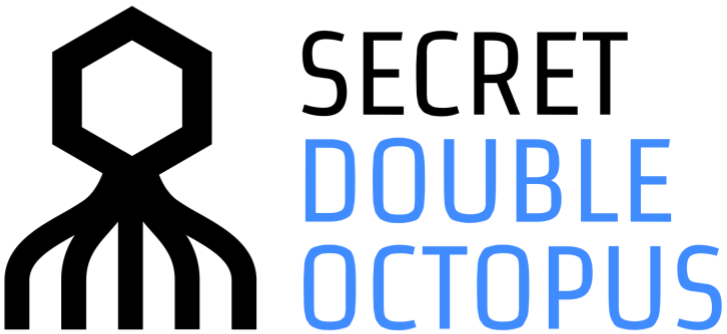
March 7, 2019



Octopus Authentication Server
Version 3.1.2 Release Notes

Overview

These release notes describe the new features and enhancements available in Octopus Authentication Server version 3.1.2

Pre-Requisite

For Upgrade Only: Authentication server 3.0.2 or 3.0.6 installed and working

Release Features

Authentication Server version 3.1.2 is a major upgrade that supports new Look & Feel, new UX with simple configuration flow and many new features supporting solution scalability and no phone solution.

What's new

1. Mobile Device Information (Management Console can now present the device type, version and Octopus Authenticator version)
2. SMTP Test email (The admin can now test that the SMTP is working by sending test mail)
3. SAML Services added logout process from service
4. Octopus Services overwrite parameters per directory (allows setting service parameters for each directory)
5. Added support email to allow replacing the support mail in the user invitation from the default (support@doubleoctopus.com) which was confusing for end customers
6. Added Admin email to allow sending system notifications on status changes in one of the critical system components (DB, Authentication Server, License, SMTP, Cloud Server). The notification email will be sent on any changes in one of these components to let the admin know that the system is not operational, and action should be made.
7. The Management Console enhanced the UX and UI capabilities to allow simple and smooth operations.
8. Added AD sync new feature: when user is deleted from the AD it will automatically be blocked on the Octopus Management Console; when user is disabled on the AD, it will be presented as disabled on the Octopus Management Console.
9. Active directory sync now presents the last sync time of the directory to allow the admin to track the sync timing
10. Improve notification bar, with display icons with notifications on each component status
11. Improve active directory sync (new sync now and re-sync all in case admin selects to resync all AD again)

12. Users view now includes the tree of all users. Now it is simple to navigate on the tree. The location of the tree is saved once you go back to the tree of users
13. New feature to support system failure mode: when there is a connection problem in Octopus cloud or no internet connection outside of the organization, the admin can switch to system failure mode and allow all users to authenticate with username and password (placed on the Octopus authenticator mobile app →Credentials)
14. New feature presenting list of user's workstations used. With this feature the admin can track what workstations this user is authenticated to.
15. Improvement in Audit messages
16. Directory now supports multi-domain controllers, which allows setting a list of domain controllers for high availability
17. Changes in Service tabs: combined directory and users tab to allow simple configuration of users and directories.
18. New feature – Bypass unenrolled users: when a user is not enrolled in the system but is available in the AD, once this user is authenticated then the Octopus Authentication Server will bypass the Octopus authentication and will authenticate this user directly with the AD with username and password.
19. AWS service now supports additional options for use of Role ARN. The admin can now set the Role ARN in one of the aliases and choose it directly from the login page in the following format username:1
20. Database configuration now support encrypted format to allow connection with DB that require encryption as part of the connection string
21. New and improved online help
22. New feature – Automatic invite group members: the admin selects group/groups that will be user as automatic invite group members. When a user is added to this group he/she will be automatically invited to enroll to Octopus Authentication system. When a user is removed from the group, he/she will be blocked
23. New feature – Allow access from external network: for each SAML service the admin can now choose if to allow users to access this service from outside of the organization.
24. New feature – for users who forgot their phone or lost their phone (temporary), the admin can mark this user as bypass and then the user can continue working with username and temporary password generated by the IT admin.
25. New publish button: even if the system presents that there are no pending items to publish, the admin can choose to publish the changes again by pressing on the DB icon and redirect to database configuration page. There is a new button for publish

OS Support

1. RH 7.4 and above
2. CentOS 7.4 and above