



What's New in MidPoint 4.8

Katarína Bolemant, November 2023

Development Team Leader

Agenda

- New support model
- What's new in midPoint 4.8
- Changes since midPoint 4.4
- Deprecations, removals and incompatible changes
- A plan for 4.9
- Webinars



New Support Model

- Feature releases ~~1~~ 2 years of support
 - No possibility for extended support
- LTS releases ~~3~~ 5 years of support
 - Possibility for extended support +3 years
 - Possibility for vintage support +2 years
 - => up to 10 years of support
- LTS released every 4th year
 - Next LTS in 2027
- New support model applicable since version 4.8



MidPoint 4.8 “Curie” at a Glance

- LTS release (5 years support)
- New features
 - Role Mining
 - Identity Recovery
- Improvements
 - Security-related Improvements
 - Streamline Upgrades
 - First steps methodology

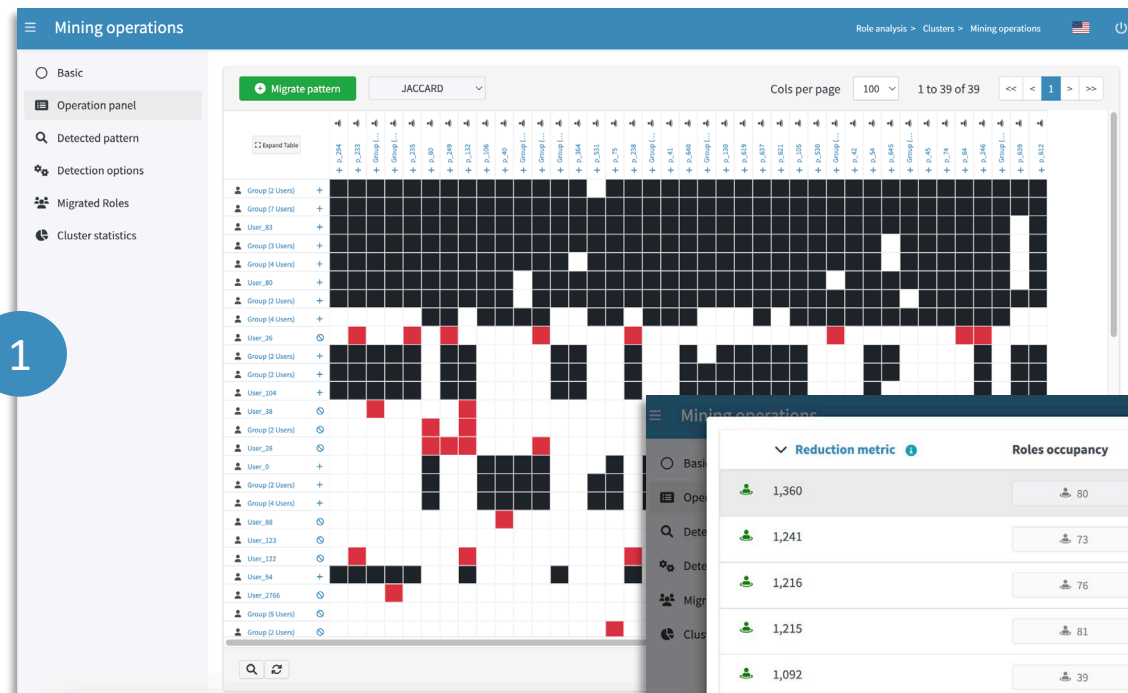


Role Mining

- AI/ML powered functionality for mining roles based on the existing data in midPoint
 - Analyzing existing assignments to application roles
 - Detection based on data clustering, pattern recognition and similarity methods.
 - Suggestion of new business roles candidates
- Bottom-up approach to create business roles
- Helps with simplifying role-based access control
- Reduces risk of access escalation
- Makes entire IGA more understandable and manageable



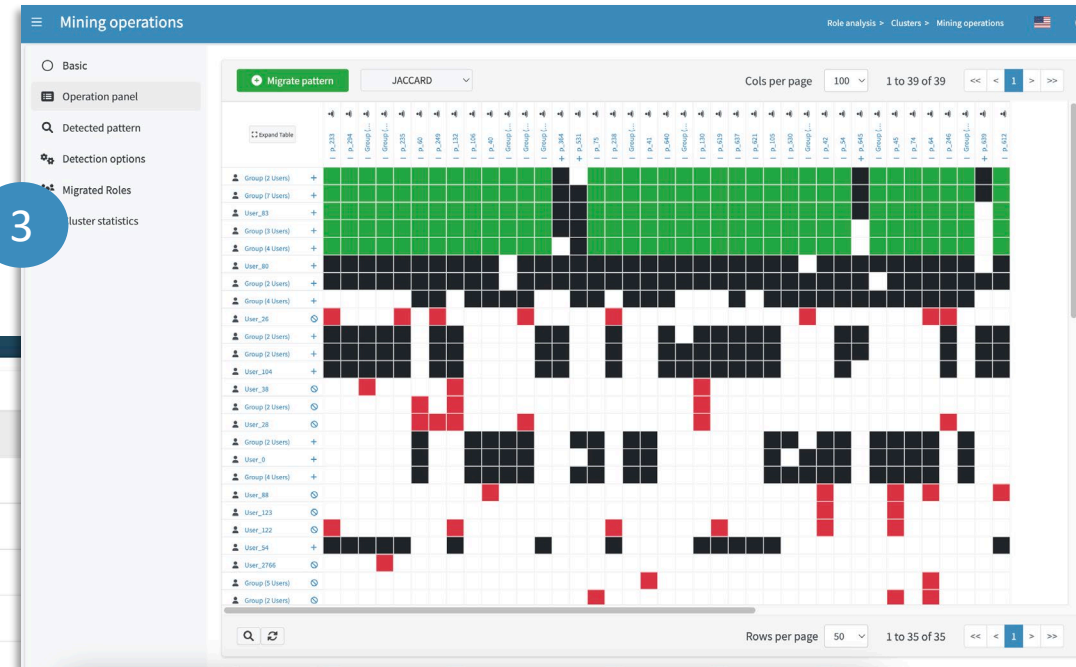
Role Mining in Action



2

Reduction metric	Roles occupancy	Users occupancy	
1,360	80	17	
1,241	73	17	
1,216	76	16	
1,215	81	15	
1,092	39	28	
1,080	40	27	
1,066	41	26	Explore
1,053	81	13	Explore
1,050	42	25	Explore
1,044	36	29	Explore

Rows per page 10 1 to 10 of 30



Role Mining - Benefits

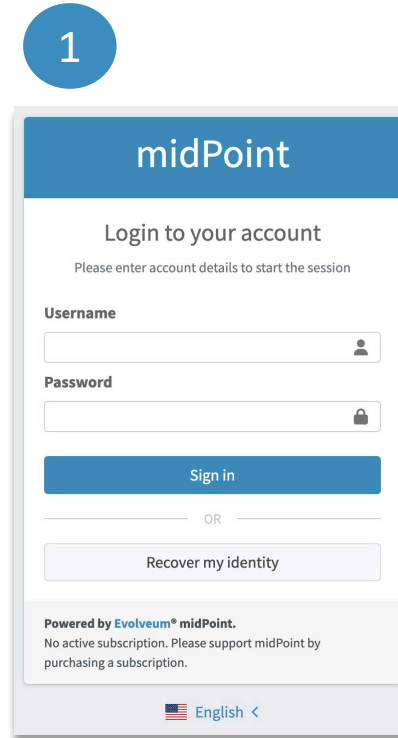
- Simplified access management
 - Assign one business role rather than multiple individual accesses.
- Reduced administrative overhead
 - No need to picking up multiple accesses related to job position or project.
- Transparent access
 - Simplifies compliance reporting.
- Efficient audit trails
 - Capturing more significant, meaningful changes and reducing the noise
- Enhanced business agility



Identity Recovery

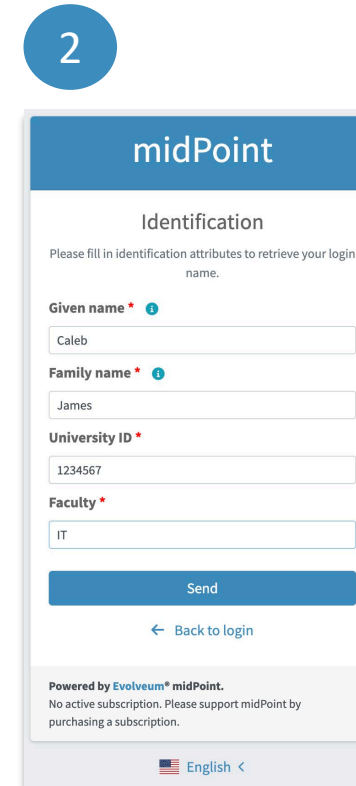
- Possibility to recover identity data
- Configuration adjusted according to the type of identity
- Different recovery options available for different types of identities
- Using existing midPoint functionality
 - Smart correlation
 - Flexible authentication
- Disclosure information auditing
- Requested by subscriber

1



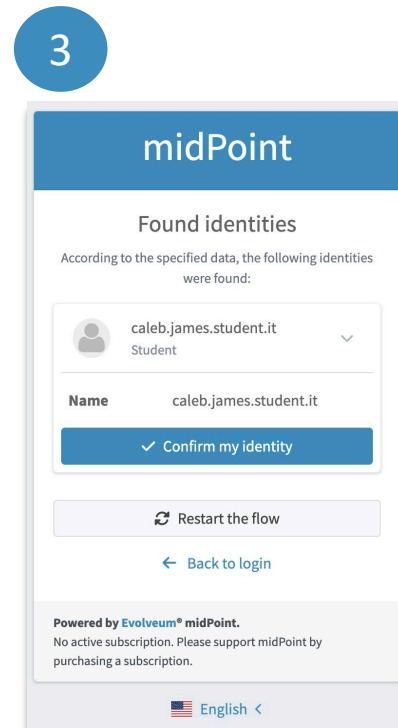
The first screen is the 'midPoint' login page. It has a blue header with the 'midPoint' logo. Below the header, it says 'Login to your account' and 'Please enter account details to start the session'. There are two input fields: 'Username' and 'Password'. Below the password field is a 'Sign in' button. There is an 'OR' separator and a 'Recover my identity' button. At the bottom, it says 'Powered by Evolveum® midPoint. No active subscription. Please support midPoint by purchasing a subscription.' and has a language selector for 'English'.

2



The second screen is the 'midPoint' identification page. It has a blue header with the 'midPoint' logo. Below the header, it says 'Identification' and 'Please fill in identification attributes to retrieve your login name.' There are four input fields: 'Given name' (with value 'Caleb'), 'Family name' (with value 'James'), 'University ID' (with value '1234567'), and 'Faculty' (with value 'IT'). Below the fields is a 'Send' button. There is a 'Back to login' link. At the bottom, it says 'Powered by Evolveum® midPoint. No active subscription. Please support midPoint by purchasing a subscription.' and has a language selector for 'English'.

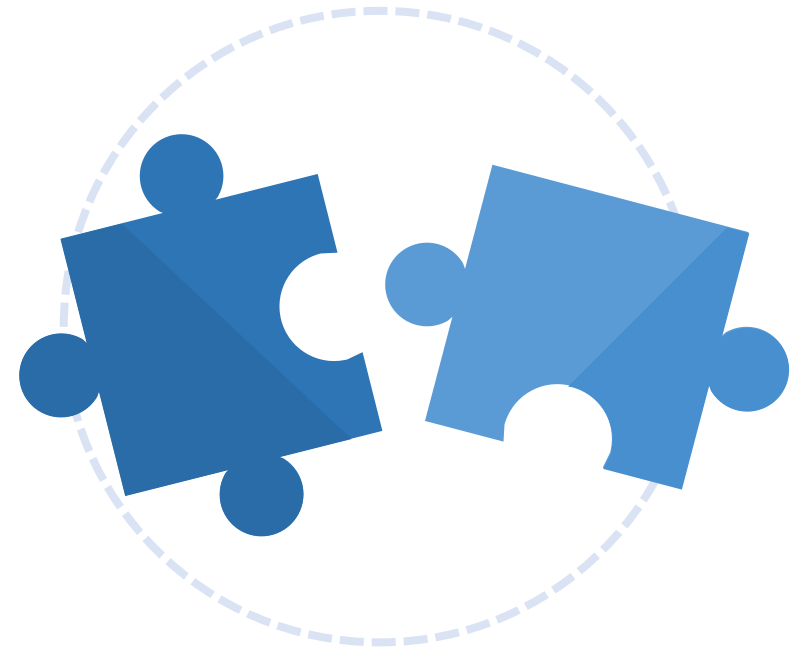
3



The third screen is the 'midPoint' 'Found identities' page. It has a blue header with the 'midPoint' logo. Below the header, it says 'Found identities' and 'According to the specified data, the following identities were found:'. There is a dropdown menu showing 'caleb.james.student.it Student'. Below the dropdown is a 'Name' field with the value 'caleb.james.student.it'. There is a 'Confirm my identity' button. There is a 'Restart the flow' button. There is a 'Back to login' link. At the bottom, it says 'Powered by Evolveum® midPoint. No active subscription. Please support midPoint by purchasing a subscription.' and has a language selector for 'English'.

Flexible Authentication

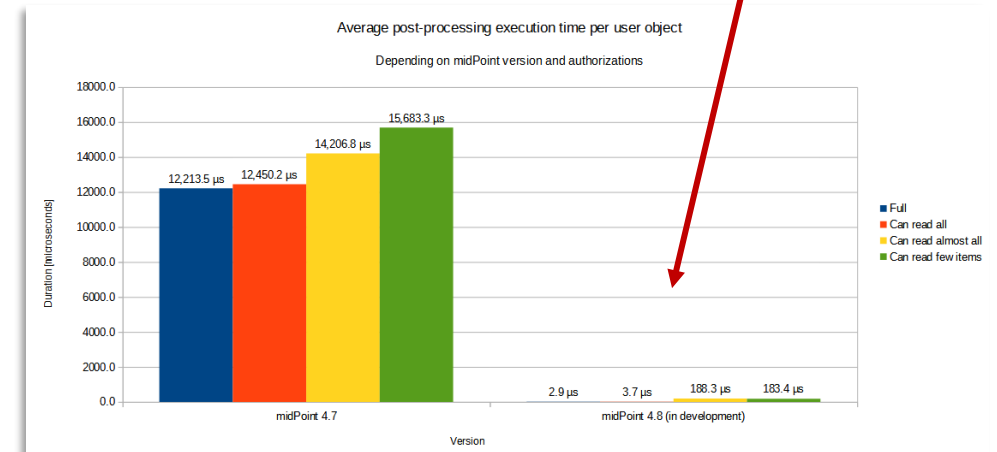
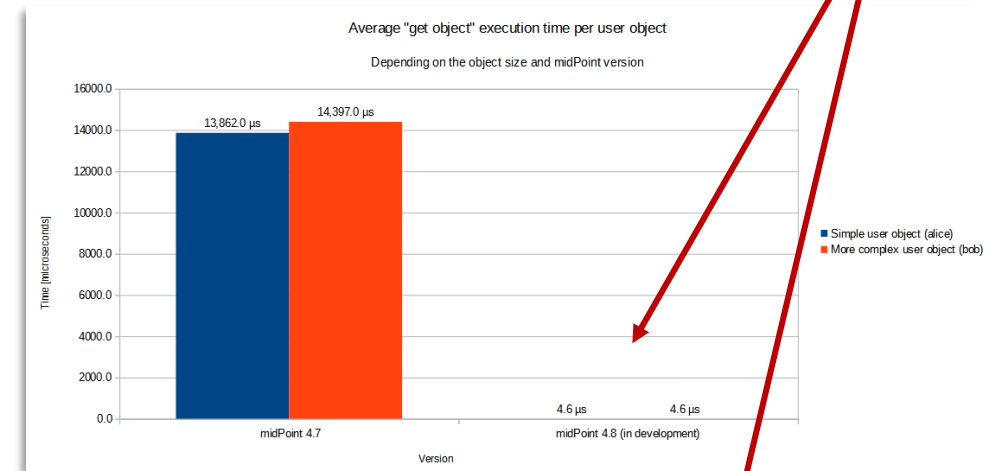
- New modules added:
 - Archetype selection module
 - Correlation module
 - DUO module
- Improved OIDC module
- Support for MFA



Security-related Improvements

- Performance improvements
 - GUI,
 - Reports,
 - Scripts using `midpoint.getObject(..)`, `midpoint.searchObejcts(..)`
- Priviledge elevation
 - `runAsRef` vs. `runPrivileged`
 - Improved auditing
- Trusted bulk actions
 - Custom actions executable by non-super users
- OWASP dependency - check

midPoint 4.8



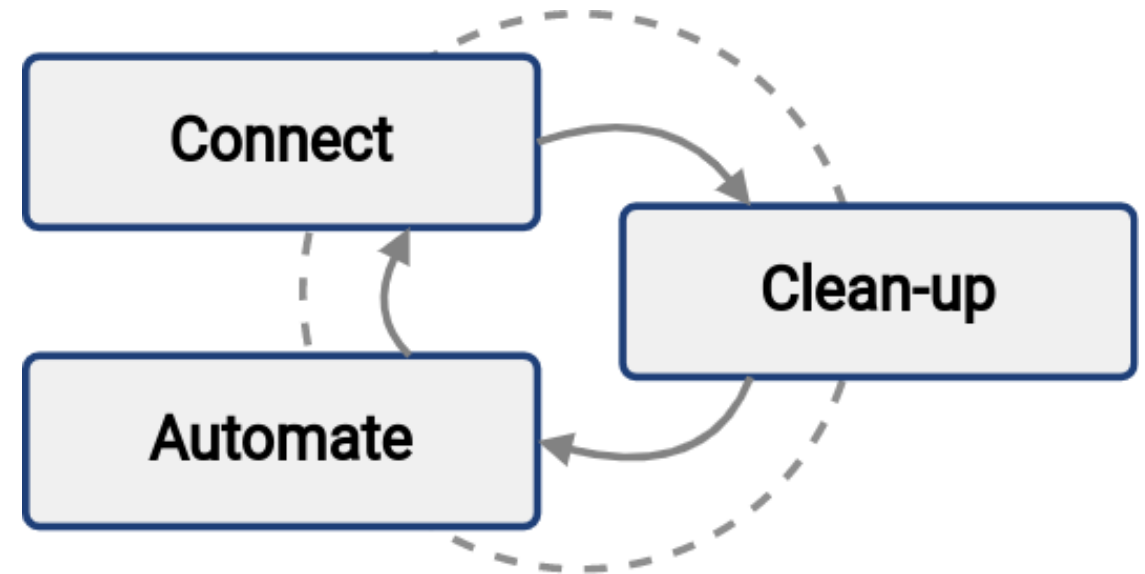
Streamline Upgrades

- Ninja
 - A command line tool for low level management of data
- Significantly improved during 4.8
 - Focusing on upgrade procedure
- Verification and objects upgrade
- Pre-upgrade checks
- DB schema upgrade
- Installation upgrade
- Initial objects upgrade (experimental)



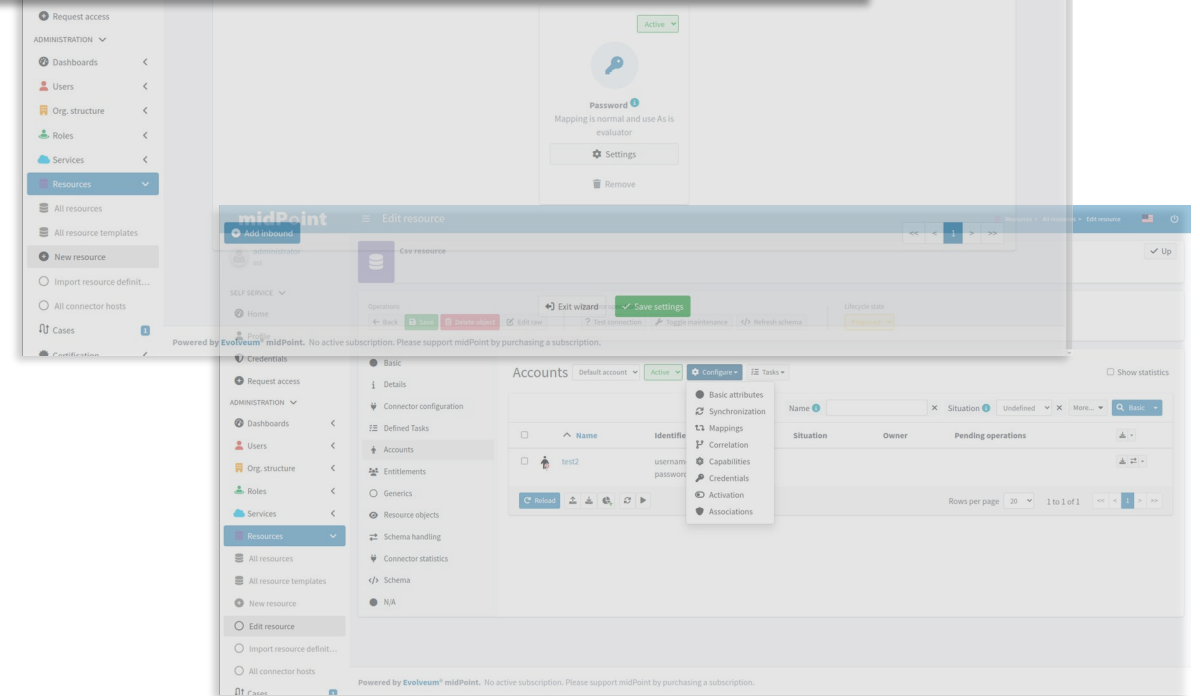
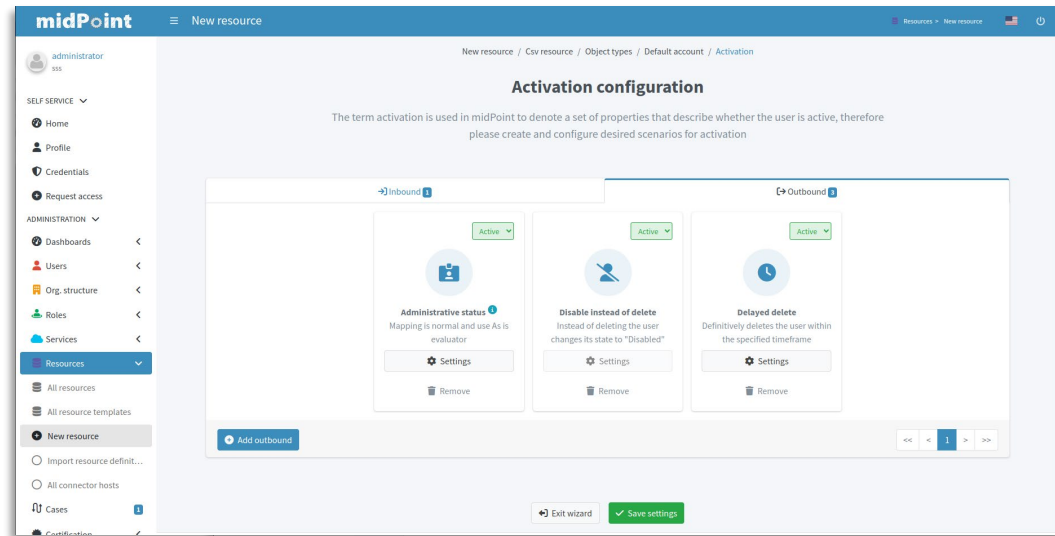
Firsts Steps Methodology

- midPoint deployment methodology
 - Describing iterative approach
 - Providing value in small steps asap
- Steps included
 - Connecting source/target system
 - Using smart correlation
 - Testing with simulations
 - Detecting and handling orphaned accounts with marks
 - Managing identity lifecycle
 - Automating the JML processes
 - Managing a birthright permissions
 - Go live with any quality of data



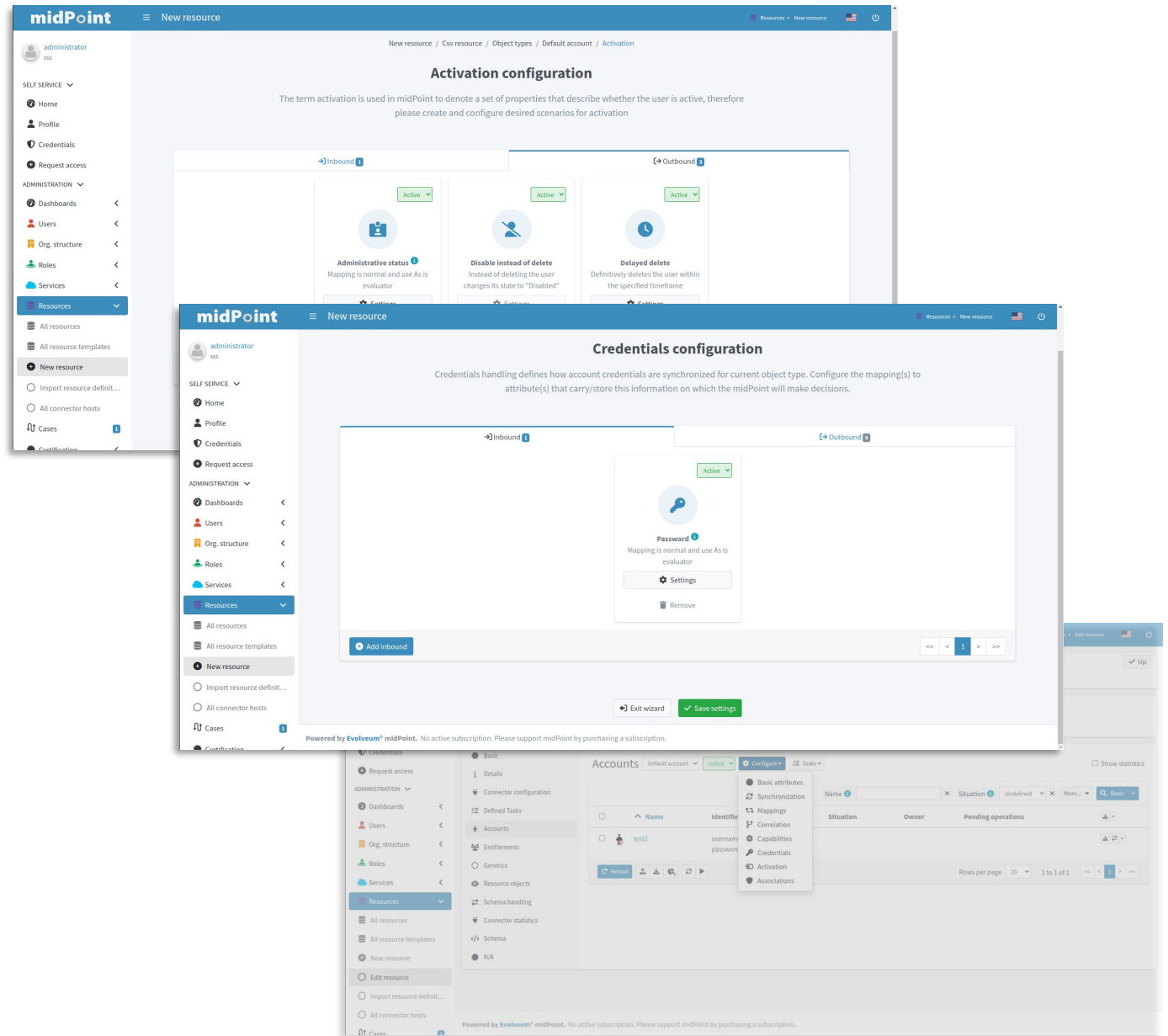
Resource Wizard

- Pre-defined activation mappings
 - Delayed delete
 - Disable instead of delete
 - Pre-create
- Password step
- Better integration with resource details



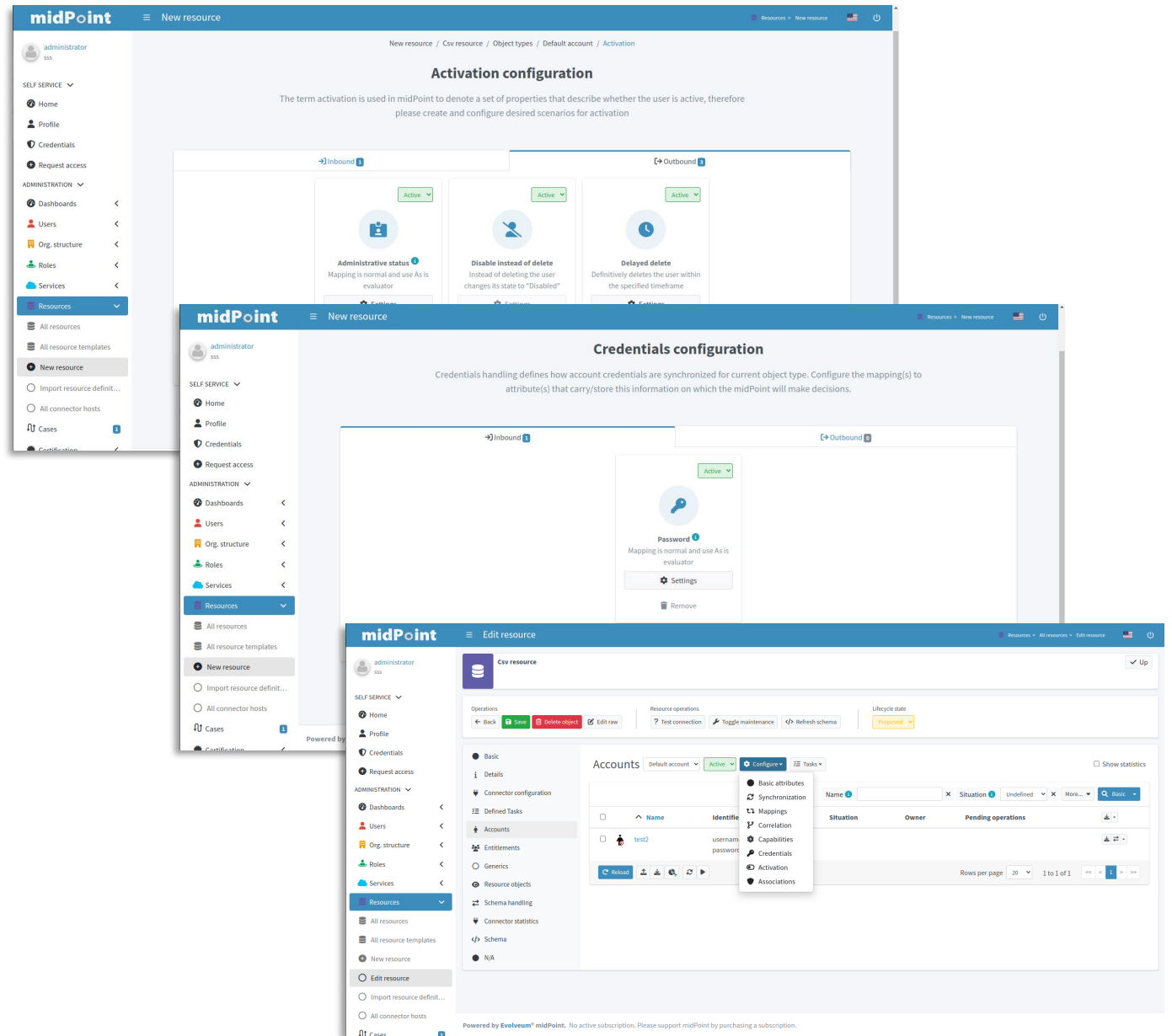
Resource Wizard

- Pre-defined activation mappings
 - Delayed delete
 - Disable instead of delete
 - Pre-create
- Password step
- Better integration with resource details



Resource Wizard

- Pre-defined activation mappings
 - Delayed delete
 - Disable instead of delete
 - Pre-create
- Password step
- Better integration with resource details



Changes Since midPoint 4.4

- Simulations
- Object marks
- Smart correlation
- Request access wizard
- Improved IGA reporting
- Resource templates
- Refreshed look&feel



| Platforms

- Operations systems
 - Linux
 - Windows Server 2022
- Java
 - Java 21 – recommended
 - Java 17
- Databases
 - PostgreSQL 14, 15, 16 (native implementation)
 - Oracle 21c (generic implementation)
 - Microsoft SQL Server 2019 (generic implementation)



Deprecations, Removals and Incompatible Changes

- Support for PostgreSQL with generic repository implementation was removed
 - Migrate to native implementation when using PostgreSQL
- Ninja options were consolidated, which resulted to the incompatible changes
 - See the release notes and documentation
- Password reset with only mailNonce or securityQuestions authentication module won't work. Another module before the those two is required to identify the user.
 - focusIdentification module can be used.
- Initial objects changes
 - See the release notes
- Schema deprecations
 - Use ninja to show you the deprecations



A plan for 4.9

- Planned release date October 1, 2024
 - One-year release cycle
 - Feature release
- Features and Improvements planned
 - WCAG Compliance
 - Attribute caching
 - Lightweight processing
 - Role Engineering improvements
 - Configuration management
 - Certifications improvements
 - Advanced lifecycle model
 - Simplified groups and memberships management



A Timeline

MidPoint Version	Release Date
4.8.1	29-Jan-2024
4.8.2	10-May-2024
4.8.3	19-Aug-2024
4.9	1-Oct-2024
4.8.4	8-Oct-2024
4.8.5	16-Jan-2024
...	...

- Planned timeline
- May differ in reality
- Security updates might change the planned release dates

Webinars

- First Steps Methodology Webinar, November 9, 2023
- Resource Wizard, November 21, 2023
- Navigating the Access Control Maze, December 5, 2023
- Simulations, December 7, 2023
- Upgrade with Ninja, January 25, 2024
- More webinars coming in 2024



Meet Us at TIIME

- Jan 29 - Feb 01, 2024, Copenhagen, Denmark
- MidPoint Working Group (Jan 29 - 30)
 - Share midPoint experience
 - Knowledge exchange and collaboration
- See the [agenda](#)
- Call for speakers
 - Contact us at marketing@evolveum.com
- Register here: <https://tiime-unconference.eu/>



Conclusion



- MidPoint 4.8 supported for 5 years
- Preparing
 - Report from penetration testing
 - MidPoint and ISO 27001
 - Webinars
- Meet us at TIIME
- Join the First Steps training
- Any feedback welcomed

Thank you for your time

Do you have any **questions**? Feel free to contact us at info@evolveum.com

Follow us on social media or **join us** at GitHub or Gitter!



Evolveum

© 2023 Evolveum s.r.o. All rights reserved.