RELEASE NOTES
AUTHCONTROL SENTRY 4.1

JULY 2019

CURRENT PRODUCTION VERSIONS

	Version	Build Number
AuthControl Sentry	4.0.5	(5560)
AuthControl User Portal	4.0.5	(5518)
AuthControl Single sign-on	4.0.5	(5521)

RECOMMENDED UPGRADE SPECIFICATIONS

Version 4.1 recommendations
4cores 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 4.1.

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

1.0 Update guidance

2.0 AuthControl Sentry® updates

3.0 User Portal updates

4.0 Single sign-on (SSO) Unified Portal updates

5.0 Resolved issues

© 2019 Swivel Secure
Swivel Secure, Equinox 1, Audby Lane, Wetherby, Leeds LS22 7RD
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

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

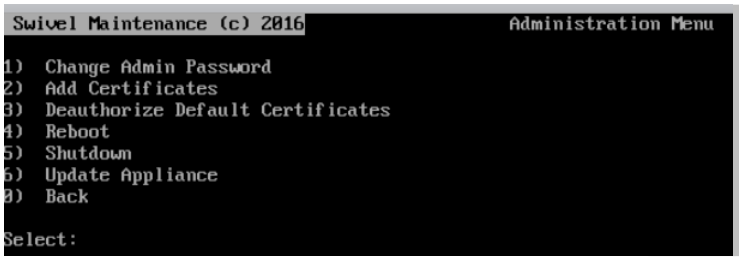

Fig. 1.0 shows the Administration menu in Command Management Interface in AuthControl Sentry®

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)
3. AuthControl Sentry®

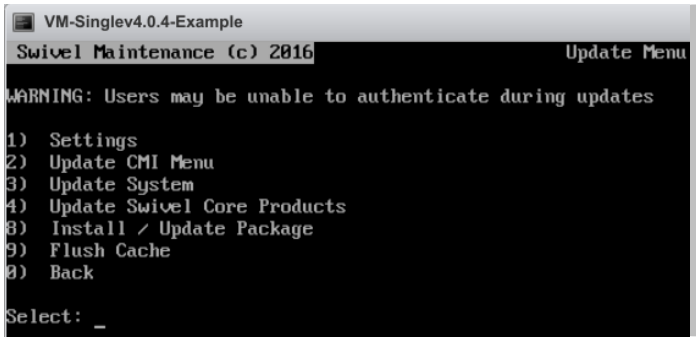

Fig. 1.1 shows the Update menu in AuthControl Sentry®

It is recommended that following a full update the appliance be rebooted.

© 2019 Swivel Secure
Swivel Secure, Equinox 1, Audby Lane, Wetherby, Leeds LS22 7RD
www.swivelsecure.com

2.0 AUTHCONTROL SENTRY®

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

2.1 Added possibility to authenticate non-users for multiple repositories by adding “ANY” option to "Server to use to attempt to authenticate non-users" in "Repository > Servers" (CO-887)

- Users that do not appear in the AuthControl Sentry® database can now be authenticated against multiple repositories using the username/password for the repository. This aids in the migration of users to the Swivel Secure AuthControl Sentry® platform

2.2 New Transport:

- FoxBox SMS Gateway (CO-892)
- AppDragon SMS Gateway (CO-919)

2.3 Added option to “Use password mask as policy” (CO-906)

- Previously the Password mask option was only used for system generated passwords. It has now been made available to the Change Password section in User Portal to control when a user creates a new password and is enabled through a policy.

2.4 Added new button “Reset PIN/Password” in user administration. This allows to change both PIN and Password and send a single credentials email. (CO-907)

- This allows changing both PIN and Password and to send a single credentials email rather than having to change each one individually.

2.5 Changed Mobile Provisioning to immediately delete existing Security Strings when the administrator requests the provision. This is instead of removing them only when the process is complete (CO-866)

- Existing Security Strings will be deleted immediately when the Administrator requests a new mobile Provision. Previously this would happen on completion of the provisioning process for the user’s new device. This posed a risk: a lost mobile phone could still be used to authenticate, until the new device was fully provisioned.

2.6 Added new button “Abort sync” in user administration. This provides the ability to abort the current running User Sync job. (CO-896)

- This allows to abort the currently running User Sync job.

2.7 Added the possibility to choose Mobile App version in PNA Transport (CO-972)

2.8 Changed repository names to be case-insensitive. (CO-300)

© 2019 Swivel Secure

2.9 Added support for ExcelSecu tokens (CO-881)

2.10 Updated encryption ciphers for SSH Daemon – supported ciphers are now aes128-ctr, aes192-ctr and aes256-ctr - (AP-228)

2.11 Repositories are now non-case-sensitive (CO-300)

3.0 USER PORTAL UPDATES

This section lists all the enhancements to the User Portal feature within AuthControl Sentry®.

3.1 Added Change Password option (when using local repository only) (UP-63)

- This allows a user to change the password to something they choose, rather than have a random password generated by AuthControl Sentry®

3.2 Check password mask when using change password option. Requires "Use password mask as policy" enabled (CO-906)

- The password mask determines the length and type of characters allowed when creating or changing passwords. It requires "Use password mask as policy" enabled. This is used in conjunction with UP-63 above.

3.3 Added Branding customisation feature (UP-64)

- Allows the customisation of colours, logos and backgrounds for the user portal.

4.0 SINGLE SIGN-ON (SSO) UNIFIED PORTAL UPDATES

This section lists all the changes within the SSO functionality of AuthControl Sentry®

4.1 Added branding customisation feature (SE-214)

- Allows the customisation of colours, logos and backgrounds for the Unified Portal

4.2 Added IP forwarding header to allow the usage of load balancing with SSO (SE-201)

- SSO rules allow checking users IP address in policy, if this is hidden by the load balancer, then it can't be used. Most load balancers allow forwarding of HTTP headers to identify original users IP address, which can now be accessed by SSO

4.3 Improved navigability in authentication (added back button) (SE-207)

- If a user makes a mistake when authenticating at the Unified Portal, it is no longer necessary to close the browser and start again. A back button has been added which allows a user to return to the start of the authentication.

© 2019 Swivel Secure

4.4 Changed SAML IDP-initiated flow. It no longer requires a redirect to the Service Provider before authentication. (SE-177)

- SAML IDP-initiated authentications no longer require a redirect to the Service Provider before authentication

4.5 Added new authentication method: PICpad (SE-213)

- PICpad is now available for use in the Unified Portal for SSO.

4.6 Added new rule: Mobile App, checks if the user has a provisioned device (SE-211)

- Single sign-on now has the ability, to check to see if the user has a provisioned device (AuthControl Mobile®), as part of the SSO rules.

4.7 Added the possibility to change PIN for first login when the user has this policy (CO-908)

- When configured, users accessing Unified Portal and authenticating for the first time are redirected to the User Portal to change their PIN.

4.8 Added multi-factor authentication (MFA) support to authentication methods (SE-219)

- Using SSO rules it is possible to create a specific order for authentications for MFA to take place. It is possible to configure as many authentication options as you have available. This could be any combination of username & password, TURing, PINpad®, PICpad, SMS, AuthControl Mobile® OTC, AuthControl Mobile® PUSH, Hardware Token, AuthControl Voice or fingerprint.

4.9 Added support for UTF-8 in localization (for ex: Japanese characters) (SE-216)

- This provides support for the correct display of additional characters (e.g. Japanese characters).

4.10 Changed Images upload to work properly in HA environment (SE-220)

- The location of stored and uploaded images has been changed, so only a single upload is required, and the images will be synchronised between HA devices. Previously images needed to be uploaded to each appliance in HA pair.

4.11 Username is taken from X509 client certificate automatically (SE-221)

© 2019 Swivel Secure
Swivel Secure, Equinox 1, Audby Lane, Wetherby, Leeds LS22 7RD
www.swivelsecure.com

5.0 RESOLVED ISSUES

This section lists all the bug fixes within the AuthControl Sentry® platform.

5.1 Fixed issue with using cached passwords on AuthControl Desktop® (CP-94)

5.2 Fixed issue where credential email was sent even if new credentials were not set. Now it requires Policy "Auto. set credentials on user creation" to be enabled (CO-904)

5.3 Fixed issue when "require password" was set to true, changing the PIN is User Portal would return error (CO-905)

5.4 Fixed issue with initial credentials not being imported on first user sync when "Auto-Set Credentials on User Creation" is disabled (CO-910)

5.5 Fixed issue with Mobile app provisioning failing when using User Portal QR Code together with OATH Mode (CO-899)

5.6 Fixed migration failure when source database was Oracle (CO-913)

5.7 Fixed User Portal confirmation code failing in HA (CO-898)

5.8 Fixed SMTP messages encoding when using non-ASCII characters (CO-902)

5.9 Fixed Transport Queue (Active-MQ) not sending messages (CO-911)

5.10 Fixed accounts not being locked when authenticating with Username and Password within the single sign-on functionality (SE-212)

5.11 Fixed AuthControl Desktop® risk-based authentication (RBA) not requesting offline Security Strings (CP-79)

5.12 Fixed Favicon so it now shows in Sentry Core Administration console (CP-932)

5.13 Resolved issue where under certain circumstances MON service does not react to a tomcat failure in HA deployment - (AP-227)

5.14 Removed Windows Gina Menu (CO-1038)

5.15 Fixed MS-CHAP challenge check (CO-702)

5.16 Remove ExcelSecu support

© 2019 Swivel Secure

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

COPYRIGHT

All contents copyright © 2019 Swivel Secure. All rights reserved.

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