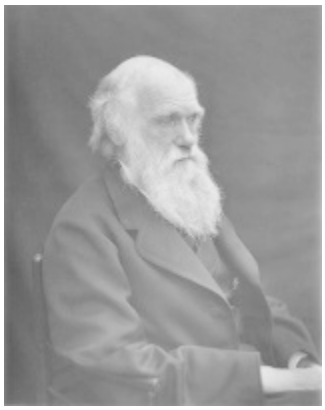
Release 3.7.2

Darwin

Release 3.7.2 is a twenty fifth midPoint release. It is the second maintenance update for 3.7.x version family code-named Darwin. The 3.7.2 release brings bugfixes and several minor improvements.

Release date: 8th June 2018

Charles Darwin



Charles Darwin (1809 - 1882) was English naturalist, geologist and biologist, best known for the theory of evolution. Darwin's famous book On the Origin of Species described theory of evolution, mechanism of natural selection that explains the diversity of life. His voyage on HMS Beagle established him as an eminent geologist and made him famous as a popular author. Darwin has been described as one of the most influential figures in human history.

Darwin's theory of evolution is the unifying theory of the life sciences. The theory describes the process how species evolve and adapt over successive generations. MidPoint 3.7 is such an evolutionary step in midPoint development. This midPoint release brings gradual improvements in many diverse areas. Identity governance features are improved, both in capabilities of the engine and the user interface. MidPoint expressions have gained more power and ease of use. There are notable improvements in user interface, security, task management and many smaller improvements in various areas. The scope of almost the entire release was guided by midPoint subscribers and sponsors - which provided the perfect environment for this step in midPoint evolution.

Credits

Majority of the work on the *Darwin* 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 our thanks to all the people that contributed to the midPoint project both by providing financial support, their own time or those that maintain a pleasant and creative environment for midPoint team. However, midPoint project would not exist without proper funding. Therefore we would like to express our deepest gratitude to all midPoint subscribers that made midPoint project possible.

Features

midPoint 3.7.2 provides following features:

- **Common identity management data model**
    - Extensible object types:
        - User objects to represent users, physical persons and personas
        - Role objects to represent roles, privileges, jobs and so on

        - Org objects to represent organizational units, teams, workgroups, etc.
        - Service objects to represent servers, network devices, mobile devices, network services, etc.
    - Numerous built-in properties
    - Extensibility by custom properties
    - Completely schema-aware system
        - Dynamic schema automatically retrieved from resource
        - Support for primitive data types
        - Native support of multi-value attributes
        - Limited support for complex data types
    - Processing and computation fully based on relative changes
    - Off-the-shelf support for user password credentials
    - Off-the-shelf support for activation (users, roles, orgs, services)
        - 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
    - Representation of all configuration and data objects in XML, JSON and YAML
- **Identity management**
    - Enabling and disabling accounts
    - Support for mapping and expressions to determine account attributes
    - 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
    - Import from file and resource
        - Object schema validation during import (can be switched off)
        - Smart references between objects based on search filters
    - 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)
    - Notifications
    - Bulk actions
    - Passive Attribute Caching (EXPERIMENTAL)
    - Partial multi-tenancy support
- **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
    - Self-healing consistency mechanism
- **Advanced RBAC**
    - 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
    - Rule-based RBAC (RB-RBAC) ability by using conditional mappings in user template and role autoassignment
- **Entitlements and entitlement associations**
    - GUI support for entitlement listing, membership and editing
    - Entitlement approval
- **Identity governance**
    - Powerful organizational structure management
    - Workflow support (based on Activiti engine)

        - Declarative policy-based multi-level approval process
        - Visualization of approval process
    - Object lifecycle property
    - Object history (time machine)
    - Policy Rules as a unified mechanism to define identity management, governance and compliance policies
    - 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
    - Rich assignment meta-data
- **Expressions, mappings and other dynamic features**
    - Sequences for reliable allocation of unique identifiers
    - Customization expressions
        - Groovy
        - Python
        - JavaScript (ECMAScript)
        - 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 identifier
    - Function libraries
- **Web-based administration user interface**
    - 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
- **Connectors**
    - Integration of ConnId identity connector framework
        - Support for Evolveum Polygon connectors
        - Support for ConnId connectors
        - Support for OpenICF connectors (limited)
    - 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
    - Unified Connector Framework (UCF) layer to allow more provisioning frameworks in the future
- **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
- **Security**
    - Fine-grained authorization model
        - Authorization expressions
        - Limited power of attorney implementation
    - Organizational structure and RBAC integration
    - Delegated administration
    - Password management
        - Password distribution
        - Password policies
        - Password retention policy
        - Self-service password management
        - Password storage options (encryption, hashing)
        - Mail-based initialization of passwords for new accounts
    - CSRF protection
- **Auditing**
    - Auditing to file (logging)
    - Auditing to SQL table
    - Interactive audit log viewer
- **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
        - API accessible using a REST, web services (SOAP) and local JAVA calls
- **Reporting**
    - Scheduled reports
    - Lightweight reporting (CSV export) built into user interface
    - Comprehensive reporting based on Jasper Reports
    - Post report script
- **Internals**
    - Task management
        - Task template
        - Node-sticky tasks
- **Operations**
    - Lightweight deployment structure with two deployment options:
        - Stand-alone deployment
        - Deployment to web container (WAR)
    - Multi-node task manager component with HA support
    - Comprehensive logging designed to aid troubleshooting
    - Enterprise class scalability (hundreds of thousands of users)
- **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 3.7.1

- Support for CredSSP version 5 and 6.
- Various bugfixes
- Ninja tool ready for upgrade to midPoint 3.8

Old CSVFile Connector is deprecated and it is no longer bundled with midPoint.
Support for PostgreSQL 8.4 is deprecated. The support will be dropped in the future.
Oracle database 11g support was deprecated in midPoint 3.7. This will be replaced for Oracle 12c database support in midPoint 3.8.
Suport for MySQL 5.6 is deprecated.
Support for Microsoft SQL Server 2008, 2008 R2 and 2012 is deprecated. The support will be dropped in the future.

Quality

Release 3.7.2 (*Darwin*) 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 3.7.2 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 with 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_151)
- Sun/Oracle Java SE Runtime Environment 8 (1.8.0_45, 1.8.0_65, 1.8.0_74, 1.8.0_131)

Web Containers

- Apache Tomcat 8 (8.0.14, 8.0.20, 8.0.28, 8.0.30, 8.0.33, 8.5.4)
- BEA/Oracle WebLogic (12c) - ⚠️ special subscription required

Web container (application server) support

MidPoint 3.7 introduced Stand-alone deployment form that does not need an application server. This is the primary deployment model for midPoint. The deployment to web container is still supported. However the only supported web container is Apache Tomcat. Other web containers (application servers) may be supported if the support is explicitly negotiated in midPoint subscription. Except for those cases midPoint development team will not provide any support for other web containers.

Currently there are no plans to remove support for deployed midPoint installation using a WAR file. However, it is possible that this deployment form will get phased out eventually unless there are active subscribers preferring this deployment method. MidPoint subscription is strongly recommended if you plan to use this method in the future.

Databases

- H2 (embedded). Supported only in embedded mode. Not supported for production deployments. Only the version specifically bundled with midPoint is supported.
  H2 is intended only for development, demo and similar use cases. It is **not** supported for any production use. Also, upgrade of deployments based on H2 database are not supported.
- PostgreSQL (8.4.14, 9.1, 9.2, 9.3, 9.4, 9.4.5, 9.5, 9.5.1)
  Support for PostgreSQL 8.4 is deprecated. The support will be dropped in the future.
- MariaDB (10.0.28)
- MySQL (5.6.26, 5.7)
  Support for MySQL version is 5.6.x is deprecated.
- Oracle 11g (11.2.0.2.0)
  Oracle 11g support is deprecated in midPoint 3.7. This will be replaced for Oracle 12c support in midPoint 3.8.
- Microsoft SQL Server (2008, 2008 R2, 2012, 2014)
  Support for Microsoft SQL Server 2008, 2008 R2 and 2012 is deprecated. The support will be dropped in the future.

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	1.4.3.0	ConnId Connector Framework
LDAP connector bundle	1.6	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

Stand-alone deployment model

MidPoint 3.7 and 3.7.2 deployment method has changed. Stand-alone deployment is now the default deployment method. MidPoint default configuration, scripts and almost everything else was adapted for this method.

- **New midPoint users** and **new deployments** should simply follow the installation manual.
- **Existing deployments** may keep using exactly the same configuration as before. Deployment of midPoint as Web Application is still supported as an alternative. However, stand-alone deployment is now the primary option. It is recommended to migrate the deployment based on application server to a stand-alone deployment in the future. See our brief migration guide.

Release Form	Download	Install Instructions
Binary	http://evolveum.com/downloads/midpoint/3.7.2/midpoint-3.7.2-dist.zip	Installing midPoint v3.7.2
Source	From Git repository (tag "v3.7.2") https://github.com/Evolveum/midpoint	Building MidPoint From Source Code
Java API	https://www.evolveum.com/downloads/midpoint/3.7.2/midpoint-api-3.7.2-javadoc/ [JAR]	
Schema Doc	https://www.evolveum.com/downloads/midpoint/3.7.2/schema-3.7.2-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, 3.5.1, 3.6, 3.6.1 and 3.7

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 3.6.1. 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, 3.6.1 and finally to 3.7.2.

Upgrade from midPoint 3.7 and 3.7.1

MidPoint 3.7.2 data model have not changed since midPoint 3.7. Therefore there is no need to update the database.

Changes in initial objects since 3.7 and 3.7.1

There were no changes to initial object since midPoint 3.7.

Bundled connector changes since 3.7 and 3.7.1.

LDAP and AD connectors were upgraded to latest versions.

Behavior changes since 3.7

- URLs used by Stand-Alone Deployment were changed to match the URLs used by Tomcat-based deployments of midPoint 3.6 and earlier. This means that all deployment forms now use `/midpoint/` context root path in the URL by default (e.g. `http://localhost:8080/midpoint/`). This choice was made based on user feedback to keep the compatibility with previous midPoint versions and to keep the two deployment models as closely aligned as possible. For the stand-alone deployment there is an automatic HTTP redirect from the root URL (e.g. `http://localhost:8080/`) to midPoint context root (e.g. `http://localhost:8080/midpoint/`). Therefore in midPoint 3.7.2 both deployment method should behave in a natural, expected and compatible way.
- Processing of authorizations for proxy authentication in the REST interface was corrected. The processing of proxy authorizations now behave as documented.
- Processing of object authorizations was corrected. Authorizations now take into consideration also the properties of existing removed containers even in *replace* and *id-only delete* cases. Therefore, appropriate property authorization is needed even when deleting a value that contains those properties.
- Password reset schema was deprecated. Existing password reset configuration still works, but it will be replace by new password reset configuration in the future.

Public interface changes since 3.7

- REST interface was extended with experimental password reset method.

Important internal changes since 3.7

There were not critical internal changes since midPoint 3.7.

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 at 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 3.7.2 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 3.7.2 *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 3.7.2 may or may not be fixed in midPoint 3.8. 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 v3.7.2
- Building MidPoint From Source Code