RELEASE NOTES
AUTHCONTROL 4.1.1 Release Notes

NOVEMBER 2020

CURRENT PRODUCTION VERSIONS

	Version	Build Number
AuthControl Sentry	4.1.1	(5560)
AuthControl User Portal	4.1.1	(5518)
AuthControl Single sign-on	4.1.1	(5521)

RECOMMENDED UPGRADE SPECIFICATIONS

Version 4.1.1 recommendations
2cores 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 4.1.1

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

1.0 Update guidance

2.0 AuthControl Sentry® updates

3.0 Software improvements.

4.0 New appliances improvement.

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.

- 2GB RAM (minimum), 4GB RAM Recommended
- 2 cores Minimum, 4 cores recommended
- 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®

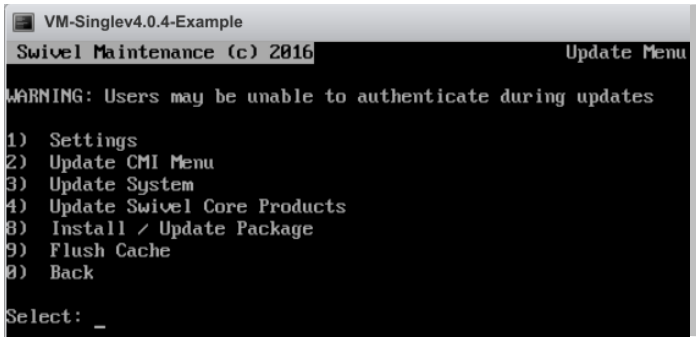

Fig. 1.1 shows the Update menu in AuthControl Sentry®

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

2.0 AUTHCONTROL SENTRY® (ACS 4.1.1)

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

2.1 MFA - We have on our core MFA, feasible to integrate with any SSO technology.

- Improve Session Sync.
- Sync session sharing
- Improve the usability of the automatic provision.
- Security improvements : Tomcat 9.0.37.
- Prevent OATH token OTPs being used more than once
- New helpdesk policy to disable editing user policy
- User Portal: Add description panel to PIN change
- User Portal: Disable mobile provisioning or show message if user not permitted
- Increment lock count if password is incorrect.
- Removed restriction on number of groups / attributes.
- Changes to the way “Check Password with Repository” works on RADIUS and Agents.

More specificly, the core authentication server and administration console have had a number of improvements for version 4.1.1.

New Features / Improvements

- Removed restriction on number of groups / attributes
  - Because of limitations in the underlying database, there was an effective limit of 50 groups and custom attributes combined. Any more than this and some of the views in User Administration would not work. This did not, however, affect the performance of the authentication engine.
  - The user administration display has been re-engineered to use multiple database queries when there are over a certain number of groups or attributes, to work around these limitations
- Changes to the way “Check Password with Repository” works on RADIUS and Agents:
  - XML repositories will always check against database password irrespective of setting
  - Database repositories depends on whether the database has a password field defined
- Line feed after security string in email/SMS is now optional
  - To allow for more control over the format of the security strings message, there is now an option (under Server -> Dual Channel) to suppress the line feed at the end of the string.
- Push support for Android high-latency mobile app.
  - The new High Latency (HL) version of the mobile app did not work with Push in 4.1, because of a different application ID.
  - Because versions 5.1 and 5.2 (currently in beta) of the HL use different API keys, it has been necessary to add two new options.

- TLS now defaults to version 1.2 in clients.
    - This affects requests to third party servers, such as LDAP repositories. Previously, the default was TLS 1.1, and a configuration file had to be edited manually to change it. This change would be overwritten by upgrades.
- New transports added:
    - Euskaltel
    - Gabia
    - MM7
    - UPlus
- You can now specify that RADIUS passwords are received as Base64 encoded
    - Certain RADIUS clients send the password as Base64 encoded, which resulted in an authentication failure. There is now an option on RADIUS -> NAS to specify that passwords are Base64-encoded.
- When using OATH in the mobile app, or TOTP-based OATH tokens, it is no longer possible to use the same code multiple times within the validity window. Once a code has been used successfully, you cannot authenticate again until a new code is shown. This does not apply, however, if you enter the code incorrectly.
- A new Helpdesk policy has been added, which prevents helpdesk users from changing user policy.

Bug Fixes

- Restarting RADIUS server now works properly without having to restart Tomcat
    - Previous updates to 4.1 added the ability to use a virtual IP for the RADIUS server, by stopping and starting the RADIUS server depending on whether the virtual IP was available. However, it was found that, once stopped, RADIUS would not start again without restarting the Tomcat server, limiting the usefulness of this feature. This problem has now been fixed, meaning that RADIUS over virtual IP for HA solutions works properly.
- RADIUS supports calling station ID format as sent by Microsoft NPS
    - The RADIUS Calling Station ID format as sent by Microsoft NPS includes the port number as well as the IP address. Previously this would cause RADIUS authentication to fail. Now, this format is interpreted correctly.
    - Additionally, if the calling station ID is not recognised as a valid IP address, it is simply ignored, rather than causing authentication to fail.
- RADIUS two-stage login now fails at the first stage if the account is locked.
    - Previously, if the first stage was checking the repository password, it would be passed through to the repository irrespective of whether the account was locked. The second stage would always fail in this case anyway, but now the user's status is checked before passing the password to the repository, and authentication will fail at the first stage.
- Fix for authenticating non-users in RADIUS
    - Some customers found that the option to authenticate unknown users using just the repository password in RADIUS was not working successfully. The check for unknown users has now been made more robust.
- Fixed RADIUS proxy problems
    - It was found that RADIUS proxying had stopped working due to a recent change This has now been resolved.
- Disabled flag is not reset on user if it is not imported from the repository
    - A change in 4.1 meant that if the user disable flag was not imported from the repository, it was always reset by User Sync, making the manual disabled setting effectively useless. This flag is now left unchanged by user sync, unless

the repository settings specify that it should be imported.

- Provision button now works for usernames with underscore
    - Due to an error in the coding, a provision message would not be sent out if the username contained an underscore.
- User lock count always increases if the password is incorrect
    - In certain RADIUS authentications, if the user entered a password incorrectly, although authentication would fail, the lock count would not increase. This no longer happens.

User Portal

The user portal has undergone a major change for this release. The main change is in the number of authentication options available. Additionally, it is now easier to for administrators to maintain the user portal without the need to edit the settings file directly.

Authentication Options

Access to the user portal can now be configured to use one of a number of options:

- Name Only
    - This is the default setting, and the only option available in earlier versions of the user portal. A user only needs their username in order to access the user portal
- Confirmation Code
    - After a user enters their username, they are sent a confirmation code by SMS or email.
    - If a user has no transport configured, they can enter just their username, or optionally a password as well. They can then specify their own phone number or email address.
    - This feature relies on suitable messaging being configured in the Core server, and users being in the right group to use them.
- Password Only
    - The user must enter their username and password in order to access the user portal. Whether this is the Sentry password or repository password depends on the Agent configured for the user portal to use.
- Sentry
    - The user must login using their Sentry credentials. Which methods are available is configurable.
    - If the user has forgotten their Sentry credentials, they can request a Reset code from the login screen.

Administration Settings

It is now much easier to administer the user portal without having to edit settings files directly. Further, these settings are now applied immediately, without having to restart Tomcat. The exception is that changes to the display menu require the user to log out before the changes are applied.

The exceptions to this are:

- Custom Agent settings
    - If the user portal needs to be linked to a Core server other than localhost it must be done directly in the file.
- Administrator group
    - If the name of the group permitted to carry out administration changes is not “SwivelAdmin”, the group name must be edited directly.

In order to access the administration screens, users must be a member of the specified group.

They must also authenticate using Sentry credentials, irrespective of the authentication requirements for normal users. If an administrator logs in using other settings and wishes to access the administrator settings, they will have to log in again using Sentry credentials.

Display Options

The Display Options screen was available to administrators in previous versions. The only change is the addition of the option “Change Mobile Number”, to allow users to set their own mobile number (or email address, depending on messaging settings).

Authentication Settings

This is a new screen, which allows administrators to configure how users can access the user portal.

- Authentication Options
  - This allows the selection of one of the authentication options described earlier in the notes.
- Allowable Sentry Methods
  - If the authentication method is set to Sentry, there is a choice of TURing, PINpad and Message On Demand.
- Change PIN Method
  - This specifies how users can change their PIN. The options are Direct, None, PicturePad, PINpad and TURing.
  - Note that if “Direct” is selected, special configuration is required in the Core to allow security strings to be sent as plain text.
- Require Password if no email/phone
  - This applies to the confirmation code authentication option. If a user has not yet configured an email or phone number, they can optionally be required to use a password to access the user portal.
- Show Reset Password
  - If set, the Reset PIN form shows an option to reset the Sentry password as well as the PIN.
- Require email/SMS confirmation for Provision QR code.
  - This controls whether a user will be sent a confirmation code to enter before a QR code is displayed for them to provision the mobile app. If not set, the QR code is displayed immediately.
- Phone/Email attribute
  - This is the name of the attribute used to set the destination for the confirmation code. This must be a valid attribute name from the Core custom attributes, and should not be configured as Synchronised (or else it will be overwritten by user sync).
- Phone checked attribute
  - This is an optional feature related to the phone number. It should be the name of a non-synchronised attribute. This attribute is used to indicate that the user has confirmed their phone number (or email address). If set, after a user enters their phone number, they will be sent a confirmation code to that number. Once they enter the confirmation code in the space provided, the phone number is confirmed and the user must use confirmation codes to access the user portal. Until they do this, they can continue to log into the user portal without a confirmation code.
  - If this attribute is blank, the phone number is assumed to be confirmed as soon as it is entered.

Single Sign-On

The only change to single Sign-On is a single bug fix:

- All applications a user has access to are now shown on the home page.

  There was a bug in version 4.1 whereby applications that were limited to a particular user group were not displayed, even if the user was a member of that group. This has now been corrected.

Appliance

Changes to the appliance are mainly updates to third party packages and security fixes:

- Apache Tomcat version 9.0.37:
  - The version of Tomcat has been updated to 9.0.37, the latest currently available. It fixes security issues reported in previous versions.Disabled TCP timestamps service
  - Removed insecure ciphers from SSH service
  - Updated certificates for database replication using SHA-256 signatures.

3.1 AuthControl Mobile (MSP)

- Stability improvement
- Resource Usage improvement
- Bug Fixes – Less calls to you it support desk.
- Research about Widget and the usability of IOS
- Compatibility with Ipad
- Code Update to latest Apple directives
- Provisioning flow review and improvement

3.2 AuthControl Mobile Android

- Increase the usability of apps.
- Optimize the mobile apps functionality and its relation with the high latency scenarios.
- Stability improvement.
- Resource Usage improvement
- Bug Fixes.
- Provisioning and deprovision flow review and improvement

3.3 AuthControl Mobile Android

- Increase the usability of apps.
- Optimize the mobile apps functionality and its relation with the high latency scenarios.
- Stability improvement.
- Resource Usage improvement
- Reingener of provision and deprovision flow; mitigating the automatic deprovision.
- Bug Fixes.

3.4 AuthControl Mobile IOS

- Increase the usability of apps.
- Optimize the mobile apps functionality and its relation with the high latency scenarios.
- Stability improvement.
- Resource Usage improvement
- Reingener of provision and deprovision flow; mitigating the automatic deprovision.
- Bug Fixes.

4.0 New improvements of security in the new release.

This section lists include all of benefits:

- Upgrade the security appliance with new OS.
- Upgrade the Java Version.
- Upgrade the DataBase engine.

Focus on:

- Encrypted management and structure with cloud
- On rest data also encrypted.
- Triple handshake in the Java Version.
- Enviroment upgrade with new appliance .
- Vulnerabilities removed due to analysis in:
- Improve the security in the admin remote Access.
- Delete the support on “not compliance or unsecure ” algoritms.
- Mitigation of SSH vulnerabilities.

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

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