Release 3.6.1

Comenius

Release 3.6.1 is a twenty second midPoint release. It is the fist maintenance update for 3.6.x version family code-named *Comenius*. The Comenius family brings numerous new features especially in the field of identity governance, password management and identity connectors.This maintenance update brings number of smaller improvements, fixes and stability enhancements.

Release date: 11th October 2017

John Amos Comenius

John Amos Comenius (1592 - 1670) was Czech philosopher, pedagogue and theologian. He is considered to be the father of modern education. Comenius first introduced pictorial textbooks written in native language. He applied effective teaching based on the natural gradual growth from simple to comprehensive concepts. He supported lifelong learning and logical thinking. Comenius lived and worked in numerous countries where he widely spread his ideas. He is undoubtedly one of the most significant educational reformers in history.

Not entirely unlike the educational reforms of Comenius, midPoint 3.6 brings substantial and revolutionary changes in understanding the identity management field. Primary focus of midPoint 3.6 is identity governance. This makes midPoint 3.6 a very unique product that can handle broad range of deployments: from very small and simple to the large and complex. Similarly to the gradual method introduced by Comenius, midPoint 3.6 allows to start small with simple identity management deployment and gradually evolve the solution to support complex identity governance scenarios. With midPoint 3.6 this process is smooth and evolutionary which provides business continuity and excellent investment protection. This is further supported by the open nature of midPoint which allows complete understanding and wide spread of midPoint deployments all around the world.

Credits

Majority of the work on the *Comenius* release was done by the Evolveum team. However, this release would not be possible without the help of our partners, customers, contributors, friends and families. We would like to express a great gratitude to all the people that contributed to the midPoint project.

Special thanks: AMI Praha and the academic community

MidPoint 3.6 version family is named after John Amos Comenius, known as Jan Amos Komenský in his native lands of Bohemian Crown, today known as Czech Republic. By naming midPoint 3.6 after one of the greatest men that originated in this region we would like to thank AMI Praha for their hard work, inspiring ideas and wonderful cooperation since the early years of midPoint project. MidPoint would not be such a great product without your cooperation.

There is also one more motive to name midPoint 3.6 after one of the greatest educational reformers of all times. By doing so we would like to thank all universities, schools, academic institutions and individual members of the academic community that made a significant contribution to midPoint project. We thank you all for your support to the midPoint project, your feedback and ideas.

We would also like to thank:

- All the translators from midPoint community and especially Petr Gašparík for taking the lead and coordinating all the translation efforts.
- All MidPoint subscribers. MidPoint subscriptions are the crucial essence that makes midPoint development possible. MidPoint project would not exist without the funding provided by midPoint subscriptions.

Features

midPoint 3.6.1 provides following features:

- Common user data model suitable for easy integration
    - Numerous built-in properties based on IDM de-facto standards (LDAP inetOrgPerson, FOAF, ...) and experience
    - Extensibility by custom properties
    - Off-the-shelf support for user password credentials
    - Off-the-shelf support for user activation
        - Enabled/disabled states (extensible in the future)
        - Support for user validity time constraints (valid from, valid to)
    - Object template to define policies, default values, etc.
        - Ability to use conditional mappings (e.g. to create RB-RBAC setup)
        - Ability to include other object templates
        - Global and resource-specific template setup
    - Sequences for reliable allocation of unique identifiers
    - Object lifecycle property
    - Object history (time machine)
- Identity management (create, read, update, delete accounts)
    - Enabling and disabling accounts
    - Support for mapping and expressions to determine account attributes
    - Support of multi-value attributes
    - Processing and computation fully based on relative changes
    - Multi-layer attribute access limitations
    - Provisioning dependencies
        - Higher-order dependencies (enables partial support for circular provisioning dependencies)
    - Provisioning robustness - ability to provision to non-accessible (offline) resources
    - Provisioning consistency - ability to handle provisioning errors and compensate for inconsistencies
    - Support for tolerant attributes
        - Ability to select tolerant and non-tolerant values using a pattern (regexp)
    - Support for volatile attributes (attributes changed by the resource)
    - Matching Rules
        - Matching rules to support case insensitive attributes, DN and UUID attributes, XML attributes, etc. (extensible)
        - Automatic matching rule discovery
    - Ability to execute scripts before/after provisioning operations
    - Advanced support for account activation (enabled/disabled states)
        - Standardized account activation that matches user activation schema for easy integration
        - Ability to simulate activation capability if the connector does not provide it
        - Support for account lock-out
        - Support for account validity time constrains (valid from, valid to)
        - Support easy activation existence mappings (e.g. easy configuration of "disables instead of delete" feature)
        - Support for mapping time constraints in activation mappings that allow configuring time-related provisioning features such as deferred account delete or pre-provisioning.
    - Ability to specify set of protected accounts that will not be affected by IDM system
    - Support for base context searches for connectors that support object hierarchies (such as LDAP)
    - Passive Attribute Caching (EXPERIMENTAL)
- Connectors
    - Integration of Identity Connector Framework (ConnId)
        - Support for Evolveum Polygon connectors
        - Support for ConnId connectors
        - Support for OpenICF connectors
    - Unified Connector Framework (UCF) layer to allow more provisioning frameworks in the future
    - Automatic generation and caching of resource schema from the connector
    - Local connector discovery
    - Support for connector hosts and remote connectors, identity connector and connectors host type
    - Remote connector discovery
    - Manual Resource and ITSM Integration
- Identity governance
    - Policy Rules as a unified mechanism to define identity management, governance and compliance policies
    - Multi-level flexible approval workflows
    - Segregation of Duties (SoD)
        - Many options to define role exclusions
        - SoD approvals
        - SoD certification
    - Assignment constraints for roles and organizational structure
    - Access certification
    - Ad-hoc recertificaiton
    - Basic role lifecycle management (role approvals)
    - Deputy (ad-hoc privilege delegation)
    - Escalation in approval and certification processes
    - Personas

- Organizational structure management
- Web-based administration GUI
    - Ability to execute identity management operations on users and accounts
    - User-centric views
    - Account-centric views (browse and search accounts directly)
    - Resource wizard
    - Layout automatically adapts to screen size (e.g. for mobile devices)
    - Easily customizable look & feel
    - Built-in XML editor for identity and configuration objects
    - Identity merge
- Self-service
    - User profile page
    - Password management page
    - Role selection and request dialog
    - Self-registration
    - Email-based password reset
- Flexible identity repository implementations and SQL repository implementation
    - Identity repository based on relational databases
    - Keeping metadata for all objects (creation, modification, approvals)
    - Automatic repository cleanup to keep the data store size sustainable
- Synchronization
    - Live synchronization
    - Reconciliation
        - Ability to execute scripts before/after reconciliation
    - Correlation and confirmation expressions
        - Conditional correlation expressions
    - Concept of *channel* that can be used to adjust synchronization behaviour in some situations
    - Generic Synchronization allows synchronization of roles to groups to organizational units to ... anything
- Advanced RBAC support and flexible account assignments
    - Expressions in the roles
    - Hierarchical roles
    - Conditional roles and assignments/inducements
    - Parametric roles (including ability to assign the same role several times with different parameters)
    - Temporal constraints (validity dates: valid from, valid to)
    - Metaroles
    - Role catalog
    - Role request based on shopping cart paradigm
    - Several assignment enforcement modes
        - Ability to specify global or resource-specific enforcement mode
        - Ability to "legalize" assignment that violates the enforcement mode
- Entitlements and entitlement associations
    - GUI support for entitlement listing, membership and editing
    - Entitlement approval
- Advanced internal security mechanisms
    - Fine-grained authorization model
    - Organizational structure and RBAC integration
    - Delegated administration
- Password management
    - Password policies
    - Self-service password management
    - Password storage options (encryption, hashing)
    - Mail-based initialization of passwords for new accounts
- Customization expressions
    - Groovy
    - Python
    - JavaScript (ECMAScript)
    - XPath version 2 (deprecated)
    - Built-in libraries with a convenient set of functions
- PolyString support allows automatic conversion of strings in national alphabets
- Mechanism to iteratively determine unique usernames and other identifiers
- Extensibility
    - Custom schema extensibility
    - Scripting Hooks
    - Lookup Tables
    - Support for overlay projects and deep customization
    - Support for programmatic custom GUI forms (Apache Wicket components)
    - Basic support for declarative custom forms
- Reporting based on Jasper Reports
- Comprehensive logging designed to aid troubleshooting
- Rule-based RBAC (RB-RBAC) ability by using conditional mappings in user template
- Auditing
    - Auditing to file (logging)
    - Auditing to SQL table
    - Interactive audit log viewer
- Credential management
    - Password distribution
    - Password policies
    - Password retention policy
- Support for Service objects (ServiceType) to represent servers, network devices, mobile devices, network services, etc.

- Partial multi-tenancy support
- Deployment and customization
    - Lightweight deployment structure
    - Multi-node task manager component with HA support
    - Support for Apache Tomcat web container
- Import from file and resource
    - Object schema validation during import (can be switched off)
    - Smart references between objects based on search filters
- Self-healing consistency mechanism
- Representation of all configuration and data objects in XML, JSON and YAML
- Enterprise class scalability (hundreds of thousands of users)
- API accessible using a REST, web services (SOAP) and local JAVA calls
- Workflow support (based on Activiti engine)
- Notifications
- Documentation
    - Administration documentation publicly available in the wiki
    - Architectural documentation publicly available in the wiki
    - Schema documentation automatically generated from the definition (schemadoc)

Changes with respect to version 3.6

- Auxiliary object class improvements
- GUI skin switching support (contributed by Andrew Cope)
- Minor shopping cart improvements
- Reliability improvements for parallel processing
- Improved use of constants
- Improved error handling (provisioning scripts, GUI)
- LDAP and Active Directory connector improvements
- CSV connector improvements (file locking)
- Authorization improvements

Java 7 environment is no longer supported.
XPath2 scripting is no longer supported.
Old CSVFile Connector is deprecated and it is no longer bundled with midPoint.

Quality

Release 3.6.1 (*Comenius* Update 1) is intended for full production use in enterprise environments. All features are stable and well tested - except the features that are explicitly marked as *experimental* or *partially implemented*. Those features are supported only with special subscription and/or professional services contract.

Limitations

- MidPoint 3.6.1 comes with a bundled LDAP-based eDirectory connector. This connector is stable, however it is not included in the normal midPoint support. Support for this connector has to be purchased separately.

Platforms

MidPoint is known to work well in the following deployment environment. The following list is list of **tested** platforms, i.e. platforms that midPoint team or reliable partners personally tested this release. The version numbers in parentheses are the actual version numbers used for the tests. However it is very likely that midPoint will also work in similar environments. Also note that this list is not closed. MidPoint can be supported in almost any reasonably recent platform (please contact Evolveum for more details).

Java

- OpenJDK 8 (1.8.0_91, 1.8.0_111, 1.8.0_131)
- Sun/Oracle Java SE Runtime Environment 8 (1.8.0_45, 1.8.0_65, 1.8.0_74)

Java 8 only

MidPoint 3.6 is supported only on Java 8 platforms. MidPoint supported both Java 7 and Java 8 for several years. The support for Java 7 was deprecated in midPoint 3.4.1 and it was removed in midPoint 3.5. It is finally the time to abandon obsolete technology and to move on.
Java 9 is not supported yet. Java release train strategy changed recently and midPoint has to adapt as well. MidPoint will officially support Java long-term-support releases. As Java 9 is not a long-term support release the support for Java 9 in midPoint is questionable. For now we are providing only Java 8 support and we will reconsider the situation after the new Java release train stabilizes.

Web Containers

- Apache Tomcat 8 (8.0.14, 8.0.20, 8.0.28, 8.0.30, 8.0.33, 8.5.4)
- Apache Tomcat 7 (7.0.29, 7.0.30, 7.0.32, 7.0.47, 7.0.50, 7.0.69)
- Sun/Oracle Glassfish 3 (3.1)
- BEA/Oracle WebLogic (12c)

Databases

- H2 (embedded, only recommended for demo deployments)
- PostgreSQL (8.4.14, 9.1, 9.2, 9.3, 9.4, 9.4.5, 9.5, 9.5.1)
- MariaDB (10.0.28)
- MySQL (5.6.26, 5.7)
  Supported MySQL version is 5.6.10 and above (with MySQL JDBC ConnectorJ 5.1.23 and above).
  MySQL in previous versions didn't support dates/timestamps with more accurate than second fraction precision.
- Oracle 11g (11.2.0.2.0)
- Microsoft SQL Server (2008, 2008 R2, 2012, 2014)

Unsupported Platforms

Following list contains platforms that midPoint is known **not** to work due to various issues. As these platforms are obsolete and/or marginal we have no plans to support midPoint for these platforms.

- Java 6
- Java 7
- Sun/Oracle GlassFish 2
- Apache Tomcat 6

Supported Browsers

- Firefox (any recent version)
- Safari (any recent version)
- Chrome (any recent version)
- Opera (any recent version)
- Microsoft Internet Explorer (version 9 or later)

Recent version of browser as mentioned above means any stable stock version of the browser released in the last two years. We formally support only stock, non-customized versions of the browsers without any extensions or other add-ons. According to the experience most extensions should work fine with midPoint. However, it is not possible to test midPoint with all of them and support all of them. Therefore, if you chose to use extensions or customize the browser in any non-standard way you are doing that on your own risk. We reserve the right not to support customized web browsers.

Microsoft Internet Explorer compatibility mode is **not** supported.

Important Bundled Components

Component	Version	Description
ConnId	1.4.2.35	ConnId Connector Framework
LDAP connector bundle	1.5	LDAP, Active Directory and eDirectory connector
CSV connector	2.1	Connector for CSV files
DatabaseTable connector	1.4.2.0	Connector for simple database tables

Download and Install

Release Form	Download	Install Instructions
Binary	http://evolveum.com/downloads/midpoint/3.6.1/midpoint-3.6.1-dist.zip	Installing midPoint from Binary Distribution v3.6.1
Source	From Git repository (tag "v3.6.1") https://github.com/Evolveum/midpoint	Installing midPoint from Source Code v3.6.1
Java API	(javadoc not available) [JAR]	

Schema Doc	https://www.evolveum.com/downloads/midpoint/3.6.1/schema-3.6.1-schemadoc/ [ZIP]	

Upgrade

MidPoint is software that is designed for easy upgradeability. We do our best to maintain strong backward compatibility of midPoint data model, configuration and system behavior. However, midPoint is also very flexible and comprehensive software system with a very rich data model. It is not humanly possible to test all the potential upgrade paths and scenarios. Also some changes in midPoint behavior are inevitable to maintain midPoint development pace. Therefore we can assure reliable midPoint upgrades only for midPoint subscribers. This section provides overall overview of the changes and upgrade procedures. Although we try to our best it is not possible to foresee all possible uses of midPoint. Therefore the information provided in this section are for information purposes only without any guarantees of completeness. In case of any doubts about upgrade or behavior changes please use services associated with midPoint subscription or purchase professional services.

Upgrade from midPoint 3.0, 3.1, 3.1.1, 3.2, 3.3, 3.3.1, 3.4, 3.4.1, 3.5 and 3.5.1

Upgrade path from MidPoint 3.0 goes through midPoint 3.1, 3.1.1, 3.2, 3.3, 3.4.1, 3.5.1 and 3.6. Upgrade to midPoint 3.1 first (refer to the midPoint 3.1 release notes). Then upgrade from midPoint 3.1 to 3.1.1, from 3.1.1 to 3.2 then to 3.3, then to 3.4.1, 3.5.1, 3.6 and finally to 3.6.1.

Upgrade from midPoint 3.6

MidPoint 3.6.1 data model is backwards compatible with midPoint 3.6. MidPoint 3.6.1 data model was slightly extended, but the database data model used in midPoint 3.6 is not affected by this upgrade. No change to the database schema is necessary.

MidPoint 3.6.1 is a release that fixes some issues of previous versions. Although all the changes should be backwards compatible, the changes may still affect deployments that haven't used midPoint correctly or deployments that relied on wrong midPoint behavior that was fixed in 3.6.1 release. The most importa changes include.

- Introduction of authorization exceptions for automatic items.
- Version numbers of some bundled connectors have changed. Therefore connector references from the resource definitions that are using the bundled connectors need to be updated.

Changes in initial objects since 3.6

MidPoint has a built-in set of "initial objects" that it will automatically create in the database if they are not present. This includes vital objects for the system to be configured (e.g. role `superuser` and user `administrator`). These objects may change in some midPoint releases. But to be conservative and to avoid configuration overwrite midPoint does not overwrite existing objects when they are already in the database. This may result in upgrade problems if the existing object contains configuration that is no longer supported in a new version. Therefore the following list contains a summary of changes to the initial objects in this midPoint release. The complete new set of initial objects is in the `config/initial-objects` directory in both the source and binary distributions. Although any problems caused by the change in initial objects is unlikely to occur, the implementors are advised to review the following list and assess the impact on case-by-case basis:

- 010-value-policy.xml: Removed deprecated `lifetime` element.
- 040-role-enduser.xml: Changes with respect to execution-phase authorization exception.
- 160-report-certification-decisions.xml: corrections, optimize for excel, minor design tweaks
- 200-lookup-languages.xml: New languages
- 210-lookup-locales.xml: New languages

Bundled connector changes since 3.6

- The **LDAP connector, AD connector** and **CSV connector** were upgraded to the latest available version.

Known Issues and Limitations

There is a support to set up storage of credentials in either encrypted or hashed form. There is also unsupported and undocumented option to turn off credential storage. This option partially works, but there may be side effects and interactions. This option is not fully supported yet. Do not use it or use it only on your own risk. It is not included in any midPoint support agreement.

Native attribute with the name of 'id' cannot be currently used in midPoint (**MID-3872** - Getting issue details... STATUS). If the attribute name in the resource cannot be changed then the workaround is to force the use of legacy schema. In that case midPoint will use the legacy ConnId attribute names (icfs:name and icfs:uid).

JavaDoc is temporarily not available due to the issue in Java platform. This issue is fixed in Java 9 platform, but backport of this fix to Java 8 is (quite surprisingly) not planned.

As all real-world software midPoint 3.6.1 has some known issues. Full list of the issues is maintained in jira. As far as we know at the time of the release there was no known critical or security issue.

There is currently no plan to fix the known issues of midPoint 3.6.1 *en masse*. These issues will be fixed in future maintenance versions of midPoint only if the fix is requested by midPoint subscriber. No other issues will be fixed - except for severe security issues that may be found in the future.

The known issues of midPoint 3.6.1 may or may not be fixed in midPoint 3.7. This depends on the available time, issue severity and many variables that are currently difficult to predict. The only reliable way how to make sure that an issue is fixed is to purchase midPoint subscription. Or you can fix the bug yourself. MidPoint is always open to contributions.

This may seem a little bit harsh at a first sight. But there are very good reasons for this policy. And in fact it is no worse than what you get with most commercial software. We are just saying that with plain language instead of scrambling it into a legal mumbo-jumbo.

See Also

- midPoint History
- Installing midPoint from Binary Distribution v3.6.1
- Installing midPoint from Source Code v3.6.1