippets (such as objectLinks), display texts containing commas were cut off because the JavaScript renderer incorrectly treated them as DNs and only showed the last RDN part. The renderer logic was extended with a new noDnEval property (set to true for non-DN renderers like objectLinks), so that display texts with commas are shown in full and DN evaluation only happens where intended.

Problem	Solution
In Web Center multi-value fields based on string list snippets (such as **objectLinks**), display texts containing commas were truncated because the JavaScript renderer treated the entire display text as a DN and only showed the last RDN part. This caused location or object link values to be displayed incompletely when the configured pattern contained commas (for example in descriptions).	The renderer logic was enhanced with a new *noDnEval* property that allows the JavaScript code to distinguish between plain text and DNs; for non-DN renderers like **objectLinks** this is set to true so that commas in display texts are shown correctly, while DN evaluation is only applied where actually intended.

▾ *details SDX-1524*

Date values for group members in Web Center were returned in DXI GeneralizedTime format instead of *java.util.Date*, causing date columns (such as user and account end dates) to be displayed in raw LDAP format or as invalid NaN values despite using *date/time* renderers. The group member retrieval was corrected to convert DXI GeneralizedTime values to *java.util.Date*, so that customer-configured date renderers now show dates correctly in the expected localized format.

Problem	Solution
In Web Center group member lists, user and account end dates (**dxrEndDate**) were delivered as raw DXI GeneralizedTime LDAP strings instead of java.util.Date, so date/time cell renderers showed unreadable LDAP values or invalid NaN outputs instead of localized dates.	The group member retrieval was corrected to convert DXI GeneralizedTime values to proper *java.util.Date* objects before rendering, so customer-configured date/time renderers now display user and account end dates correctly in the expected localized format.

▾ *details SDX-1416*

Date display and REST/SCIM queries for certain pre-1970 dates could return no results because an extra minute was added during date conversion in DirX Identity and DirX Directory Manager. The date conversion logic was corrected so that date attributes (such as *dayOfBirth*) are handled consistently, ensuring accurate display and reliable filtering in REST queries.

Problem	Solution
For certain dates before 1 January 1970, DirX Identity and DirX Directory Manager added an extra minute during date conversion, causing incorrect display (e.g. in the Manager UI) and preventing REST/SCIM queries (e.g. on *dayOfBirth*) from matching the correct user entries.	The date conversion logic was corrected so that pre-1970 date values are no longer shifted by one minute, ensuring that stored values, UI display, and REST/SCIM filter handling for attributes like *dayOfBirth* are consistent and queries reliably return the expected user records.

▾ *details SDX-1527*

In DirX Identity 8.10.11, the *NoApprovalAdmin* no-approval mechanism stopped working: even when using access policies with *assignDirect* and without *execute*, assigning approval-required roles still triggered approval workflows, blocking customer from upgrading. The handling of *assignDirect* has been corrected so that such assignments no longer start approval workflows, restoring the previous no-approval behavior and enabling automated rule-based role assignments again.

Problem	Solution
In DirX Identity 8.10.11, the *NoApprovalAdmin* no-approval mechanism stopped working: even with access policies configured to use *assignDirect* (and only *grant*, not *execute*), assigning approval-required roles started approval workflows, breaking all rule-based role assignments and blocking customer from upgrading.	Solution was implemented in SDX-1511. The root cause was identified in the service logic handling permission assignments (**SvcObjAss.class** in **dxrServices.jar**). A condition in this class did not correctly evaluate the *assignDirect* access policy in versions 8.10.12/8.10.14 and 9.0, so the system always triggered the approval workflow. The implementation was corrected in **SvcObjAss.class** This fix restores the original and expected behavior of *assignDirect*-based access policies in DirX Identity.

▾ *details SDX-1561*

When permissions with group obligations and JavaScript were assigned via the REST API, the script could no longer determine the actual initiating user, because privilege resolution now ran asynchronously under *DomainAdmin*, breaking customer logic that needs the real requester DN. The REST privilege assignment flow was enhanced so that the effective REST user is stored on the target object (e.g. in *dxrCreator*), allowing JavaScript obligations to reliably read the correct initiator DN even in the asynchronous 8.10.x behavior.

Problem	Solution
In DirX Identity 8.10.x, when permissions with group obligations and JavaScript were assigned via the REST API, the obligation script saw *DomainAdmin* as the initiator (due to asynchronous privilege resolution), so *storage.getInitiatorDN()* returned the wrong DN and customer logic could no longer identify and log the real requester.	The REST privilege assignment flow was enhanced to store the effective REST user on the target object (e.g. in the *dxrCreator* attribute) during privilege assignment, so JavaScript obligations can now reliably read the correct initiator DN (for example via *obj.getProperty("dxrCreator"))* even with the asynchronous 8.10.x behavior.

▾ *details SDX-1517*

The upgrade from DirX Identity 8.10 SP1 to 8.10.13 initially failed with “Installation was cancelled during Pre-Installation ... file cannot be deleted because it is locked” for various Web Center files, although no actual file locks or permission issues were present. The issue was resolved by starting the installer directly in the current shell (*./dirxidty.bin*) instead of via *sh dirxidty.bin*, after which the locked-file checks passed and the upgrade completed successfully.

Problem	Solution
During an upgrade from DirX Identity 8.10 SP1 to 8.10.13, the installer repeatedly aborted in the pre-installation phase with “file cannot be deleted because it is locked” for various customized Web Center files, even though Tomcat was stopped, the files were writable for the dirxid user, and independent checks (*fuser, lsattr*, custom *locking.jar*) showed no real locks or permission issues. The root cause turned out not to be the files themselves, but the way the installer was started: invoking it via *sh dirxidty.bin* led to a different execution context/environment (involving su and possibly differing SELinux/FS context handling), causing the locked-file verification to fail on multiple Web Center paths and blocking the upgrade.	The installation was rerun by starting the installer ***directly*** in the current shell as the correct installation user (*./dirxidty.bin*), as documented for the product, instead of wrapping it with *sh*; under this execution context the locked-file verification passed for all Web Center files and the upgrade to 8.10.13 completed successfully while preserving the customer’s heavy Web Center customizations. The ticket was then closed with the recommendation to always start the installer as described in the documentation and avoid additional shells/wrappers (like *sh*) that can alter environment, permissions, or file-system semantics during pre-installation checks.

▾ *details SDX-1440*

The AMQ service custom account was set using sc config command, which may have led to the log of parameters (including credentials). The update process was reimplemented to use Windows native functions for all services (AMQ, IdsC, IdsJ). By using these functions, it was also discovered, that IdsC and IdsJ services used deprecated (since Windows Vista) flag SERVICE_INTERACTIVE_PROCESS when custom account was used. That not work with the new functions, therefore this flag was removed from these services (also for security reasons).

▾ *details SDX-1444*

For DirX Identity 8.10.14, the Mail Connector was verified and configured so that SMTP connections using STARTTLS work correctly against a mail relay that requires at least TLS 1.2, with the secure port taken from the bind profile and supported protocols derived from the Java SSL configuration. With this setup, the “Send Mail TS” workflow can now successfully send emails via such a TLS-secured mail relay when SSL is enabled in the bind profile.

Problem	Solution
The DirX Identity Mail Connector could not establish a TLS-secured SMTP connection (“Can not connect”) to a mail relay that requires at least TLS 1.2, even though non -TLS SMTP worked and the same credentials succeeded via PowerShell. The customer was unsure how to configure TLS in DirX Identity (which port to use, whether *dxmSecurePort* is correct, how to verify TLS settings and protocols), and for 8.10.x the STARTTLS option used in 9.0 was in fact missing, so the connector could not negotiate the required TLS connection.	The Mail Connector behavior in DirX Identity 8.10.14 was aligned with 9.0 and configured so that STARTTLS is supported and works correctly against a mail relay that enforces TLS ≥ 1.2. In this setup, the secure SMTP port is taken from the bind profile/service definition, while the set of supported TLS protocols is derived from the underlying Java SSL configuration (via *SSLSocketFactoryImpl*), and with SSL enabled in the bind profile the “Send Mail TS” workflow can now successfully send emails through the TLS-protected relay.

▾ *details SDX-1488*

The DirX Identity Status Tracker no longer cleaned up *dxmC=Status Data,dxmC=DirXmetahub* because very long activity display names were truncated in LDAP, so they no longer matched the corresponding cn values; this caused continuous CDB3642 warnings and uncontrolled growth of the DirX Directory database at Dataport. The matching logic between **ActivityStatusData.cn** and **Activity.dxmDisplayName** was corrected so that statistics are handled correctly even when activity names are shortened, and a fix was provided (included from SDX-1488) so the Status Tracker can again purge old status data as expected.

Problem	Solution
At Dataport, the DirX Identity Status Tracker stopped cleaning up entries under *dxmC=Status Data,dxmC=DirXmetahub*, causing continuous **CDB3642: Can’t evaluate disable statistics flag for ActivityStatusData** warnings and unchecked growth of the DirX Directory database up to the point of an availability incident. Root cause analysis showed that very long workflow activity display names (**dxmDisplayName**) were stored in LDAP with truncation due to the schema limit on name attributes (64 characters minus timestamp), so the truncated cn in **ActivityStatusData** no longer matched the full **dxmDisplayName** of the corresponding *Activity*; the Status Tracker therefore “could not find” the activity for many status objects and skipped the cleanup logic.	The matching logic in the Status Tracker between **ActivityStatusData.cn** and **Activity.dxmDisplayName** was corrected so that it still finds the right activity even when the display name has been shortened by LDAP. In addition, the product behavior was aligned with the schema constraints (limiting effective activity name length) and a fix package from SDX-1488 was provided and delivered to Dataport; with this fix in place, the Status Tracker can again purge old status data as designed, preventing future database overflows and eliminating the recurring **CDB3642** warnings.

▾ *details SDX-362*

Approval workflows for RACF groups at customer could end in state

FAILED.INCOMPLETE with application state **NOAPPROVER** when the target group was deleted during the running workflow, so the real root cause of the failure was not visible. The workflow handling and customer constraint logic were adjusted so that missing groups are detected as **RESOURCE_MISSING** and reported with the more accurate application state **GROUPDELETED**, giving administrators clear feedback when a group is removed during an approval process.

Problem	Solution
At customer, approval workflows for RACF group assignments could end in **FAILED.INCOMPLETE** with application state **NOAPPROVER** when the target group was deleted during the running workflow, so administrators saw a misleading “no approver” error instead of the real cause that the group no longer existed.	The workflow engine and the customer’s custom constraint class (*xxxxRACFParticipantConstraintMinOne*) were extended so that missing resources are detected as **RESOURCE_MISSING** and reported with the clearer application state **GROUPDELETED** by throwing exception on deleted resource and provide precise cause in *ConstraintViolationException*, ensuring workflows surface the correct root cause when a group is removed during an approval process.

▾ *details SDX-1486*

In DirX Identity installations using **HCL Notes** extension groups and group member limits, extension groups were not created correctly and their DNs were not written back into the master group’s membership attribute; in some cases, group creation also failed with “No value entered for object id.” The handling of Notes target system group object descriptors and extension-group creation was corrected (including removal of problematic *cn/description* definitions and using the proper target system for the extension group), and the documentation (“**Customization Guide**”, chapter 8.9 *Setting Group Member Limits*) was updated so that extension groups are created as expected and recorded as members in the master group.

Problem	Solution
In DirX Identity installations using **HCL Notes** extension groups and group member limits, extension groups were not created and handled as documented: attempts to exceed the configured member limit led to errors like "**Cannot create extension group … No value entered for object id**," and even where extension groups were created, their DNs were not added to the master group's membership attribute as expected. In addition, the internal handling of membership attributes and the 90% fill rule for master groups was incorrect (e.g. wrong distribution of accounts between master and extension groups, extra extension groups on delete/TBDEL, inconsistent *dxrGroupMemberAdd/Delete* updates), and the product documentation for group member limits did not reflect the actual behavior, causing confusion for operations teams.	The Notes target system group object descriptions were cleaned up (removing custom *cn/description* naming rules that interfered with DXI's own extension-group name generation) and the extension-group creation logic was adapted so that *cn* values for extension groups are generated only by the service layer code using the standard DXI rules. The *dxrGroupMemberAdd/Delete* are updated consistently (including TBDEL/DELETED scenarios) without creating additional extension groups); corresponding unit and manual tests were added, and the Customization Guide (chapter 8.9 Setting Group Member Limits) was updated in both 8.10 and 9.0 to match the implemented behavior. The membership handling for master and extension groups has been specified and implemented already so that only accounts are stored in the membership attributes (extension groups are referenced via *dxrExtensionGroup* on the master group as the supported model), configured member limit is taken as 100% to fill instead of the 90%.

▾ *details SDX-1520*

When installing DirX Identity 8.10.13 on Windows with IDS-J services already stopped manually, the installer still tried to stop them again, raised a *NonfatalInstallException*, and ended with "Installation finished with errors," causing unnecessary irritation for administrators. For 8.10.14 and 9.0, the Windows installer was improved to first check whether services are already stopped, attempt all service checks/stops without aborting on the first problem, and only log warnings/info instead of reporting the installation as finished with errors in this situation.

Problem	Solution
When installing DirX Identity 8.10.13 on Windows with the IDS-J services already stopped manually, the installer still attempted to stop them again, threw a *NonfatalInstallException*, and ended with the message “Installation finished with errors,” even though the environment was actually correct. This misleading error message confused administrators and triggered unnecessary troubleshooting because it suggested a real installation failure instead of simply reporting that the services were already down.	For DirX Identity 8.10.14 and 9.0, the Windows installer logic was improved to first check whether the IDS-J services are already stopped and, if so, skip the stop attempt, perform all service stop/check operations without aborting on the first issue, and only log non-critical information or warnings instead of flagging the installation as “finished with errors” in this situation. This ensures that a clean pre -stopped service state is handled gracefully and administrators see a successful installation result without confusing error messages.

▾ *details SDX-568*

When creating a new role and adding existing permissions that require approval, the configured approval workflows were not triggered, so high-trust permissions could be assigned without the expected approval step. The approval handling was enhanced so that workflows now start correctly during object creation for all supported cases: adding approval-required permissions while creating a role, assigning approval-required groups while creating a permission, and assigning approval-required junior roles while creating a senior role.

Problem	Solution
In DirX Identity, approval workflows configured as “for assignment to roles requires approval” were only triggered when adding or removing permissions on an *existing* object, but not during *creation* of that object. When a new role was created and high-trust, approval-required permissions were attached in the same step, no workflow was started; similarly, creating a new permission with an approval-required group, or a new senior role with an approval-required junior role, also bypassed approvals. This behavior allowed high-trust entitlements at the customer to be granted without the expected approval step and audit trail whenever they were assigned as part of object creation instead of as a follow-up modification.	The approval handling for object creation was reworked so that assignments made while creating a role, permission, or senior role are now checked for approval requirements in the same way as later modifications. Concretely, the system now detects approval-required permissions when creating a role, approval-required groups when creating a permission, and approval-required junior roles when creating a senior role, and automatically creates the corresponding approval orders and starts the configured workflows (e.g. “Manager Nomination”). This closes the approval gap for creation scenarios, ensures consistent enforcement of customer governance policies across all assignment paths, and restores full workflow-based control for high-trust entitlements.

▾ *details SDX-1479*

In DirX Identity 8.10.12, REST-based approvals for request workflows failed with HTTP 500 (“Assigning resource … is not allowed according to the task configuration”) when an approver tried to change the *dxrEndDate* of an assignment, even though the resource and task configuration were correct. The request workflow service was corrected (PeopleActivityConfig / TaskUpdater validation and related logic) so that 4-eye approval tasks now accept the configured permission/group as a valid resource and REST updates of the end date succeed with HTTP 204 as expected.

Problem	Solution
At customer, REST-based approvals for DirX Identity request workflows in 8.10.12 failed with HTTP 500 “Assigning resource … is not allowed according to the task configuration” when an approver tried to change only the dxrEndDate of an assignment in a 4-eye approval task, even though the permission/group and workflow configuration were correct and the use case had worked in 8.9. The root cause was that the request workflow service’s validation (TaskUpdater / *PeopleActivityConfig*) incorrectly rejected the configured permission/group as a disallowed resource for approval tasks, and subsequent retries against an already -completed task produced additional confusing error messages.	The request workflow service implementation was corrected to recognize properly the configured permission or group as an accepted resource when updating assignments via REST, including changes to dxrEndDate. The fix (delivered in builds 8.10.14 and 9.0) in *PeopleActivityConfig* includes validation for *isApproveAssignment()* in *isRequestPermissions(), isRequestGroups()* and *isRequestRoles()* and the implementation of *UserNotParticipantException* to handle cases where a user is not a participant in a workflow task. When triggered in *updateTask*, the system now responds with HTTP 403 (Forbidden) and includes the exception message in the POST REST API response payload.

▾ *details SDX-1617*

In earlier 8.10.x builds at customer, obligations linked to target system groups via an **Obligation Link** were not executed when the group assignment was performed, even though the same logic worked when configured directly under **OnAssignment/OnRevocation** on the groups. With DirX Identity 8.10.14 (build 1858), this behavior could not be reproduced in integration and regression tests, and the issue is considered fixed; customers are advised to upgrade to 8.10.14 to ensure obligations assigned via Obligation Link are applied correctly during group assignments.

Problem	Solution
At customer, obligations attached to target system groups via an Obligation Link were not executed when users were added to those groups, even though the same obligation logic worked correctly when configured directly on the target system groups under **OnAssignment** and **OnRevocation**. This led to inconsistent behavior: from the customer's perspective, identical business rules behaved differently depending on whether they were configured via an Obligation Link or directly on the group.	The reported behavior was tested in DirX Identity 8.10.14 (build 1858) using integration and regression scenarios, and the issue could not be reproduced; obligations linked via Obligation Link were applied as expected during group assignments. Based on these results, the bug is considered fixed in 8.10.14, and customers are advised to upgrade to 8.10.14 so that obligations attached through Obligation Links to target system groups are executed reliably during assignment and revocation operations.

▾ *details SDX-1190*

The classic ADS agent used for synchronizing TSAccount objects from DirX to Active Directory always treated its import files as Windows-1252 (ANSI Latin1), so UTF-8 encoded data (e.g. names with Turkish characters) were written to AD with garbled characters. The agent was enhanced with configurable InputCodePage/OutputCodePage options so customers can properly process UTF-8 input and convert it to the desired target encoding, and the updated binaries are delivered with DirX Identity 8.10.14 and 9.0.0.

Problem	Solution
The classic DirX ADSAgent.exe used for synchronizing TSA objects from DirX into Active Directory always interpreted its input file as Windows-1252 (ANSI Latin1), even when the metaCP job correctly produced UTF-8 encoded files. As a result, names and attributes containing characters outside CP1252 (e.g. "Doğan, Pelin" with Turkish "ğ") were written into AD with garbled characters ("DoÄŸan, Pelin"), and existing agent/compiler tweaks did not resolve the encoding mismatch, blocking a broader rollout that required full UTF-8 support.	The ADS agent was enhanced to support configurable character set conversion, controlled via new InputCodePage and OutputCodePage options in options.ini under [Configuration]. Customers can now set InputCodePage=65001 for UTF-8 input and an appropriate output code page (e.g. 1252) so that the agent converts text safely between encodings, handling characters outside the target charset in a sensible way; updated Unicode-capable binaries and example configurations were provided and verified, and these improvements are delivered in DirX Identity 8.10.14 and 9.0.0.

▾ *details SDX-1656*

MetaCP workflows writing to DirX Directory could fail with "Cannot check attribute dxmADsSamAccountName for duplicates" when handling special characters (e.g. "ü", "ß") because of mixed UTF-8 and extended ASCII encodings in directoryString attributes. The issue is resolved by using the updated ADSAgent delivered with DirX Identity 8.10.14, which correctly processes UTF-8 encoded attribute values and prevents these duplicate-check errors.

Problem	Solution
MetaCP workflows writing accounts to DirX Directory failed with errors like “Cannot check attribute *dxmADsSamAccountName* for duplicates” when values contained special characters such as “ü” or “ß”. The root cause was a character-encoding mismatch (mixed UTF-8 and extended ASCII encodings for directoryString attributes), so the duplicate check on *dxmADsSamAccountName* could not reliably compare existing and new values and aborted the operation.	The customer should switch to the updated ADS agent delivered with DirX Identity 8.10.14, which correctly processes UTF-8 encoded attribute values and keeps the encoding consistent for directoryString attributes. With this agent in place, the duplicate check on *dxmADsSamAccountName* works reliably even for names with special characters, and the MetaCP workflows complete successfully.

1.6. DirX Identity 8.10.13

1.6.1. Bug Fixes

- Fixed issue related to a missing attribute dxrCancellerLink in the DirX Identity schema affecting the RQWF cancel process (SDX-1423)
- Fixed issue related to recurring error message in the J-Server log when executing JDBC RT Workflows (SDX-1398)
- Fixed issue in the Office365 Connector following an update to version 8.10, which caused connection issues with Microsoft accounts (SDX-1323)
- Fixed issue in HCL Notes where extension groups are created without reaching the set member limit and even when the status is TBDEL/DELETED (SDX-1009)
- Fixed issue related to NullPointerException occurring after updating from DXI 8.10.11 to DXI 8.10.12 during synchronization with an Avaya phone system (SDX-1391)
- Fixed issue related to the group overview where changing language or font size results in an error message and empty attribute fields (SDX-1394)
- Fixed issue related to the UserHook ProzessSourceEntry function returning a null value after a system upgrade (SDX-1356)
- Fixed issue where environment variables in the export filter are not resolved in the "to" channel (SDX-1340)
- Fixed issue where the Cleanup Rule in DXI 8.10.11 is not deleting objects as expected (SDX-1315)
- Fixed issue where a severe error "java.lang.ArrayIndexOutOfBoundsException" occurring during the modification of SAP UM group assignments (SDX-1284)
- Fixed issue in the Identity Manager GUI where the dxrUID value remains unchanged when objects are copied and pasted (SDX-1251)
- Fixed issue related to a memory issue in DirX Directory related to a DXD LDAP Exception caused by a CtxLimitExceeded error when resolving a user (SDX-1040)
- Fixed issue where the REST API DELETE function fails when an assignment has an end

date (SDX-1230)

- Updated ActiveMQ on servers to version 5.19.0 (SDX-1203)

1.7. DirX Identity 8.10.12

1.7.1. Bug Fixes

Customers benefit from the following fixes of the 8.10.12+1634 patch:

- Fixed issue how PrivilegeResolution works/ PrivRes resolves "too many" users (SDX-1231)
- Fixed issue with DXI WebCenter: Action /listPermissionUsers limited to 500 roles (SDX-504)
- Fixed issue with maintenance of the Role assignment to a user where the Role has required re-approval (SDX-642)
- Fixed PasswordPolicies: Minimum password age can be defined in the pw policies (SDX-1011)
- Fixed issue with duration for PrivilegeResolution (SDX-904)
- Fixed issue with creation of JMS message publisher for topic alias TOPIC_PROVISION_TO_TS bzw. TOPIC_USER_CHANGE (SDX-1256)
- Fixed issue with nested group memberships in PrivilegedGrantedLink / privilege resolution (SDX-1273)
- Fixed issue with Users with enddate and no permissions, have dxrAssignment entries (SDX-1137)
- Fixed issue with User Lock values in Domain Configuration in J-Server log files (SDX-1214)
- Fixed issue with No Attributes Read & Modify for Create AccessPolicies (SDX-1259)
- Fixed issue with EventBasedUserResolution does not respect the SearchBase of the policy (SDX-1335)
- Fixed issue with DependsOn to react immediately when a GeneralizedTime field is modified (SDX-1314)

Customers benefit from the following fixes of the 8.10.12+1637 patch:

- Fixed issue with Nullpointer Exception for Provisioning (SDX-1340, SDX-1391, SDX-1390)

Customers benefit from the following fixes of the 8.10.12+1638 patch:

- Fixed issue with NullPointerException for Provisioning (SDX-1340, SDX-1391, SDX-1390)

1.8. DirX Identity 8.10.11

1.8.1. Bug Fixes

- Fixed issue with DirX Identity RQWF and Cancel Process (SDX-933)

- Fixed issue with Variable in Export Filter of Real-Time channel in Join Filter <filterExtension> (SDX-1269)
- Fixed issue with Accounts-Channel, specific Attributes are not resolved (SDX-1205)
- Fixed issue with Tomcat during InitialConfiguration (SDX-1189)
- Fixed issue with LinkCheckers (SDX-1199)
- Introduce new Flag to allow PrivilegeResolution for disabled users (SDX-1163)

1.9. DirX Identity 8.10.10

1.9.1. 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)

1.10. DirX Identity 8.10.9.a

1.10.1. Bug Fixes

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

1.11. DirX Identity 8.10.9

1.11.1. 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)

1.12. DirX Identity 8.10.8

1.12.1. 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)

1.13. DirX Identity 8.10.7

1.13.1. 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)

1.14. DirX Identity 8.10.6

1.14.1. 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)

1.15. DirX Identity 8.10.5

1.15.1. 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)

1.16. DirX Identity 8.10.4

1.16.1. 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)

1.17. DirX Identity 8.10.3

1.17.1. 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)

1.18. DirX Identity V8.10 SP2

1.18.1. New Features

1.18.1.1. 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).

1.18.1.2. 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)

1.18.1.3. 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).

1.18.1.4. 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).

1.18.1.5. Request Workflow Engine

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

1.18.1.6. Identity Domain Connector

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

1.18.1.7. 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.

1.18.1.8. Support of OpenSSL

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

1.18.1.9. Support of Systemd for Red Hat 9

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

1.18.1.10. 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).

1.18.1.11. 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).

1.18.1.12. Message broker

- Update Tanuki Service wrapper to v3.5.51.

1.18.1.13. 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
  ```

1.18.2. Bug Fixes

1.18.2.1. 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)

1.18.2.2. 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).

1.18.2.3. 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)

1.18.2.4. 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).

1.18.2.5. Provisioning Web Services

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

1.18.2.6. 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).

1.18.2.7. 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)

1.18.2.8. 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).

1.18.2.9. 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).

1.18.2.10. 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).

1.18.2.11. 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).

1.18.2.12. C++-based Server

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

1.18.2.13. 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).

1.18.2.14. 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).

1.18.2.15. 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)

1.18.3. 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).

1.18.4. 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

1.19. DirX Identity V8.10 SP1

1.19.1. New Features

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

1.19.1.1. Support of Windows Server 2022

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

1.19.1.2. 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).

1.19.1.3. 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).

1.19.1.4. 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).

1.19.1.5. TCL Workflows

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

1.19.1.6. Security Settings for Identity SSL Connections

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

1.19.1.7. 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).

1.19.1.8. 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).

1.19.2. Bug Fixes

1.19.2.1. 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).

1.19.2.2. 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).

1.19.2.3. 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).

1.19.2.4. 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).

1.19.2.5. 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).

1.19.2.6. 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).

1.19.2.7. 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).

1.19.2.8. 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).

1.19.2.9. 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).

1.19.2.10. C++-based Server

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

1.19.2.11. 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).

1.19.2.12. CSV Connector

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

1.19.2.13. 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).

1.19.2.14. RACF Connector

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

1.19.2.15. LDAP Connector / ADS Connector

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

1.19.2.16. Sharepoint Connector

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

1.19.2.17. 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).

1.19.2.18. JDBC Connector/Agent

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

1.19.2.19. 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).

1.19.2.20. 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).

1.19.2.21. 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).

1.19.2.22. 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).

1.19.2.23. 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).

1.19.3. 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

1.20. DirX Identity V8.10

1.20.1. 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:

1.20.1.1. 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.

1.20.1.2. 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”.

1.20.1.3. 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.

1.20.1.4. 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).

1.20.1.5. 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).

1.20.1.6. 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).

1.20.1.7. Handling of Consistency Rules

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

1.20.1.8. 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).

1.20.1.9. Support of Encrypted E-mails

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

1.20.1.10. Anonymous Access to Connectivity and Provisioning Store

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

1.20.1.11. 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).

1.20.1.12. Delta Mode for Combined Workflows

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

1.20.1.13. 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).

1.20.1.14. 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.

1.20.1.15. 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).

1.20.1.16. Certification Controller

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

1.20.1.17. 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).

1.20.1.18. 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).

1.20.1.19. 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).

1.20.1.20. 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).

1.20.1.21. Support of Apache Embedded Tomcat 9.0.56

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

1.20.1.22. 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.

1.20.2. Bug Fixes

1.20.2.1. Business User Interface

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

1.20.2.2. 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).

1.20.2.3. 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).

1.20.2.4. 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).

1.20.2.5. 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).

1.20.2.6. 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).

1.20.2.7. 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).

1.20.2.8. 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).

1.20.2.9. 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).

1.20.2.10. 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).

1.20.2.11. 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).

1.20.2.12. 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).

1.20.2.13. 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).

1.20.2.14. 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).

1.20.2.15. 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).

1.20.2.16. 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).

1.20.2.17. 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).

1.20.3. 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

1.21. Dirx Identity V8.9 SP3

1.21.1. New Features

1.21.1.1. 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).

1.21.1.2. 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).

1.21.1.3. 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).

1.21.1.4. Role Assignments with Mandatory End Dates

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

1.21.1.5. 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).

1.21.1.6. Support of Apache Embedded Tomcat

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

1.21.2. Bug Fixes

1.21.2.1. 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).

1.21.2.2. 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).

1.21.2.3. 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).

1.21.2.4. 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).

1.21.2.5. 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).

1.21.2.6. 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).

1.21.2.7. 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).

1.21.2.8. 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).

1.21.2.9. Provisioning Servlet

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

1.21.2.10. 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).

1.21.2.11. 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).

1.21.2.12. 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).

1.21.2.13. 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).

1.22. DirX Identity V8.9 SP2

1.22.1. New Features

1.22.1.1. 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".

1.22.1.2. 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

1.22.1.3. 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".

1.22.1.4. 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).

1.22.1.5. 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).

1.22.1.6. 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.

1.22.2. Bug Fixes

1.22.2.1. 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).

1.22.2.2. 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).

1.22.2.3. 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).

1.22.2.4. 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).

1.22.2.5. 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).

1.22.2.6. 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).

1.22.2.7. 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).

1.22.2.8. 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).

1.22.2.9. 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).

1.22.2.10. 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).

1.22.2.11. 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).

1.22.2.12. 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).

1.22.2.13. 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).

1.22.2.14. JDBC Connector

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

1.22.2.15. JMS Audit Listener

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

1.22.2.16. 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).

1.22.2.17. 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.

1.22.2.18. 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).

1.22.2.19. 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).

1.22.2.20. 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).

1.23. DirX Identity V8.9 SP1

1.23.1. New Features

1.23.1.1. 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".

1.23.1.2. 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.

1.23.1.3. Support of Apache ActiveMQ 5.15.12

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

1.23.1.4. 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.

1.23.1.5. Sending mail in the Java-based server

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

1.23.1.6. 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).
```

1.23.2. Bug Fixes

1.23.2.1. 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).

1.23.2.2. 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).

1.23.2.3. 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).

1.23.2.4. 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).

1.23.2.5. 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).

1.23.2.6. 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).

1.23.2.7. 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).

1.23.2.8. Provisioning Web Service

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

1.23.2.9. 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).

1.23.2.10. 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).

1.23.2.11. 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).

1.23.2.12. 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).

1.23.2.13. 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).

1.23.2.14. 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).

1.23.2.15. 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).

1.23.2.16. 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".

1.23.2.17. 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).

1.23.2.18. 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).

1.24. DirX Identity V8.9

1.24.1. 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:

1.24.1.1. 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”.

1.24.1.2. 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.

1.24.1.3. 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.

1.24.1.4. 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.

1.24.1.5. Support of Apache ActiveMQ 5.15.9

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

1.24.1.6. Support of openSSL v1.0.2r

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

1.24.2. Bug Fixes

1.24.2.1. 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).

1.24.2.2. 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)

1.24.2.3. 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).

1.24.2.4. 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)

1.24.2.5. 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).

1.24.2.6. 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).

1.24.2.7. 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 occurred 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 provisioning 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).

1.24.2.8. 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).

1.24.2.9. REST Services

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

1.24.2.10. 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).

1.24.2.11. 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).

1.24.2.12. 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).

1.24.2.13. 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).

1.24.2.14. 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).

1.24.2.15. 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).

1.24.2.16. 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).

1.24.2.17. 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).

1.24.2.18. 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).

1.24.2.19. 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).

1.24.2.20. 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).

1.24.2.21. 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).

1.24.2.22. 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).

1.24.2.23. 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).

1.24.3. 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

1.25. DirX Identity V8.7 SP4

1.25.1. New Features

1.25.1.1. 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.

1.25.1.2. 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).

1.25.1.3. Support of Apache ActiveMQ 5.15.10

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

1.25.1.4. Upgrade of embedded Tomcat

- Upgrade of embedded Tomcat in Java server to 8.5.46.

1.25.1.5. Java-based Server

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

1.25.2. Bug Fixes

1.25.2.1. 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).

1.25.2.2. 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).

1.25.2.3. 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).

1.25.2.4. 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).

1.25.2.5. 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).

1.25.2.6. 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).

1.25.2.7. 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).

1.25.2.8. 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).

1.25.2.9. Configuration Data

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

1.25.2.10. 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).

1.25.2.11. 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).

1.25.2.12. 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).

1.25.2.13. Identity Manager

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

1.25.2.14. Identity REST service

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

1.25.2.15. 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).

1.25.2.16. 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.

1.25.2.17. 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).

1.26. DirX Identity V8.7 SP3

1.26.1. New Features

1.26.1.1. 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.

1.26.1.2. 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).

1.26.1.3. Support of Apache ActiveMQ 5.15.6

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

1.26.1.4. Support of openSSL v1.0.2p

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

1.26.1.5. Support of VMware ESXi 6.5

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

1.26.1.6. 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).

1.26.1.7. 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.

1.26.2. Bug Fixes

1.26.2.1. 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).

1.26.2.2. 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).

1.26.2.3. 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).

1.26.2.4. 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).

1.26.2.5. 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).

1.26.2.6. 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).

1.26.2.7. Configuration Wizard

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

1.26.2.8. 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).

1.26.2.9. Default Applications

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

1.26.2.10. Metacp

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

1.26.2.11. 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>
```

1.27. DirX Identity V8.7 SP2

1.27.1. New Features

None.

1.27.2. Bug Fixes

1.27.2.1. 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).

1.27.2.2. 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).

1.27.2.3. 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).

1.27.2.4. 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).

1.27.2.5. 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).

1.27.2.6. 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.

1.27.2.7. 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).

1.27.2.8. 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).

1.27.2.9. Message Broker

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

1.27.2.10. 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.

1.28. DirX Identity V8.7 SP1

1.28.1. New Features

1.28.1.1. 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.

1.28.1.2. 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).

1.28.1.3. Support of Apache ActiveMQ 5.15.3

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

1.28.1.4. Support of openSSL v1.0.2n

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

1.28.1.5. C++-based Server

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

1.28.2. Bug Fixes

1.28.2.1. 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).

1.28.2.2. Web Center API

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

1.28.2.3. 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).

1.28.2.4. 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).

1.28.2.5. 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.

1.28.2.6. 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).

1.28.2.7. 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).

1.28.2.8. 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.

1.28.2.9. 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.

1.28.2.10. 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).

1.29. DirX Identity V8.7

1.29.1. 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:

1.29.1.1. 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).

1.29.1.2. 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.

1.29.1.3. Support of Apache ActiveMQ

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

1.29.1.4. Support of openSSL

- OpenSSL libraries were updated to openSSL version 1.0.2l.

1.29.1.5. 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.

1.29.2. Bug Fixes

1.29.2.1. 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).

1.29.2.2. 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).

1.29.2.3. 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).

1.29.2.4. Certification Campaign

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

1.29.2.5. 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).

1.29.2.6. Request Workflow Service

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

1.29.2.7. 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).

1.29.2.8. 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).

1.29.2.9. 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).

1.29.2.10. 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).

1.29.2.11. 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).

1.29.2.12. Default Applications

1.29.2.13. 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).

1.29.2.14. 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).

1.29.2.15. 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).

1.29.2.16. 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).

1.29.2.17. 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).

1.29.3. 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

Eviden is a registered trademark © Copyright 2026, Atos Group – All rights reserved.

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.