RELEASE NOTES

AUTHCONTROL 4.2.0 Release Notes

JUNE 2022

CURRENT PRODUCTION VERSIONS

	Version	Build Number
AuthControl Sentry	4.2.0	(6595)
AuthControl User Portal	4.2.0	(6598)
AuthControl Single sign-on	4.2.0	(6599)

RECOMMENDED UPGRADE SPECIFICATIONS

Version 4.2.0 recommendations
4 cores and 4gb Ram. For high load environments please contact Swivel Secure for sizing recommendations.

INTRODUCTION

This document provides an overview of what is new and what has been updated in AuthControl Sentry®. Please ensure you have read and understood the release notes before deploying this updated version 4.2.0.

The list below provides a summary of the different sections in this document

Swivel Secure, 1200 Century Way, Thorpe Park, Leeds LS15 8ZA
www.swivelsecure.com

1.0 UPDATE GUIDANCE

This section provides basic guidance on updating your AuthControl Sentry® appliance using our YUM update service. If you require additional assistance please contact your Swivel Secure Partner, or if you have a maintenance agreement in place, contact the Swivel Secure Support team.

- Only direct upgrades from AuthControl Sentry® V4.x are supported. If you have a previous version of AuthControl Sentry®, please contact your Swivel Secure Partner or Swivel Secure Support team.
- Upgrades require a V4.x license
- Internet Access is required
- Working external DNS is required

1.1 SPECIFICATION REQUIREMENTS

Before commencing the update, please ensure your Swivel Secure appliance or appliances meet the required specification below.

The required specifications for AuthControl Sentry® V4 virtual appliances.

- 4 GB RAM (minimum)
- 4 cores (minimum)
- 80GB HDD (Thick Provisioned)
- VMware ESX/ESXi 4 or above
- 1 vNIC (minimum)
- Hardware only – please ensure your hardware appliance has sufficient memory to perform the upgrade before starting

For high load virtual environments more resources (Memory & CPU) can be added. Please contact supportdesk@swivelsecure.com for more information as additional settings may be required.

For virtual appliances - ensure you take a snapshot before you start

For hardware appliances - ensure you take a full backup through the CMI before you start

1.1 PERFORMING THE UPDATE

To perform the update, please connect to the Console/CMI and navigate to Menu > Administration > Update Appliance.

Fig. 1.0 shows the Administration menu in Command Management Interface in AuthControl Sentry®

The order in which you perform a system update is important. Please follow the order below:

1. CMI - Please ensure you logout and then back in again after CMI Update.
2. System (Linux OS, services, drivers, etc). There may be a requirement to perform multiple system updates depending on your current version. Please re-run the system update until no further updates are required. After each system update, a reboot should be performed.
3. AuthControl Sentry®

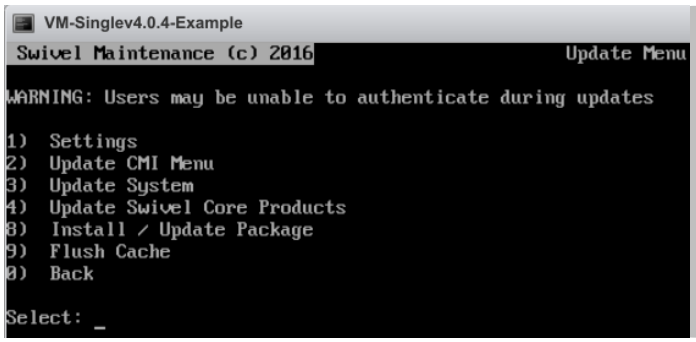

Fig. 1.1 shows the Update menu in AuthControl Sentry®

If you have an high availability (HA) environment, update the standby appliance first.
Once successful, update the primary appliance.

2.0 AUTHCONTROL SENTRY® (ACS 4.2.0)

This section lists all the changes to the AuthControl Sentry®.

2.1 **Core Improvements and features**.

- Push notification authentication can now be configured using reverse proxy
- Database migration process from older appliances are improved
- Database migration process from older MSSQL databases are improved
- Login sessions now sync via database
- IP addresses reserver for user VPN account can be sent via RADIUS and retrieved from AD
- Reporting now includes source IP and authentication method used by the user
- Group display order is now consistent across all screens
- Policy for account lockout time

2.2 **User Portal improvements and features**

- AD password management in User Portal
- Account 'claim code' feature for users with no email or telephone in repository
- Self management: users can now change their PIN with account locked
- Self management: users can now unlock the account with *Reset PIN* or *Change PIN* option

2.3 **Single Sign-On improvements and features**

- Local applications can be defined in SSO portal with new PAM method / user known credential storage
- Local applications can be defined in SSO portal with new P2AM method / user will never know credentials
- Web applications supporting OAUTH2 can be integrated in SSO portal
- Web applications supporting OpenID can be integrated in SSO portal

3.0 BUG FIXES (4.2.0)

- Log4J updated to 2.17.1 and necessary maintenance undertaken to make this compatible
- Name ID format now available in SAML SSO integrations
- PINless policy and PINpad implementation caused duplicated digits to be displayed, now handled
- Handling of special non UTF-8 digits in passwords to avoid invalid characters logging
- Reset password option was ignored unless policy indicated that password is required. Fixed option by resetting password irrespective of whether password required policy is set / not set.
- User groups with . character in the name were not being assigned to repository on first sync
- Connectivity loss during User Sync now results in aborted sync
- Latest ActiveMQ libraries updated to fix vulnerabilities
- App provision issues for usernames containing spaces rectified by URL decode fix
- Fixed reported behaviour conflict of timed lock out policy with other policies

4.0 RECOMMENDATIONS

- Any reports that reference the policy flags table, PINSAFEC, will not work with Sentry version 4.2 or later, and must reference the new status flags table, PINSAFES.

FURTHER ASSISTANCE

If you are an existing customer and have purchased through a Swivel Secure Partner, please contact them for further assistance

If you are an Accredited Partner and you wish to raise a ticket, please use the link below.

Click here

As a customer with a Premium Maintenance Agreement, our team of security experts are here to help you 24/7. The service agreement you received categorises issues in priority order P1 through to P4.

Click here

SWIVEL SECURE PRIVACY POLICY

Swivel Secure Limited a private limited company registered in England and Wales, whose registered address is Equinox 1, Audby Lane, Wetherby, LS22 7RD (registered company number 04068905). ("Swivel," "We" or "Us"), is committed to respecting the privacy rights of visitors to the Swivel Secure website at www.swivelsecure.com and our associated customer support portal at supportdesk.swivelsecure.com (the "Site").

For more information on the Swivel Secure Privacy Policy click here